

ООО «ВЭБ КОНТРОЛ ДК»



**АВТОМАТИЗИРОВАННАЯ СИСТЕМА КОНТРОЛЯ И
УПРАВЛЕНИЯ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ
«SPACE»**

ВЕРСИЯ 1.3.0

РУКОВОДСТВО АДМИНИСТРАТОРА

Москва, 2023

СОДЕРЖАНИЕ

1. ОБ ЭТОМ ДОКУМЕНТЕ.....	9
2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ.....	10
3. ОБЩИЕ СВЕДЕНИЯ О СИСТЕМЕ sPACE	12
3.1. Назначение программы.....	12
3.2. Функции программы.....	12
3.3. Перечень эксплуатационной документации.....	13
3.4. Уровень подготовки пользователя.....	13
3.5. Права доступа к функционалу sPACE.....	13
3.5.1. Роли пользователей в Системе sPACE.....	13
3.5.1.1. Базовый пользователь.....	13
3.5.1.2. Стандартный пользователь.....	14
3.5.1.3. Продвинутый пользователь.....	15
3.5.1.4. Администратор.....	15
3.5.1.5. Аудитор.....	15
3.5.1.6. Продвинутый аудитор.....	15
3.5.1.7. Привилегированный администратор.....	15
3.5.2. Перечень функционала, доступный для каждой роли.....	16
3.5.3. Настройка прав доступа для каждой роли.....	19
3.6. Состав и содержание дистрибутивного носителя данных.....	19
3.7. Условия работоспособности Системы.....	19
3.7.1. Стороннее программное обеспечение, необходимое для работы sPACE.....	19
3.7.2. Требования к аппаратному обеспечению серверной части.....	20
3.7.3. Требования к программному обеспечению серверной части.....	20
3.7.4. Требования к аппаратному обеспечению рабочих станций.....	20
3.7.5. Требования к программному обеспечению рабочих станций.....	21
4. СТРУКТУРА СИСТЕМЫ sPACE	22
4.1. Защищенная среда привилегированного доступа.....	22
4.2. Портал sPACE.....	22
4.3. sPACE Mono (Base).....	23
4.4. Сервер обмена сообщениями.....	23
4.5. Архитектура Системы.....	23

5.	НАСТРОЙКА SPACE.....	25
5.1.	Управление пользователями	26
5.1.1.	Просмотр списка всех пользователей Системы.....	27
5.1.2.	Добавление новых пользователей	27
5.1.3.	Редактирование данных существующего пользователя.....	29
5.1.4.	Удаление пользователей из Системы	30
5.1.5.	Обновление таблицы пользователей.....	30
5.1.6.	Добавление или отключение поддержки двухфакторной аутентификации	30
5.2.	Управление группами согласования	31
5.2.1.	Добавление групп согласования.....	32
5.2.2.	Редактирование группы согласования	32
5.2.3.	Добавление пользователей в группу согласования.....	33
5.2.4.	Удаление пользователей из группы согласования	34
5.2.5.	Единовременное задание внешнего ID для нескольких записей из таблицы групп согласования	34
5.3.	Управление учетными записями	35
5.3.1.	Добавление учетной записи.....	35
5.3.2.	Редактирование учетной записи.....	37
5.3.3.	Обновление таблицы учетных записей.....	39
5.3.4.	Удаление строк в таблице учетных записей.....	39
5.3.5.	Удаление нескольких записей из таблицы учетных записей одновременно.....	39
5.3.6.	Единовременное задание внешнего ID для нескольких записей из таблицы учетных записей.....	40
5.4.	Управление объектами администрирования.....	40
5.4.1.	Добавление объекта администрирования/типа объекта администрирования	41
5.4.2.	Редактирование объекта администрирования/типа объекта администрирования. .	43
5.4.3.	Обновление таблицы объекта администрирования/типа объекта администрирования	44
5.4.4.	Удаление строки в таблице объекта администрирования/типа объекта администрирования	44
5.4.5.	Удаление нескольких записей из таблицы одновременно	45

5.4.6.	Единовременное задание внешних ID для нескольких объектов администрирования	45
5.4.7.	Единовременное добавление серверов ЗС для нескольких объектов администрирования	46
5.5.	Управление приложениями.....	46
5.5.1.	Добавление приложения/сценария.....	48
5.5.2.	Редактирование приложения/сценария.....	49
5.5.3.	Обновление таблицы приложений/сценариев.....	53
5.5.4.	Удаление строки в таблице приложений/сценариев.....	53
5.5.5.	Удаление нескольких записей из таблицы одновременно	54
5.5.6.	Единовременное задание внешнего ID для нескольких записей из таблицы приложений	54
5.5.7.	Единовременное добавление серверов ЗС для нескольких приложений	54
5.6.	Управление интерпретаторами.....	55
5.6.1.	Добавление интерпретаторов	55
5.6.2.	Редактирование интерпретаторов	56
5.6.3.	Обновление таблицы интерпретаторов	58
5.6.4.	Удаление строки в таблице интерпретаторов.....	58
5.6.5.	Удаление нескольких записей в таблице интерпретаторов.....	58
5.7.	Управление задачами администрирования	58
5.7.1.	Добавление задачи	59
5.7.2.	Редактирование задачи	60
5.7.3.	Обновление таблицы задач	62
5.7.4.	Удаление строки в таблице задач	62
5.7.5.	Удаление нескольких записей из таблицы задач одновременно	62
5.7.6.	Единовременное задание внешнего ID для нескольких записей из таблицы задач	62
5.8.	Настройка и управление нарядами-допусками	63
5.8.1.	Добавление наряда-допуска.....	64
5.8.2.	Просмотр информации о нарядах-допусках	64
5.8.3.	Обновление таблицы нарядов-допусков.....	65
5.8.4.	Удаление строк в таблице нарядов-допусков.....	65
5.8.5.	Удаление нескольких записей из таблицы нарядов-допусков	65

5.8.6.	Единовременное задание внешнего ID для нескольких записей из таблицы нарядов-допусков.....	65
5.9.	Управление серверами защищенной среды (ЗС).....	65
5.9.1.	Добавление сервера ЗСА.....	67
5.9.2.	Изменение настроек сервера ЗСА.....	68
5.9.3.	Обновление таблицы серверов ЗСА.....	69
5.9.4.	Удаление строки в таблице серверов ЗСА.....	69
5.9.5.	Удаление нескольких записей из таблицы серверов ЗС одновременно.....	69
5.9.6.	Единовременное задание внешнего ID для нескольких записей из таблицы серверов ЗС.....	69
5.10.	Просмотр системных настроек.....	69
5.10.1.	Изменение настроек серверов NATS.....	71
5.10.2.	Изменение настроек парольной политики.....	71
5.10.3.	Изменение настроек уровня логирования.....	72
5.10.4.	Изменение настроек внешней тикет системы.....	73
5.11.	Управление провайдерами аутентификации.....	76
5.11.1.	Просмотр доменов Системы.....	77
5.11.2.	Добавление нового домена.....	77
5.11.3.	Редактирование домена.....	78
5.11.4.	Обновление таблицы доменов.....	79
5.11.5.	Удаление строки в таблице доменов.....	79
5.11.6.	Удаление нескольких записей из таблицы доменов одновременно.....	79
5.11.7.	Импорт конфигурации LDAP.....	80
5.11.8.	Изменение названия ролей.....	82
5.12.	Управление пользовательскими ролями.....	82
5.12.1.	Добавление новой пользовательской роли.....	83
5.12.2.	Редактирование пользовательской роли.....	84
5.12.3.	Обновление таблицы пользовательских ролей.....	85
5.12.4.	Удаление строки в таблице пользовательских ролей.....	85
5.12.5.	Удаление нескольких записей из таблицы пользовательских ролей одновременно.....	85
5.13.	Управление агентами паролей.....	86
5.13.1.	Просмотр агентов паролей.....	86

5.13.2.	Добавление агента паролей.....	87
5.13.3.	Редактирование агента паролей.....	88
5.13.4.	Обновление таблицы агентов и типов агентов	89
5.13.5.	Удаление строки в таблице агентов	89
5.13.6.	Единовременное удаление нескольких записей из таблицы агентов	89
5.13.7.	Единовременное добавление внешних ID для нескольких записей	90
5.14.	Управление внутренней системой аудита сеансов (BCAC).....	90
5.14.1.	Просмотр параметров внутренней системы видеаудита сеансов	91
5.14.2.	Обновление страницы внутреннего видеаудита	92
5.14.3.	Редактирование глобальных настроек внутреннего видеаудита	92
5.14.4.	Удаление строки в таблице хранилищ BCAC.....	92
5.14.5.	Редактирование настроек внутреннего видеаудита для отдельного сервера ЗС93	
5.14.6.	Выбор стратегии балансировки хранилищ BCAC	93
5.15.	Управление фильтрацией ввода	94
5.15.1.	Добавление фильтрации ввода	95
5.15.2.	Редактирование фильтрации ввода	96
5.15.3.	Обновление страницы фильтрации ввода	97
5.15.4.	Удаление строки в таблице списков фильтрации ввода	97
5.15.5.	Удаление нескольких записей из таблицы списков фильтрации ввода	97
5.16.	Управление лицензией	97
5.16.1.	Просмотр лицензии	98
5.16.2.	Обновление страницы лицензии	99
5.16.3.	Скачивание запроса на лицензию	99
5.16.4.	Загрузка лицензии.....	100
5.17.	Просмотр статуса компонентов Системы	101
5.17.1.	Просмотр компонентов системы и их значений	101
5.17.2.	Фильтрация элементов раздела	102
5.17.3.	Обновление таблицы статуса компонентов.....	103
5.17.4.	Экспорт компонентов в виде html-файла.....	103
5.17.5.	Индикатор быстрого информирования о состоянии системы "Светофор"	103
5.18.	Управление сеансами привилегированного доступа	104
5.18.1.	Фильтрация сеансов по состоянию	104
5.18.2.	Фильтрация сеансов по дате создания	105

5.18.3.	Обновление таблицы сеансов	105
5.18.4.	Удаление строки в таблице сеансов	105
5.18.5.	Удаление нескольких записей из таблицы сеансов одновременно	106
5.19.	Управление операциями с секретами	106
5.19.1.	Фильтрация раздела по состоянию	107
5.19.2.	Фильтрация раздела по дате создания	107
5.19.3.	Обновление таблицы операций с секретами	107
5.19.4.	Просмотр информации о каждом сеансе	108
5.20.	Формирование отчетности по использованию Системы	108
5.21.	Перевод Системы в аварийный режим	109
5.22.	Осуществление аудита Системы	110
5.23.	Осуществление аудита сеансов	110
5.23.1.	Фильтрация раздела по состоянию	111
5.23.2.	Фильтрация раздела по дате создания	112
5.23.3.	Обновление таблицы Сеансы	112
5.23.4.	Просмотр детальной информации о каждом сеансе	113
5.23.5.	Просмотр записи сеанса	113
5.23.6.	Просмотр записи работающего сеанса в режиме онлайн	116
5.23.7.	Скачивание изображений сеанса	118
5.23.8.	Экстренное завершение работающего сеанса	118
5.23.9.	Поиск по метаданным	119
5.23.10.	Просмотр записи сеанса по данным Key Logger	119
5.24.	Осуществление аудита доступа к порталу	120
5.24.1.	Просмотр информации о пользовательской сессии	120
6.	ПРОВЕРКА SPACE	123
6.1.	Проверка изоляции сеансов ПД	123
6.2.	Отслеживание в реальном времени выполняемых работ	123
6.3.	Проверка возможности добавления новых объектов администрирования	124
7.	РЕЗЕРВНОЕ КОПИРОВАНИЕ	125
8.	ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ	126

1. ОБ ЭТОМ ДОКУМЕНТЕ

Этот документ является руководством администратора программного продукта «sPАСЕ» (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.

2. 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, иницирующее и согласующее лицо, обоснование и объекты администрирования.
ОА	<ul style="list-style-type: none"> • Объект администрирования. Целевая система, действия с которой производятся с использованием привилегированного доступа
ИА	<ul style="list-style-type: none"> • Инструмент Администрирования. Приложение, запускаемое на сервере ЗСА, с помощью которого осуществляются привилегированный доступ к ОА.
ЗСА	<ul style="list-style-type: none"> • Защищенная Среда Администрирования. Выделенный сервер, на котором выполняется сеанс привилегированного доступа.
FQDN	Fully Qualified Domain Name, имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS
СОС	Служба Обмена Сообщениями. Служба, обеспечивающая коммуникацию между компонентами sPACE.
ВСАС	Внутренняя система аудита сеансов, осуществляющая запись скриншотов действий пользователей.

3. ОБЩИЕ СВЕДЕНИЯ О СИСТЕМЕ SPACE

3.1. Назначение программы

«SPACE» — это автоматизированная система организации и управления рабочим процессом привилегированных пользователей с интегрированной защищенной средой реализации полномочий и подсистемой управления жизненным циклом паролей и ключей доступа.

Система «SPACE» 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 привилегий, децентрализации процесса предоставления привилегированного доступа и организации объективного контроля сеансов привилегированного доступа на крупных предприятиях и в компаниях среднего и малого бизнеса.

3.2. Функции программы

В программе реализован следующий функционал:

- 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;
- контроль доступа к совместным учетным данным;
- контроль команд и действий, выполняемых специалистами;
- мониторинг и запись сеансов привилегированного доступа;
- поддержка протоколов удаленного администрирования;
- предоставление аналитических данных о действиях привилегированных пользователей с помощью консоли, отчетов и аналитики;
- двухфакторная аутентификация с использованием технологии RuToken, TOTP;
- разграничение доступа к управлению программой;
- управление работой программы;

- добавление новых объектов и инструментов привилегированного доступа;
- аварийный режим;
- возможность интеграции с существующими системами информационной безопасности посредством API.

3.3. Перечень эксплуатационной документации

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

3.4. Уровень подготовки пользователя

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

3.5. Права доступа к функционалу sPACE

3.5.1. Роли пользователей в Системе sPACE

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

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

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

3.5.1.1. 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 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 sPASE, 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.

3.5.1.2.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.

3.5.1.3.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.

3.5.1.4.Администратор

Администратор sPASE осуществляет управление задачами на работу с информационными ресурсами, объектами ИТ-инфраструктуры компании, инструментами администрирования и учетными записями. Он также может входить в группу согласования и согласовывать наряды-допуски.

3.5.1.5.Аудитор

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

3.5.1.6.Продвинутый аудитор

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

3.5.1.7.Привилегированный администратор

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

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.

3.5.2. Перечень функционала, доступный для каждой роли

Таблица Функционал, доступный каждой роли

Наименование	Права	Описание роли в веб интерфейсе	Имя группы в AD при активной галочке по умолчанию
Базовый пользователь	<p>Доступен раздел "Сеансы"</p> <ul style="list-style-type: none"> Запуск сеансов администрирования на основе согласованных "Нарядов-допусков". 	<p>ROLE_SPACE_RESTRICTED_USER</p>	<p>SPACE_RESTRICTED_USERS</p>
Стандартный пользователь	<p>Доступен раздел "Сеансы"</p> <ul style="list-style-type: none"> 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 	<p>ROLE_SPACE_STANDARD_USER</p>	<p>SPACE_STANDARD_USERS</p>

Наименование	Права	Описание роли в веб интерфейсе	Имя группы в AD при активной галочке по умолчанию
Продвинутый пользователь	<p>Доступен раздел "Сеансы"</p> <ul style="list-style-type: none"> • 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. • Просмотр записей собственных сеансов, если 	ROLE_SPACE_USER	SPACE_USERS
Администратор	<p>Доступен раздел "Управление системой"</p> <ul style="list-style-type: none"> • Управление пользователями. • Управление группами согласования. • Управление учетными записями. • Управление объектами и инструментами администрирования. • Управление сценариями запуска и приложений. • Управление задачами. • Управление нарядами-допусками. • Управление сеансами привилегированного доступа. • Управление серверами защищенной среды (ЗС). • Просмотр системных настроек и статуса компонентов системы. • Управление ролями AD. • Управление доменами. • Управление лицензией. • Управление агентами паролей. • Управление системами видеоаудита, в том числе 	ROLE_SPACE_ADMIN	SPACE_ADMINS

Наименование	Права	Описание роли в веб интерфейсе	Имя группы в AD при активной галочке по умолчанию
Аудитор	<p>Доступен раздел "Аудит"</p> <ul style="list-style-type: none"> • Просмотр журнала доступа пользователя. • Просмотр сеансов администрирования в реальном времени. • Просмотр видеозаписей данных сеансов. • Просмотр списка сеансов. 	ROLE_SPACE_AUDITOR	SPACE_AUDITORS
Продвинутый аудитор	<p>Доступен раздел "Аудит"</p> <ul style="list-style-type: none"> • 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	<p>Доступен раздел "Управление системой"</p> <ul style="list-style-type: none"> • Управление пользователями. • Управление группами согласования. • Управление учетными записями. • Управление объектами и инструментами администрирования. • Управление сценариями запуска и приложений. • Управление задачами. • Управление нарядами-допусками. • Управление сеансами привилегированного доступа. • Управление серверами защищенной среды (ЗС). • Просмотр системных настроек и статуса компонентов системы. • Управление ролями AD. • Управление доменами. • Управление лицензией. • Управление агентами паролей. • Управление системами видеоаудита, в том числе внутренней системой видеоаудита (ВСАС) и 	ROLE_SPACE_SUPERADMIN	SPACE_SUPERADMINS

3.5.3. Настройка прав доступа для каждой роли

При работе Система автоматически добавляет в Систему пользователей из соответствующих групп службы каталогов Windows. Для этого необходимо наличие пользователей в Active Directory Users and Computers.

Назначение или изменение роли учетной записи происходит путем добавления пользователя в соответствующую группу Active Directory. Рекомендуемое соответствие ролей в Системе группам Active Directory приводится в Инструкции по развертыванию.

3.6. Состав и содержание дистрибутивного носителя данных

Программный продукт «sPACE» 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);
- sPACE-Jump-Server-Installer.msi – исполняемый файл сервера защищённой среды sPACE, предназначенный для установки на сервер ЗСА.

Для работы sPACE необходимо осуществить обе этих установки.

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

3.7. 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.

3.7.1. 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».

ПО	Описание
JRE	Java SE Runtime Environment (x64)
JCE	Java Cryptography Extension
Postgres DB	База данных Postgres
Tomcat	Контейнер сервлетов (x64)
NATS	Платформа, реализующая систему обмена сообщениями (СОС)
AutoIt	Скрипт для автоматизации выполнения задач в ОС Microsoft Windows.
Docker CE	Система контейнеров для Linux.

3.7.2. 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 ЗСА	Процессор: 4 ядра, 2,2 ГГц Оперативная память: 8 ГБ Дисковое пространство: 150 ГБ
Хранилище архива сессий	Требуется рассчитать дополнительно.

3.7.3. Требования к программному обеспечению серверной части

Таблица Требования к программному обеспечению серверов

Сервер	Состав ПО
Сервер sPACE Mono (Base)	CentOS 7-8, Ubuntu 18.04, Ubuntu 20.04, Astra Linux «Орёл»
Сервер ЗСА	Microsoft Windows Server 2012 R2, Remote Desktop Server (RDS), Windows PowerShell 5.1 и выше.

3.7.4. 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

3.7.5. 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 72.0 и выше, Mozilla Firefox 66.0 и выше; Совместимый клиент RDP

Установка, настройка и использование Системы должна 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.

4. 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 привилегированного доступа;
- портал sPACE;
- sPACE Mono (Base).

Взаимодействие между 3 базовыми компонентами осуществляется при помощи сервера обмена сообщениями.

Для аутентификации и авторизации пользователей и сбора информации об информационных ресурсах Система взаимодействует со службами каталогов MS Active Directory.

4.1. Защищенная среда привилегированного доступа

Защищенная Среда Привилегированного Доступа — это выделенный сервер, на котором выполняется сеанс привилегированного доступа. Привилегированные учетные данные используются изолированно от потенциально вредоносной среды рабочей станции пользователя. Этот компонент представляет собой набор элементов (RDP RemoteApp), каждый из которых реализует возможность графического или командного удаленного доступа. Элементы используются для запуска сеансов ПД и управления ими. Элементы различаются используемой платформой (Windows, Linux), поддерживают протокол удаленного доступа RDP. В базовой конфигурации один сервер ЗСА поддерживает до 50 параллельных сеансов.

4.2. 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.

4.3. sPACE Mono (Base)

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

4.4. Сервер обмена сообщениями

Система sPACE построена на основе микросервисной архитектуры, для управления потоками между микросервисами используется сервис обмена сообщениями (COC) 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.

4.5. Архитектура Системы

Архитектура Системы представлена на Рисунке 1. Подробно о ней можно прочитать в Инструкции по разворачиванию sPACE.

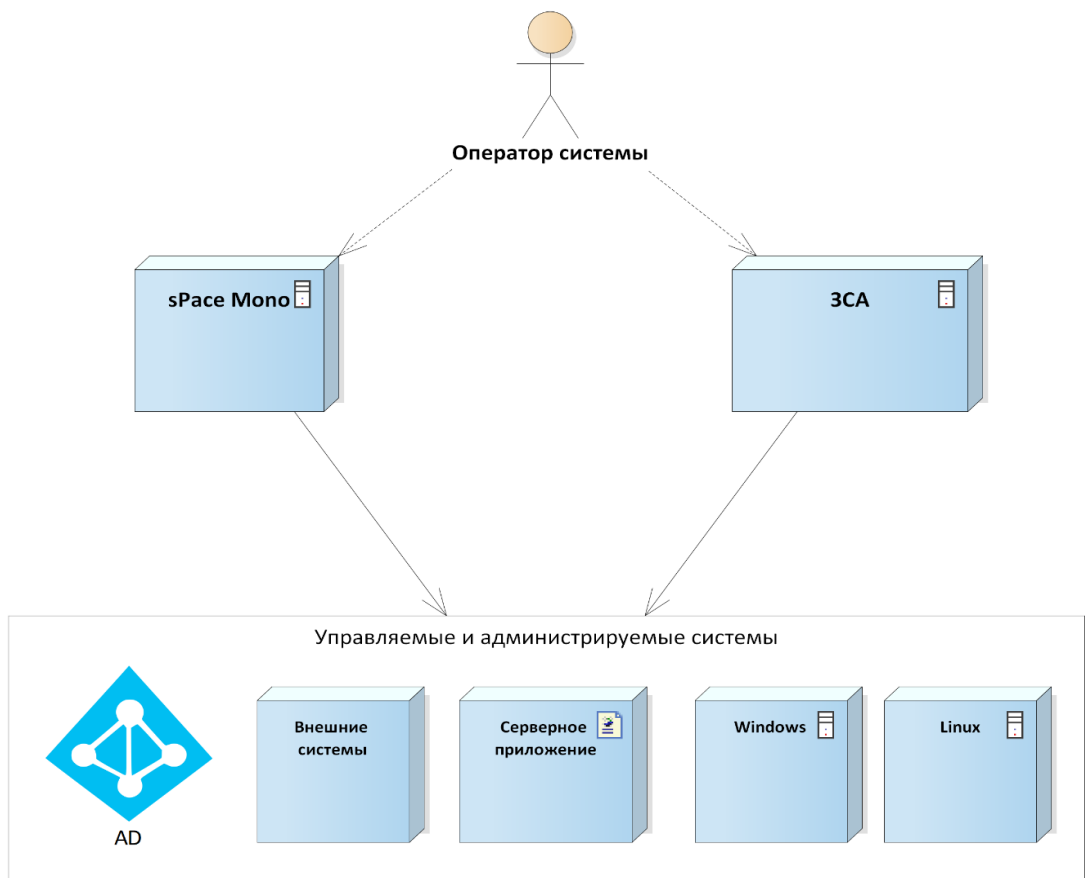


Рис. 1. Архитектура Системы

5. НАСТРОЙКА 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. Описание интерфейса приведено в Руководстве пользователя, раздел 6.

Для выполнения действий по настройке sPACE необходимо наличие роли «Администратор», для перевода Системы в аварийный режим необходимо наличие роли «Привилегированный администратор».

Функционал Системы предполагает выполнение следующих действий по настройке Системы.

- Управление пользователями;
- Управление группами согласования;
- Управление учетными записями;
- Управление объектами и инструментами администрирования;
- Управление сценариями запуска и приложений;
- Управление задачами;
- Управление нарядами-допусками;
- Управление сеансами привилегированного доступа;
- Управление серверами защищенной среды (ЗС);
- Просмотр системных настроек;
- Просмотр статуса компонентов системы;
- Управление ролями AD;
- Управление доменами;
- Управление лицензией;
- Управление агентами паролей;
- Управление системами видеоаудита;
- Управление внутренней системой видеоаудита (ВСАС);
- Управление хранилищами ВСАС;
- Просмотр статистики;

- Осуществление аудита системы.

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

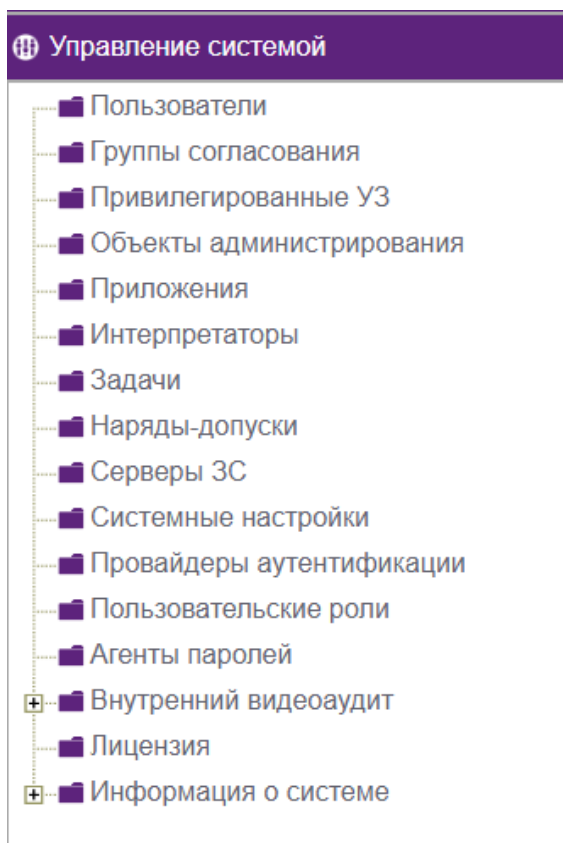


Рис. 2. Раздел «Управление системой»

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:

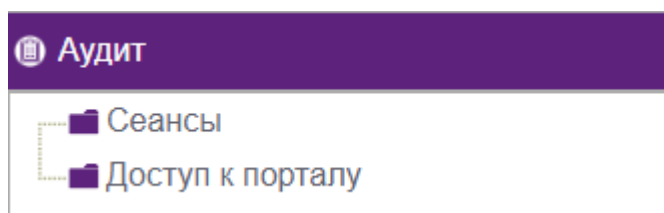


Рис. 3. Раздел «Аудит»

5.1. Управление пользователями

Для управления пользователями необходимо перейти в узел **Пользователи**, где администратор может выполнить следующие действия:

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

5.1.1. 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;
- Роли (только для внутренних пользователей);
- 2FA (2-факторная аутентификация);
- Ограничен.

Имя пользователя	Домен	ФИО	Роли	2FA	Ограничен
787	eval	787 777		<input type="checkbox"/>	<input type="checkbox"/>
admin	internal	a admin space	ROLE_API_MANAGEME...	<input type="checkbox"/>	<input type="checkbox"/>
ad-user-001	lbdemo.local	Isaev Dmitry Vasilievich		<input type="checkbox"/>	<input type="checkbox"/>
ad-user-001	space.local	Рубцов		<input type="checkbox"/>	<input type="checkbox"/>
ad-user-001	hq.company.local	Исаев Дмитрий Василь...		<input type="checkbox"/>	<input type="checkbox"/>
ad-user-002	lbdemo.local	Sleptsov Vladislav Genn...		<input type="checkbox"/>	<input type="checkbox"/>
ad-user-002	hq.company.local	Сленцов Vladislav Genn...		<input type="checkbox"/>	<input type="checkbox"/>
ad-user-003	lbdemo.local	Davletshin Andrey Dmitri...		<input type="checkbox"/>	<input type="checkbox"/>

Рис. 4. Список пользователей

5.1.2. 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 Active Directory Users and Computers.

Форма добавления пользователей **Пользователь** содержит следующие поля (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.

The screenshot shows a web form titled "Пользователь" (User) with a purple header. The form contains the following fields and controls:

- Имя пользователя :** Input field with an information icon (i).
- Фамилия :** Input field with an information icon (i).
- Имя :** Input field with an information icon (i).
- Отчество :** Input field with an information icon (i).
- Домен :** Dropdown menu with an information icon (i).
- Мобильный телефон :** Input field with an information icon (i).
- Телефон :** Input field with an information icon (i).
- Электронный адрес :** Input field with an information icon (i).
- Ограничить**
- Сохранить** button
- Закрыть** button

Рис. 5. 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;
- Роль (обязательное поле) – одна или несколько ролей, которые соответствуют функционалу, доступному этому пользователю на портале.

Рис. 6. Добавление внутреннего пользователя

5.1.3. 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. 7. Форма просмотра данных пользователя

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

Рис. 8. Форма редактирования данных пользователя

5.1.4. 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.

5.1.5. Обновление таблицы пользователей

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

Имя пользователя	Домен	ФИО	2FA	Ограничен
<input type="checkbox"/> ad-user-062	hq.company.local		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> ad-user-085	hq.company.local		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> ad-user-060	hq.company.local		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> spc-user-001	space.local		<input type="checkbox"/>	<input type="checkbox"/>

Рис. 9. Форма редактирования данных пользователя

5.1.6. Добавление или отключение поддержки двухфакторной аутентификации

Для добавления или отключения поддержки двухфакторной аутентификации пользователя необходимо перейти в узел **Пользователи** раздела **Управление системой** и поставить флажок в поле **2FA**. Подробнее о подключении двухфакторной аутентификации вы можете прочитать в руководстве пользователя в разделе 6.5.1.

5.2. Управление группами согласования

Группа согласования — это определенная группа пользователей, которые имеют право согласовать (одобрять) наряды-допуски на управление объектами администрирования в рамках выполнения 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**.

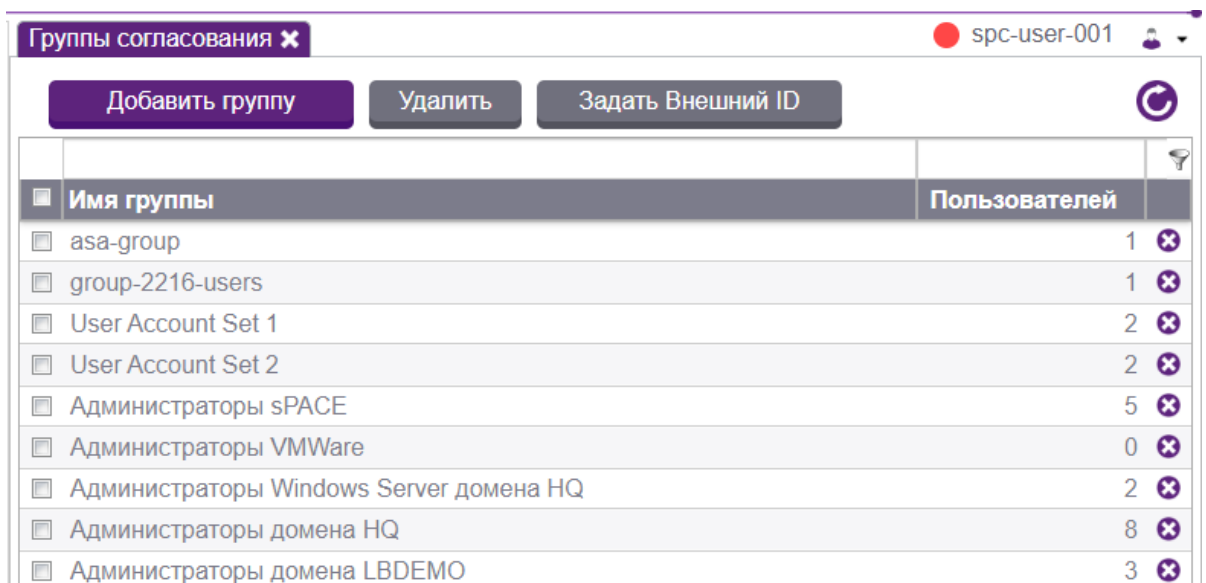


Рис. 10. Окно «Группы согласования»

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;
- одновременно задавать внешний ID для нескольких записей из таблицы групп согласования.

5.2.1. 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;
- Внешний ID – идентификатор для интеграции внешних систем через API sPАСЕ с данной сущностью. При создании группы предлагается сгенерировать идентификатор.

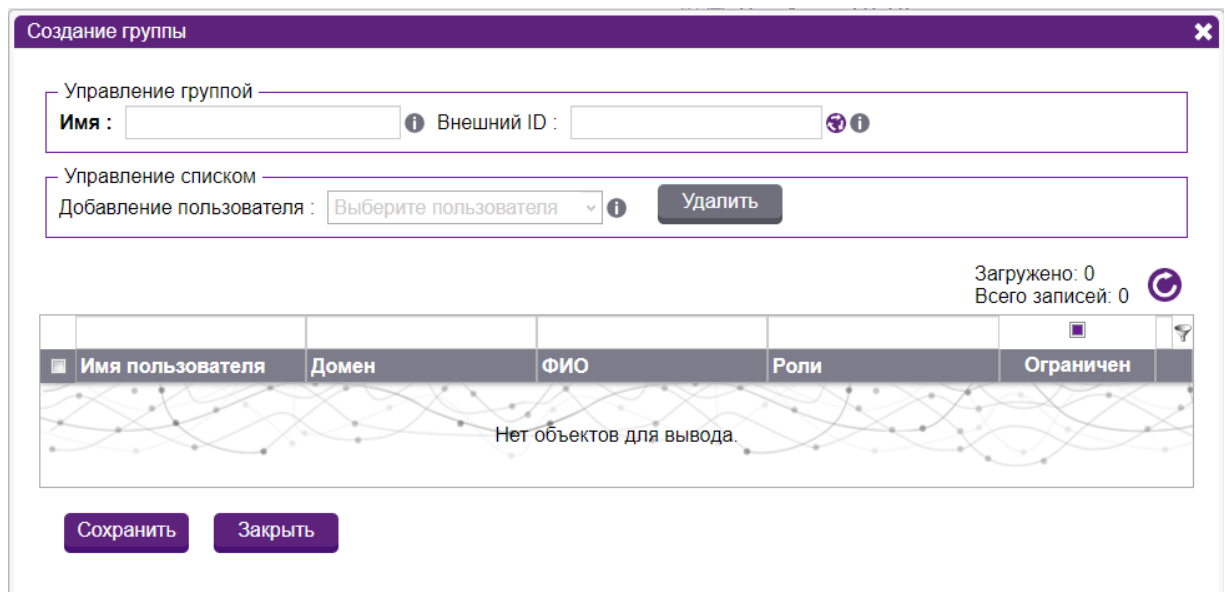


Рис. 11. Форма создания группы

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

После заполнения всех необходимых полей и нажатия кнопки **Сохранить** новая группа согласования будет добавлена в таблицу **Группы согласования**.

5.2.2. 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**.

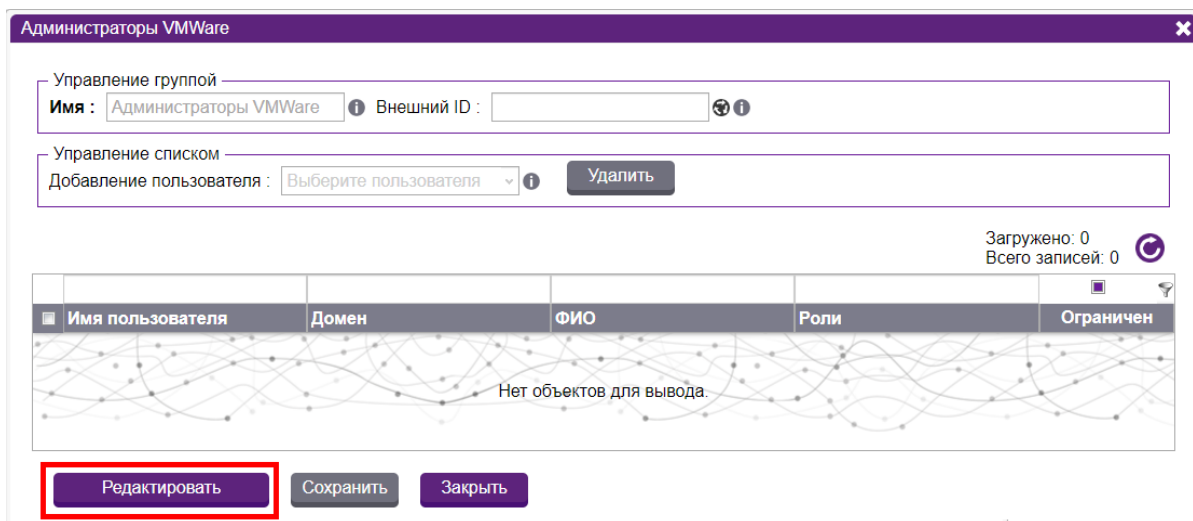


Рис. 12. Кнопка «Редактировать»

В появившейся форме редактирования группы можно изменить имя группы, добавить или изменить внешний ID, 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.

5.2.3. 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.

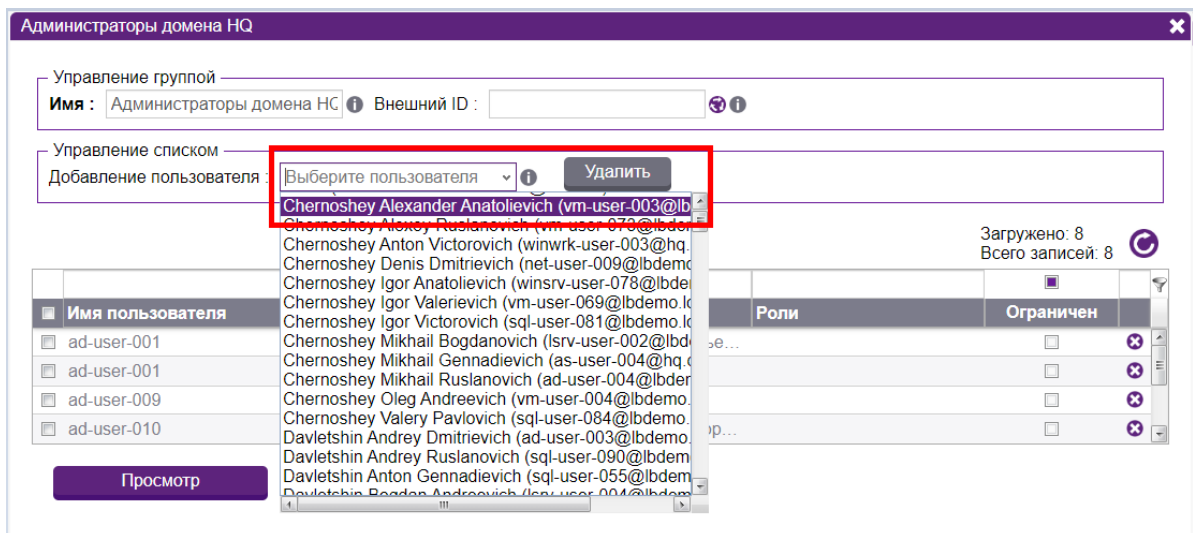


Рис. 13. Выбор пользователя из списка

5.2.4. 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.

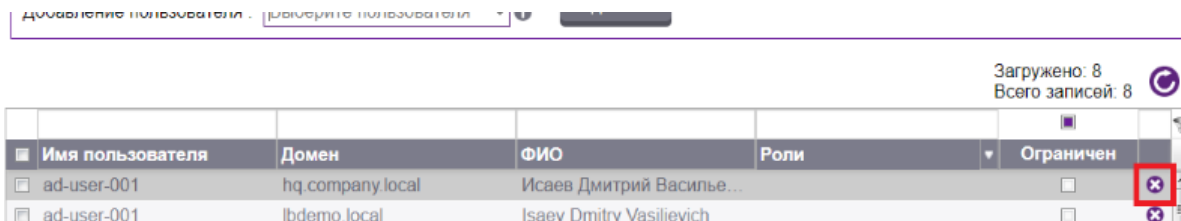


Рис. 14. Значок удаления пользователя

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.

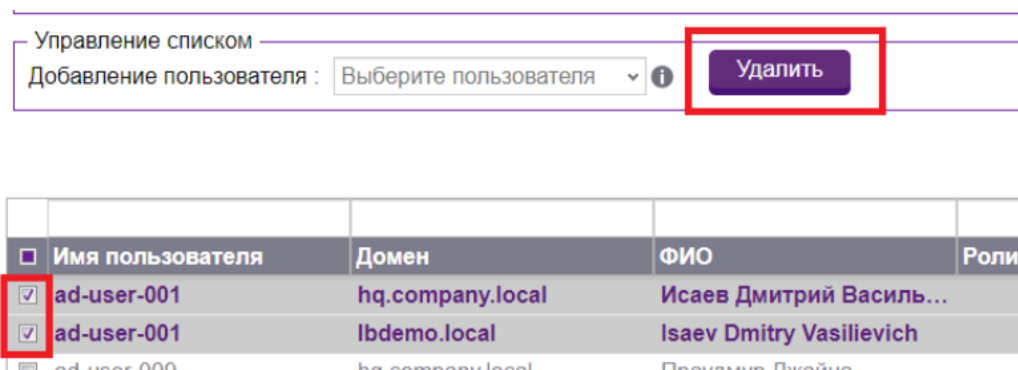


Рис. 15. Кнопка «Удалить» активна

5.2.5. Единовременное задание внешнего ID для нескольких записей из таблицы групп согласования

Для единовременного задания внешнего ID для нескольких записей необходимо перейти в узел **Группы согласования** раздела **Управление системой**, выделить нужные записи в таблице, установив флажок в соответствующем поле слева от поля **Имя группы**, после чего станет активной кнопка **Задать Внешний ID**, расположенная на панели инструментов.

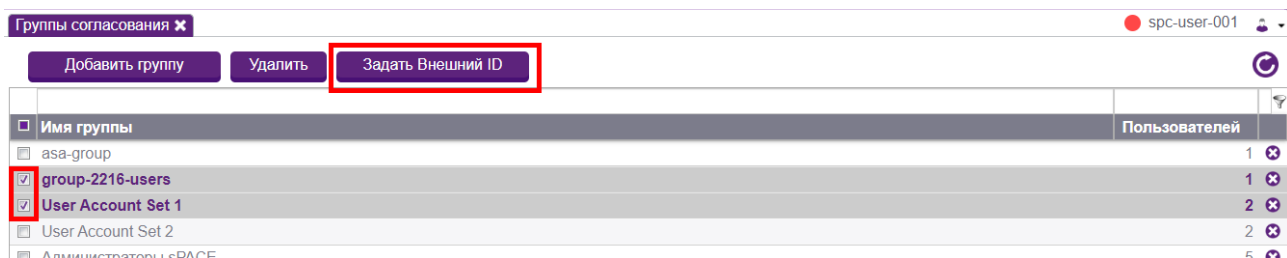


Рис. 16. Кнопка для задания внешнего ID

5.3. Управление учетными записями

Администраторы могут выполнять следующие действия с 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.

5.3.1. Добавление 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**.

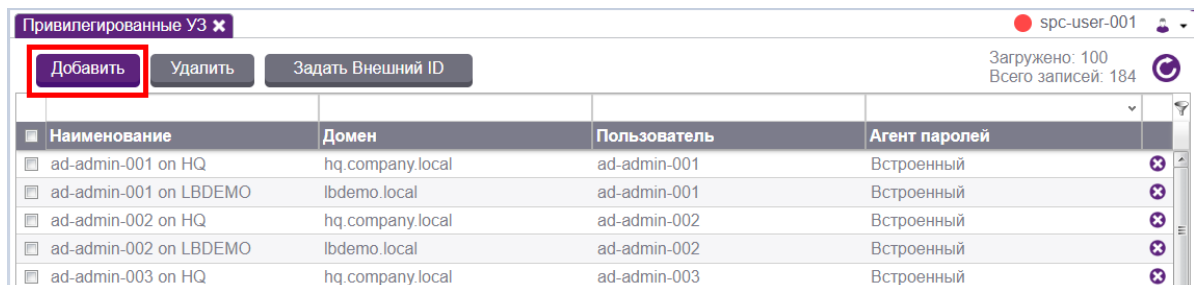


Рис. 17. Кнопка «Добавить»

Появившаяся форма добавления учетных записей **Учетная запись** содержит следующие поля:

- **Наименование** (обязательное поле) – наименование учетной записи в системе с учетом домена;
- **Домен** – сокращенное наименование домена, к которому принадлежит учетная запись. Если она является локальной для Windows-системы, то необходимо указать точку: ".";
- **Пользователь** (обязательное поле) – имя пользователя, владеющего данной учетной записью;

- FQDN – Fully Qualified Domain Name, имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS;
- Владелец – владелец данной учётной записи. После выбора владельца учётная запись становится персонифицированной (если владелец не указан, то учётная запись является общедоступной);
- Внешний ID – идентификатор для интеграции внешних систем через API sPASE с данной сущностью;
- Объект администрирования – объекты, с которыми работает пользователь-владелец учётной записи;
- Агент паролей – тип password agent-а для управления пользовательским паролем;
- Строка интеграции – строка интеграции с агентом паролей (специфично для каждого агента паролей);
- Рандомизация пароля – строка, показывающая, когда необходимо производить рандомизацию паролей для УЗ;
- Job рандомизации – выбор идентификатора job-а в агенте паролей для рандомизации пароля;
- Агент рандомизации паролей – выбор агента рандомизации паролей во вкладке "Агенты паролей" для рандомизации паролей УЗ;
- Управление расписанием – активно, если в поле "Рандомизация паролей" выбрано "Рандомизировать по расписанию". Необходимо для указания периодичности и времени рандомизации.

Поля, обязательные для заполнения, выделены полужирным шрифтом.

Учетная запись

Основные параметры

Наименование : Пользователь :

Домен : FQDN :

Дополнительные параметры

Владелец : Объект администрирования :

Внешний ID :

Параметры Агента паролей

Агент паролей : Рандомизация пароля :

Строка интеграции : Job рандомизации :

Управление расписанием

Однократно
 Периодически
 Еженедельно

Дата и время :

Сохранить Закрыть

Рис. 18. Форма добавления учетной записи

5.3.2. 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.

В появившемся с информацией об учетной записи **Учетная запись** будет активна кнопка **Редактирование учетной записи**. Для создания пароля учетной записи необходимо щелкнуть на кнопке **Задать секрет**.

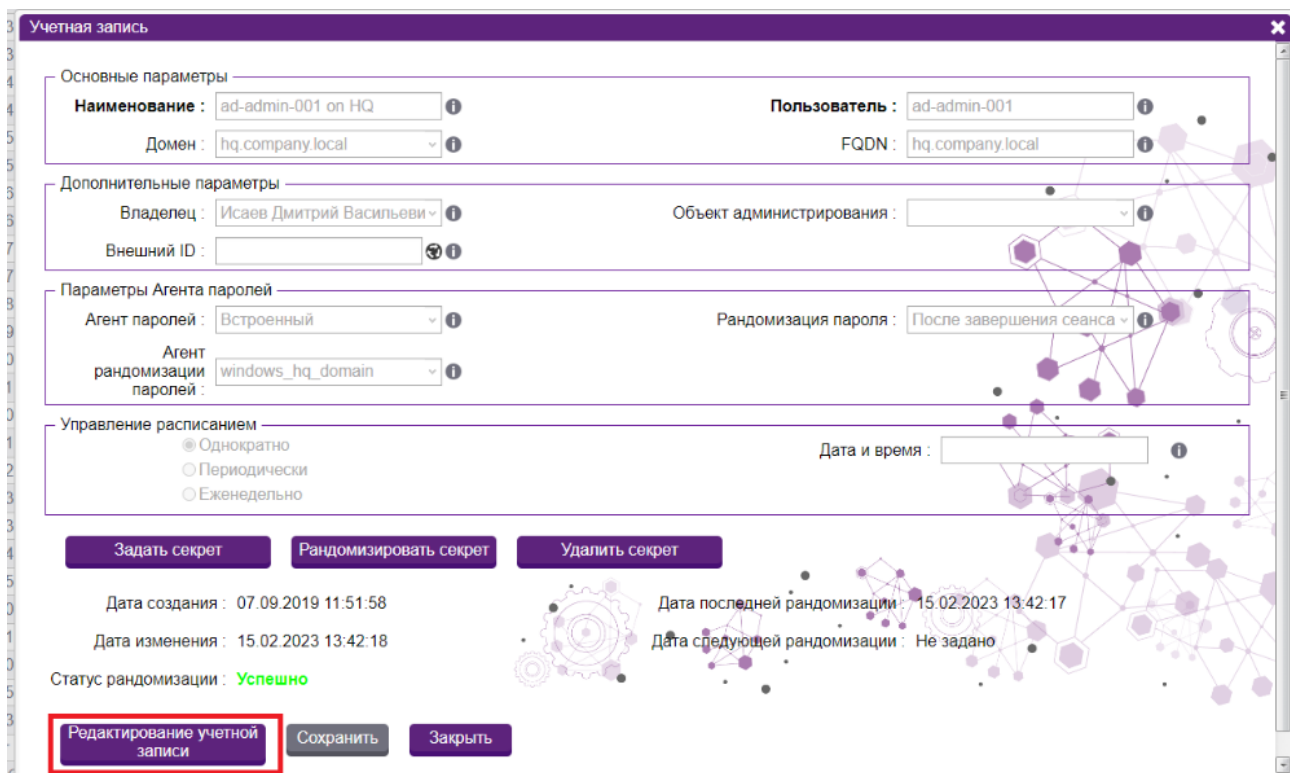


Рис. 19. Окно «Учетная запись». Кнопка редактирования активна

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

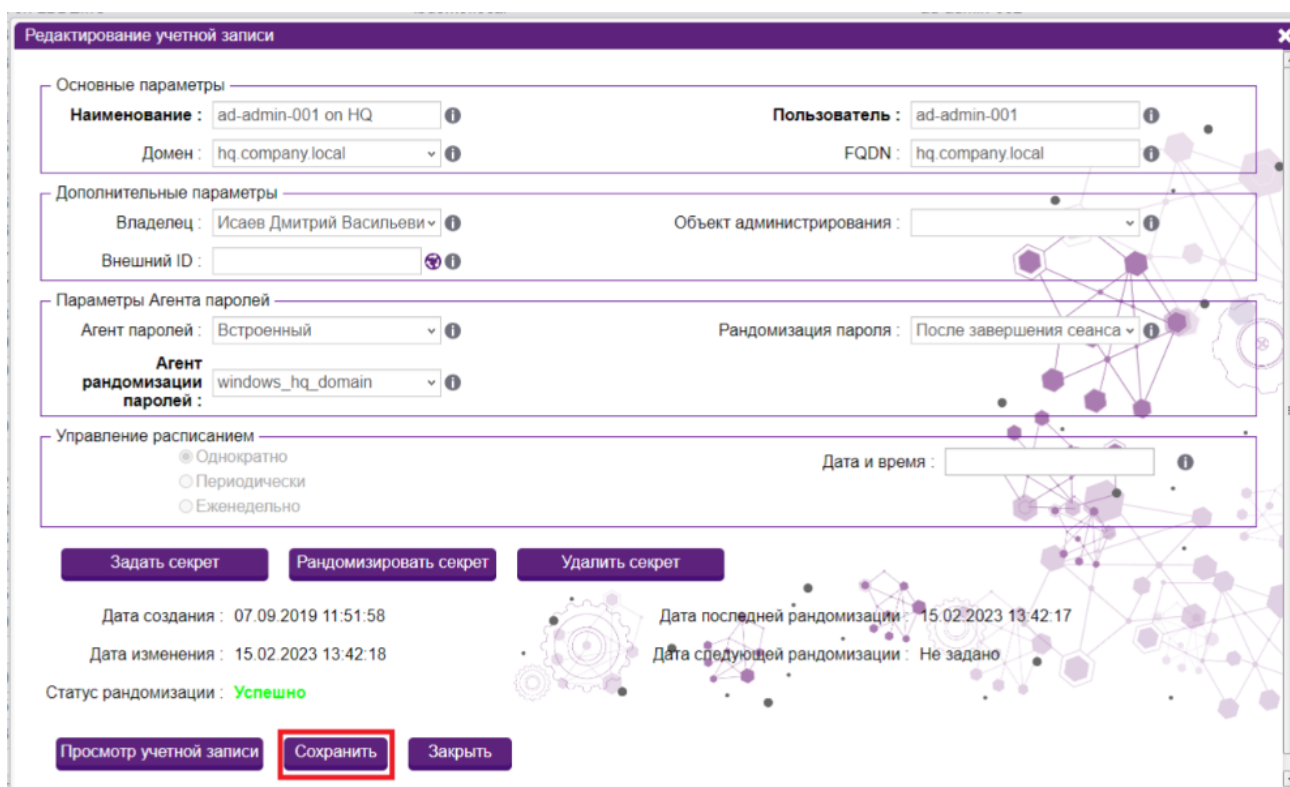


Рис. 20. Форма редактирования данных учетной записи

5.3.3. 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.

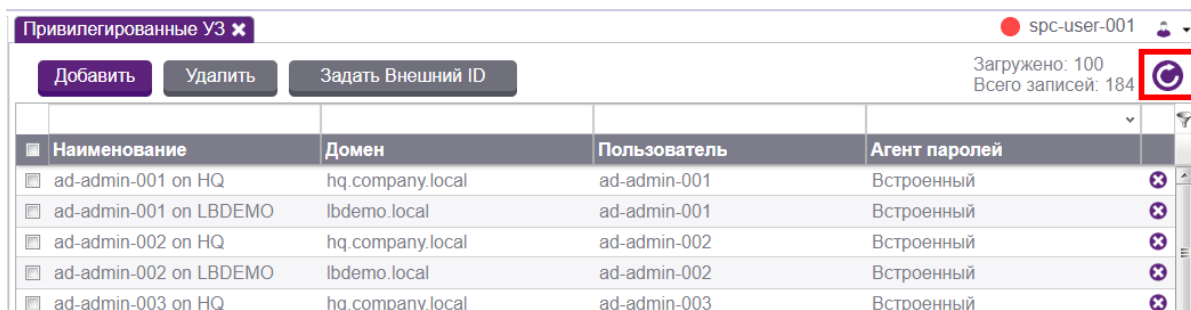


Рис. 21. Кнопка обновления таблицы учетных записей

5.3.4. Удаление строк в таблице учетных записей

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.

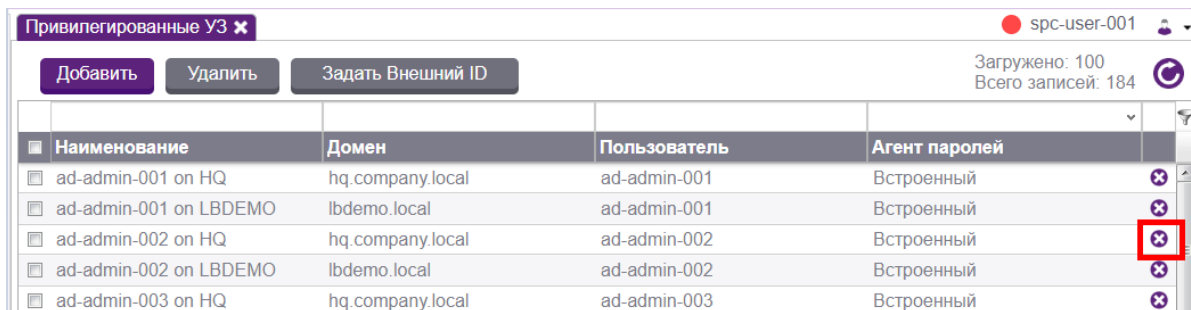


Рис. 22. Кнопка удаления учетной записи

5.3.5. Удаление нескольких записей из таблицы учетных записей одновременно

Для единовременного 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.

5.3.6 Единовременное задание внешнего ID для нескольких записей из таблицы учетных записей

Для единовременного задания внешнего ID для 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 **Задать Внешний ID**, расположенная на панели инструментов.

5.4. Управление объектами администрирования

Управление объектами администрирования 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.

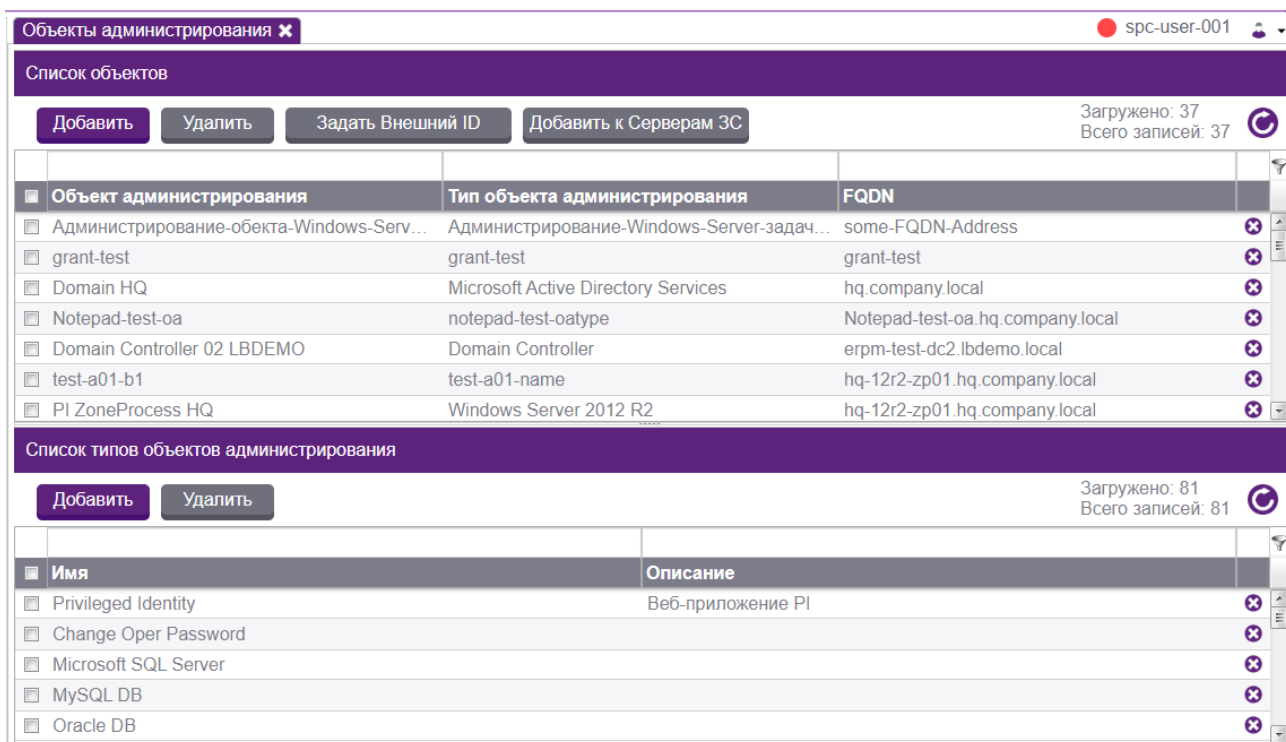


Рис. 23. Окно «Объекты администрирования»

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.

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.
- Задавать внешний ID для нескольких записей одновременно.
- Добавлять один или несколько объектов администрирования к определённому серверу защищённой среды.

5.4.1. 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. 24. 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;
- **Внешний ID** – идентификатор для интеграции внешних систем через API sPACe с данной сущностью;
- **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. 25. Кнопка «Добавить»

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.

5.4.2. 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**.

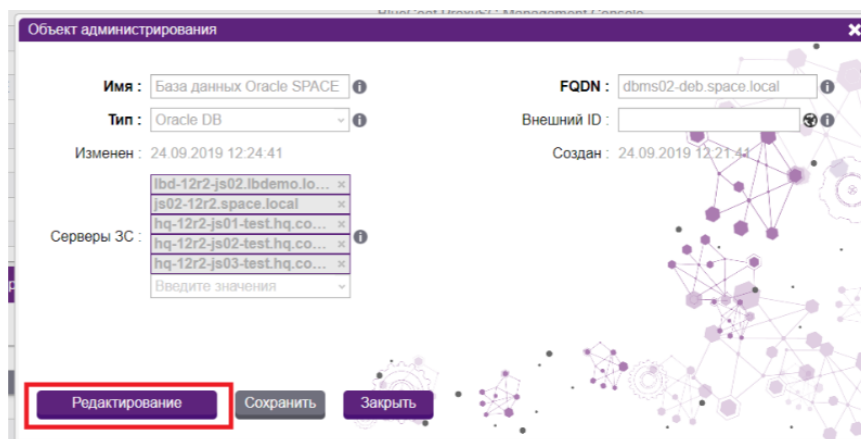


Рис. 26. Карточка объекта администрирования

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 – 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 доступны для редактирования. Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При нажатии кнопки **Закрыть** изменения не сохраняются.

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

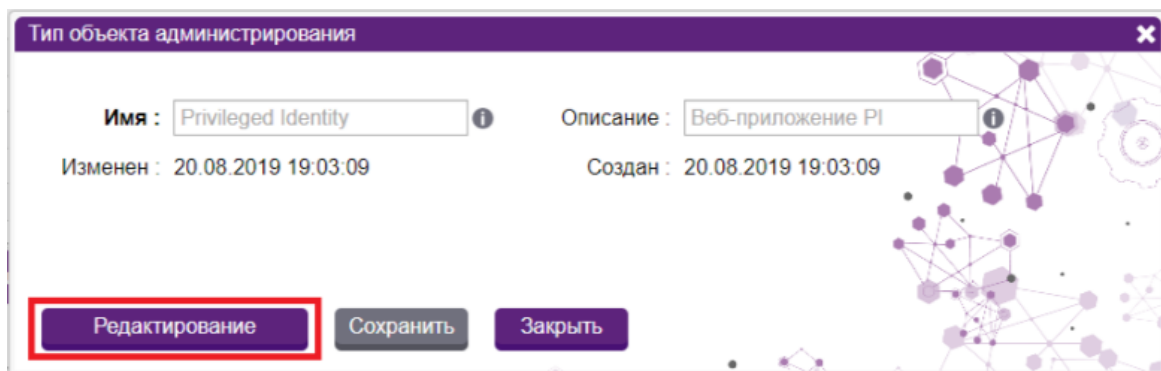


Рис. 27. Карточка типа объекта администрирования

Форма редактирования типа объекта администрирования содержит следующие поля:

- Имя (обязательное поле) – имя объекта;
- Описание – описание объекта администрирования.

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

5.4.3. 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.

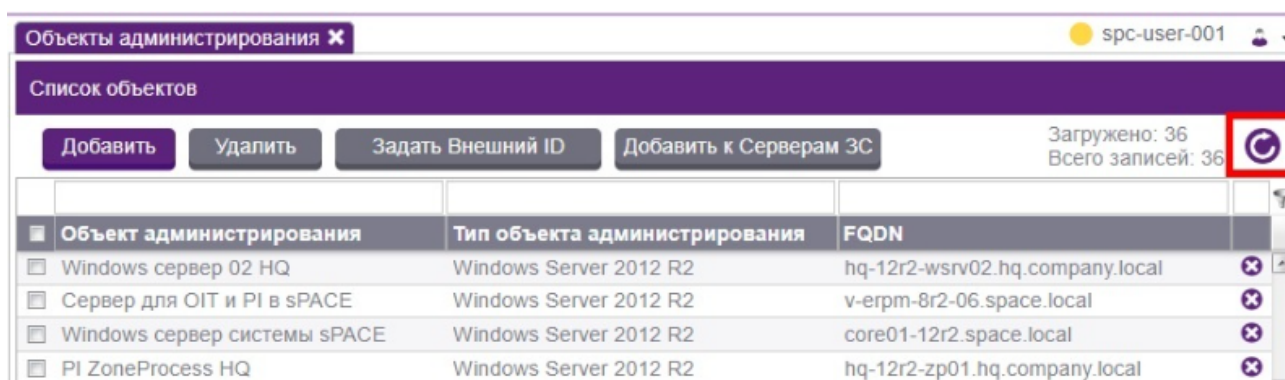


Рис. 28. Кнопка обновления записей таблицы

5.4.4. Удаление строки 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 строки из таблицы типов объектов администрирования происходит аналогичным способом.

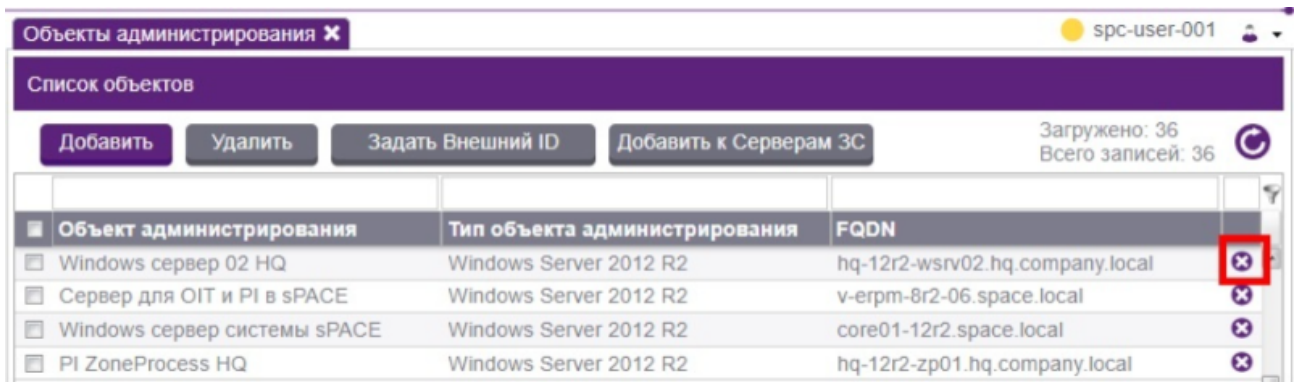


Рис. 29. Кнопка удаления строки

5.4.5. 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.

5.4.6. Единовременное задание внешних ID для нескольких объектов администрирования

Для единовременного задания внешнего ID для нескольких записей сначала следует выделить желаемые записи в таблице галочкой слева, после чего станет активной кнопка **Задать Внешний ID**, расположенная сверху над таблицей.

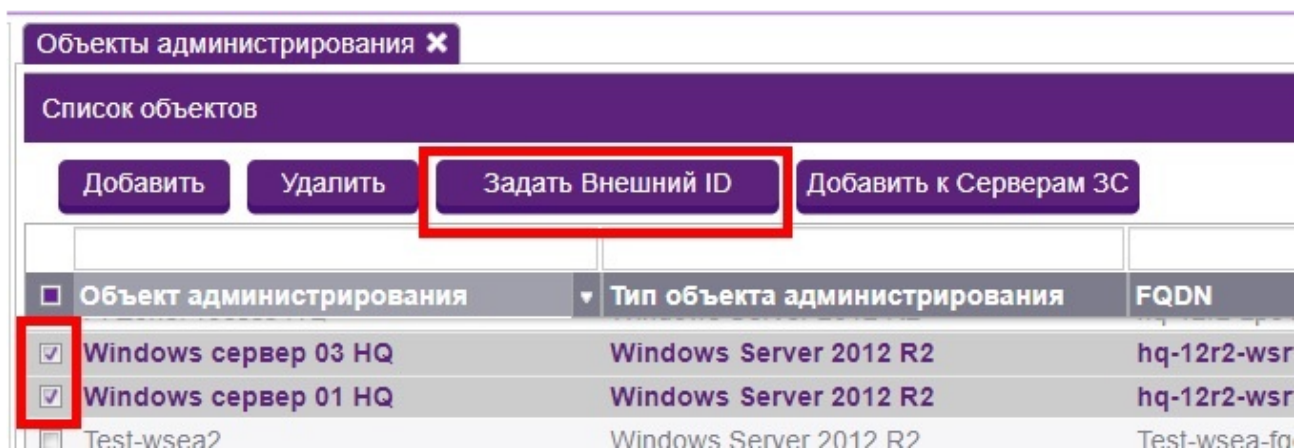


Рис. 30. Кнопка для задания внешнего ID

5.4.7. Единовременное добавление серверов ЗС для нескольких объектов администрирования

Для единовременного добавления 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.

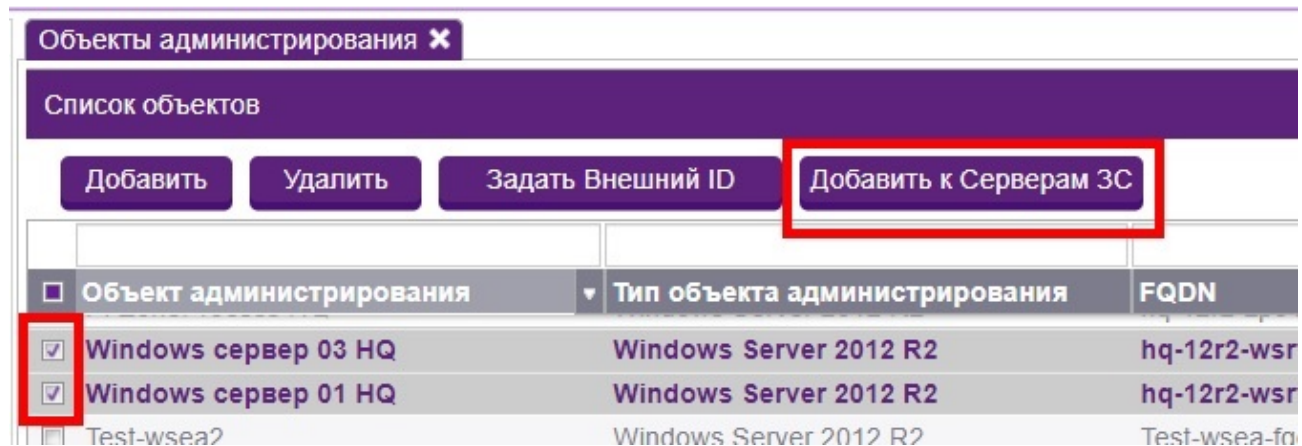


Рис. 31. Кнопка для добавления к серверам ЗС

5.5. Управление приложениями

Пользователи управляют объектами администрирования при помощи инструментов администрирования (приложений), которые предварительно настраивает администратор. Для настройки приложений и исполняемых сценариев необходимо перейти в узел **Приложения** раздела **Управление системой**.

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

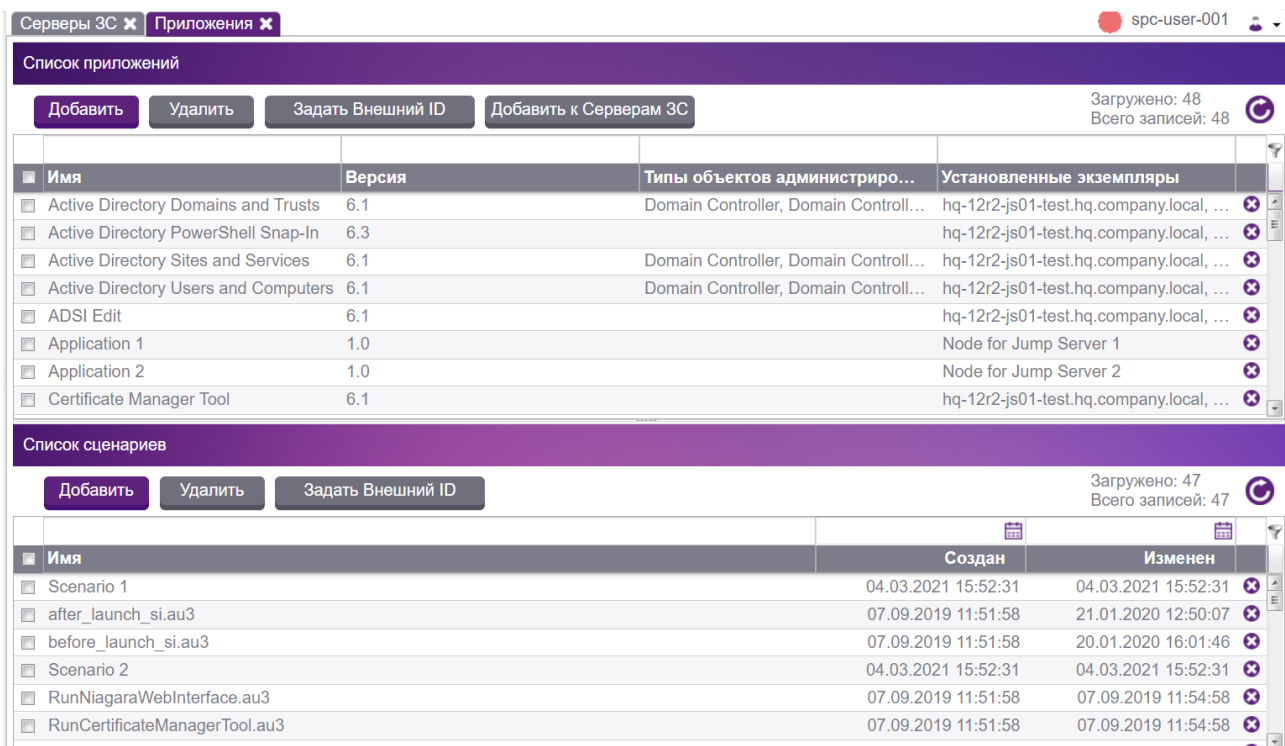


Рис. 32. Окно «Приложения»

Таблица **Список приложений** содержит следующие поля:

- Имя – наименование приложения;
- Версия – версия приложения;
- Типы объектов администрирования – разновидность объекта администрирования, определяющая правила работы с объектом;
- Установленные экземпляры – сервера ЗС, 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 нескольких записей из таблицы одновременно;
- Задавать внешний ID для нескольких записей одновременно;

- Задавать сервер ЗС для нескольких записей одновременно.

5.5.1. Добавление приложения/сценария

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

На экране отобразится форма добавления приложения.

Рис. 33. Форма добавления приложений

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

- **Имя** (обязательное поле) – наименование приложения;
- **Типы объектов администрирования** – разновидности объектов администрирования в рамках добавляемого 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;
- **Внешний ID** – идентификатор для интеграции внешних систем через API sPACe с данной сущностью;
- **Версия** – версия приложения;
- **Установленные экземпляры** (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.

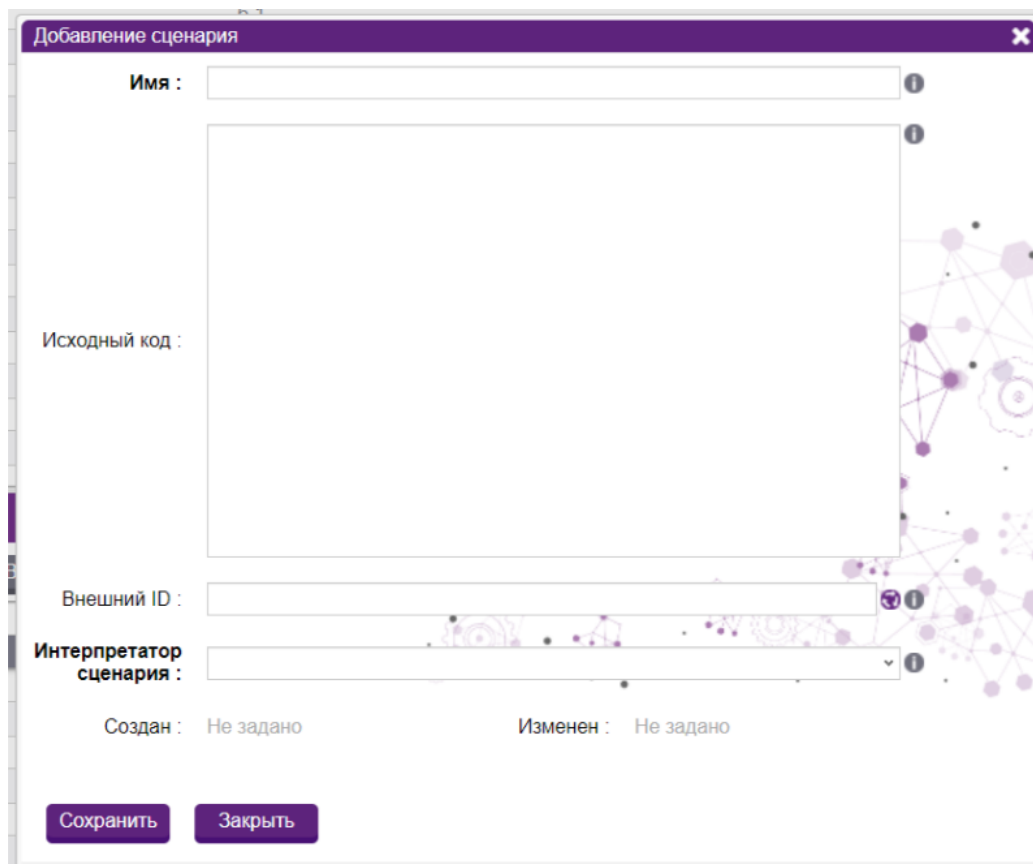


Рис. 34. Форма добавления сценария

Форма добавления сценария содержит следующие поля:

- Имя (обязательное поле) – наименование сценария;
- Исходный код – исходный код данного сценария;
- Внешний ID – идентификатор для интеграции внешних систем через API sPACE с данной сущностью;
- Интерпретатор сценария (обязательное поле) – интерпретатор, который будет преобразовывать исходный код сценария в последовательность нужных действий при использовании сценария.

5.5.2. 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.

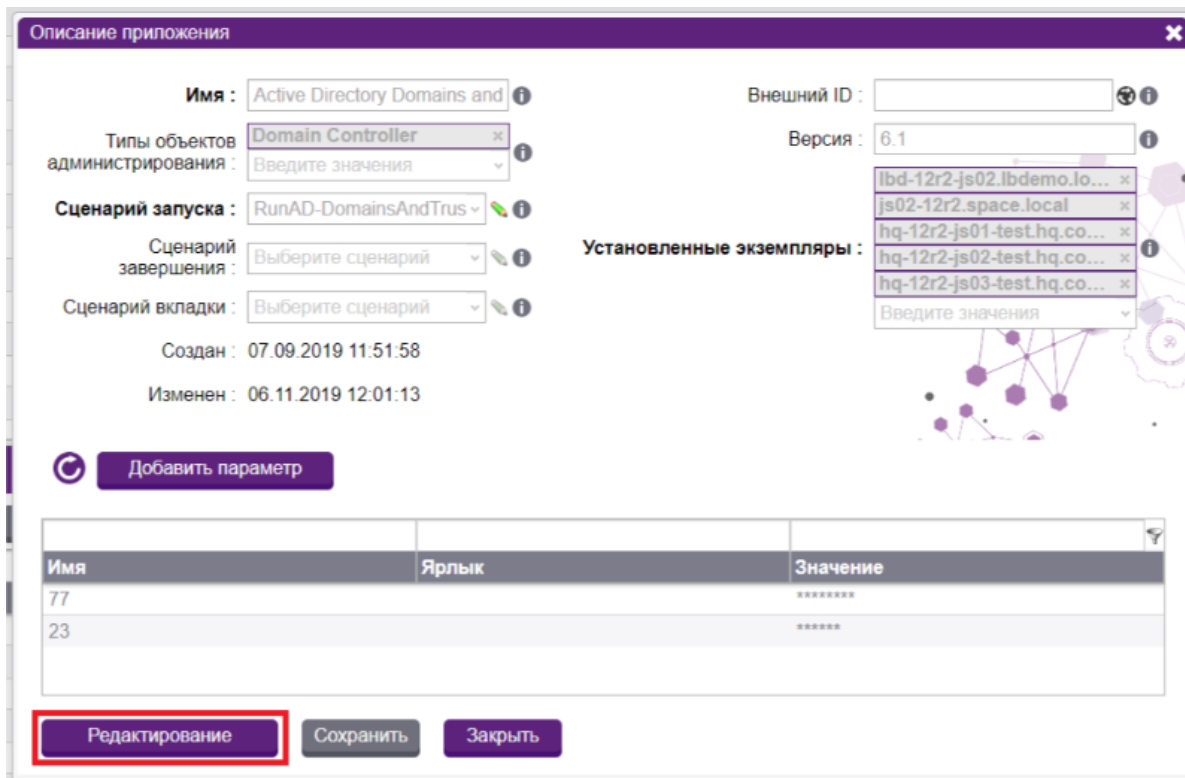


Рис. 35. Карточка приложения

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

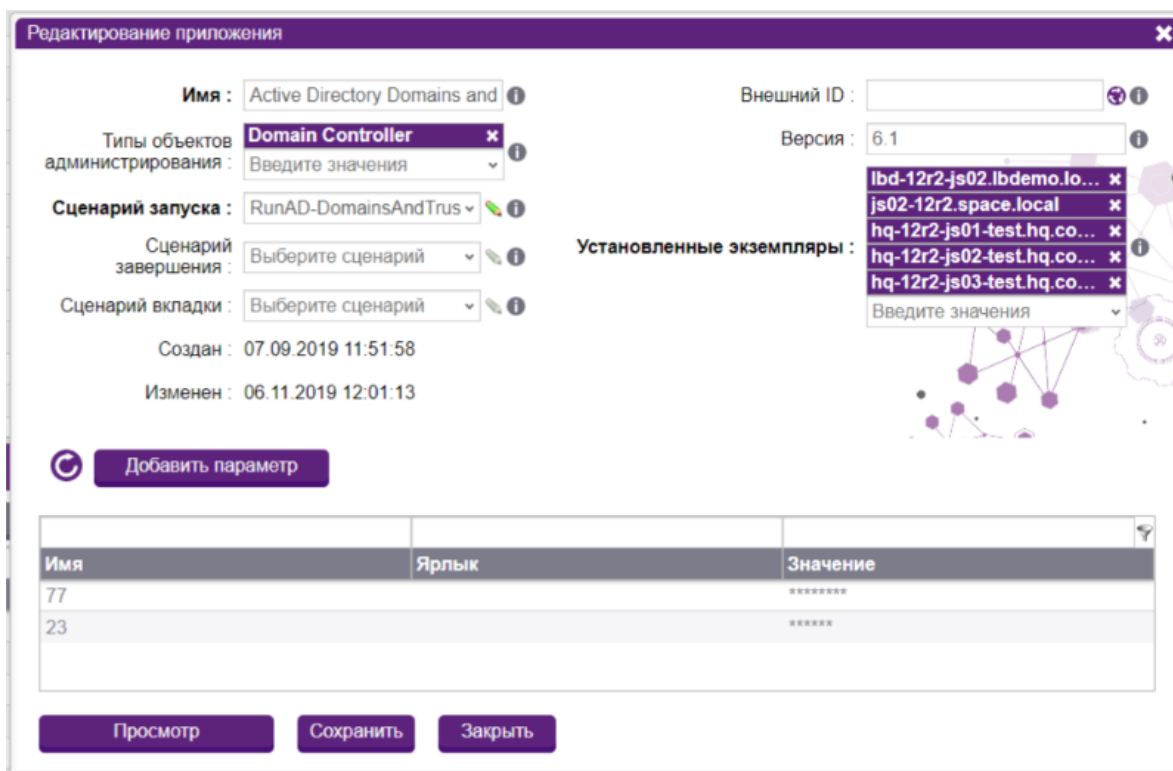


Рис. 36. Форма редактирования приложения

Все поля доступны для редактирования. Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При нажатии кнопки **Заккрыть** никаких изменений в карточке приложения не произойдет.

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

Рис. 37. Форма добавления параметра

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

- Имя (обязательное поле) – наименование параметра для приложения;
- Ярлык – ярлык для данного параметра;
- Тип (обязательное поле) – тип данного параметра;
- Внешний ID – идентификатор для интеграции внешних систем через API sPACE с данной сущностью;
- Значение – значение данного параметра;
- Описание – описание данного параметра;
- Обязательный – индикатор, определяющий, является ли данный параметр обязательным для данного приложения;
- Скрытый – индикатор, определяющий, является ли данный параметр скрытым для данного приложения;
- Только для чтения – индикатор, показывающий, может ли пользователь изменить значение данного параметра при запуске данного приложения;
- Привязать к объекту администрирования – имя объекта администрирования, к которому привязан данный параметр;

- Привязать к пользователю – имя пользователя, к которому привязан данный параметр;
- Привязать к экземпляру – имя терминального сервера с приложением, 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.

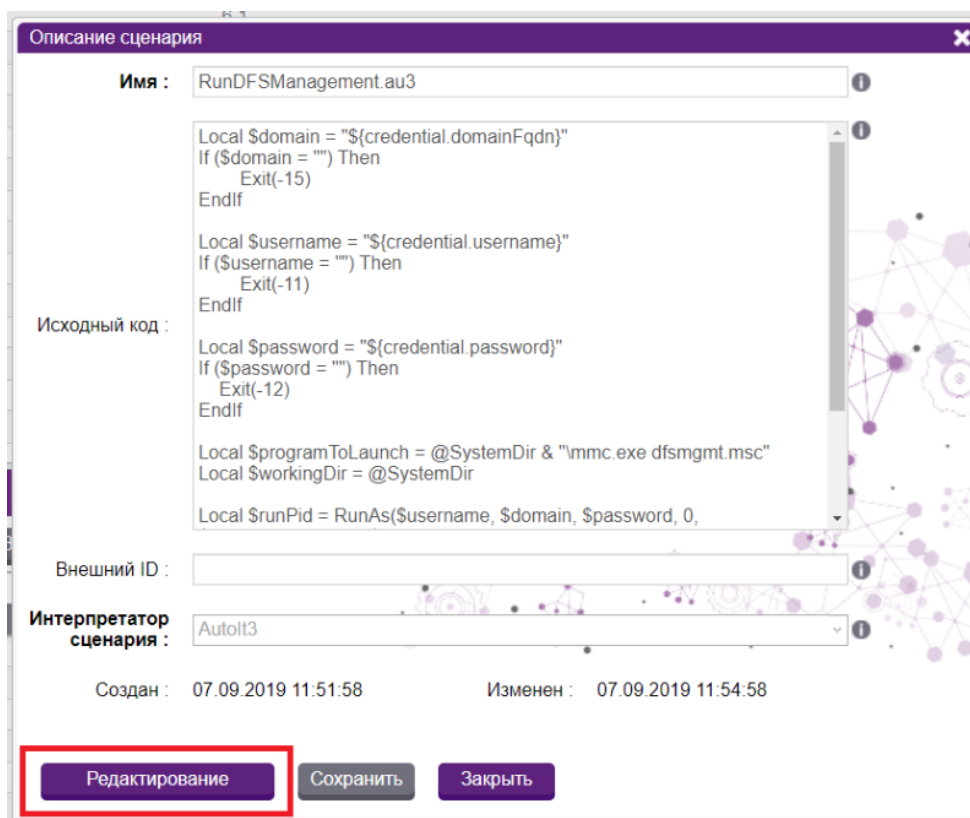


Рис. 38. Карточка сценария. Кнопка «Редактирование»

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

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

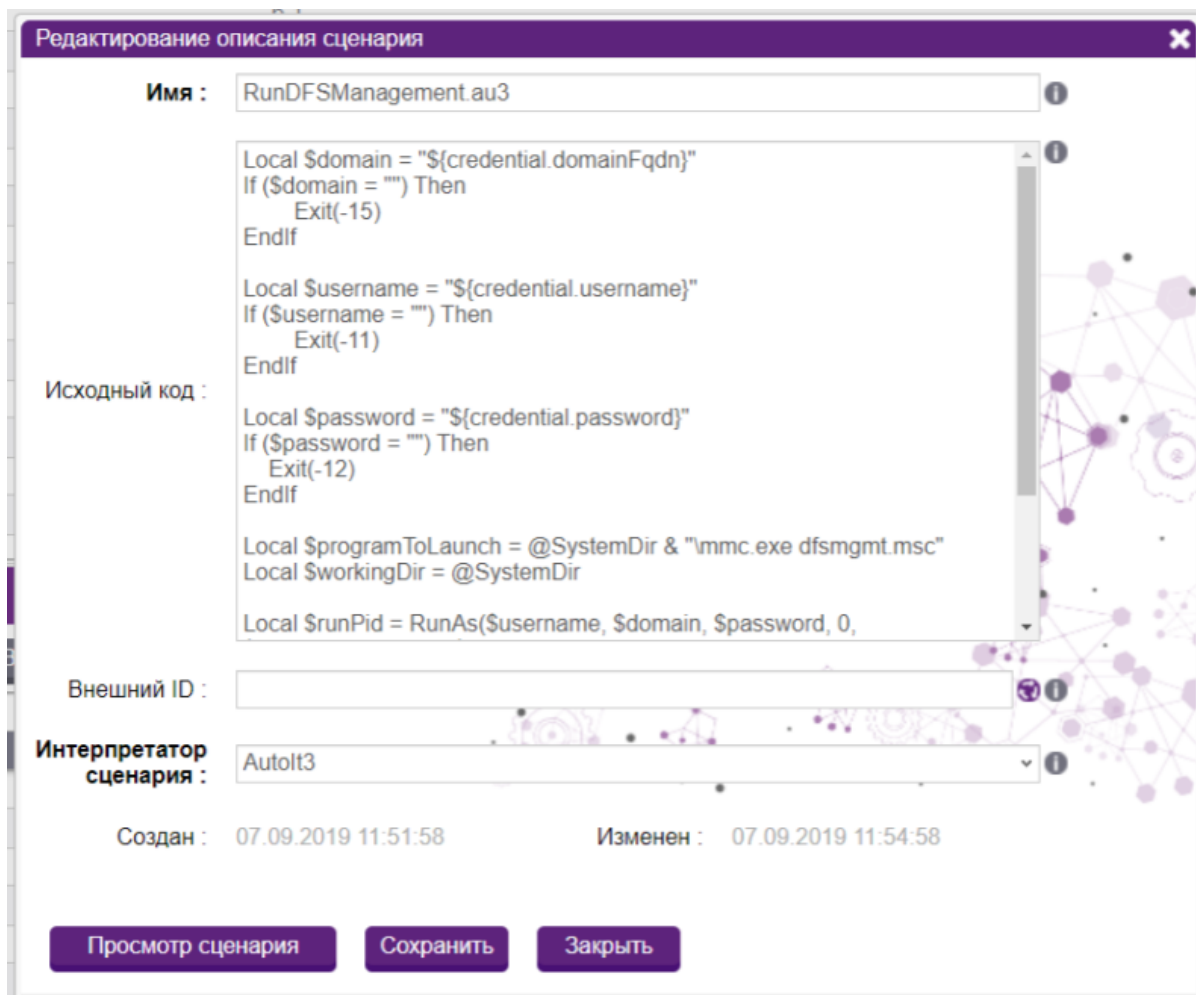


Рис. 39. Форма редактирования сценария

5.5.3. Обновление таблицы приложений/сценариев

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

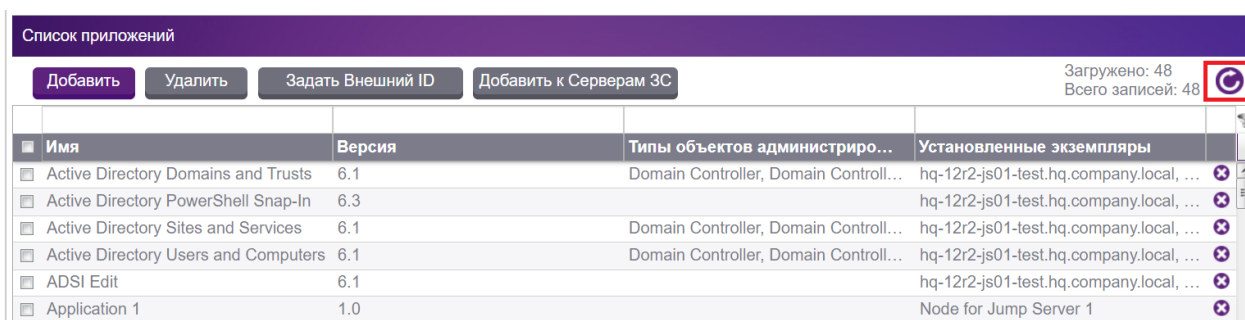


Рис. 40. Кнопка обновления информации

5.5.4. Удаление строки в таблице приложений/сценариев

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

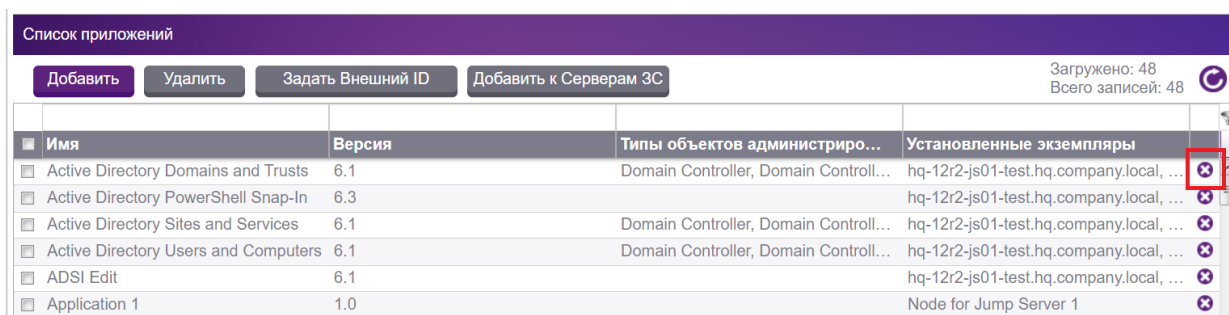


Рис. 41. Расположение кнопки удаления строки в списке приложений

5.5.5. 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.

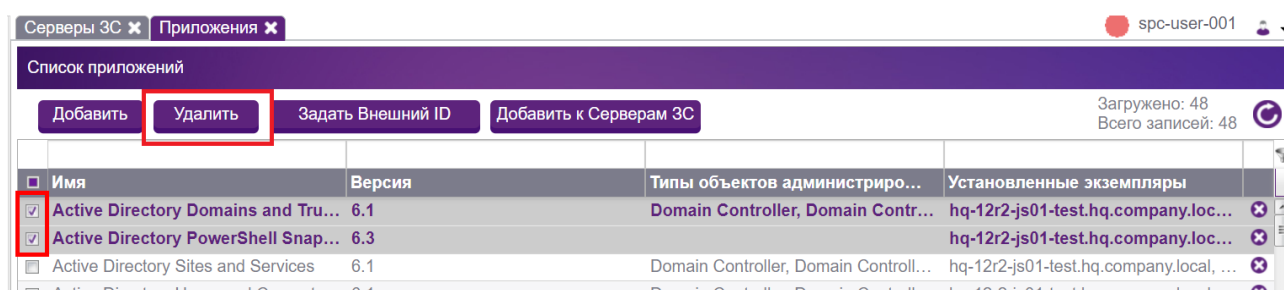


Рис. 42. Выбор двух записей таблицы и кнопка удаления

5.5.6. Единовременное задание внешнего ID для нескольких записей из таблицы приложений

Для единовременного задания внешнего ID для нескольких записей сначала следует выделить желаемые записи в таблице галочкой слева, после чего станет активной кнопка **Задать Внешний ID**, расположенная сверху над таблицей.

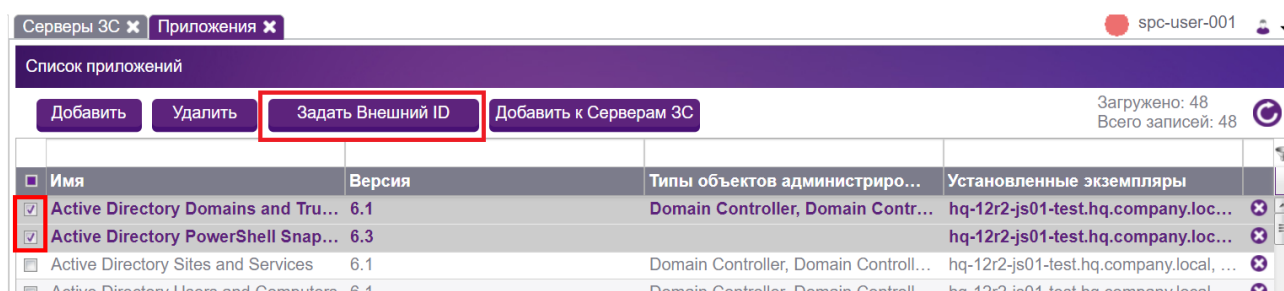


Рис. 43. Выбор двух записей таблицы и кнопка для задания Внешнего ID

5.5.7. Единовременное добавление серверов ЗС для нескольких приложений

Для единовременного добавления серверов ЗС для нескольких приложений 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.

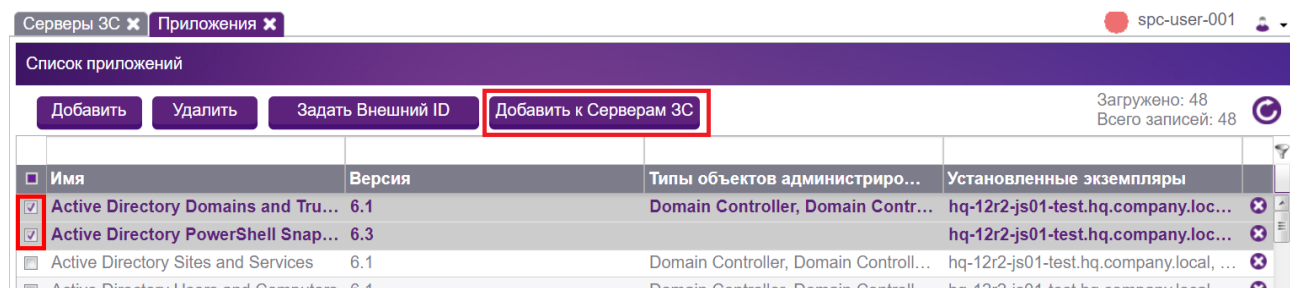


Рис. 44. Выбор двух записей таблицы и кнопка для добавления к Серверам ЗС

5.6. Управление интерпретаторами

После щелчка мышью на узле **Интерпретаторы** дерева навигации раздела **Управление системой** пользователю 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 нескольких записей в таблице интерпретаторов.

5.6.1. 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.

Добавление интерпретатора

Имя :

Интерпретатор :

Расширение для сценария :

Режим возвращения PID :

Сохранить Закреть

Рис. 45. Форма добавления интерпретатора

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

- Имя – название добавляемого интерпретатора;
- Интерпретатор – название файла с расширением exe 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.

5.6.2. Редактирование интерпретаторов

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

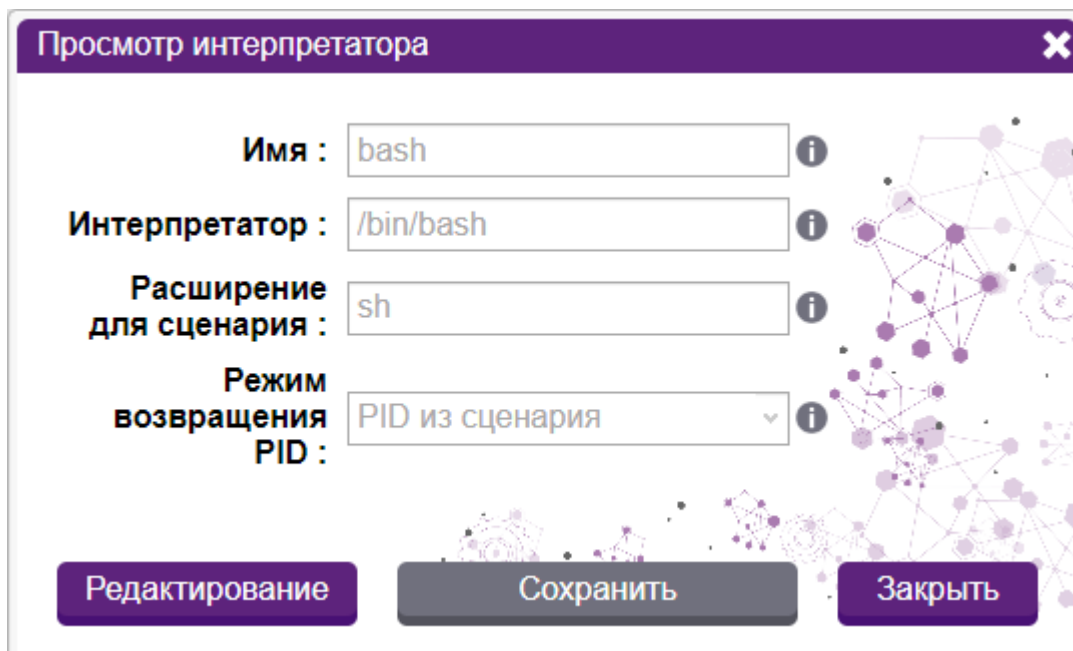


Рис. 46. Карточка интерпретатора

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

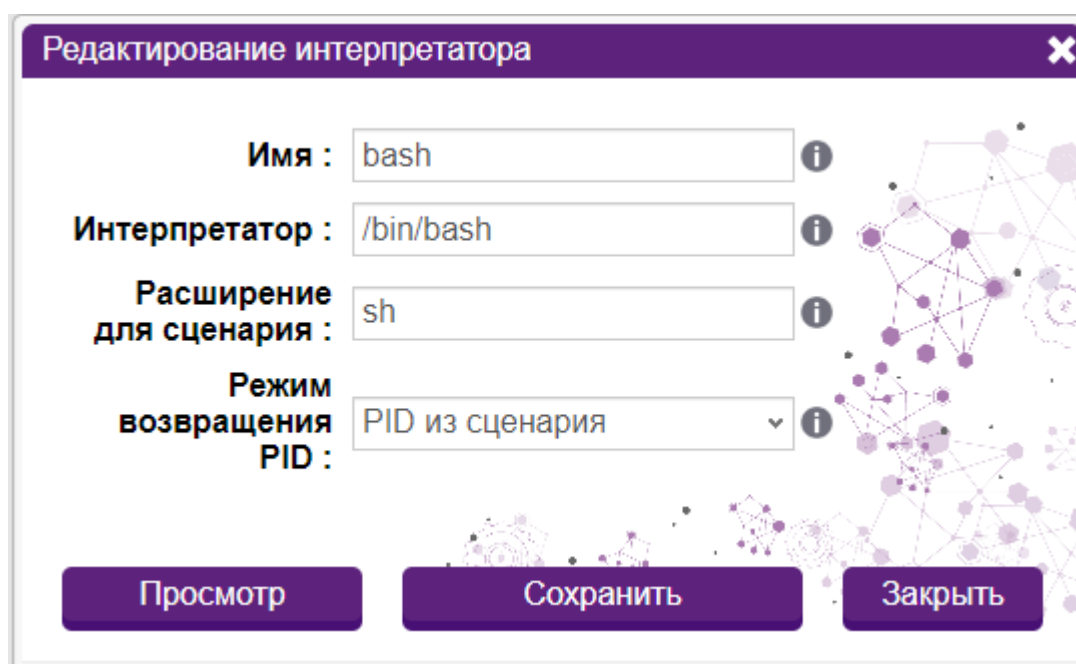


Рис. 47. Форма редактирования интерпретатора

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

5.6.3. 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.

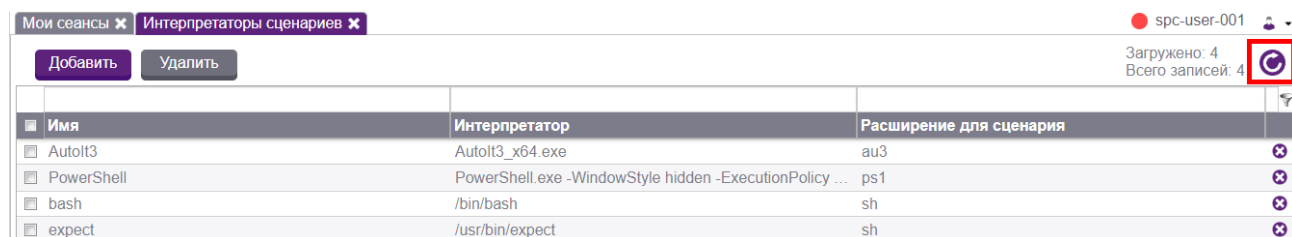


Рис. 48. Кнопка обновления информации

5.6.4. Удаление строки в таблице интерпретаторов

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

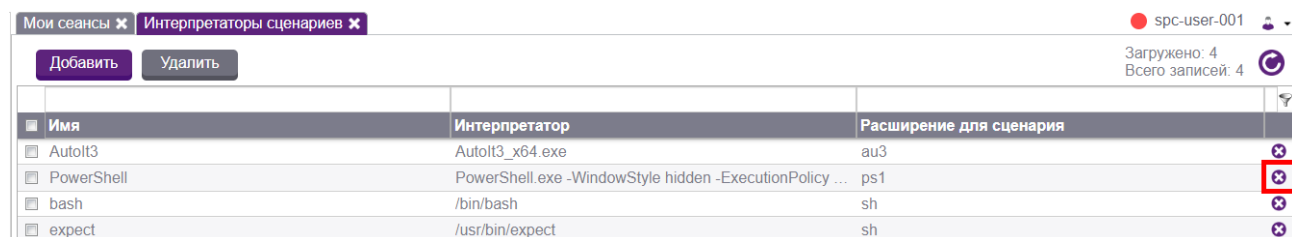


Рис. 49. Кнопка удаления строки в списке интерпретаторов

5.6.5. 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.

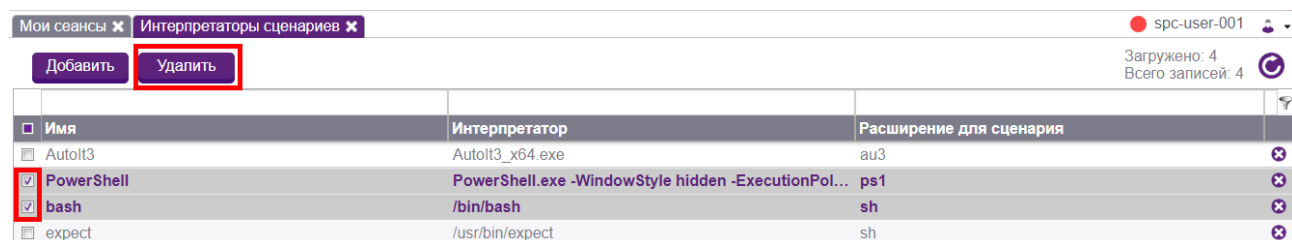


Рис. 50. Выбор двух записей таблицы и кнопка удаления

5.7. 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;
- Учетные записи – те, при помощи которых осуществляется работа с объектами администрирования в рамках соответствующих задач;
- Согласующие – группа пользователей, имеющие право на согласование данной задачи.

Задача	Объекты администрирован...	Учётные записи	Согласующие
123н342	2	1	Администраторы домена HQ
LDAP Browsing	0	0	Администраторы sPACE
Администрирование серверов ...	4	0	Администраторы домена HQ
Администрирование серверов ...	3	3	Администраторы sPACE
Администрирование серверов ...	4	1	Администраторы домена HQ
Администрирование серверов ...	2	1	Администраторы sPACE
Добавление пользователя в по...	0	0	Администраторы домена HQ
Управление 3rd Party	5	0	Администраторы sPACE
Управление VMware HQ	3	0	Администраторы домена HQ

Рис. 51. 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;
- Задавать внешний ID для нескольких записей одновременно.

5.7.1. Добавление задачи

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

Рис. 52. 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;
- **Внешний ID** – идентификатор для интеграции внешних систем через API sPACE с данной сущностью.

5.7.2. Редактирование задачи

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

Задача "LDAP Browsing"

Имя : LDAP Browsing

Согласующие : Администраторы vSPACE

Внешний ID :

Описание :

Объекты администрирования

Выберите объект --> Удалить

Объект администрирования	Тип объекта	FQDN
Нет объектов для вывода.		

Учётные записи

Выберите учётную запись --> Удалить

Наименование	Домен	Пользователь	Агент паролей
Нет объектов для вывода.			

Редактирование Сохранить Закреть

Рис. 53. Карточка задачи

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

Задача "LDAP Browsing"

Имя : LDAP Browsing

Согласующие : Администраторы vSPACE

Внешний ID :

Описание :

Объекты администрирования

Выберите объект --> Удалить

Объект администрирования	Тип объекта	FQDN
Нет объектов для вывода.		

Учётные записи


Выберите учётную запись --> Удалить

Наименование	Домен	Пользователь	Агент паролей
Нет объектов для вывода.			

Вернуться Сохранить Закреть

Рис. 54. Форма редактирования задачи

5.7.3. Обновление таблицы задач

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

5.7.4. Удаление строки в таблице задач

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







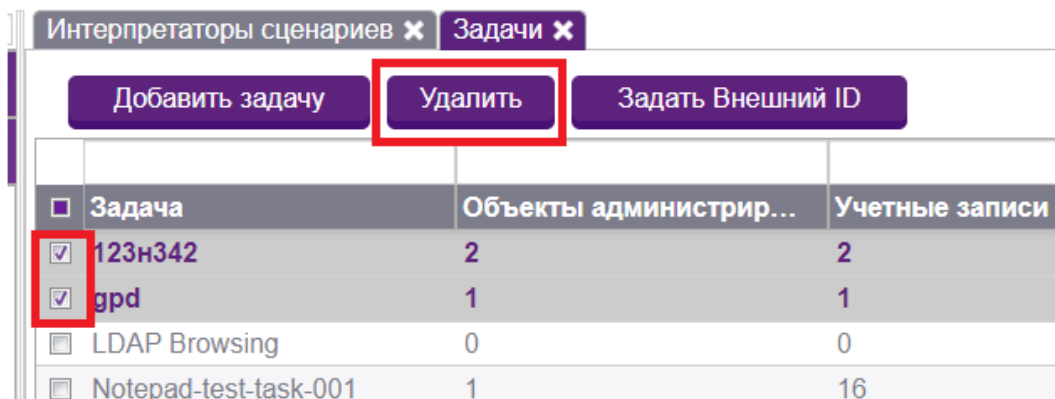
Задача	Объекты администрир...	Учетные записи	Согласующие
<input type="checkbox"/> 123н342	2	2	Администраторы домена ... 
<input type="checkbox"/> gpd	1	1	Администраторы домена ... 
<input type="checkbox"/> LDAP Browsing	0	0	Администраторы sPACE 
<input type="checkbox"/> Notepad-test-task-001	1	16	Администраторы домена ... 
<input type="checkbox"/> Task 1	2	0	User Account Set 1 
<input type="checkbox"/> Task 2	2	0	User Account Set 2 

Рис. 55. Кнопка удаления

5.7.5. 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.



Задача	Объекты администрир...	Учетные записи
<input checked="" type="checkbox"/> 123н342	2	2
<input checked="" type="checkbox"/> gpd	1	1
<input type="checkbox"/> LDAP Browsing	0	0
<input type="checkbox"/> Notepad-test-task-001	1	16

Рис. 56. Выбраны две записи таблицы. Кнопка «Удалить» активна

5.7.6. Единовременное задание внешнего ID для нескольких записей из таблицы задач

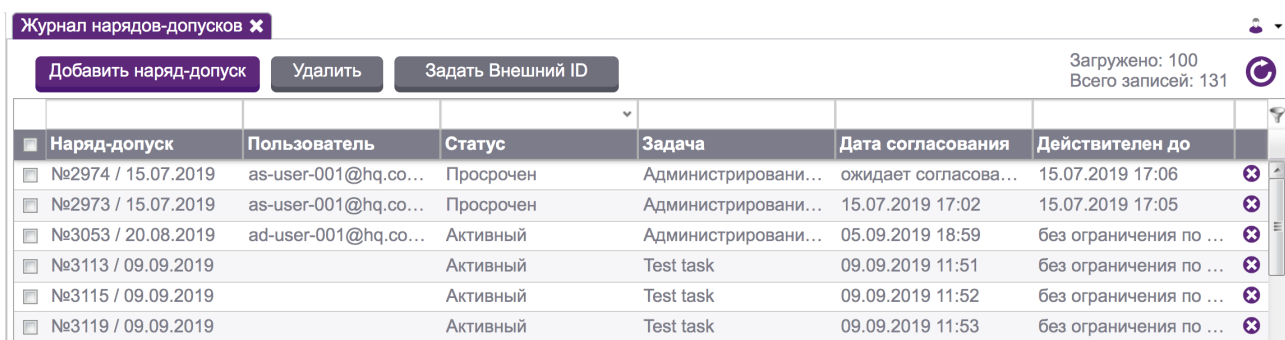
Для единовременного задания внешнего ID для нескольких записей сначала следует выделить желаемые записи в таблице галочкой слева от поля **Задача**, после чего станет активной кнопка **Задать Внешний ID**, расположенная сверху над таблицей.

5.8. 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, иницилирующее 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.



Наряд-допуск	Пользователь	Статус	Задача	Дата согласования	Действителен до
№2974 / 15.07.2019	as-user-001@hq.co...	Просрочен	Администрировани...	ожидает согласова...	15.07.2019 17:06
№2973 / 15.07.2019	as-user-001@hq.co...	Просрочен	Администрировани...	15.07.2019 17:02	15.07.2019 17:05
№3053 / 20.08.2019	ad-user-001@hq.co...	Активный	Администрировани...	05.09.2019 18:59	без ограничения по ...
№3113 / 09.09.2019		Активный	Test task	09.09.2019 11:51	без ограничения по ...
№3115 / 09.09.2019		Активный	Test task	09.09.2019 11:52	без ограничения по ...
№3119 / 09.09.2019		Активный	Test task	09.09.2019 11:53	без ограничения по ...

Рис. 57. Окно узла «Наряды-допуски»

В рамках настройки и управления нарядами-допусками администраторы 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;
- задавать внешний ID для нескольких записей из таблицы НД.

5.8.1. 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 администратор находится в группе согласования для данной задачи, то будет активна кнопка **Согласовать**. Подробно о полях можно прочитать в Руководстве пользователя или в справке на портале.


Рис. 58. Форма создания наряда-допуска

5.8.2. 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.

5.8.3. Обновление таблицы нарядов-допусков

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

5.8.4. 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.

5.8.5. 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.

5.8.6. Единовременное задание внешнего ID для нескольких записей из таблицы нарядов-допусков

Для единовременного задания внешнего ID для нескольких записей из таблицы нарядов-допусков необходимо выделить желаемые записи в таблице, установив флажок в соответствующем поле слева от поля **Наряд-допуск**, после чего станет активной кнопка **Задать Внешний ID**, расположенная сверху над таблицей.

5.9. Управление серверами защищенной среды (ЗС)

Сервер Защищенной Среды Привилегированного Доступа — 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.

Используемые Серверы 3С

Имя	FQDN	Доступен	Терм. соединения	Сессии
host-docker-internal	host.docker.internal	<input type="checkbox"/>	0	0
Node 1	fqdn-for-node-1	<input type="checkbox"/>	0	0
Node for Jump Server 1	fqdn-for-node-for-js-1	<input type="checkbox"/>	0	0
test-domain-2216-1	some-fqdn-address	<input type="checkbox"/>	0	0
aferon	aferon	<input type="checkbox"/>	0	0
hq-12r2-js02-test.hq.company.local	hq-12r2-js02-test.hq.company.local	<input checked="" type="checkbox"/>	0	0
hq-12r2-js03-test.hq.company.local	hq-12r2-js03-test.hq.company.local	<input type="checkbox"/>	0	0
igor-astra	astra	<input checked="" type="checkbox"/>	0	0
aferonHome	win-epgi0j035gt	<input type="checkbox"/>	0	0
Hanneko WS2019	winserv-test.test.hanneko.forest	<input type="checkbox"/>	0	0

Неиспользуемые Серверы 3С

Имя	FQDN	Доступен
hq-12r2-js03.hq.company.local	hq-12r2-js03.hq.company.local	<input type="checkbox"/>
js01-12r2.space.local	js01-12r2.space.local	<input type="checkbox"/>
sea-pc.space.local	desktop-vq9rprb.webc.local	<input type="checkbox"/>
hq-12r2-js01.hq.company.local	hq-12r2-js01.hq.company.local	<input type="checkbox"/>

Рис. 59. Окно «Сервера 3С» раздела «Управление системой»

Вся информация об имеющихся в Системе серверах ЗСА отображается в узле **Серверы 3С** раздела **Управление системой**. Внешне раздел представлен в виде двух таблиц. В первой находятся используемые сервера 3С (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 3С;
- Редактировать сервера 3С;
- Обновлять таблицы серверов 3С;

- Удалять строки в таблице серверов ЗС;
- Удалять несколько записей из таблицы серверов ЗС одновременно;
- Задавать внешний ID для нескольких записей из таблицы серверов ЗС;
- Добавлять и удалять сервера из балансировки.

5.9.1. Добавление сервера ЗСА

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

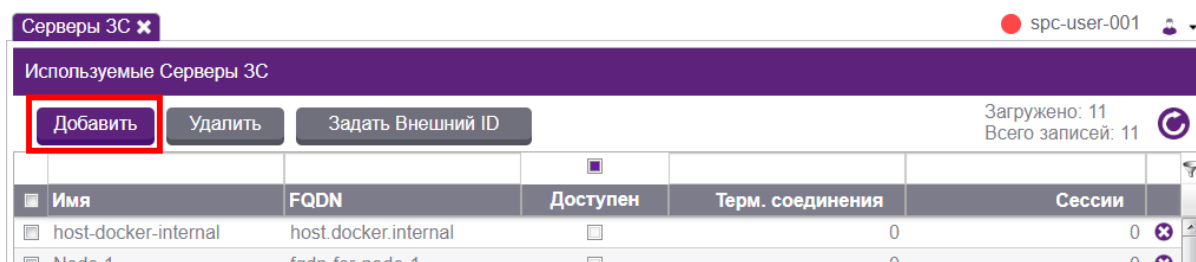


Рис. 60. Кнопка добавления сервера ЗС

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;
- **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. 61. Форма «Добавление сервера ЗС»


5.9.2. 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. 62. Редактирование сервера ЗС

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

5.9.3. Обновление таблицы серверов ЗСА

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

5.9.4. Удаление строки в таблице серверов ЗСА

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

5.9.5. 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.

5.9.6. Единовременное задание внешнего ID для нескольких записей из таблицы серверов ЗС

Для единовременного задания внешнего ID для нескольких записей сначала следует выделить желаемые записи в таблице галочкой слева от поля **Имя**, после чего станет активной кнопка **Задать Внешний ID**, расположенная сверху над таблицей.

5.10. Просмотр системных настроек

Параметры системных настроек описаны в Инструкции по развертыванию. Узел **Системные настройки** раздела **Управление системой** позволяет просмотреть текущие параметры и изменить некоторые настройки.

Внешне раздел "Системные настройки" выглядит следующим образом:

Серверы NATS

Парольная политика

Логирование

Внешняя тикет система

Источник данных :

URL : jdbc:postgresql://dbms02-deb.space.local:5432/space_db?currentSchema=space

Пользователь : space

Система доставки :

TLS : Выключен

Адрес : hq-12r2-dc01.hq.company.local:4222

Имя очереди : space-queue.core.management

Хранилище ключей : cert/core-client-keystore.jks

Хранилище сертификатов : cert/core-client-truststore.jks

Имя пользователя Nats : space-core-03

Пароль пользователя Nats : Не задано

Рис. 63. 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:

- TLS – статус TLS шифрования;
- Адрес – адрес расположения серверов системы доставки;
- Имя очереди – имя очереди для взаимодействия с системой доставки;
- Хранилище ключей – имя хранилища ключей для TLS;
- Хранилище сертификатов – имя хранилища сертификатов для TLS;
- Имя пользователя NATS – имя пользователя, под которым происходит подключение к NATS;
- Пароль пользователя NATS – пароль пользователя, под которым происходит подключение к NATS.

5.10.1. Изменение настроек серверов NATS

Для редактирования настроек серверов NATS необходимо щелкнуть на кнопку **Серверы NATS** вверху страницы.

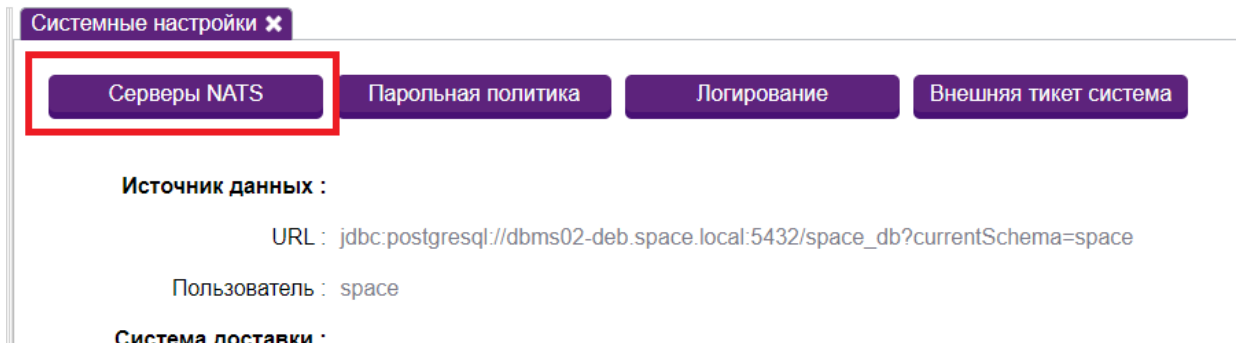


Рис. 64. Кнопка «Серверы NATS»

Откроется окно настроек серверов системы доставки сообщений. Можно сменить сервер системы доставки сообщений через выпадающий список, затем необходимо нажать на кнопку **Перезапустить**.

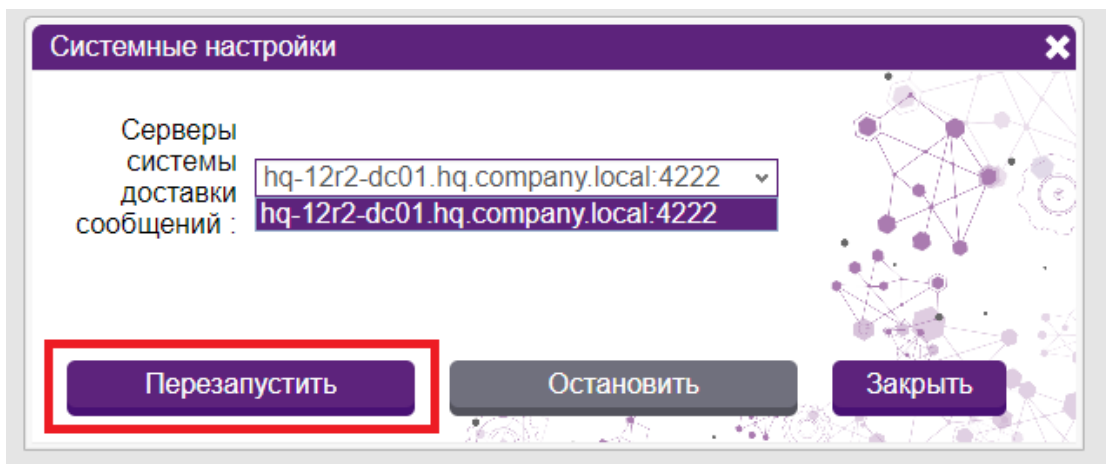


Рис. 65. Кнопка «Перезапустить»

5.10.2. Изменение настроек парольной политики

Для редактирования настроек парольной политики необходимо щелкнуть на кнопку **Парольная политика** вверху страницы.

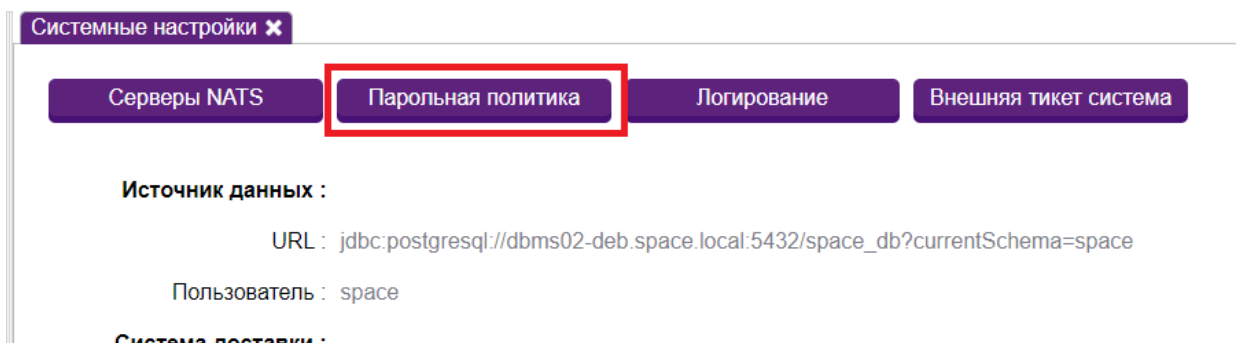


Рис. 66. Кнопка «Парольная политика»

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.

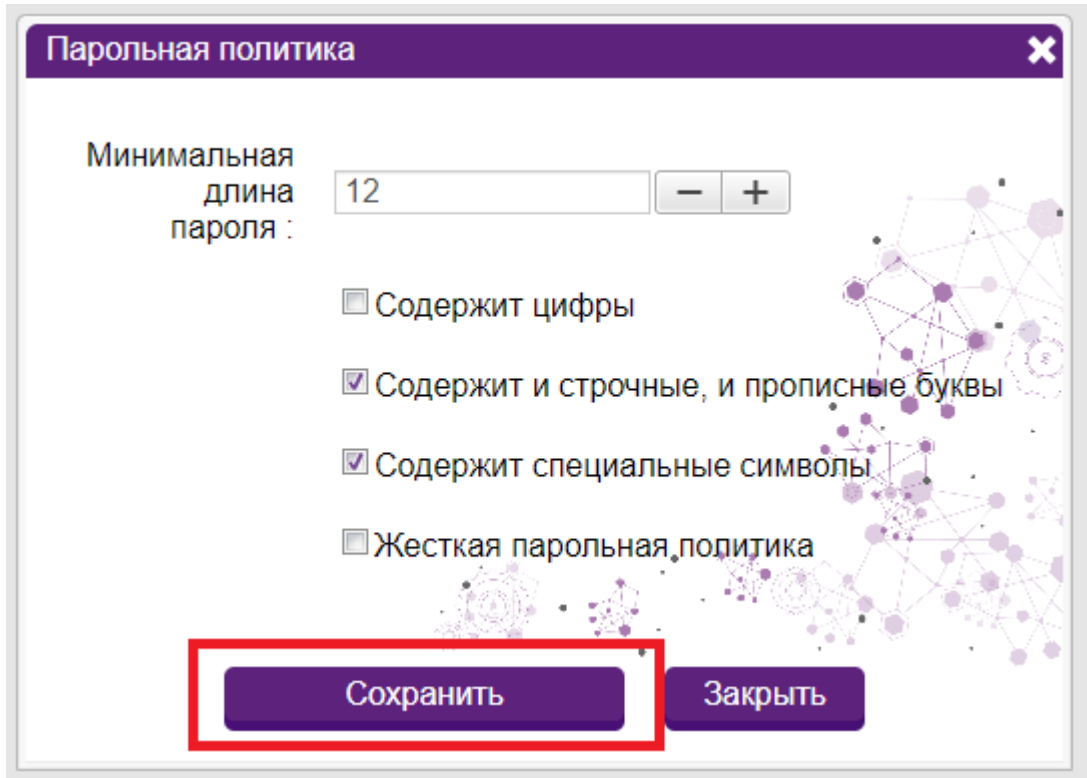


Рис. 67. Кнопка «Сохранить»

5.10.3. Изменение настроек уровня логирования

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

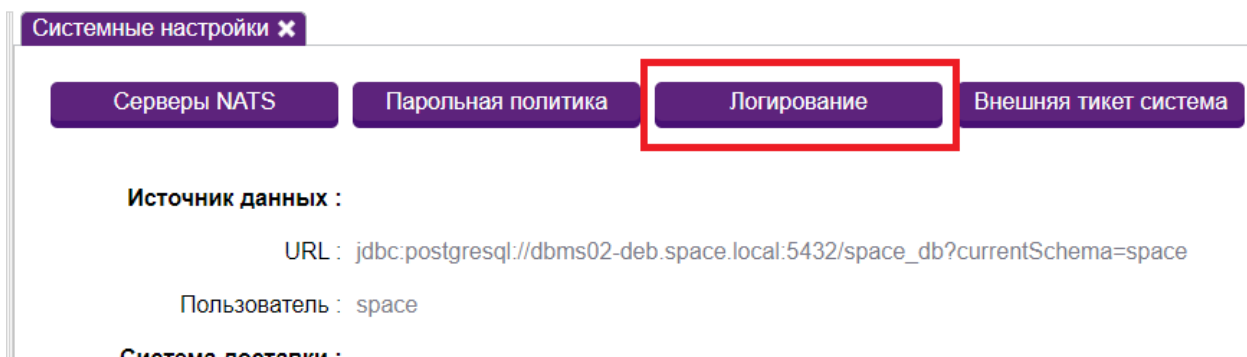


Рис. 68. Кнопка «Логирование»

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

Настройка логирования

Адрес syslog : *i*

Уровень логирования Ядра : *i*

Уровень логирования LauncherManager : *i*

Уровень логирования Launcher : *i*

Уровень логирования Watcher : *i*

Уровень логирования Агента паролей : *i*

Сохранить **Закреть**

Рис. 69. Кнопка «Сохранить»

5.10.4. Изменение настроек внешней тикет системы

Для редактирования настроек внешней тикет системы необходимо щелкнуть на кнопку **Внешняя тикет система** вверху страницы.

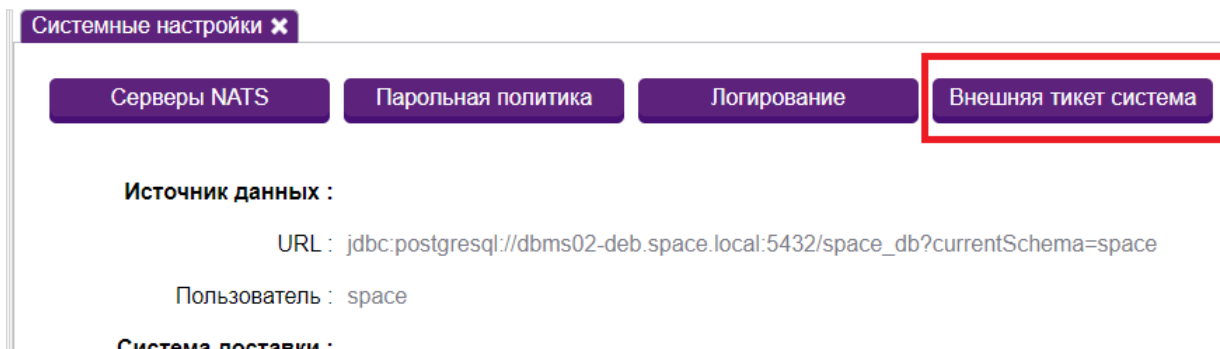


Рис. 70. Кнопка «Внешняя тикет система»

Откроется окно настройки внешней тикет системы. Данное окно позволяет ввести URL адрес для внешней тикетницы. Для этого необходимо выбрать нажать кнопку **Редактирование**.

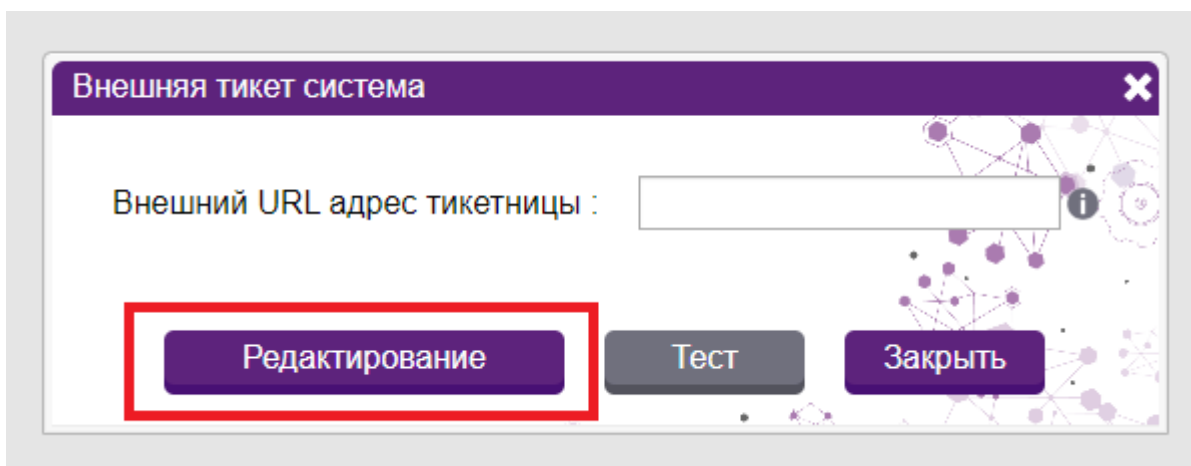


Рис. 71. Кнопка «Редактирование»

После ввода адреса внешней тикет системы (примечание: у него не должно быть символа "/" в конце адреса) требуется нажать на кнопку **Тест**.

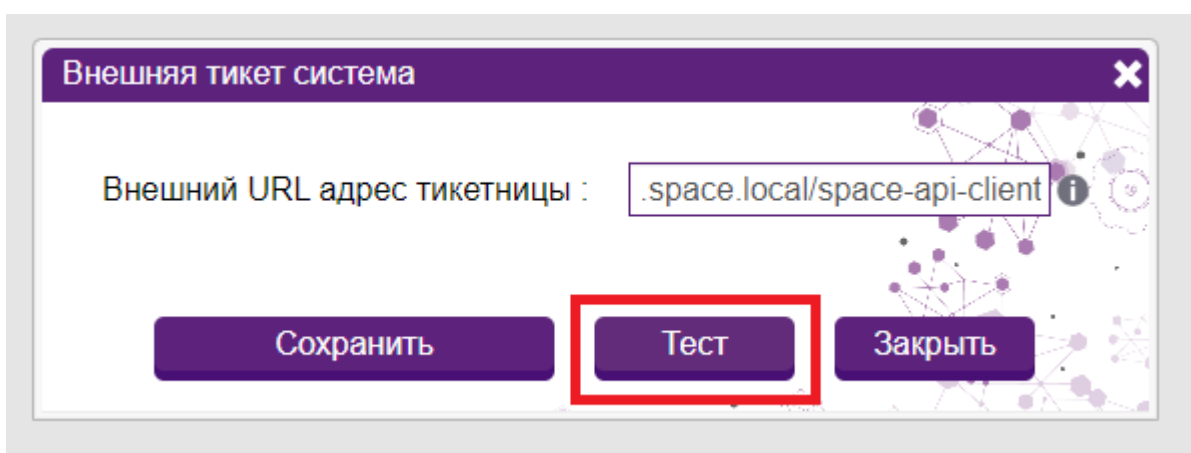


Рис. 72. Кнопка «Тест»

Если все было сделано правильно, то появится соответствующее уведомление. После того, как работоспособность внешней тикет системы подтверждена, необходимо нажать на кнопку **Сохранить**.

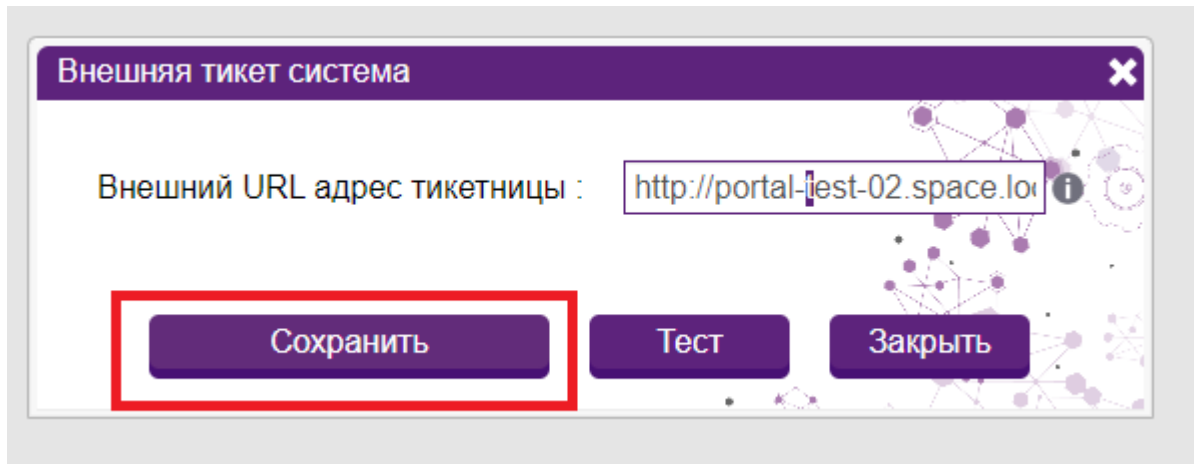


Рис. 73. Кнопка «Сохранить»

На странице настроек появится строка **Внешняя тикет система** с информацией об этой тикет системе.

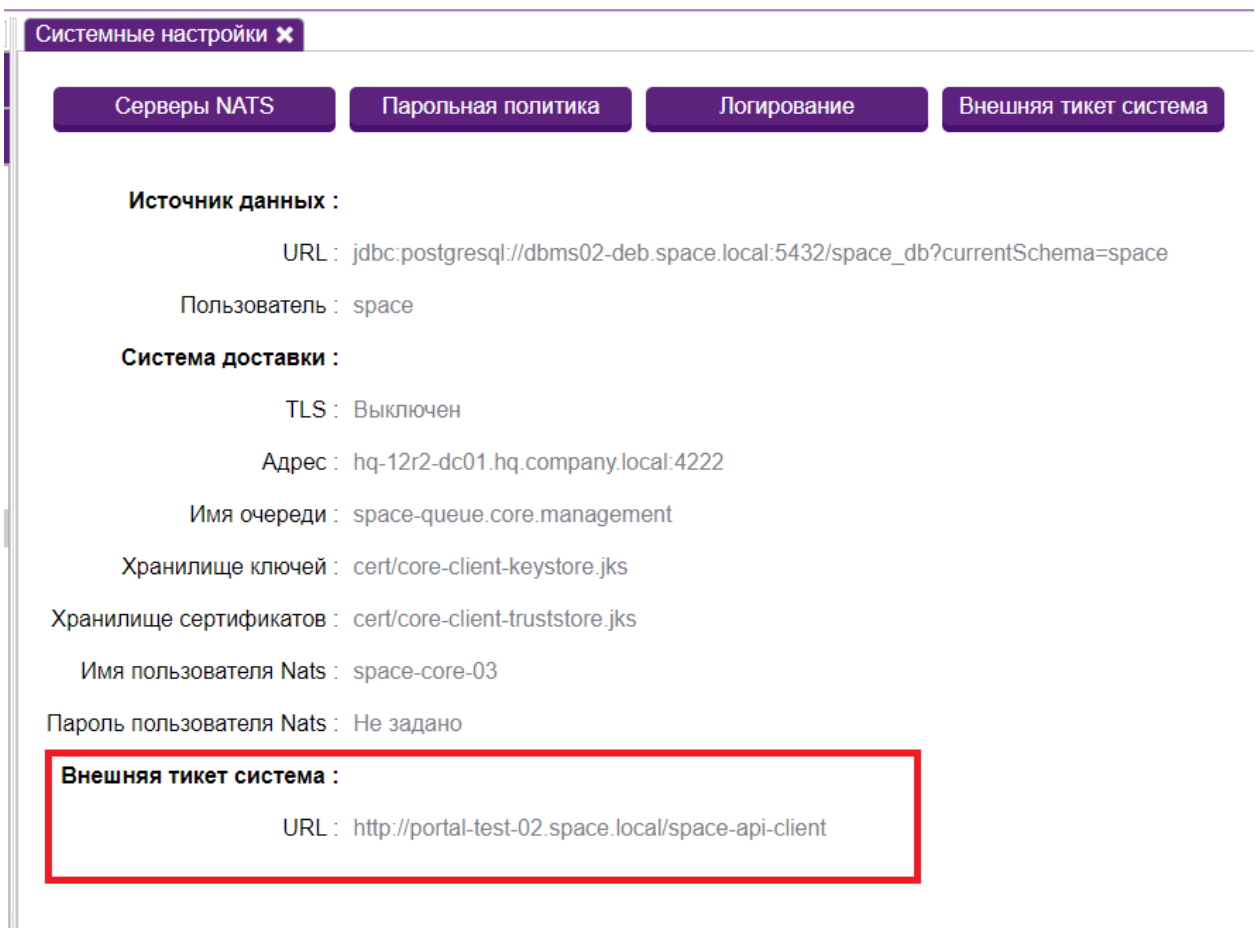


Рис. 74. Поле «Внешняя тикет система» на странице настроек

Чтобы удалить внешнюю тикет систему, нужно открыть окно ее настроек и стереть адрес системы из поля для URL. После чего нажать на кнопку **Сохранить**.

5.11. Управление провайдерами аутентификации

Вкладка **Провайдеры аутентификации** 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;
- Импорт конфигурации LDAP.

Также данная вкладка служит для отображения пользователю названий ролей AD Users and Computrs в sPACE. При необходимости пользователь может поменять их на этой вкладке.

Реализован следующий функционал:

- Просмотр названий ролей AD в sPACE;
- Изменение названий ролей AD в sPACE на необходимые.

Внешне раздел **Провайдеры аутентификации** представлен в виде двух таблиц: Домены и Названия ролей.

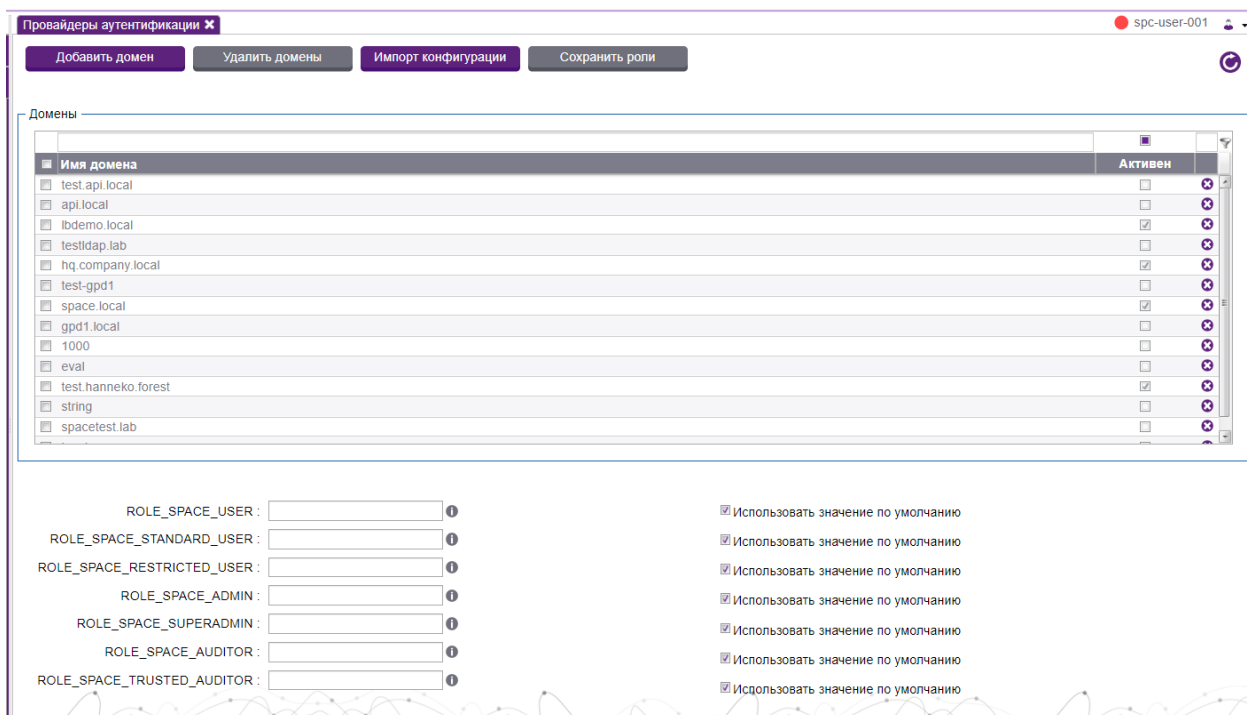


Рис. 75. Раздел «Провайдеры аутентификации»

5.11.1. Просмотр доменов Системы

Страница «Домены» представлена в виде одной таблицы.

Описание столбцов приведено ниже:

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

5.11.2. Добавление нового домена

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

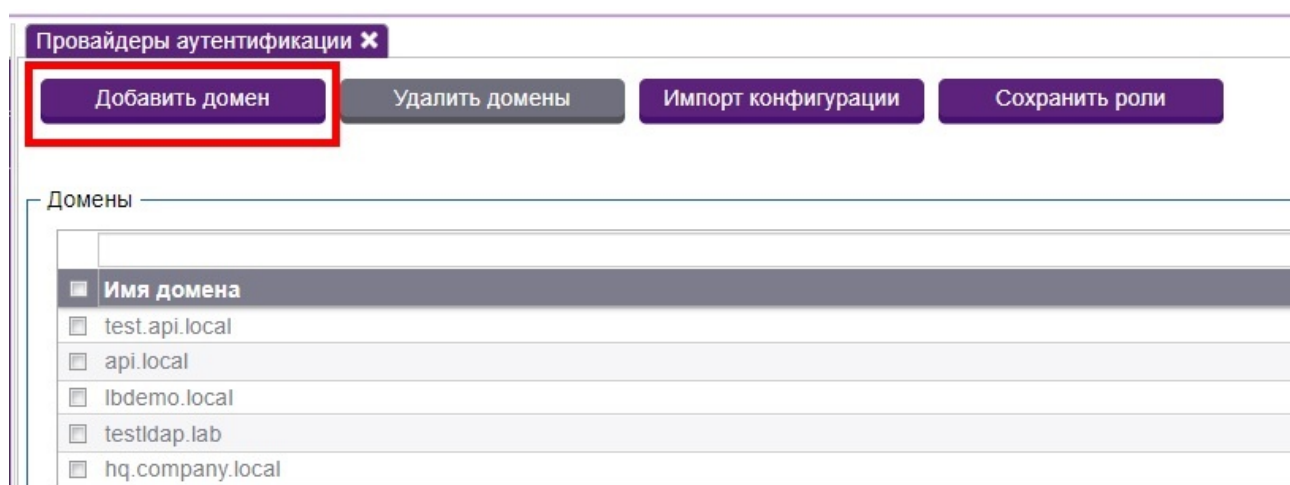


Рис. 76. Кнопка «Добавить домен»

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".

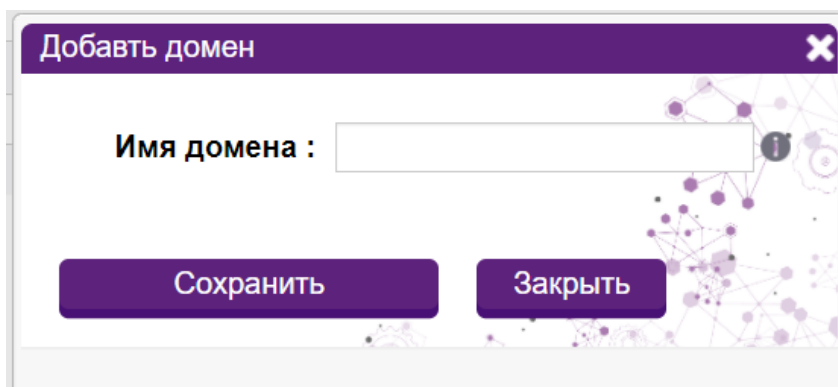
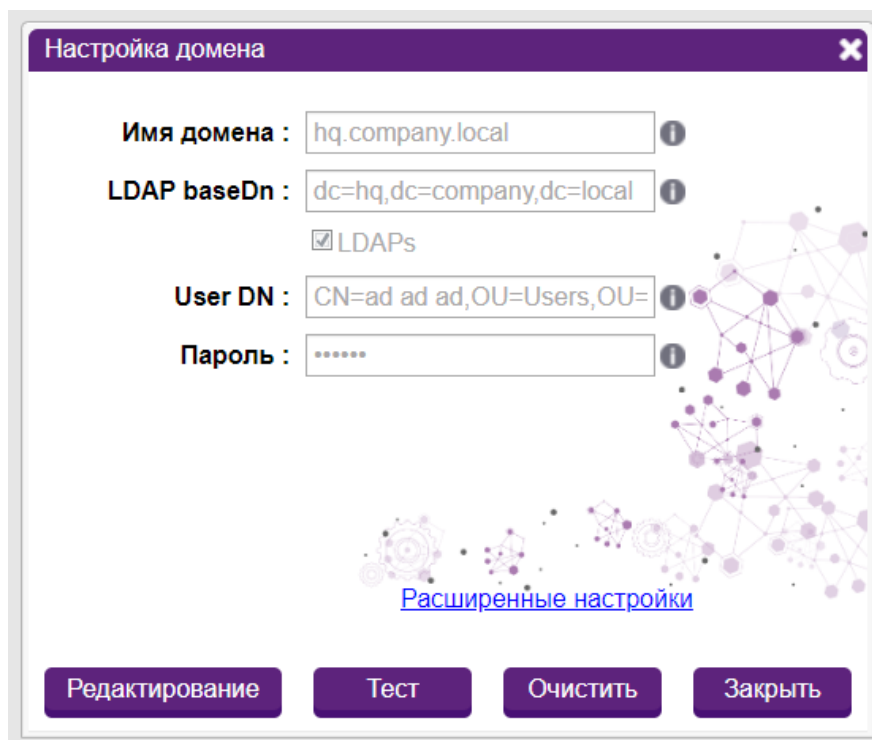


Рис. 77. Добавление домена

5.11.3. 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 при необходимости можно отредактировать расширенные настройки домена, для этого требуется нажать на соответствующую кнопку "Расширенные настройки".



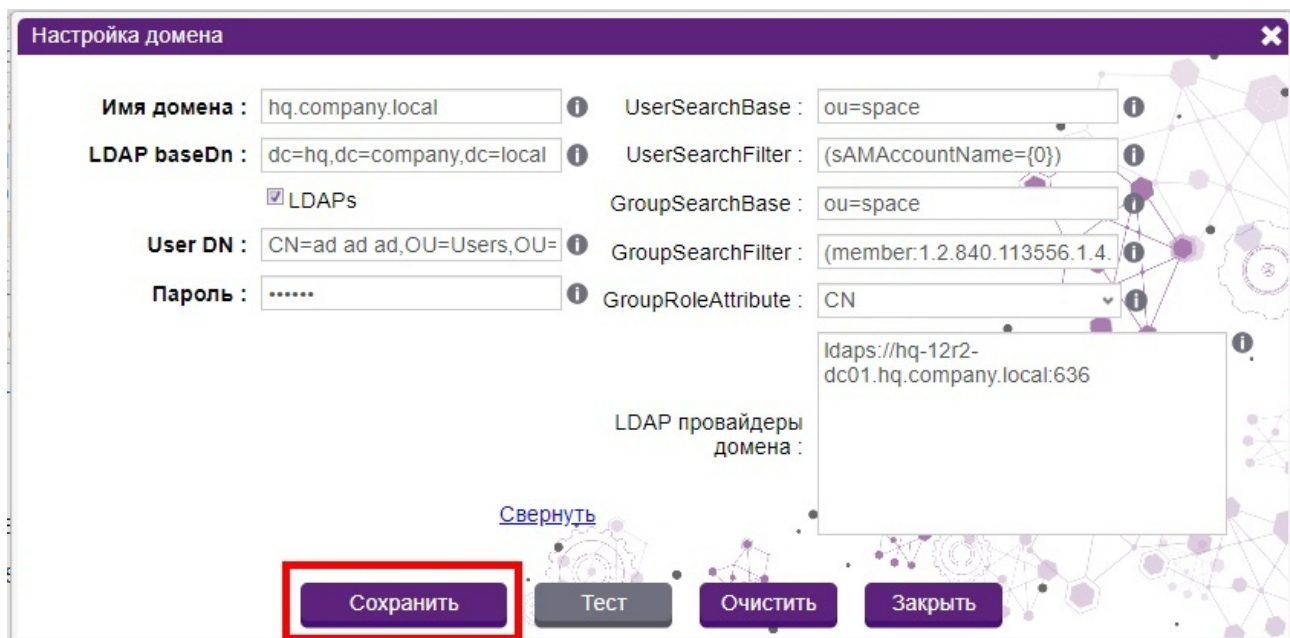



Рис. 78. Окно редактирования домена и окно расширенных настроек

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

5.11.4. Обновление таблицы доменов

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

5.11.5. Удаление строки в таблице доменов

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

5.11.6. 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.

5.11.7. Импорт конфигурации LDAP

Для импорта конфигурации LDAP необходимо нажать на соответствующую кнопку над таблицей компонентов.

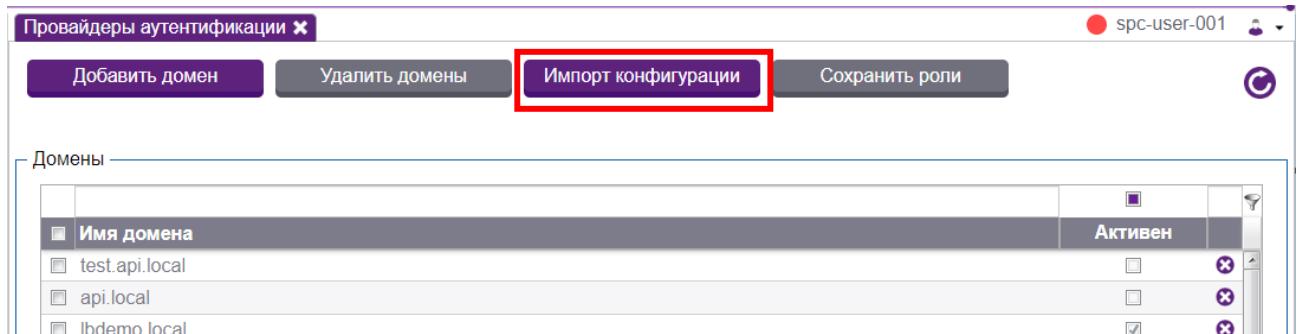
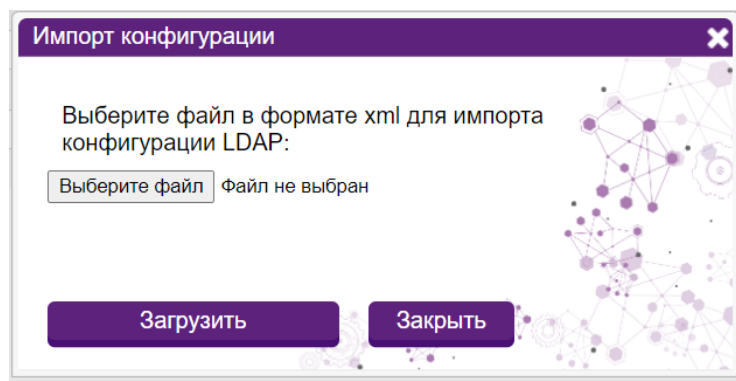


Рис. 79. Расположение кнопки «Импорт конфигурации»

Затем требуется выбрать нужный файл в формате xml на компьютере и нажать на кнопку **Загрузить**.




```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!--suppress XmlUnboundNsPrefix, CheckTagEmptyBody -->
<configurations>
  <domain name="lbdemo.local">
    <providers>
      <url>ldaps://erpm-test-dc.lbdemo.local:389/</url>
    </providers>
    <baseDn>dc=lbdemo,dc=local</baseDn>
    <userSearchBase>ou=space</userSearchBase>
    <userSearchFilter>(sAMAccountName={0})</userSearchFilter>
    <searchSubtree>true</searchSubtree>
    <anonymousReadOnly>false</anonymousReadOnly>
    <principal>CN=ad-search-user,OU=users,OU=space,DC=lbdemo,DC=local</principal>
    <credentials><![CDATA[Zaq12wsx]]></credentials>
    <convertToUpperCase>true</convertToUpperCase>
    <defaultRole>AUTHENTICATED_USER</defaultRole>
    <groupRoleAttribute>cn</groupRoleAttribute>
    <groupSearchBase>OU=space</groupSearchBase>
    <groupSearchFilter>(member:1.2.840.113556.1.4.1941:={0})</groupSearchFilter>
    <groupSearchSubtree>true</groupSearchSubtree>
    <referral>follow</referral>
    <rolePrefix></rolePrefix>
  </domain>

  <domain name="space.local">
    <providers>
      <url>ldaps://dc01-12r2.space.local:636/</url>
    </providers>
    <baseDn>dc=space,dc=local</baseDn>
    <userSearchBase>ou=space</userSearchBase>
    <userSearchFilter>(sAMAccountName={0})</userSearchFilter>
    <searchSubtree>true</searchSubtree>
    <anonymousReadOnly>false</anonymousReadOnly>
    <principal>CN=ad-search-user,OU=users,OU=SPACE,DC=SPACE,DC=LOCAL</principal>
    <credentials><![CDATA[Zaq12wsx]]></credentials>
    <convertToUpperCase>true</convertToUpperCase>
    <defaultRole>AUTHENTICATED_USER</defaultRole>
    <groupRoleAttribute>cn</groupRoleAttribute>
    <groupSearchBase>OU=space</groupSearchBase>
    <groupSearchFilter>(member:1.2.840.113556.1.4.1941:={0})</groupSearchFilter>
    <groupSearchSubtree>true</groupSearchSubtree>
    <referral>follow</referral>
    <rolePrefix></rolePrefix>
  </domain>

  <domain name="hq.company.local">
    <providers>
      <url>ldaps://hq-12r2-dc01.hq.company.local:636/</url>
    </providers>
    <baseDn>dc=hq,dc=company,dc=local</baseDn>
    <userSearchBase>ou=space</userSearchBase>
    <userSearchFilter>(sAMAccountName={0})</userSearchFilter>
    <searchSubtree>true</searchSubtree>
    <anonymousReadOnly>false</anonymousReadOnly>
    <principal>CN=ad-search-user,OU=Users,OU=SPACE,DC=HQ,DC=COMPANY,DC=LOCAL</principal>
    <credentials><![CDATA[Zaq12wsx]]></credentials>
    <convertToUpperCase>true</convertToUpperCase>
    <defaultRole>AUTHENTICATED_USER</defaultRole>
    <groupRoleAttribute>cn</groupRoleAttribute>
    <groupSearchBase>OU=space</groupSearchBase>
    <groupSearchFilter>(member:1.2.840.113556.1.4.1941:={0})</groupSearchFilter>
    <groupSearchSubtree>true</groupSearchSubtree>
    <referral>follow</referral>
    <rolePrefix></rolePrefix>
  </domain>
</configurations>

```

Рис. 80. Окно импорта конфигурации и пример такой конфигурации

5.11.8. Изменение названия ролей

Перед тем, как изменить название 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 нём необходимо ввести название, а затем нажать на кнопку **Сохранить роли** вверху вкладки. Требуется удостовериться, что вы создали роль с этим новым названием в AD и задали её пользователям.

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.

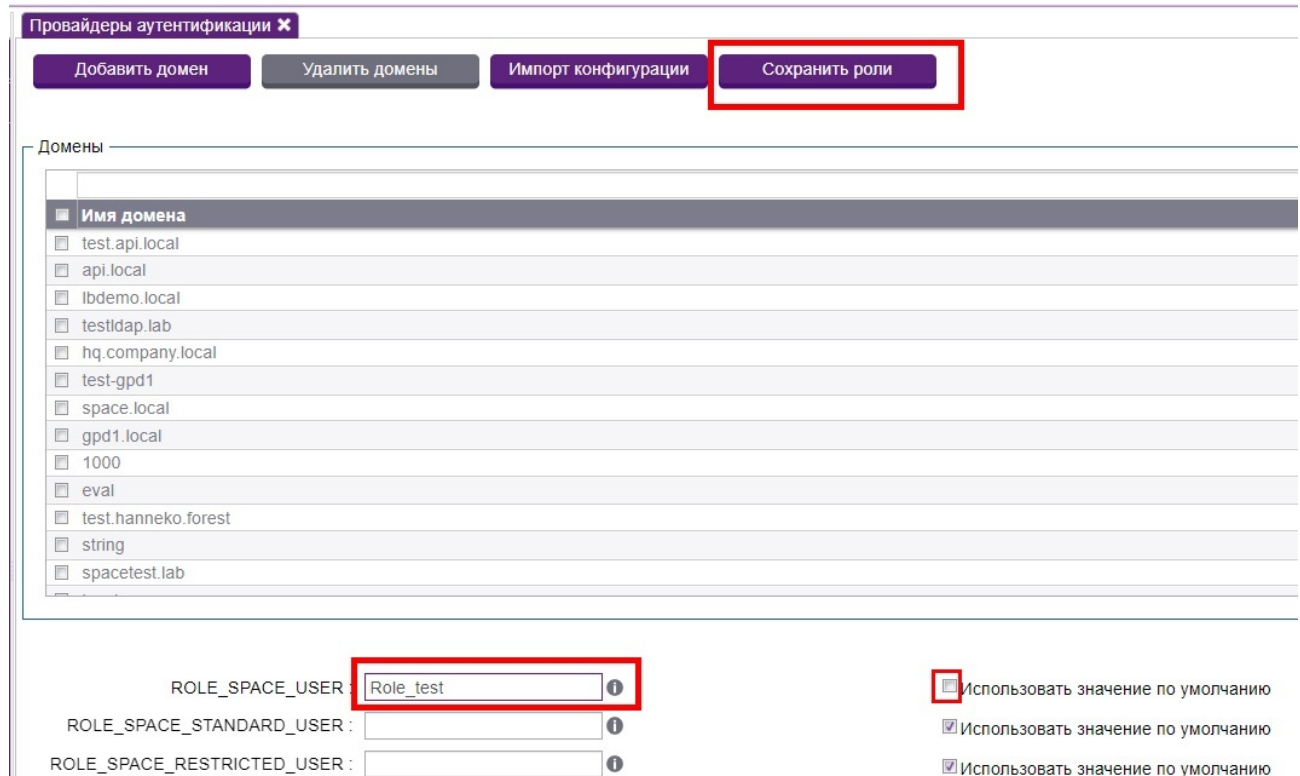


Рис. 81. Расположение кнопки «Сохранить роли»

5.12. Управление пользовательскими ролями

Вкладка **Пользовательские роли** раздела **Управление системой** позволяет настроить пользовательские роли на портале sPACE. Возможности этих ролей задает администратор на портале. Предварительно каждая роль должна быть создана в Active Directory Users and Computers и задана нужным пользователям.

В данном разделе администратор может осуществлять:

- Просмотр пользовательских ролей;
- Добавление пользовательских ролей;
- Редактирование пользовательских ролей;

- Обновление таблицы пользовательских полей;
- Единовременное удаление нескольких записей из таблицы пользовательских ролей.

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

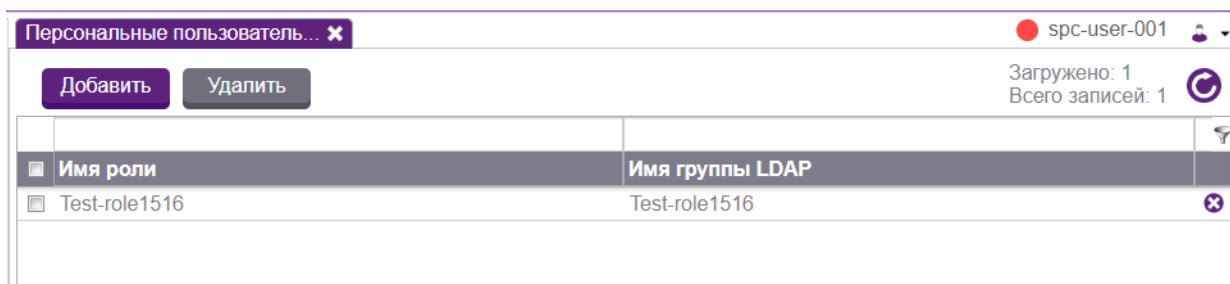


Рис. 82. Раздел «Пользовательские роли»

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.

5.12.1. Добавление новой пользовательской роли

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

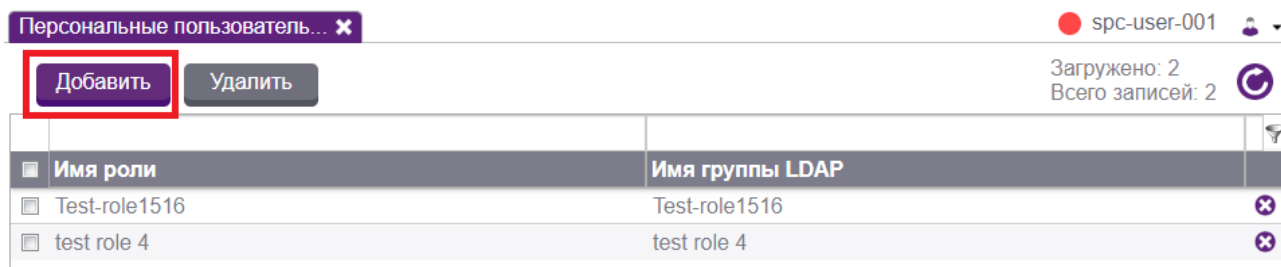


Рис. 83. Кнопка «Добавить» роль

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".

Добавление пользовательской роли

Имя роли в sPace : *i* Имя группы LDAP : *i*

Набор привилегий

- Запуск сеансов администрирования. Запрашивание наряда-допуска как для себя, так и для других. Согласование доверенных нарядов-допусков.
- Запуск сеансов администрирования. Запрашивание наряда-допуска для себя.
- Запуск сеансов администрирования.
- Настройка системы, добавление объектов. Согласование доверенных нарядов-допусков.
- Перевод системы в аварийный режим.
- Аудит действий пользователей.
- Аудит действий пользователей, включая данные key-log и clipboard.

Сохранить Закрыть

Рис. 84. Добавление роли

5.12.2. 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.

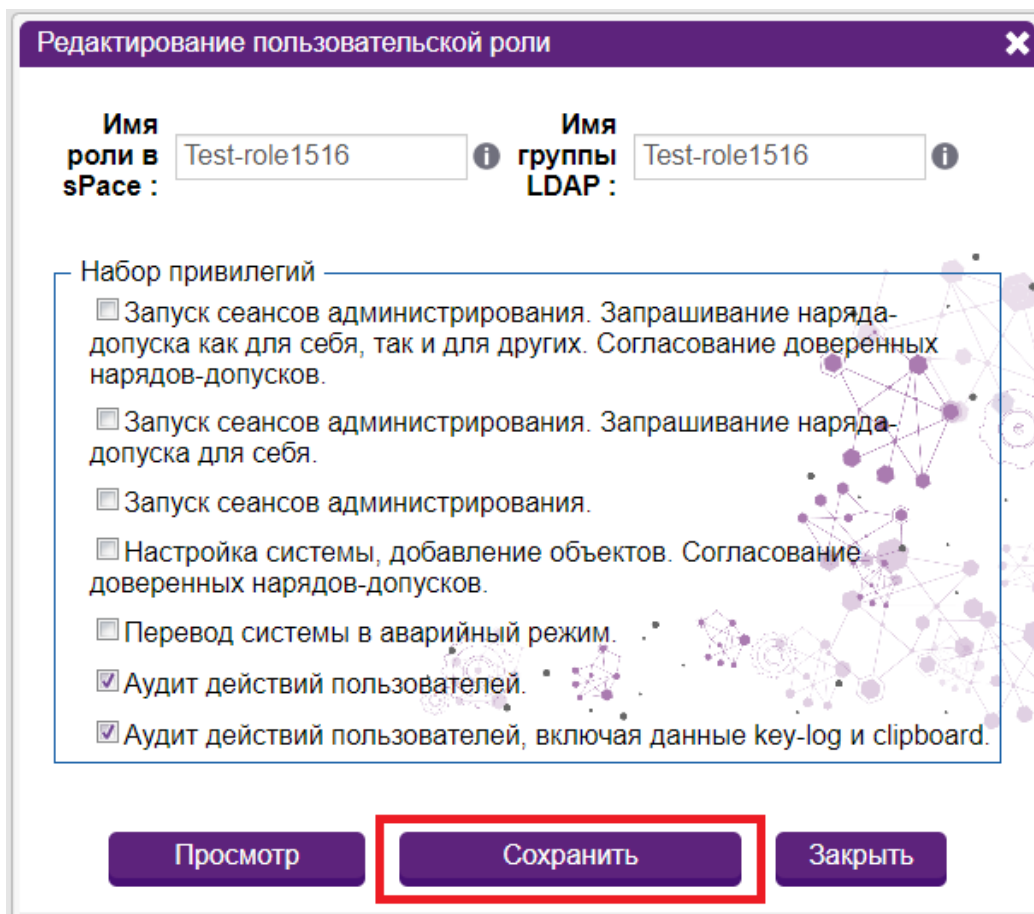



Рис. 85. Окно редактирования домена и окно расширенных настроек

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

5.12.3. Обновление таблицы пользовательских ролей

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

5.12.4. Удаление строки в таблице пользовательских ролей

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

5.12.5. Удаление нескольких записей из таблицы 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.

5.13. 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;
- Единовременное добавление внешних ID для нескольких записей.

5.13.1. Просмотр агентов паролей

Страница «Агенты паролей» представлена в виде двух таблиц: **Агенты** и **Типы агентов**.

The screenshot shows a web interface for managing password agents. At the top, there's a header 'Агенты паролей' with a close button. Below it, a sub-header 'Агенты' contains three buttons: 'Добавить', 'Удалить', and 'Задать Внешний ID'. On the right, it says 'Загружено: 14' and 'Всего записей: 14' with a refresh icon. The main table has columns for 'Наименование', 'Тип', and 'Адрес'. Below it is a section for 'Типы Агентов' with a refresh icon. The table below has columns for 'Наименование', 'Описание', and 'Исполняемый файл'.

Наименование	Тип	Адрес
<input type="checkbox"/> oracle_dbms02_test	СУБД Oracle	dbms02-deb.space.local
<input type="checkbox"/> windows_hq_domain	Microsoft Windows	hq.company.local
<input type="checkbox"/> linux_test1	Linux	192.168.60.141
<input type="checkbox"/> windows_hq-12r2-js01-test	Microsoft Windows	
<input type="checkbox"/> linux_test2	Linux	dbms02-deb.space.local
<input type="checkbox"/> linux_test3	Linux	dbms02-deb.space.local
<input type="checkbox"/> postgres_dbms02_test	СУБД PostgreSQL	dbms02-deb.space.local

Наименование	Описание	Исполняемый файл
Microsoft Windows		.exe
Linux		.sh
СУБД PostgreSQL		psql
СУБД Oracle		sql
СУБД MicrosoftSQL		sql

Рис. 86. 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.

5.13.2. Добавление агента паролей

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

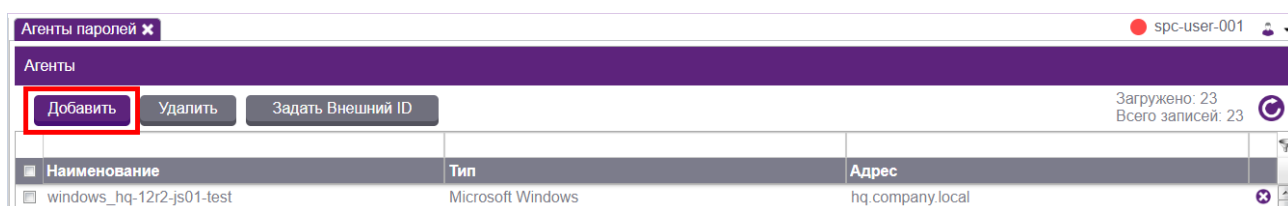


Рис. 87. Кнопка «Добавить» агент паролей

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

Агент рандомизации

Наименование : ⓘ

Сервера ЗС : ⓘ

Тип Агента : ⓘ

Внешний ID : ⓘ

Параметры подключения

Рис. 88. Добавление агента паролей

Список полей формы **Агент рандомизации**:

- Наименование (обязательное поле) – имя создаваемого агента паролей;
- Сервера ЗС (обязательное поле) – сервера ЗС, на котором расположен данный агент;
- Тип Агента (обязательное поле) – тип создаваемого агента рандомизации;
- Внешний ID – внешний ID данного агента.

5.13.3. 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.

Редактирование агента рандомизации

Наименование : linux_test_gpd

Сервера ЗС : test-server-0004

Создан : 07.09.2019 11:51:58

Тип Агента : Linux

Внешний ID :

Изменен : 12.11.2019 19:24:46

Параметры подключения

Адрес : dbms02-deb.space.local

Порт : 22

Учетная запись : ssh_test_root

Учетная запись для логина : ssh_test_conn

Просмотр Сохранить Закрыть

Рис. 89. Окно редактирования агента паролей

Список полей формы "Редактирование агента рандомизации":

- Наименование (обязательное поле) – имя создаваемого агента паролей;
- Сервера ЗС (обязательное поле) – сервера ЗС, на которых расположен данный агент;
- Тип Агента (обязательное поле) – тип создаваемого агента рандомизации;
- Внешний ID – внешний ID данного агента.

Параметры подключения:

- Адрес – адрес, на который производится подключения агента;

- Порт – порт, на который проводится подключение агента;
- Учетная запись – УЗ, под которой проводится подключение агента;
- Учетная запись для логина – УЗ для логина на подключаемую машину.

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

5.13.4. Обновление таблицы агентов и типов агентов

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

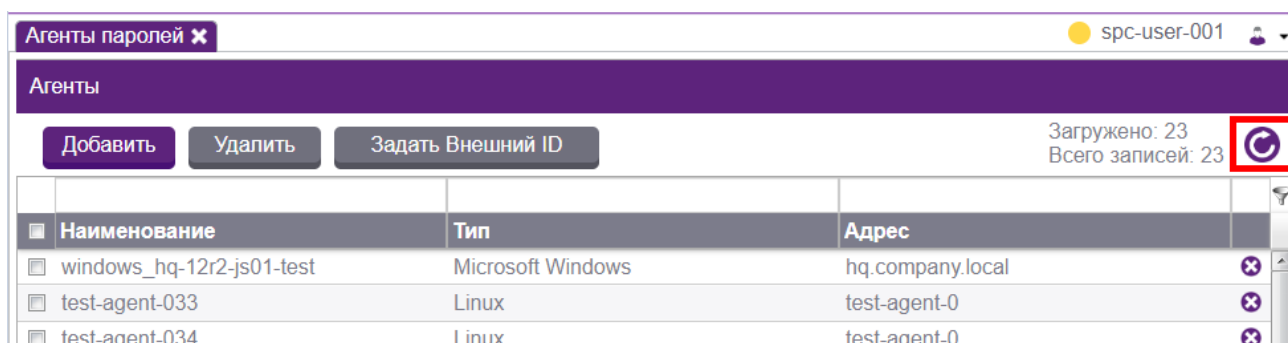


Рис. 90. Расположение кнопки «Обновить»

5.13.5. Удаление строки в таблице агентов

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

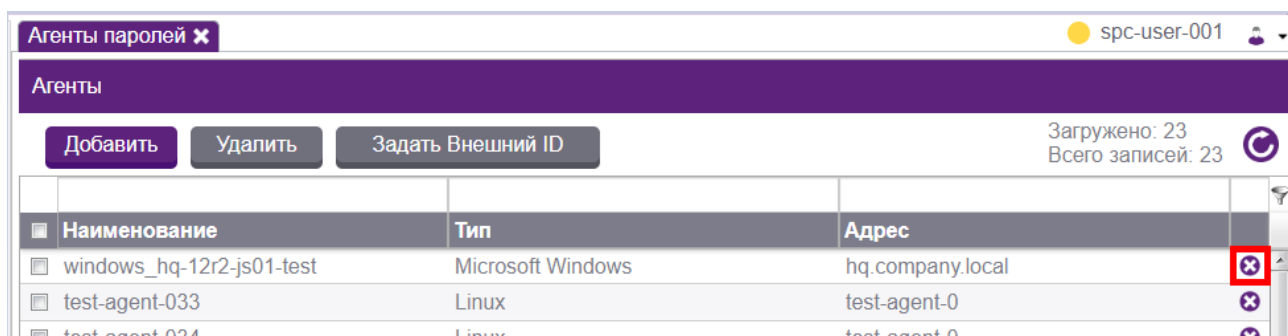


Рис. 91. Расположение кнопки «Удалить»

5.13.6. Единовременное удаление нескольких записей из таблицы агентов

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

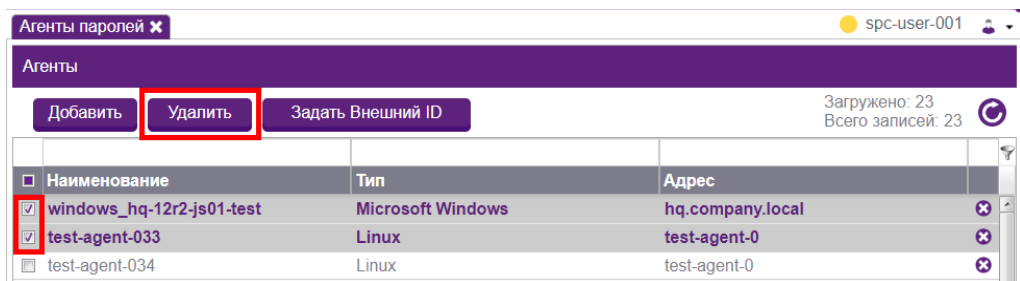


Рис. 92. Удаление двух агентов паролей

5.13.7. Единовременное добавление внешних ID для нескольких записей

Для единовременного добавления внешних ID для нескольких записей сначала следует выделить желаемые записи в таблице галочкой слева, после чего станет активной кнопка **Задать внешний ID**, расположенная сверху над таблицей.

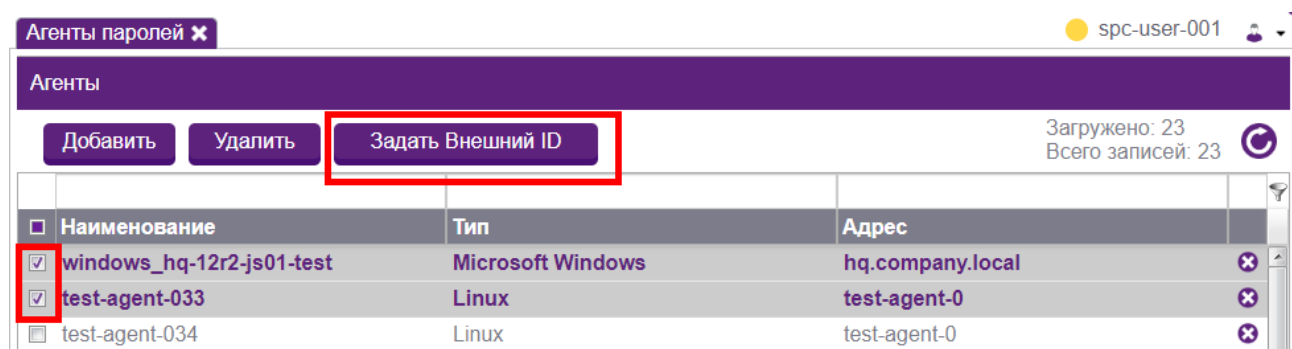


Рис. 93. Задание внешнего ID для двух агентов паролей

5.14. 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 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.

5.14.1. Просмотр параметров внутренней системы видеонаблюдения сеансов

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

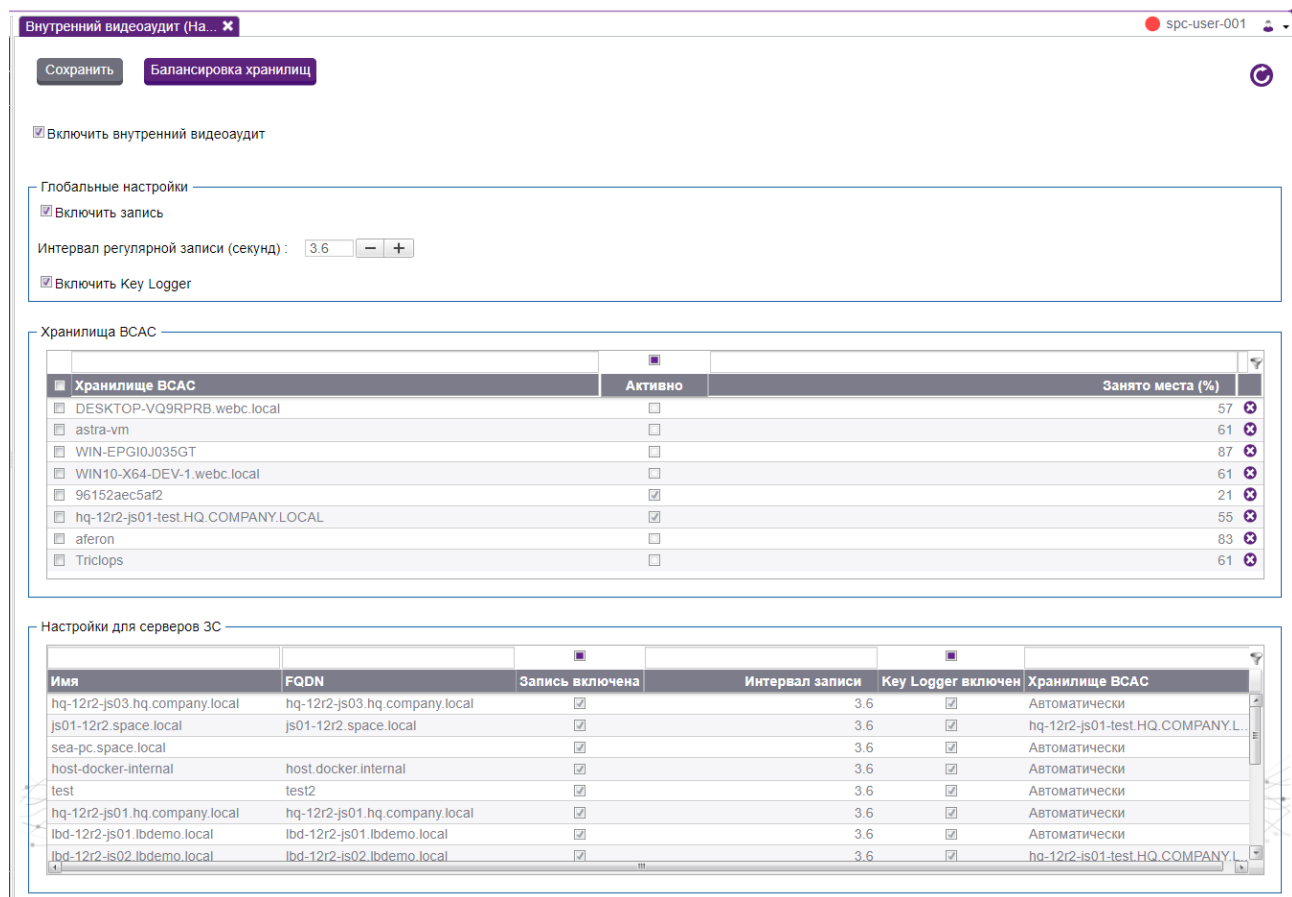


Рис. 94. Страница «Внутренний видеонаблюдение»

Описание параметров внутренней системы видеонаблюдения:

- Включить внутренний аудит – когда этот параметр включен, внутренняя система видеонаблюдения 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.

5.14.2. Обновление страницы внутреннего видеоаудита

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

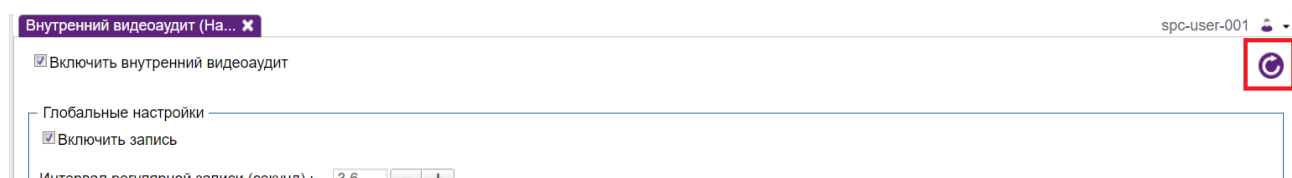


Рис. 95. Расположение кнопки «Обновить»

5.14.3. 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**.

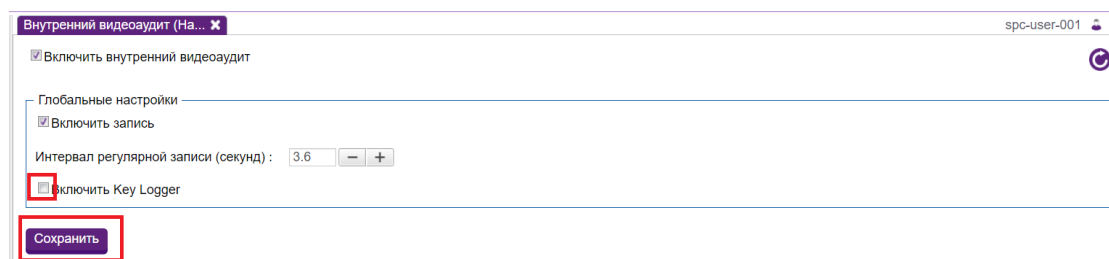


Рис. 96. Включение функции Key Logger и кнопка «Сохранить»

5.14.4. Удаление строки в таблице хранилищ ВСАС

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

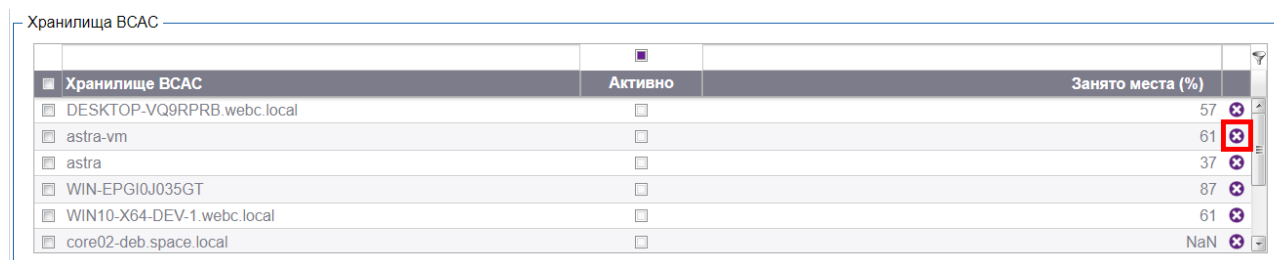
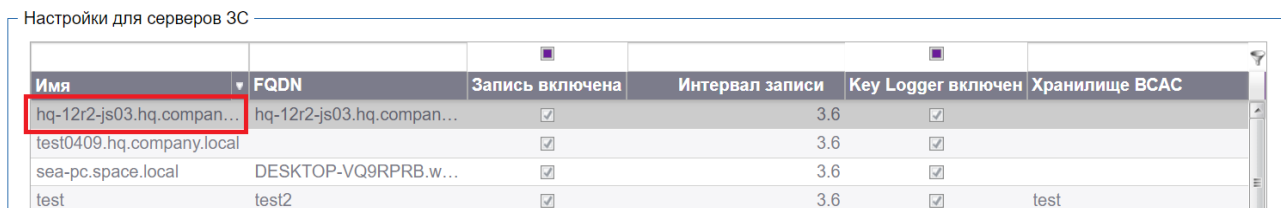


Рис. 97. Расположение кнопки «Удалить»

5.14.5. 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**:



Имя	FQDN	Запись включена	Интервал записи	Key Logger включен	Хранилище ВСАС
hq-12r2-js03.hq.compan...	hq-12r2-js03.hq.compan...	<input checked="" type="checkbox"/>	3.6	<input checked="" type="checkbox"/>	
test0409.hq.company.local		<input checked="" type="checkbox"/>	3.6	<input checked="" type="checkbox"/>	
sea-pc.space.local	DESKTOP-VQ9RPRB.w...	<input checked="" type="checkbox"/>	3.6	<input checked="" type="checkbox"/>	
test	test2	<input checked="" type="checkbox"/>	3.6	<input checked="" type="checkbox"/>	test

Рис. 98. 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.

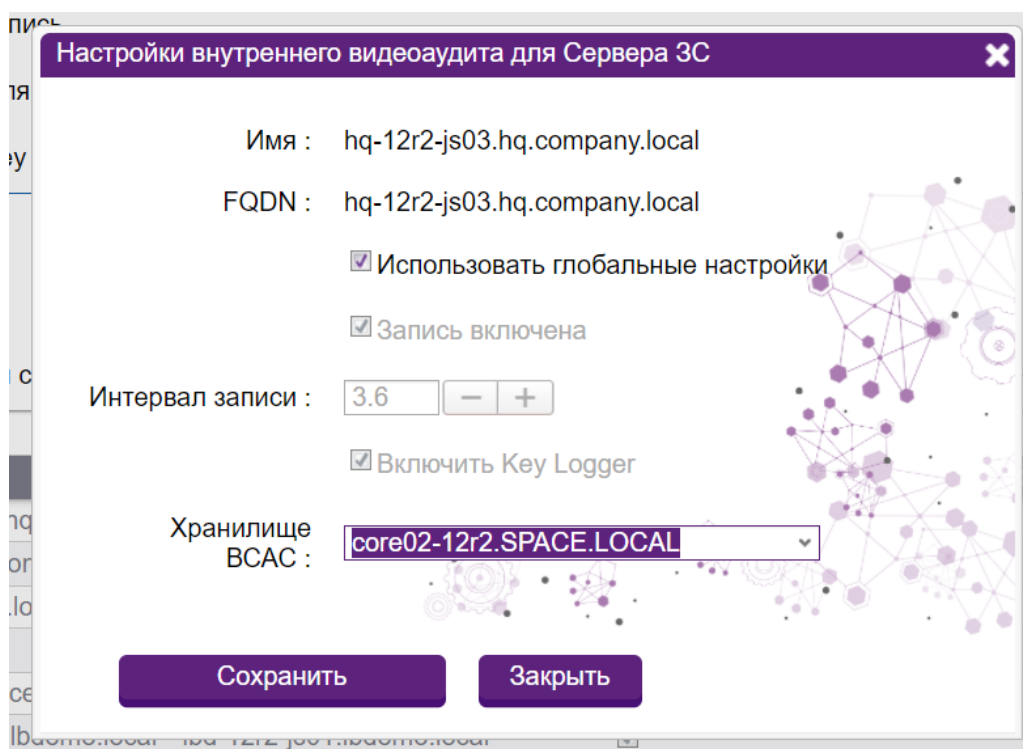


Рис. 99. Окно настройки внутреннего видеоаудита для сервера ЗС

5.14.6. Выбор стратегии балансировки хранилищ ВСАС

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

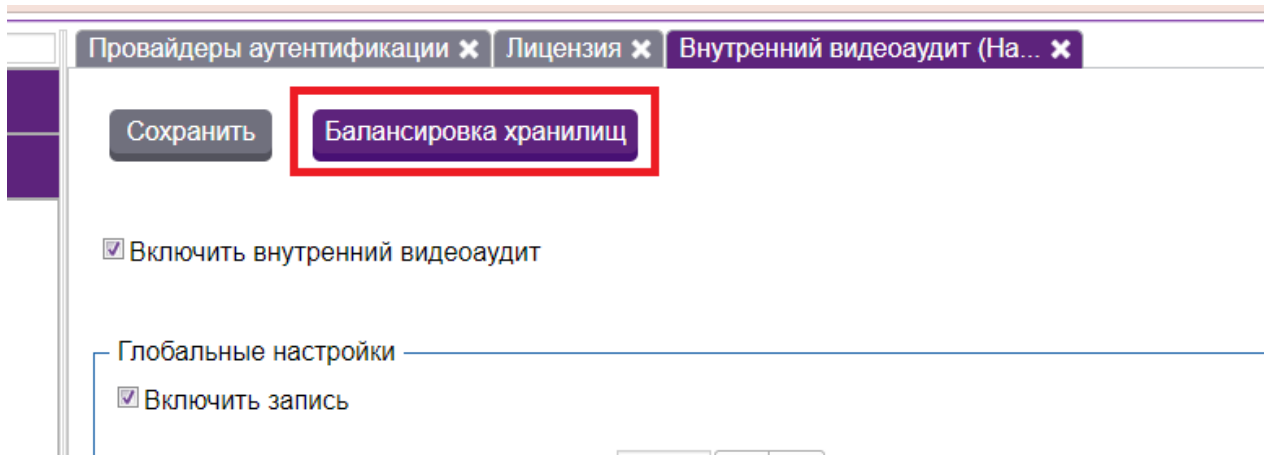


Рис. 100. Кнопка «Балансировка хранилищ»

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

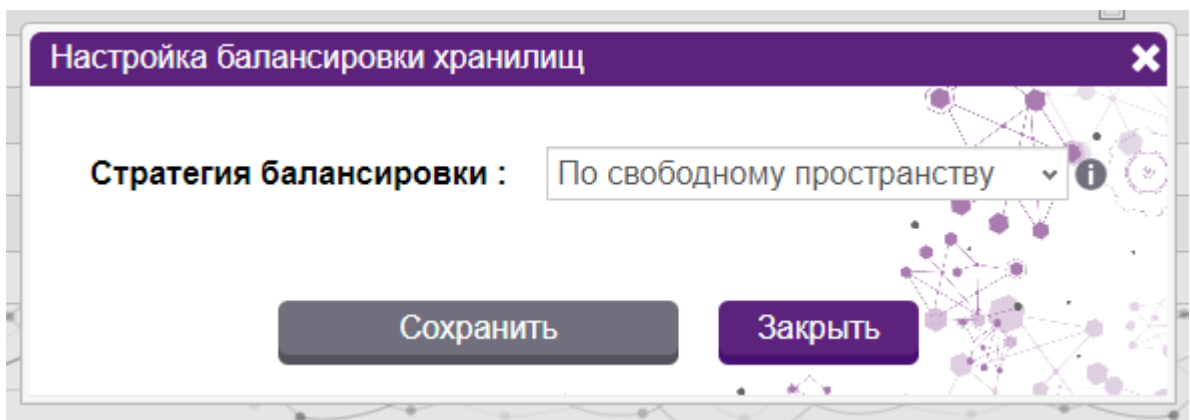


Рис. 101. Настройка балансировки хранилищ

5.15. Управление фильтрацией ввода

Данная страница позволяет настроить модели данных для фильтрации, которую будет осуществлять внутренняя система видеоаудита (ВСАС).

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 нескольких записей из таблицы списков фильтрации ввода.

5.15.1. Добавление фильтрации ввода

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

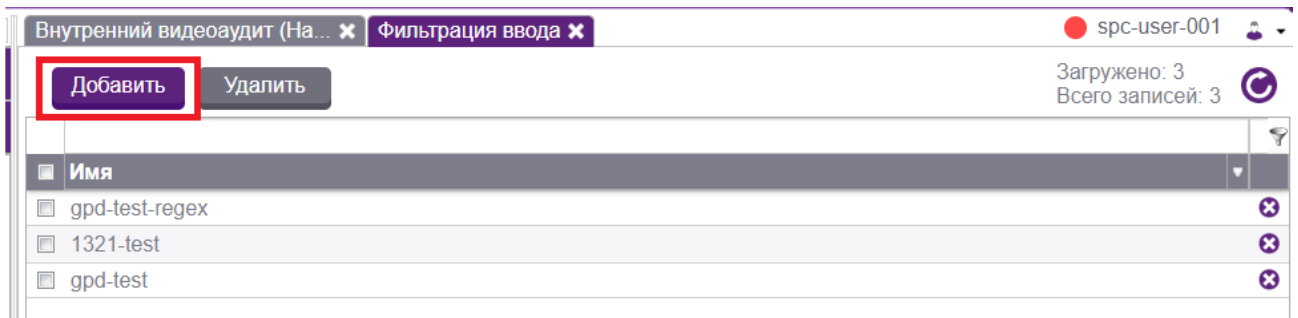


Рис. 102. Кнопка «Добавить»

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

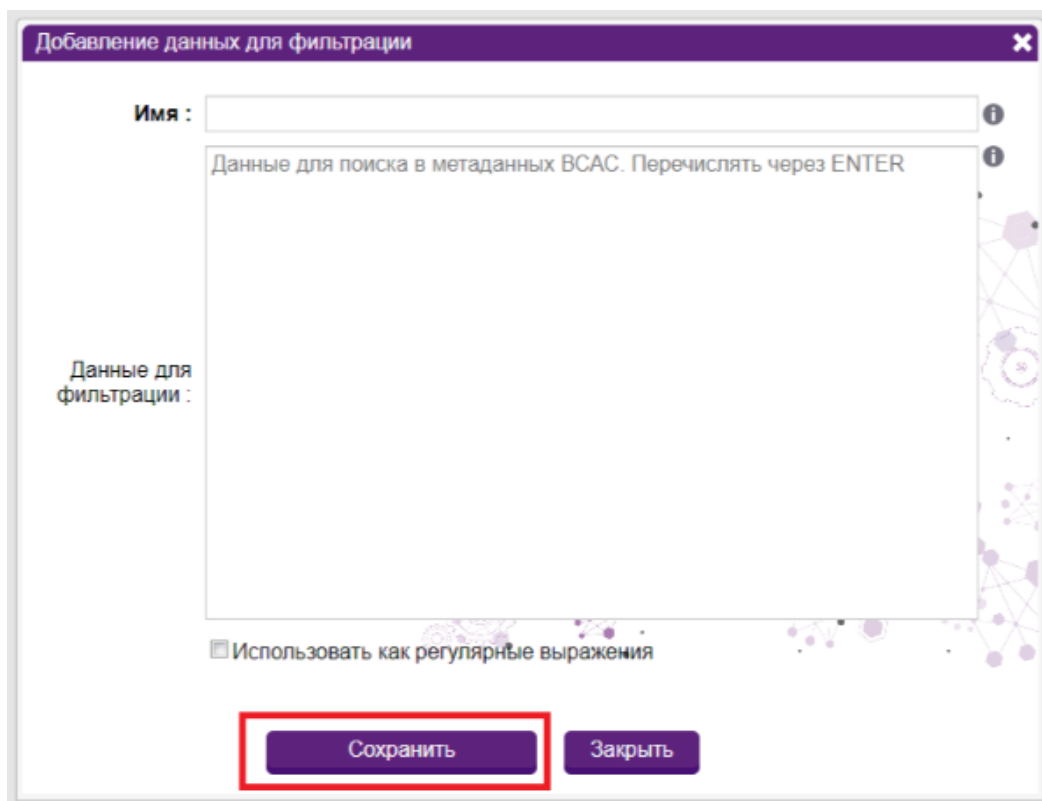


Рис. 103. Добавление данных для фильтрации

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".

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

5.15.2. 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.

Редактирование данных для фильтрации

Имя : 1321-test

Данные для фильтрации :

abcde
0909

Использовать как регулярные выражения

Просмотр Сохранить Закреть

Рис. 104. Окно редактирования данных для фильтрации

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".

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

5.15.3. Обновление страницы фильтрации ввода

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

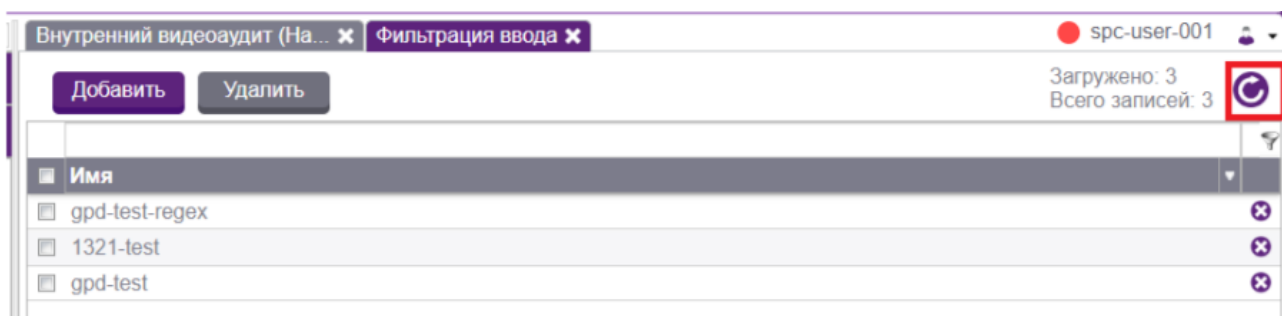


Рис. 105. Кнопка «Обновить»

5.15.4. 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.

5.15.5. 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.

5.16. 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.

5.16.1. Просмотр лицензии

Страница лицензии выглядит следующим образом:

Лицензия ✕

Запрос на лицензию Загрузка лицензии

Версия продукта : 1.3.0

Количество Серверов ЗС : 11 (Не ограничено)

Количество активных пользователей : 0 (Не ограничено)

Доступные Ядра системы : (Не ограничено)

Количество активных Ядер системы : 3 (Не ограничено)

Количество активных Хранилищ ВСАС : 2 (Не ограничено)

Всего активных сеансов : 0 (Не ограничено)

Всего активных системных сеансов : 0 (Не ограничено)

Всего активных соединений : 0 (Не ограничено)

Дата окончания действия лицензии : 31.12.2023

Серверы ЗС :

- aferon : Активных сеансов 0 (Не ограничено); активных соединений 0 (Не ограничено)
- igor-astra : Активных сеансов 0 (Не ограничено); активных соединений 0 (Не ограничено)
- host-docker-internal : Активных сеансов 0 (Не ограничено); активных соединений 0 (Не ограничено)
- hq-12r2-js03-test.hq.company.local : Активных сеансов 0 (Не ограничено); активных соединений 0 (Не ограничено)
- Node 1 : Активных сеансов 0 (Не ограничено); активных соединений 0 (Не ограничено)
- Node for Jump Server 1 : Активных сеансов 0 (Не ограничено); активных соединений 0 (Не ограничено)
- test-domain-2216-1 : Активных сеансов 0 (Не ограничено); активных соединений 0 (Не ограничено)
- hq-12r2-js02-test.hq.company.local : Активных сеансов 0 (Не ограничено); активных соединений 0 (Не ограничено)
- igor-win-new : Активных сеансов 0 (Не ограничено); активных соединений 0 (Не ограничено)
- Hanneko WS2019 : Активных сеансов 0 (Не ограничено); активных соединений 0 (Не ограничено)
- hq-12r2-js01-test.hq.company.local : Активных сеансов 0 (Не ограничено); активных соединений 0 (Не ограничено)

Рис. 106. Страница «Лицензия»

Описание параметров:

- Версия продукта – номер версии sPACE;
- 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 Ядра 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 системы – 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 системы, работающие в данный момент, и их максимально разрешённое значение;
- Всего активных соединений – все соединения системы, работающие в данный момент, и их максимально разрешённое значение;
- Дата окончания лицензии – дата, до которой действует данная лицензия (включительно);
- Серверы ЗС – перечень всех активных серверов ЗС и количество сеансов и соединений на них, активных в данный момент.

5.16.2. 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.

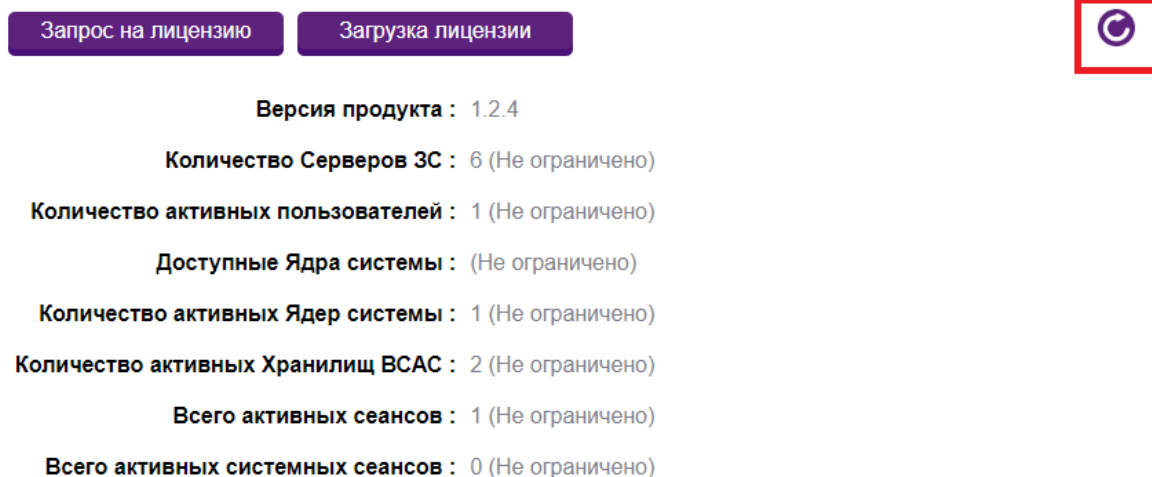


Рис. 107. Кнопка «Обновить»

5.16.3. Скачивание запроса на лицензию

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

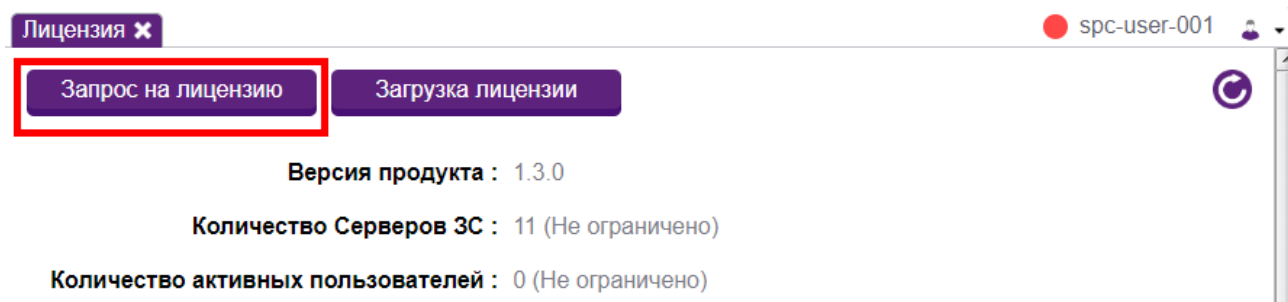


Рис. 108. Кнопка «Запрос на лицензию»

5.16.4. Загрузка лицензии

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

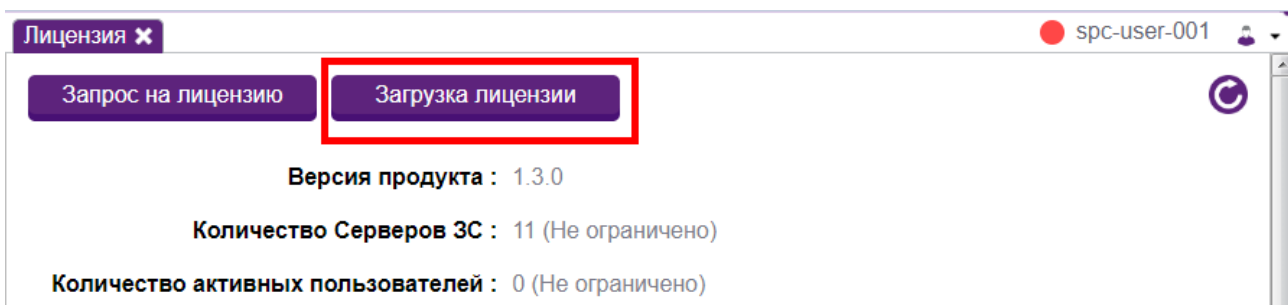


Рис. 109. Кнопка «Загрузка лицензии»

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".

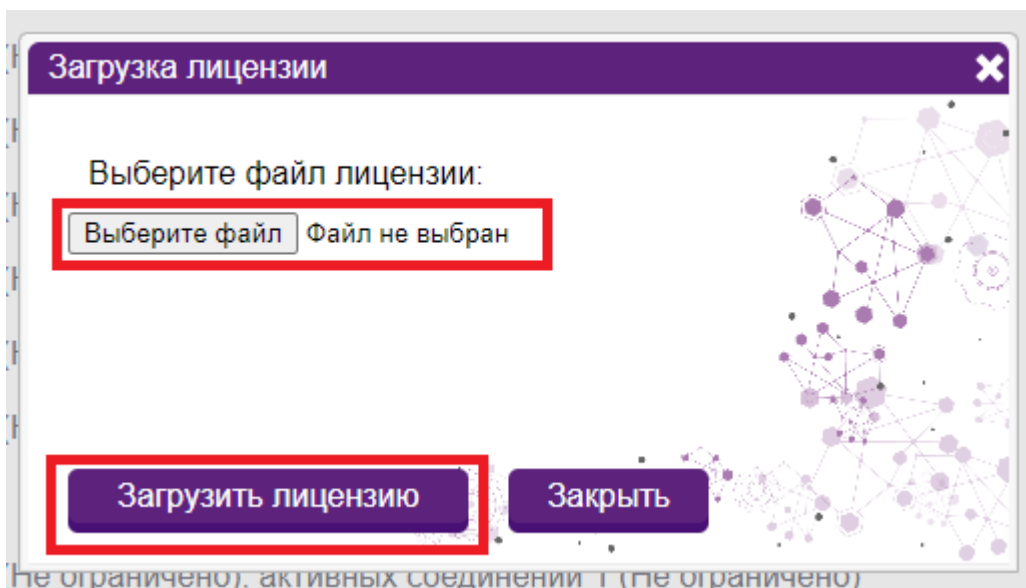


Рис. 110. Окно загрузки лицензии

5.17. Просмотр статуса компонентов Системы

Данная страница позволяет узнать статус всех компонентов Системы. 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:

Наименование	Значение
➕ Основные	
➕ Ядра системы	
➕ Сервера ЗС	
➕ Адреса DNS	
➕ Контроллеры домена	
➕ Сервера системы доставки сообщений	
➕ Сервера Consul	
➕ Состояние агентов Observelt	
➕ Разница в системном времени компонентов системы	
➕ Состояние Хранилищ ВСАС	

Рис. 111. 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.

5.17.1. Просмотр компонентов системы и их значений

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

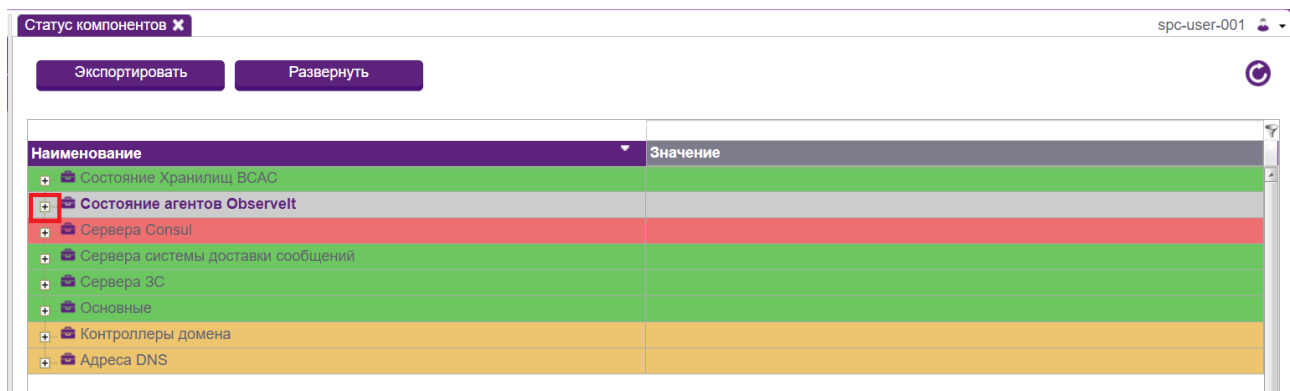


Рис. 112. Кнопка плюс

После этого раскроется подробный список составляющих.

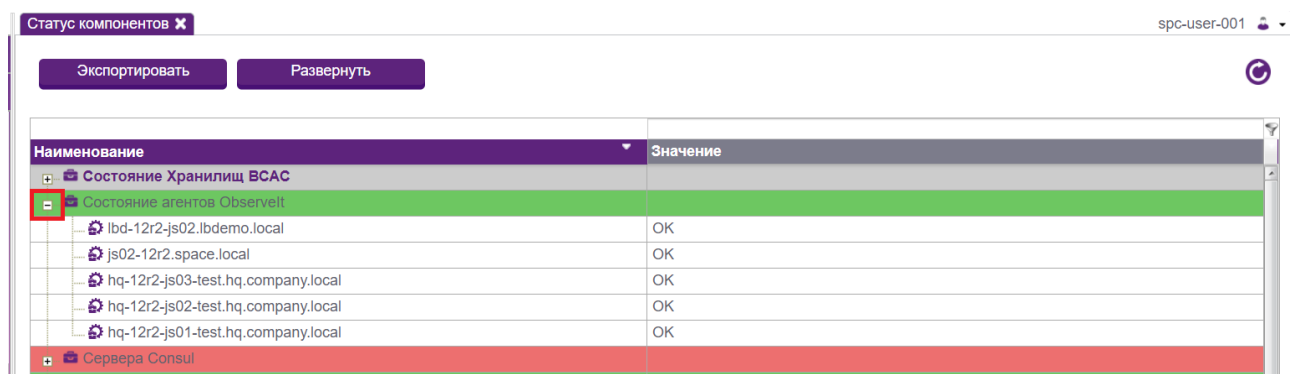


Рис. 113. Подробная информация о каждом компоненте

5.17.2. 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.

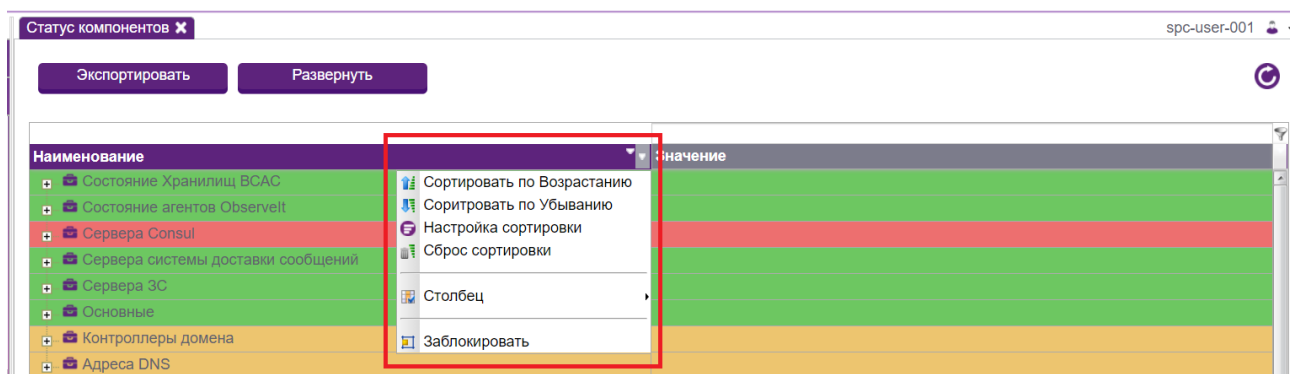


Рис. 114. Выпадающее меню для выбора типа сортировки

5.17.3. Обновление таблицы статуса компонентов

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

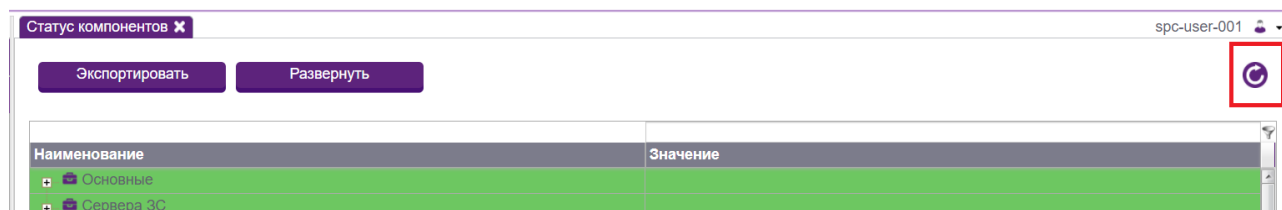


Рис. 115. Кнопка «Обновить»

5.17.4. 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.

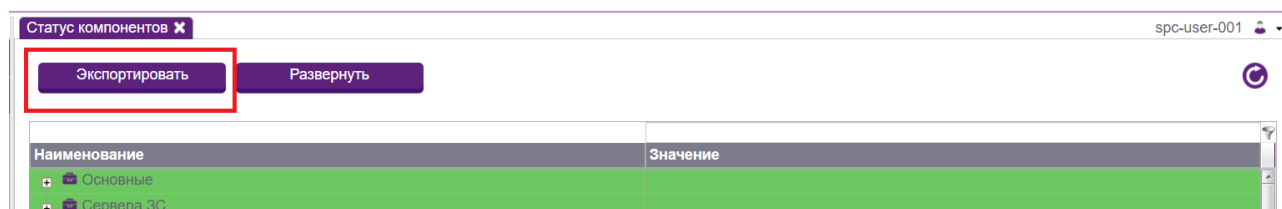
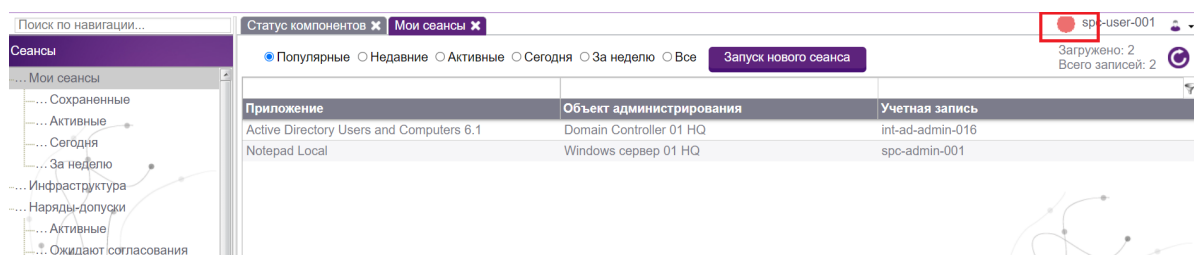


Рис. 116. Кнопка «Экспортировать»

5.17.5. Индикатор быстрого информирования о состоянии системы "Светофор"

Администраторы могут быстро узнать общее состояние вкладки "Статус компонентов", не открывая ее. Для этого справа сверху, 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.



5.18. Управление сеансами привилегированного доступа

Все сеансы ПД отображаются в узле **Сеансы** раздела **Управление системой**.

Пользоват...	Состояние	Создан	Приложение	Объект ад...	FQDN	Сервер ЗС
	Ошибка ожид...	10.01.2019 17:40:54	DNS 6.1	Domain Contr...	dc01-12r2.spa...	js02-12r2.spac...
	Ошибка ожид...	10.01.2019 17:23:34	DNS 6.1	Domain Contr...	dc01-12r2.spa...	js02-12r2.spac...
	Ошибка ожид...	10.01.2019 17:22:56	DNS 6.1	Domain Contr...	dc01-12r2.spa...	js02-12r2.spac...

Рис. 118. 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.

5.18.1. Фильтрация сеансов по состоянию

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

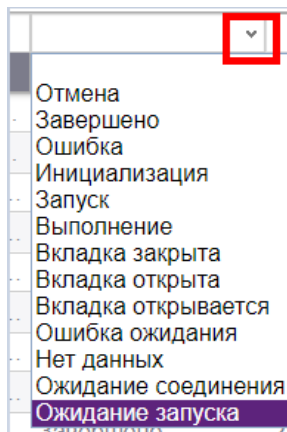


Рис. 119. Фильтрация сеансов по состоянию. Раскрывающееся меню

5.18.2. 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.

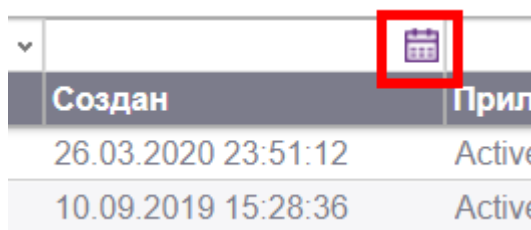


Рис. 120. Фильтрация сеансов по дате создания

5.18.3. Обновление таблицы сеансов

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

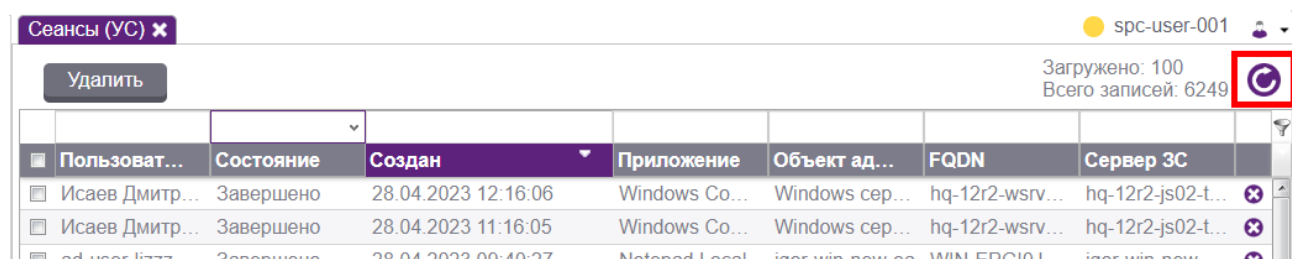


Рис. 121. Кнопка обновления

5.18.4. Удаление строки в таблице сеансов

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

Пользоват...	Состояние	Создан	Приложение	Объект ад...	FQDN	Сервер 3С
Исаев Дмитр...	Завершено	28.04.2023 12:16:06	Windows Co...	Windows сер...	hq-12r2-wsrv...	hq-12r2-js02-t...
Исаев Дмитр...	Завершено	28.04.2023 11:16:05	Windows Co...	Windows сер...	hq-12r2-wsrv...	hq-12r2-js02-t...
ad-user-lizzz...	Завершено	28.04.2023 09:40:27	Notepad Local	igor-win-new-oa	WIN-EPGI0J...	igor-win-new

Рис. 122. Окно «Сессии». Кнопка удаления строки таблицы

5.18.5. Удаление нескольких записей из таблицы сессий одновременно

Для удаления нескольких записей из таблицы **Сессии** 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.

Пользоват...	Состояние	Создан	Приложение	Объект ад...	FQDN	Сервер 3С
<input checked="" type="checkbox"/> Исаев Дмитр...	Завершено	28.04.2023 12:16:06	Windows Co...	Windows се...	hq-12r2-wsrv...	hq-12r2-js02-...
<input checked="" type="checkbox"/> Исаев Дмитр...	Завершено	28.04.2023 11:16:05	Windows Co...	Windows се...	hq-12r2-wsrv...	hq-12r2-js02-...
<input type="checkbox"/> ad-user-lizzz...	Завершено	28.04.2023 09:40:27	Notepad Local	igor-win-new-oa	WIN-EPGI0J...	igor-win-new

Рис. 123. Выделены две записи таблицы «Сессии». Кнопка «Удалить» активна

5.19. Управление операциями с секретами

Доступ к сессиям рандомизации паролей учетных записей (операциям с секретами) осуществляется в узле **Операции с секретами** раздела **Управление системой**.

Тип агента рандомизации	Агент рандомизации	Учетная запись	Состояние	Создан
Microsoft Windows	windows_hq_domain	ad-admin-001 on HQ	Ошибка	20.04.2023 15:51:16
Linux	change_password_igo...	igor_localhost_linux	Завершено	13.04.2023 11:43:32
Linux	change_password_igo...	igor_localhost_linux	Завершено	13.04.2023 11:42:48
Linux	change_password_igo...	igor_localhost_linux	Завершено	13.04.2023 11:42:19
Linux	change_password_igo...	igor_localhost_linux	Ошибка	13.04.2023 11:38:24

Рис. 124. Окно «Операции с секретами» раздела «Управление системой»

Данные о сессиях 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.

5.19.1. 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.

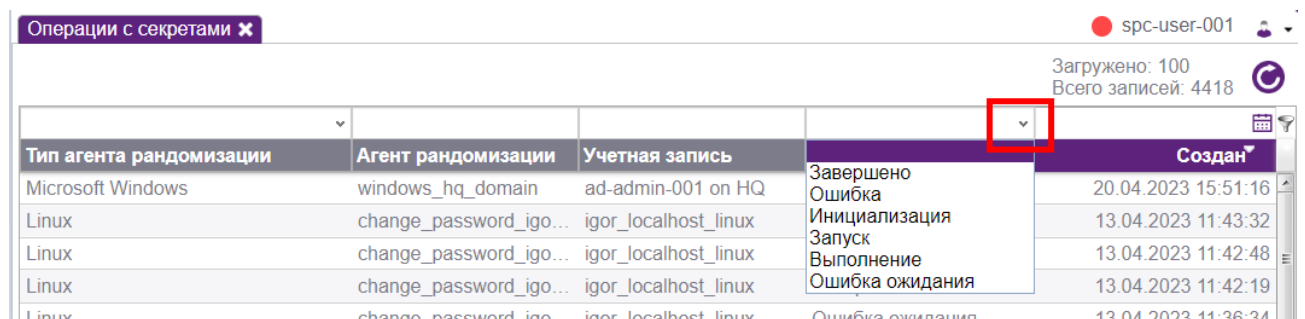


Рис. 125. Фильтрация сеансов по состоянию. Раскрывающееся меню

5.19.2. Фильтрация раздела по дате создания

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

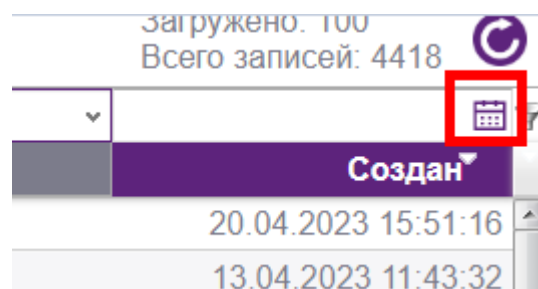


Рис. 126. Фильтрация сеансов по дате создания

5.19.3. Обновление таблицы операций с секретами

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

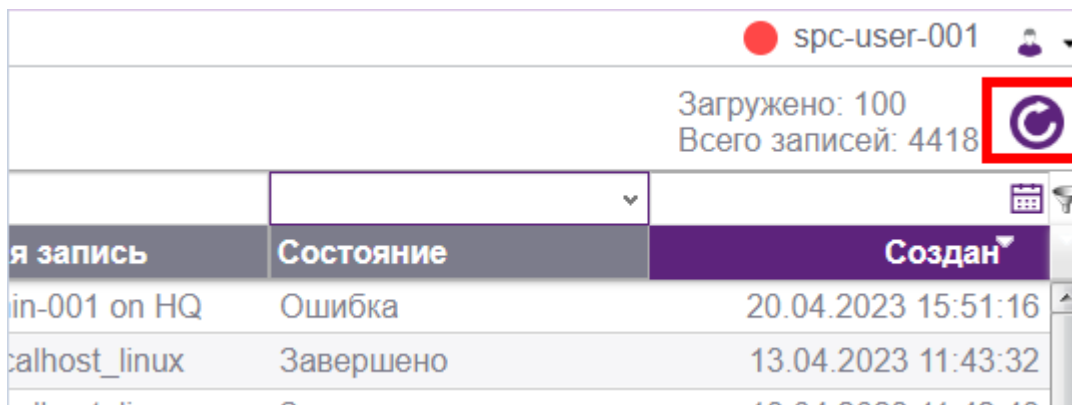


Рис. 127. Кнопка обновления

5.19.4. Просмотр информации о каждом сеансе

Для просмотра детальной информации о сеансе необходимо дважды щелкнуть левой кнопкой мыши **Типе агента рандомизации** или **Агенте рандомизации** соответствующей записи в таблице.

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

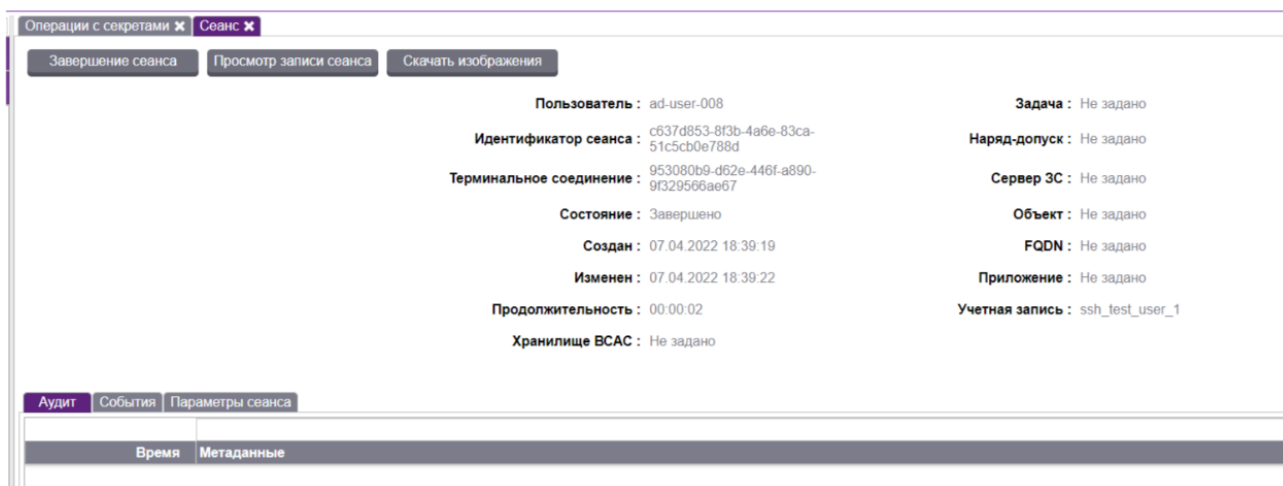


Рис. 128. Окно подробной информации о сеансе

5.20. Формирование отчетности по использованию Системы

Система sPACE позволяет формирование статистики по использованию системы на основе следующих данных:

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

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 системой** и выбрать необходимый фильтр в дереве навигации узла **Статистика**.

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-deb8-1sv01.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 @ pl.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. 129. Статистика по использованию Системы

5.21. 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**.

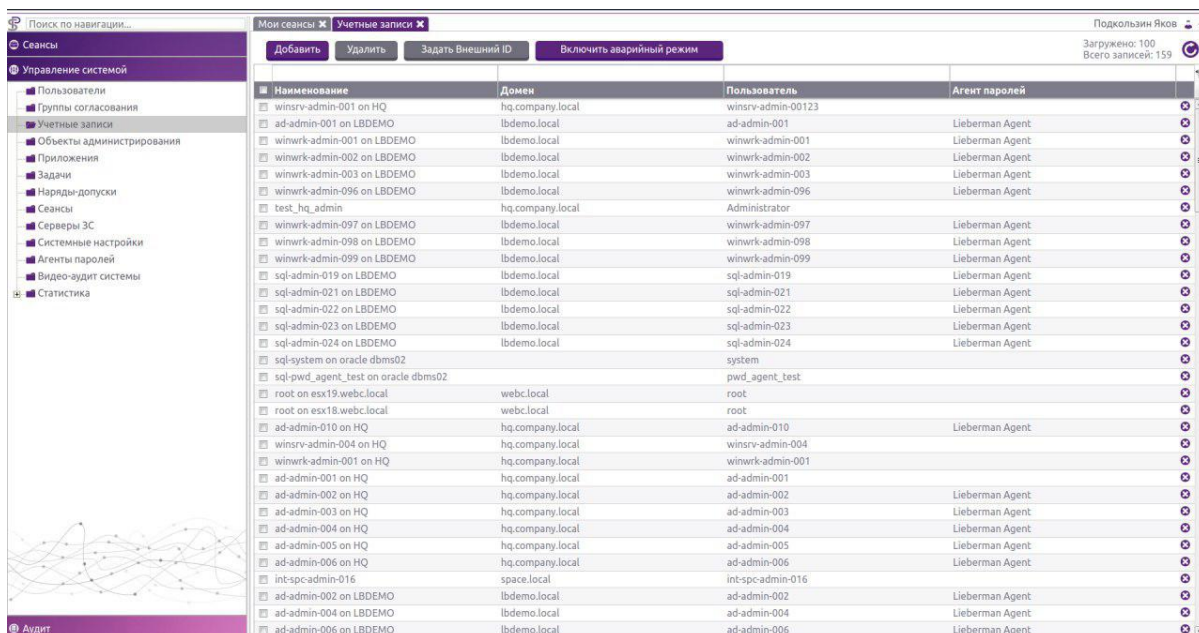


Рис. 130. Кнопка перевода Системы в аварийный режим активна

5.22. Осуществление аудита Системы

Система sPASE умеет осуществлять аудит системы, который позволяет получить данные о действиях пользователей на портале.

Для этого служит вкладка **Аудит**. Она необходима для получения объективных качественных и количественных оценок о текущем состоянии портала, имеющих в нем сеансов, пользователей и их действий.

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

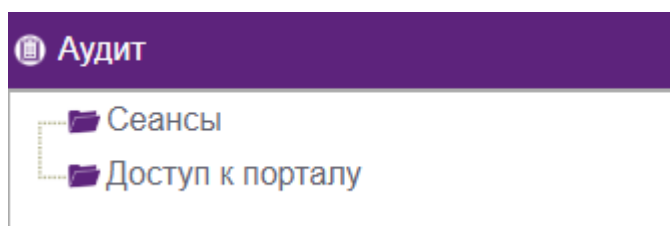


Рис. 131. Вкладка «Аудит системы»

5.23. 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	spr-user-001@space.local	31.01.2020 22:19:43	SQLPlus	База данных Oracle SPACE	dbms02-deb.space.local
Ошибка ожидания	spr-user-001@space.local	31.01.2020 22:19:39	Windows Command Line 6.1	Сервер для ОИТ и PI в sSPACE	v-erpm-8r2-06.space.local
Ошибка ожидания	spr-user-001@space.local	31.01.2020 22:19:39	Windows Command Line 6.1	Сервер для ОИТ и PI в sSPACE	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
Завершено	ad-user-008@hq.company.local	29.01.2020 14:37:36	Services 6.1	Windows сервер 01 HQ	hq-12r2-wsrv01.hq.company.local

Рис. 132. 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.

5.23.1. 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.

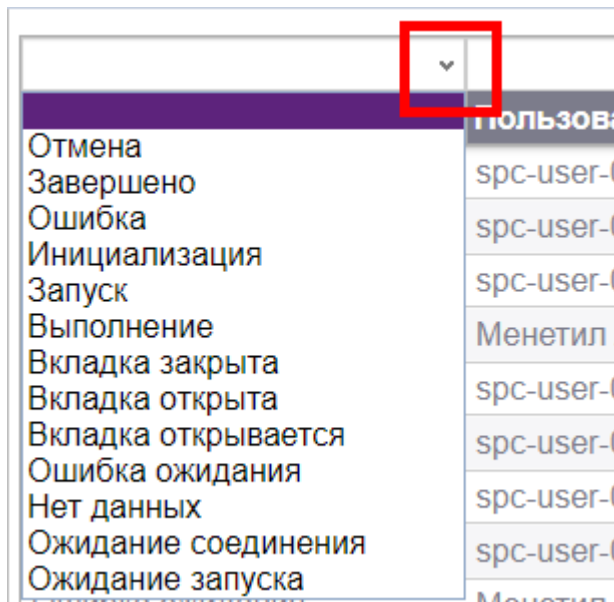


Рис. 133. Выбор фильтрации по состоянию

5.23.2. 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.

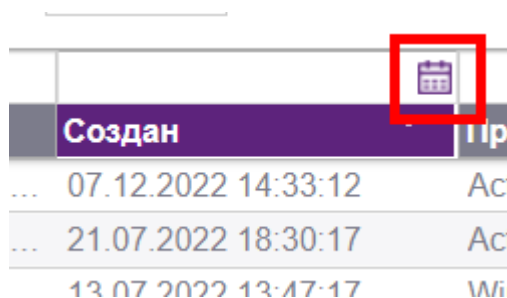


Рис. 134. Выбор фильтрации по дате создания

5.23.3. Обновление таблицы Сеансы

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

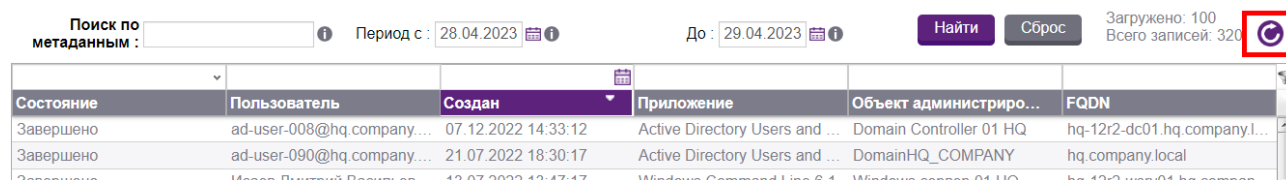


Рис. 135. Кнопка «Обновить»

5.23.4. 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.

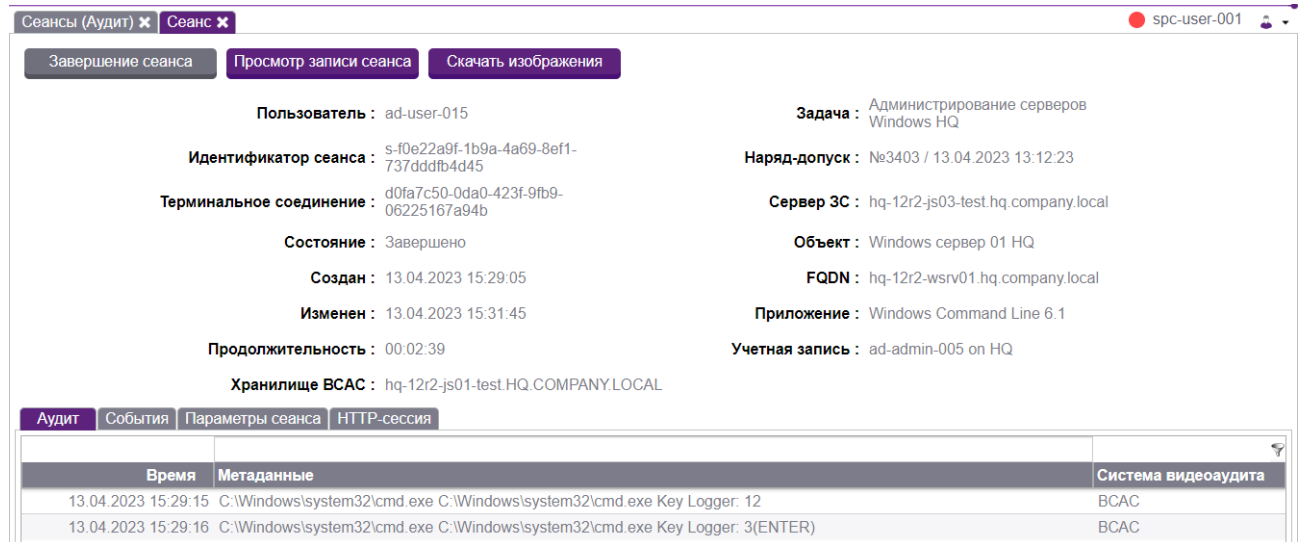


Рис. 136. Окно подробной информации о сеансе

5.23.5. Просмотр записи сеанса

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

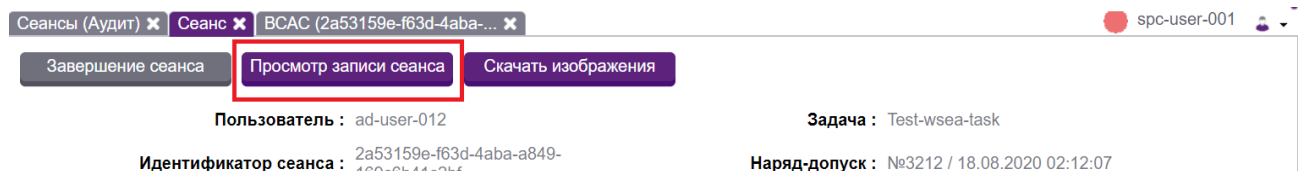


Рис. 137. Местонахождение кнопки «Просмотр записи сеанса»

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

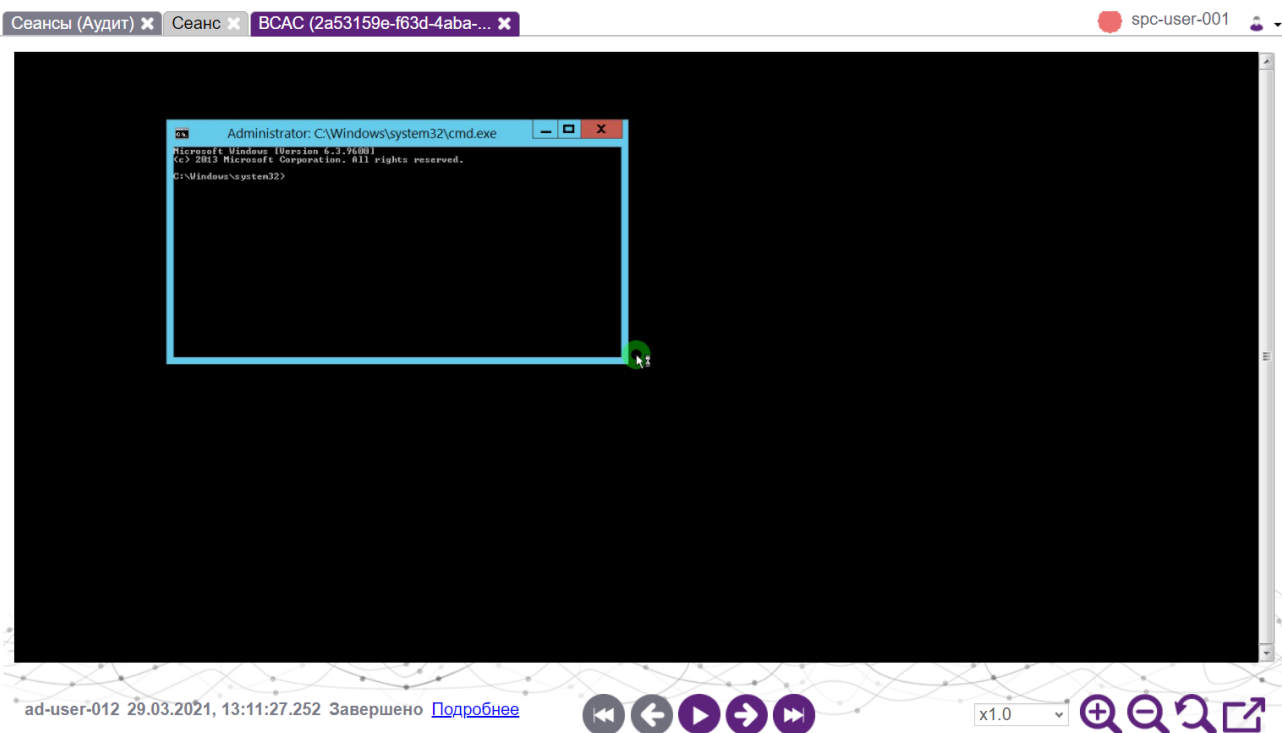


Рис. 138. Окно плеера

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

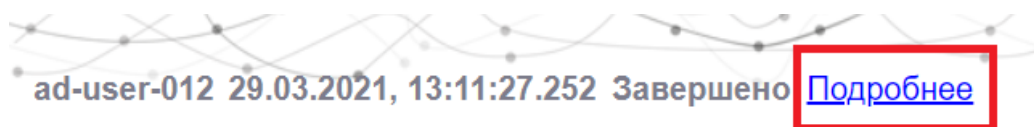


Рис. 139. Местонахождение кнопки «Подробнее»

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

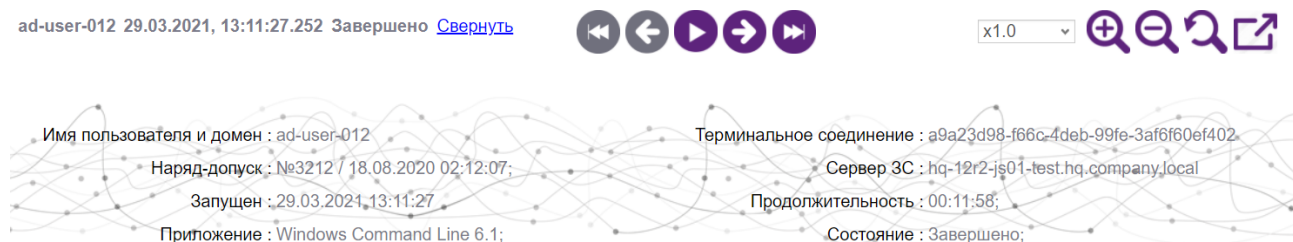


Рис. 140. Подробная информация о сеансе

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 вперед, переместиться в конец записи.



Рис. 141. 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. 142. Кнопки параметров просмотра записи сеанса

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

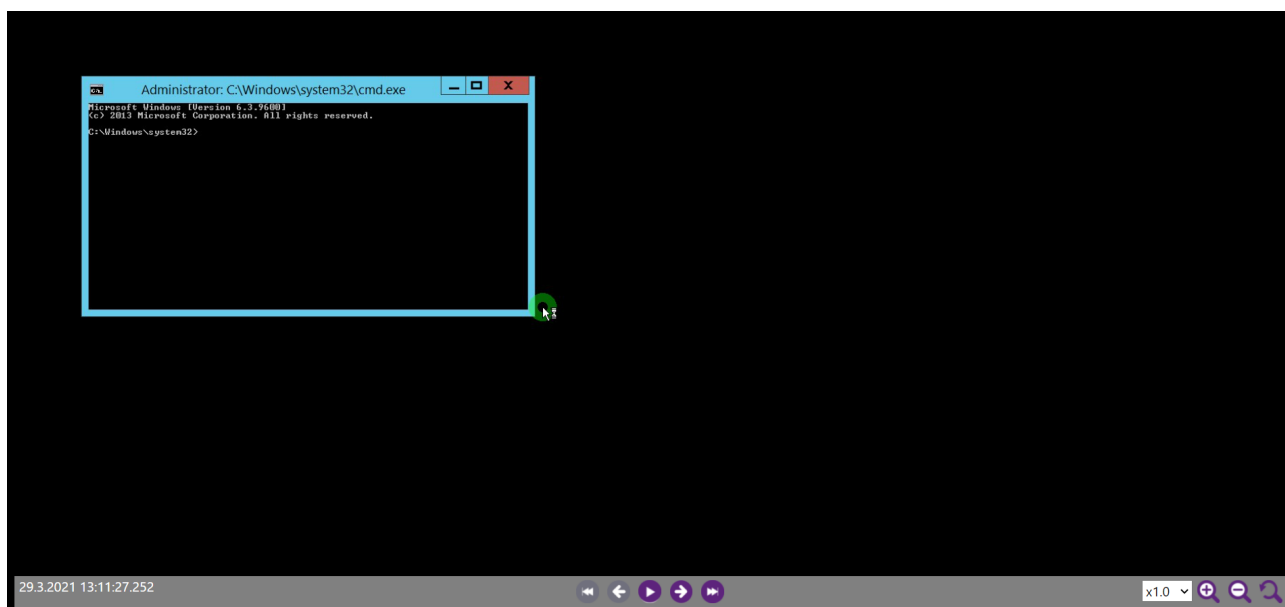


Рис. 143. Просмотр записи сеанса в отдельной вкладке браузера

Кнопки для управления просмотром в этом окне аналогичны описанным выше.

5.23.6. Просмотр записи работающего сеанса в режиме онлайн

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

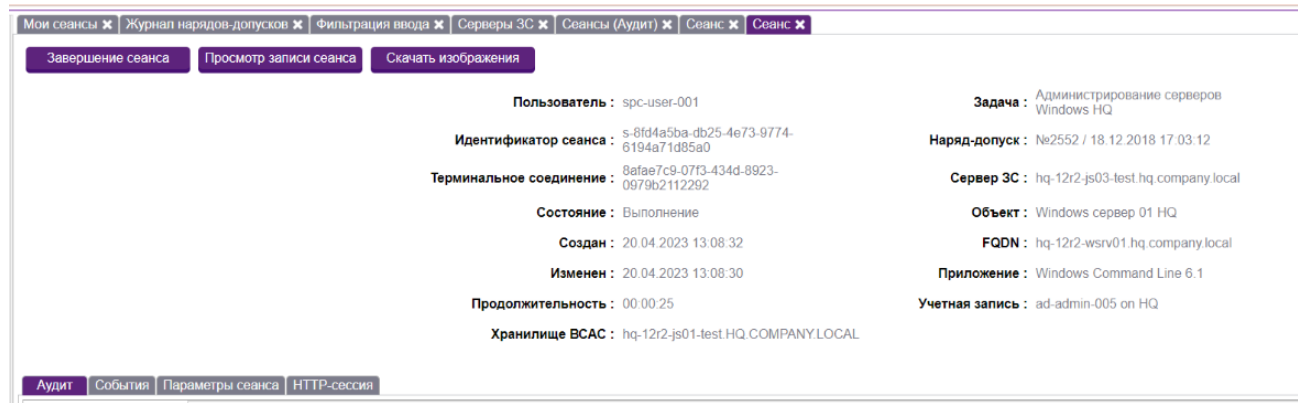


Рис. 144. Карточка сеанса, работающего в данный момент

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

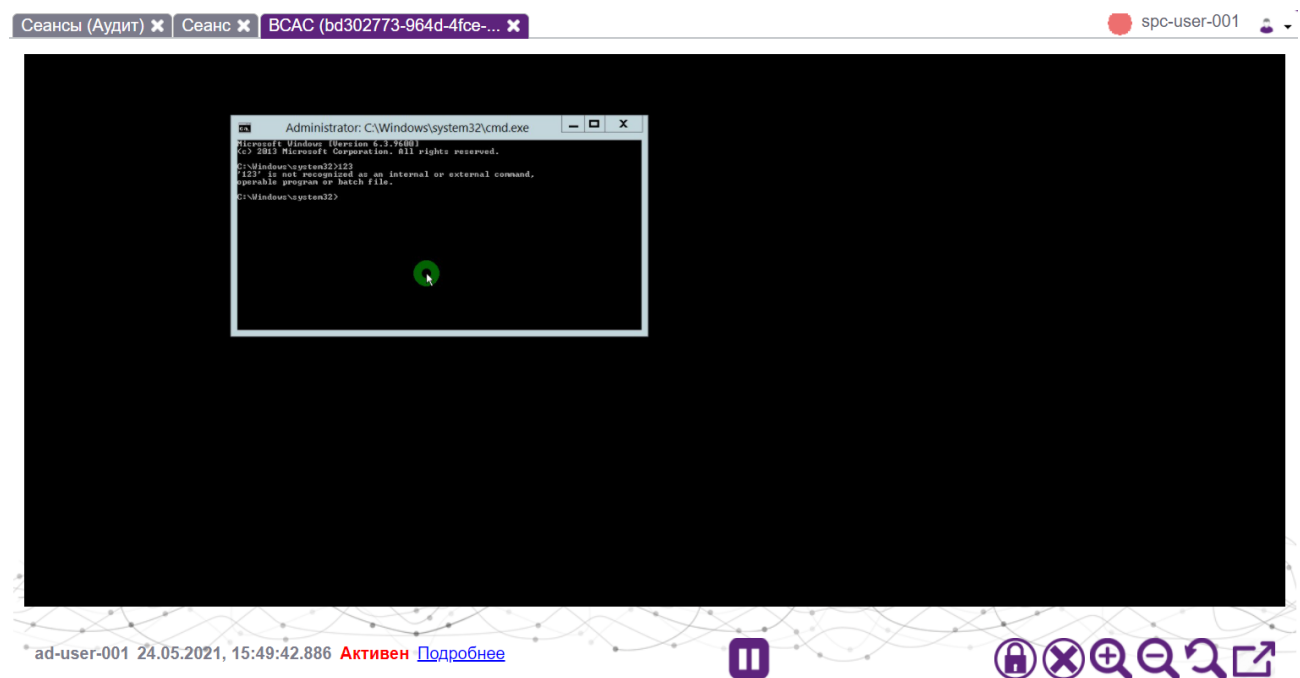


Рис. 145. Плеер сеанса, работающего в данный момент

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. 146. Рабочая панель онлайн плеера

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.

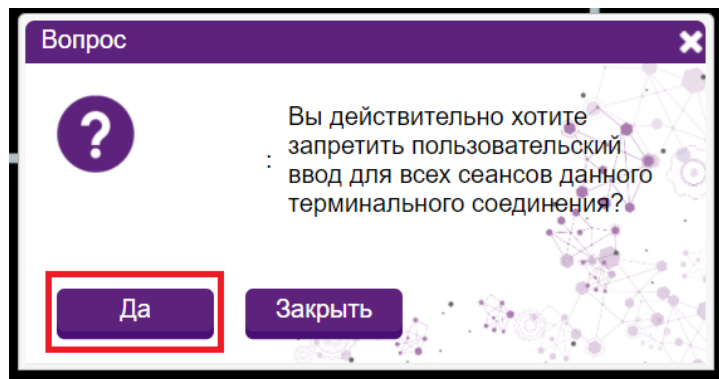


Рис. 147. Окно подтверждения запрета на пользовательский ввод

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.

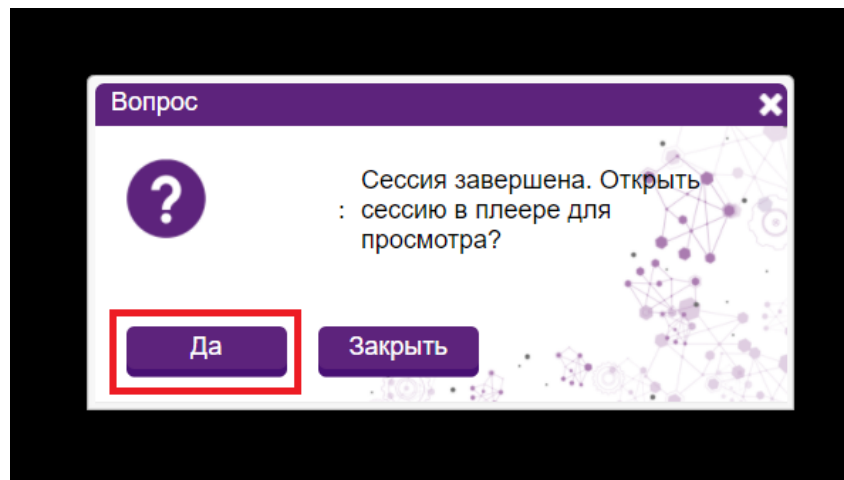


Рис. 148. Уведомление о завершении сеанса

5.23.7. 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.

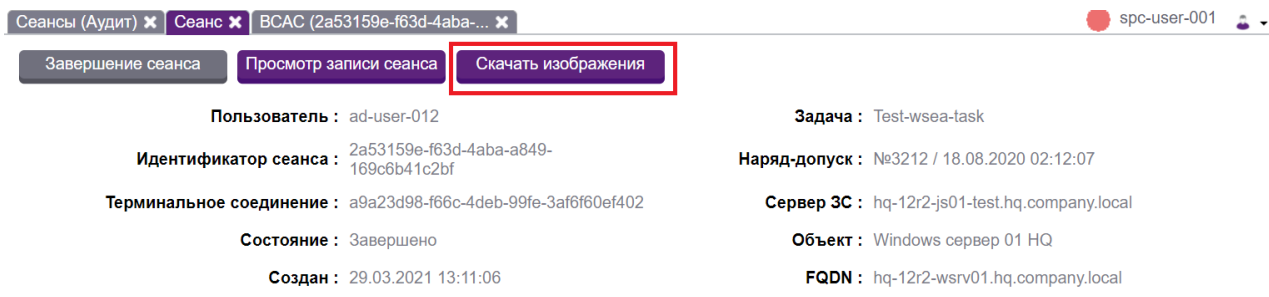


Рис. 149. Местоположение кнопки для скачивания скриншотов сеанса

5.23.8. 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**.

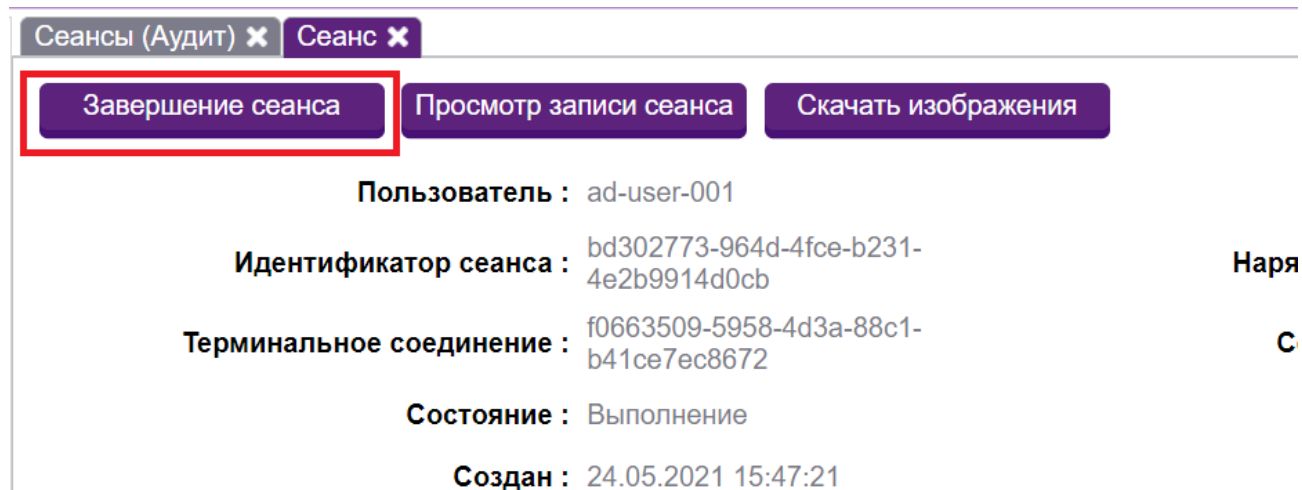


Рис. 150. Кнопка «Завершение сеанса»

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**.

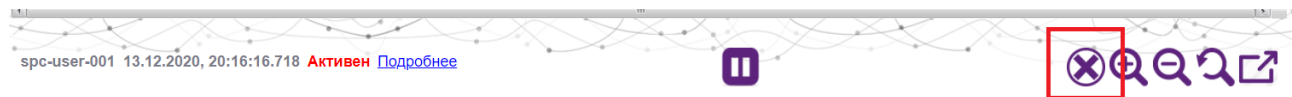


Рис. 151. Местоположение кнопки для завершения всей активной сессии

5.23.9. 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**.

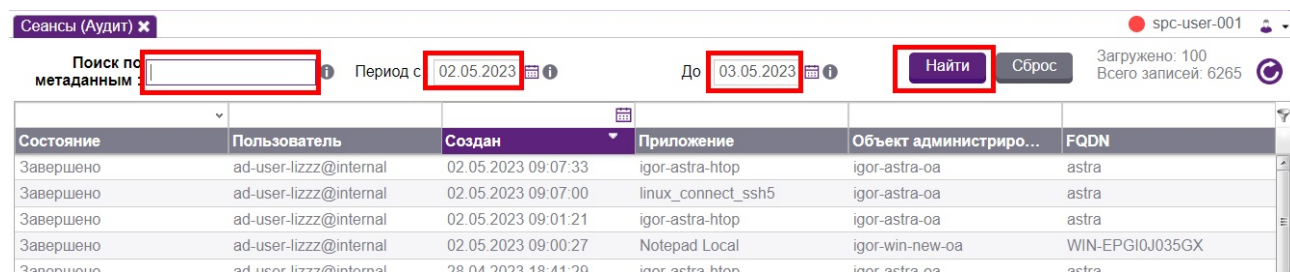


Рис. 152. Поиск по метаданным

5.23.10. 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.

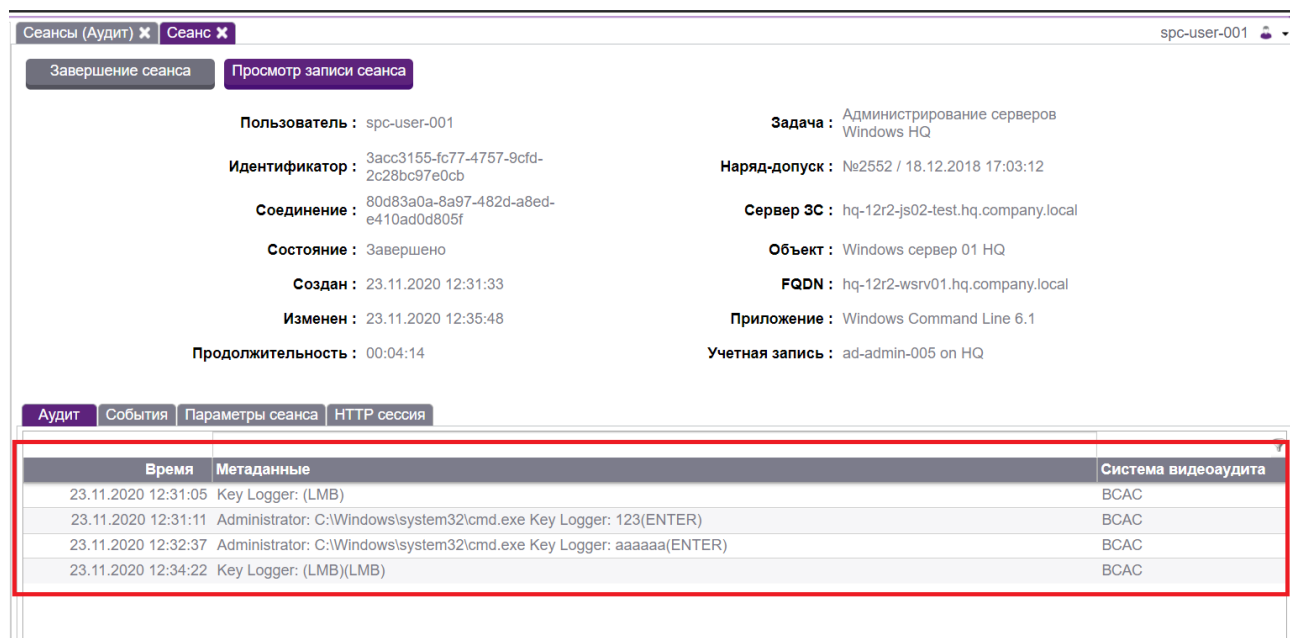
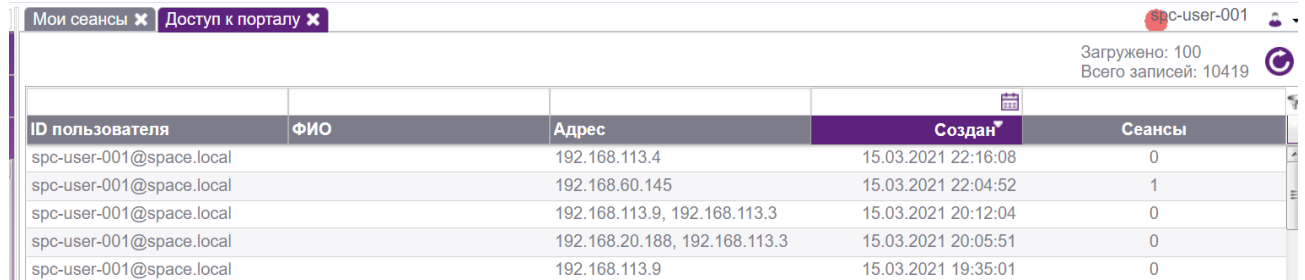


Рис. 153. Данные Key Logger

5.24. 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
sps-user-001@space.local		192.168.113.4	15.03.2021 22:16:08	0
sps-user-001@space.local		192.168.60.145	15.03.2021 22:04:52	1
sps-user-001@space.local		192.168.113.9, 192.168.113.3	15.03.2021 20:12:04	0
sps-user-001@space.local		192.168.20.188, 192.168.113.3	15.03.2021 20:05:51	0
sps-user-001@space.local		192.168.113.9	15.03.2021 19:35:01	0

Рис. 154. 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.

5.24.1. 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.

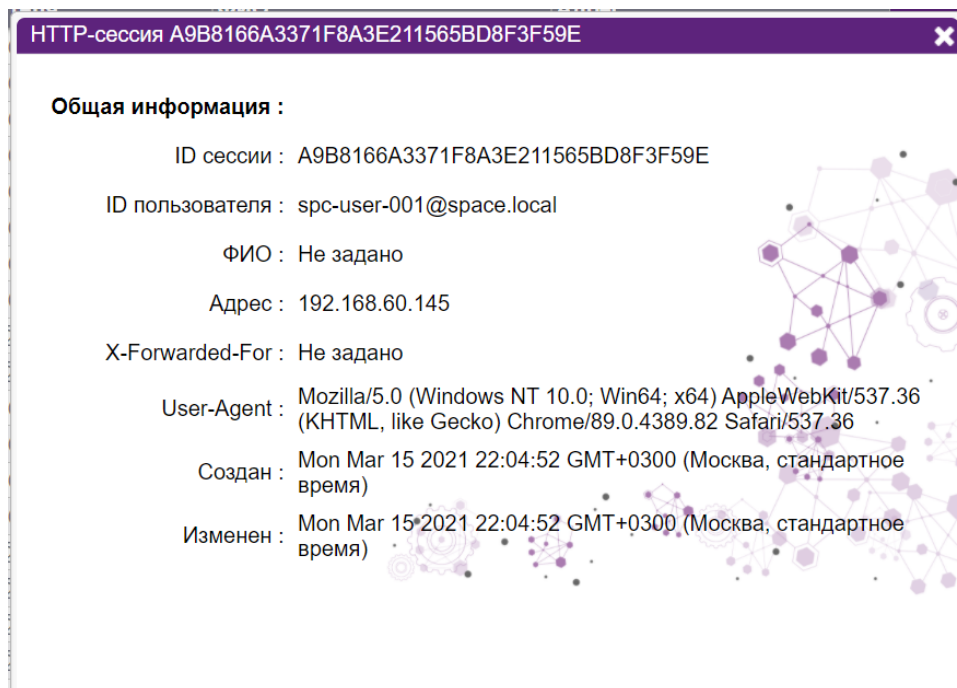


Рис. 155. Информация о пользовательской сессии

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 portalу. В случае изменения IP-адреса источника подключений к portalу 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>, <проxy1>, <проxy2>" (где <client> – IP-адрес клиента), "<проxy1>, <проxy2>" – 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.

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 1 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

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

- DATA API – конфигурация системы или синхронизация данных об объектах с внешними системами:
 - Объекты администрирования и их типы;
 - Инструменты администрирования;
 - Серверы ЗС;
 - Пользователи и группы пользователей;
 - Привилегированные учетные записи;
 - Задачи;
 - Сетевые узлы;
 - Системы видеоаудита;
 - Агенты паролей;
 - Агенты рандомизации паролей;
 - Приложения, их сценарии запуска и экземпляры;
 - Домены;
 - Наряды-допуски;
 - Параметры запуска и их типы;
- Management API:
 - Управление конфигурацией Launcher Manager;
 - Управление паролями привилегированных учетных записей;
- System audit API – выгрузка данных о сеансах во внешние системы безопасности.