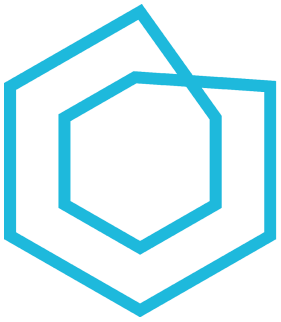
ООО «ВЭБ КОНТРОЛ ДК»



sPACE

Система Управления Привилегированным Доступом

sPACE PAM

ВЕРСИЯ 2.0.2

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Москва, 2025

СОДЕРЖАНИЕ

ОБ ЭТОМ ДОКУМЕНТЕ

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

Документ включает в себя главы с общим описанием программы, описанием ее интерфейса, ее функционала и действиями в случае аварийных ситуаций. Документ адресован специалистам, которые используют Систему для запуска сеансов привилегированного доступа.

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

Термин/сокращение	**Определение**
ПД	Привилегированный Доступ. Неограниченный доступ для просмотра и изменения данных, изменения параметров конфигурации, запуска программ и т.д.
Терминальная сессия (терминальное соединение)	Установленное соединение (SSH или RDP) между пользовательским устройством и СЗС, в рамках которой может быть запущен один или несколько сеансов.
Сеанс привилегированного доступа	Интерактивный обмен данными, имеющий ограниченный временной интервал, в ходе которого владельцу учетной записи предоставляется привилегированный доступ. Сеанс запускается в рамках установленного терминального соединения. Сеанс администрирования считается запущенным с момента отображения на экране пользователя окна инструмента администрирования и законченным в момент выхода из инструмента администрирования.
НД	Наряд-допуск. Разрешение на выполнение определенной задачи с использованием sPACE, в котором содержится название задачи, срок действия наряда-допуска, инициирующее и согласующее лицо, обоснование и объекты администрирования.
ОА	Объект администрирования. Целевая система, действия с которой производятся с использованием привилегированного доступа
ИА	Инструмент Администрирования. Приложение, запускаемое на сервере ЗСА, с помощью которого осуществляются привилегированный доступ к ОА.
ЗСА, СЗС	Защищенная Среда Администрирования, Сервер Защищенной Среды. Выделенный сервер, на котором выполняется сеанс привилегированного доступа (также защищенный сервер - ЗС).
FQDN	Fully Qualified Domain Name. Имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DN
ВСАС	Внутренняя Система Аудита Сеансов. Система отвечающая за фиксацию видеоданных пользовательского сеанса а также метаданных о действиях пользователя в рамках данного сеанса, в том числе данных клавиатурного ввода.

Термин/сокращение	Определение
ПУЗ	Привилегированная Учетная Запись. При помощи неё осуществляется управление объектами администрирования.
ИС/АС	Информационные и Автоматизированные Системы, к которым осуществляется привилегированный доступ
СОС	Система Обмена Сообщениями. Служба, обеспечивающая коммуникацию между компонентами sPACE.

1. ВВЕДЕНИЕ

1.1. Область применения

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

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

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

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

1.2. Краткое описание возможностей

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

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

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

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

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

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

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

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

1.3. Уровень подготовки пользователя

Для работы с Системой пользователи системы должны обладать общими навыками работы на ПК, навыками работы с web-браузером IE 11 и выше, Firefox, Chrome.

1.4. Роли пользователей в системе sPACE

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

- базовый пользователь;
- стандартный пользователь;
- продвинутый пользователь;
- администратор;

- технический администратор.
- аудитор;
- привилегированный аудитор;
- привилегированный администратор.

Узнать, какие роли назначены пользователю, можно в окне **Профиль** меню **Настройки**.

Настоящее Руководство пользователя предназначено для сотрудников с ролями «Базовый пользователь», «Стандартный пользователь», «Продвинутый пользователь». Функционал, доступный для каждой роли, приводится в таблице ниже.

Таблица 1 Функционал, доступный пользователям Системы

Роль	Доступный функционал
Базовый пользователь	● Запуск сеансов администрирования на основе согласованных нарядов-допусков.
Стандартный пользователь	● 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. ● Просмотр записей собственных сеансов, если для них есть соответствующие данные ВСАС. ● Согласование нарядов-допусков, если пользователь входит в группу согласующих для соответствующей задачи администрирования.
Продвинутый пользователь	● Просмотр объектов администрирования, сгруппированных в виде задач. ● Запрос наряда-допуска на объекты администрирования для своей учетной записи. ● Запрос наряда-допуска для чужих учетных записей. ● Запуск сеансов администрирования на основе согласованных нарядов-допусков. ● Просмотр записей собственных сеансов, если для них есть соответствующие данные ВСАС. ● Согласование нарядов-допусков, если пользователь входит в группу согласующих для соответствующей задачи администрирования.

1.5. Перечень эксплуатационной документации

Для работы с Системой пользователю необходимо ознакомиться с настоящим Руководством пользователя.

2. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Назначение программы

Программный продукт sPACE предназначен для автоматизации процесса предоставления защищенного доступа привилегированных пользователей к критическим ИТ- ресурсам компании, предоставления защищенной среды для работы с критическими ИТ- ресурсами компании и обеспечения прозрачности действий привилегированных пользователей.

В данном документе под привилегированными пользователями понимаются следующие группы пользователей:

- Системные администраторы информационных систем, сетевого оборудования, сети, серверов и т. д.;
- Администраторы приложений и баз данных;
- Поставщики сторонних систем и подрядчики, обслуживающие ИТ-системы компании.

sPACE используется для повышения скорости согласования доступа привилегированных пользователей к ИТ-ресурсам компании, снижения вероятности несанкционированного доступа к ИТ-ресурсам и рисков, связанных с неконтролируемыми действиями специалистов, осуществляющих эксплуатацию и обслуживание элементов ИТ-инфраструктуры компании.

2.2. Условия применения программы

В настоящем документе приводятся требования к рабочим станциям пользователей Системы. Аппаратные и программные требования к функционированию Системы приводятся в Руководстве администратора и Руководстве по установке.

Для работы с Системой компьютер пользователя должен быть подключен к Интернету или локальной сети (зависит от параметров установки Системы) и удовлетворять требованиям к программному обеспечению (таблица №1) .

Установка, настройка и использование Системы должны осуществляться в соответствии с эксплуатационной документацией. Перед началом работы необходимо установить все доступные обновления для компонентов Системы. Система должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным ниже в таблице №2.

Таблица 1. Требования к программному обеспечению рабочих станций

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

Таблица 2. 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. ПОДГОТОВКА К РАБОТЕ

3.1. Состав и содержание дистрибутивного носителя данных

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

В состав дистрибутива системы входят следующие файлы:

- spaceinstall – исполняемый файл, предназначенный для установки на машину Linux, который осуществляет установку компонентов системы sPACE Mono (Base);
- linux_js_installer.gz — архив, с помощью которого осуществляется установка JS Linux.
- space-installer-2.0.1.exe — исполняемый файл, который осуществляет установку JS Windows.

Для работы sPACE необходимо осуществить как минимум установку Моно Ядра и одного сервера ЗСА.

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

3.2. Начало работы

После развертывания Системы в соответствии с Инструкцией по развертыванию необходимо, чтобы были добавлены все необходимые пользователи в группы каталогов AD и/или LDAP в соответствии с их ролями. В Системе должны быть созданы объекты администрирования, приложения управления объектами администрирования, сценарии запуска сеансов привилегированного доступа и группы согласования. Процедуры добавления пользователей, создания объектов администрирования, групп согласования, сценариев запуска сеансов привилегированного доступа и добавления приложения описаны в Руководстве администратора.

Для начала работы с Системой необходимо открыть окно веб-браузера и ввести в адресной строке веб-адрес Портала Системы. На Портале пользователь осуществляет выбор информационного ресурса, выбор инструмента подключения к этому ресурсу и выбор учетной записи, от имени которой будет осуществляться это подключение.

После запуска Портала пользователь попадает в окно авторизации, где предлагается ввести учетные данные. В случае, если у пользователя подключена функция двухфакторной аутентификации, будет предложено ввести данные второго фактора.

После авторизации пользователь попадает в интерфейс Системы.

3.3. Порядок проверки работоспособности

Система является работоспособной, если после авторизации пользователя на Портале Системы на экране отображается интерфейс Системы.

4. ИНТЕРФЕЙС sPACE

После авторизации на Портале Системы пользователь попадает в главное окно Системы.

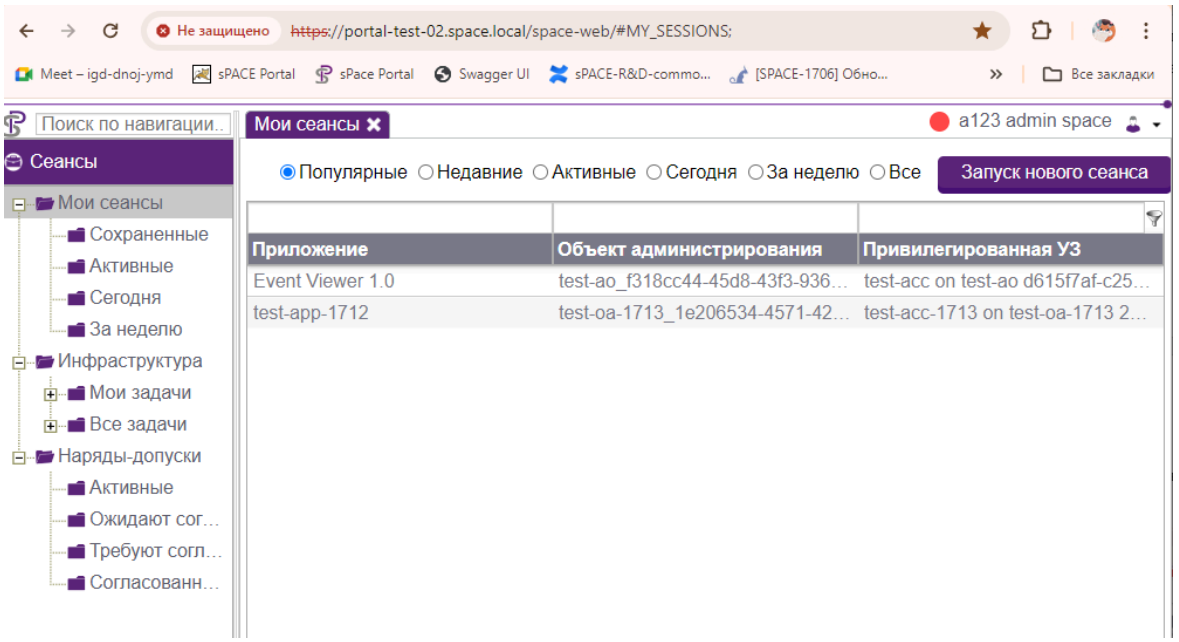


Рисунок 1. *Главное окно Системы*

Главное окно Системы имеет следующие элементы.

- Дерево навигации;
- Панель данных;
- Панель инструментов;
- Панель быстрого доступа;
- Настройки.

4.1. Дерево навигации

Дерево навигации служит для быстрого доступа к разделам и узлам. В зависимости от роли пользователя в Системе в дереве навигации могут отображаться разные разделы. При авторизации в Системе с ролью «Пользователь» в Дереве навигации отображается раздел «Сеансы», в котором содержатся 3 узла:

- Мои сеансы;
- Инфраструктура;
- Наряды-допуски.

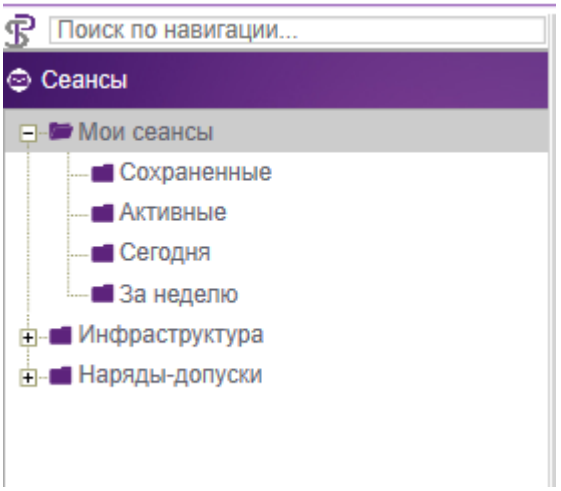


Рисунок 2. *Дерево навигации*

4.2. Панель данных

На Панели данных отображаются результаты выполненных запросов на получение данных узлов.

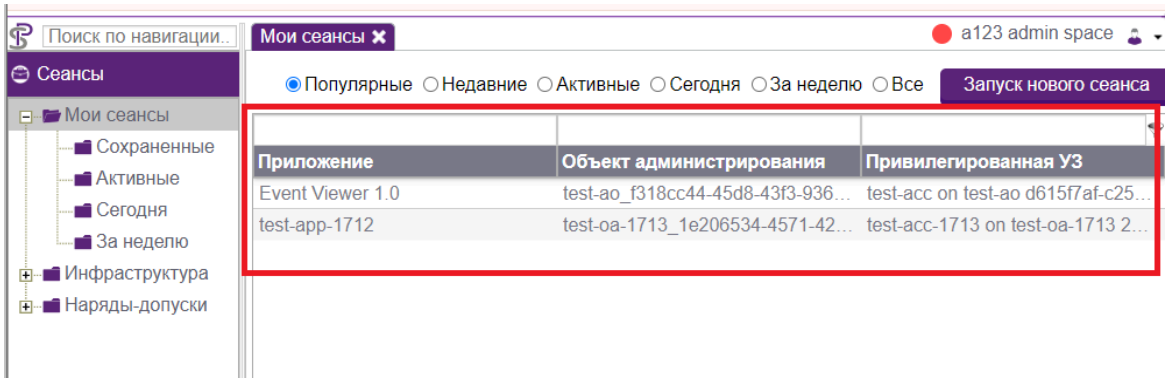


Рисунок 3. *Панель данных*

Данные отображаются в виде таблицы, названия столбцов различны для разных узлов и разделов. При отсутствии данных, соответствующих запросу, на панели данных выводится сообщение «Нет объектов для вывода.».

Над данными можно выполнить следующие действия:

- Сгруппировать по полю;
- Разгруппировать;
- Отфильтровать по полю;
- Выполнить поиск данных в столбце по ключевому слову.

Сгруппировать по полю

Для группировки данных по полю необходимо навести указатель мыши на название поля (соответствует названию столбца) и щелкнуть мышью на появившемся треугольнике вершиной вниз на сером фоне. В выпадающем меню нужно выбрать команду **Группировать по полю** (название поля).

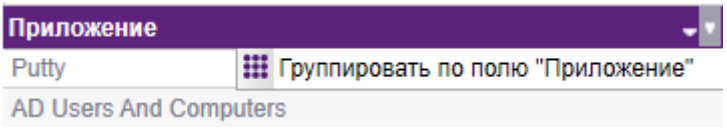


Рисунок 4. *Группировка по полу «Приложение»*

Разгруппировать

Для разгруппирования данных необходимо выбрать в выпадающем меню команду **Разгруппировать**.

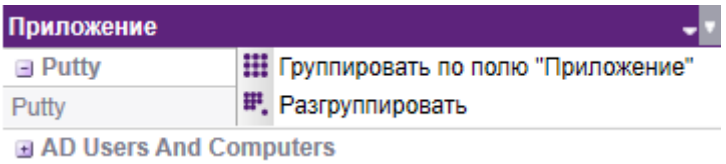


Рисунок 5. *Команда «Разгруппировать»*

Отфильтровать по полю

Данные запросов могут быть отфильтрованы по любому столбцу. Для этого необходимо выделить столбец, щелкнув на нем мышью. При этом треугольник будет указывать порядок отображения данных.

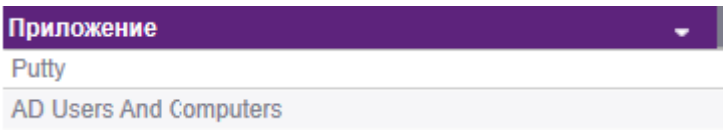
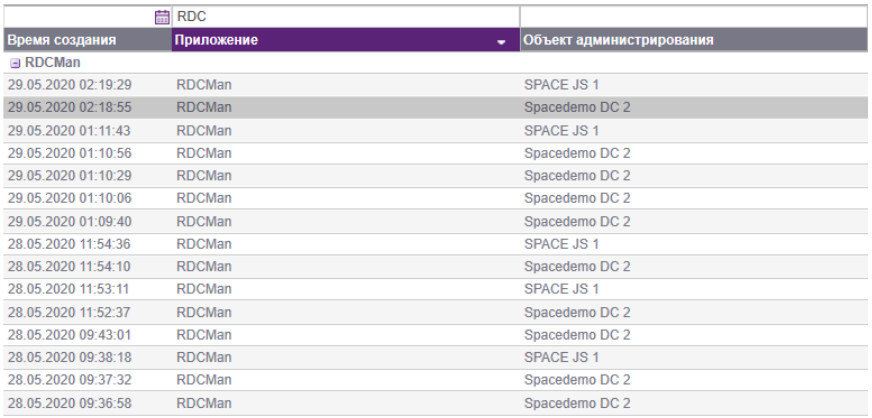


Рисунок 6. *Данные отображаются в обратном алфавитном порядке*

Поиск данных в столбце по ключевому слову

В Системе реализован поиск данных в любом столбце. Для этого необходимо ввести поисковое слово в пустом поле над названием столбца и нажать клавишу **Enter** или щелкнуть на значке фильтра  .



RDC

Время создания	Приложение	Объект администрирования
RDCMan		
29.05.2020 02:19:29	RDCMan	SPACE JS 1
29.05.2020 02:18:55	RDCMan	Spacedemo DC 2
29.05.2020 01:11:43	RDCMan	SPACE JS 1
29.05.2020 01:10:56	RDCMan	Spacedemo DC 2
29.05.2020 01:10:29	RDCMan	Spacedemo DC 2
29.05.2020 01:10:06	RDCMan	Spacedemo DC 2
29.05.2020 01:09:40	RDCMan	Spacedemo DC 2
28.05.2020 11:54:36	RDCMan	SPACE JS 1
28.05.2020 11:54:10	RDCMan	Spacedemo DC 2
28.05.2020 11:53:11	RDCMan	SPACE JS 1
28.05.2020 11:52:37	RDCMan	Spacedemo DC 2
28.05.2020 09:43:01	RDCMan	Spacedemo DC 2
28.05.2020 09:38:18	RDCMan	SPACE JS 1
28.05.2020 09:37:32	RDCMan	Spacedemo DC 2
28.05.2020 09:36:58	RDCMan	Spacedemo DC 2

Рисунок 7. *Результаты поиска по ключевому слову «RDC»*

4.3. Панель инструментов

На панели инструментов расположены команды, которые можно выполнить в данном разделе или узле. Список этих команд зависит от раздела и узла.

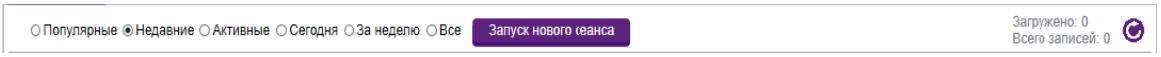


Рисунок 8. *Панель инструментов раздела «Сеансы»*

4.4. Панель быстрого доступа

Для быстрого перехода по нужным узлам в Системе предусмотрена панель быстрого доступа. Она находится в верхней части панели данных.

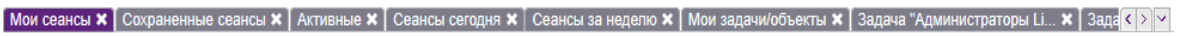


Рисунок 9. *Панель быстрого доступа*

На **Панели быстрого доступа** расположены вкладки узлов, которые пользователь открывал в текущем сеансе работы, начиная с момента авторизации в Системе и заканчивая выходом из Системы.

Активный узел выделен цветом. Для навигации по вкладкам панели быстрого доступа используются кнопки прокрутки вправо/влево.

Для быстрого перехода к вкладке в тех случаях, когда на панели быстрого доступа открыто много вкладок, используется выпадающее меню, в котором содержится список всех вкладок узлов, которые пользователь открывал в текущем сеансе работы с Системой. Для вызова выпадающего меню необходимо щелкнуть мышью на кнопке  .

4.5. Настройки

С помощью данного элемента интерфейса можно выполнить следующие действия:

- Изменить настройки веб-интерфейса Системы;

- Просмотреть личные данные в Профиле;
- Получить справку;
- Выйти из Системы.

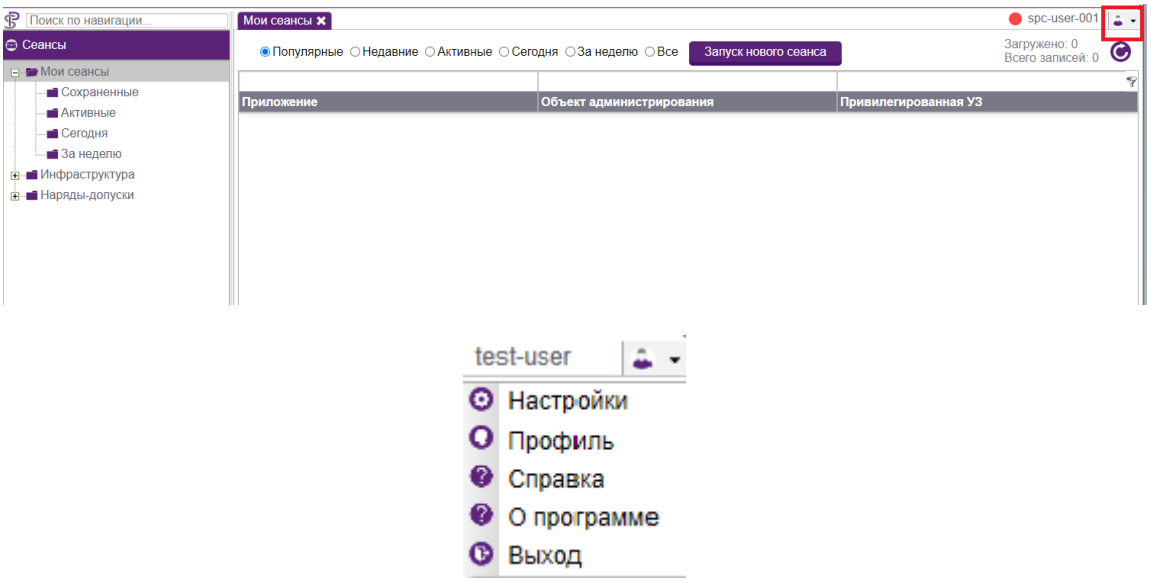


Рисунок 10. *Меню «Настройки»*

Изменение настроек Системы

С помощью этого меню можно изменить язык Системы, тему оформления и добавить двухфакторную аутентификацию. В качестве второго фактора аутентификации поддерживаются сертификаты RuToken и TOTP.

Для добавления двухфакторной аутентификации необходимо выбрать вкладку **Безопасность** в меню **Настройки**:

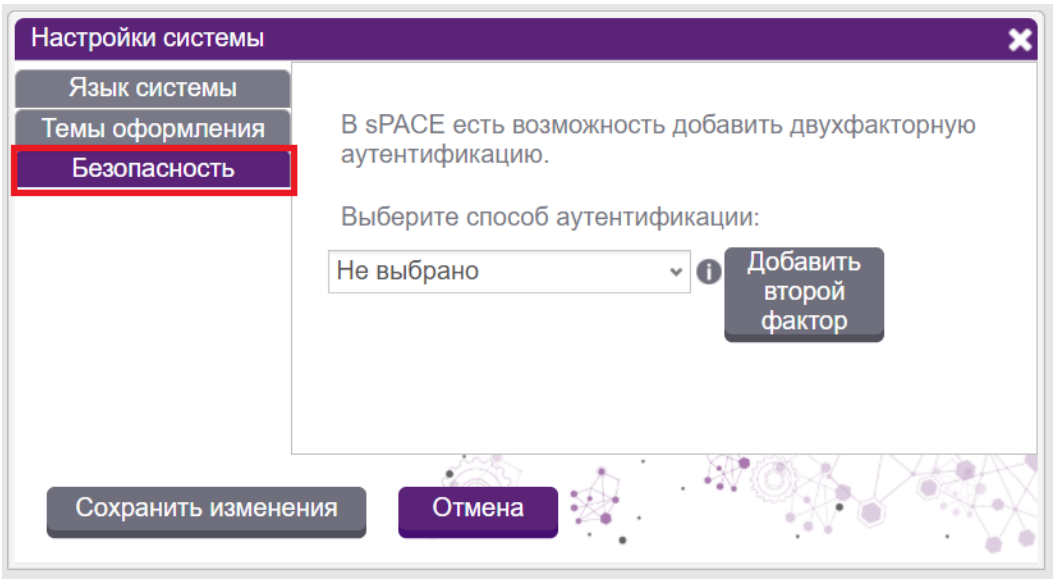


Рисунок 11. *Вкладка «Безопасность»*

Далее требуется определить желаемый способ двухфакторной аутентификации и нажать кнопку **Добавить второй фактор**. На данный момент sPACE поддерживает два метода:

- Rutoken – российская разработка, предоставляющая электронные идентификаторы и ключи, позволяющие авторизовать сотрудника при его подключении;
- TOTP – доступ к аккаунту пользователя осуществляется посредством сканирования QR-кода в специальном приложении для смартфона. В дальнейшем приложение постоянно генерирует одноразовый пароль для входа.

Для того, чтобы подключить Rutoken к аккаунту пользователя, требуется вставить его токен (например, флеш-карту) в компьютер и ввести PIN-код, уникальный для каждого токена. Затем нажмите на кнопку **Добавить сертификат Rutoken**. Пользователю будет нужно подключать токен каждый раз, когда он авторизуется а портале

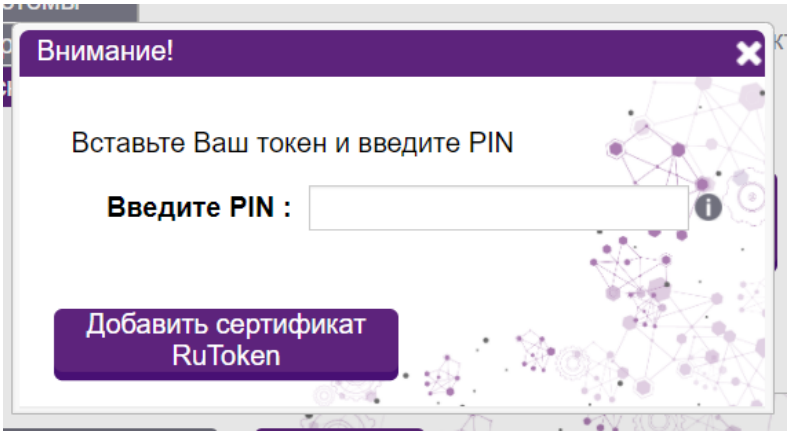


Рисунок 12. *Подключение Rutoken*

Для того, чтобы подключить TOTP к аккаунту пользователя, необходимо скачать на смартфон этого пользователя специальное приложение. Например, приложение Google Autheticator. В приложении надо выбрать функцию **Сканировать QR-код** и отсканировать код, который будет указан на портале. Приложение сгенерирует код, который требуется ввести в поле "Код" для подключения 2FA. Пользователь должен будет вводить код каждый раз при авторизации на портале. Затем нажать на кнопку **Подтвердить**.

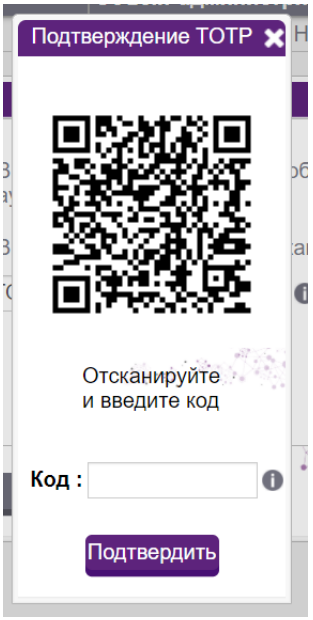


Рисунок 13. *Подключение TOTP*

Просмотр Профиля

Для просмотра личных данных необходимо выбрать пункт **Профиль** меню **Настройки**. В появившемся меню будут отображена следующая информация:

- Пользователь;
- Имя пользователя;
- Электронный адрес;
- Телефон;
- Мобильный телефон;
- Роль в Системе.

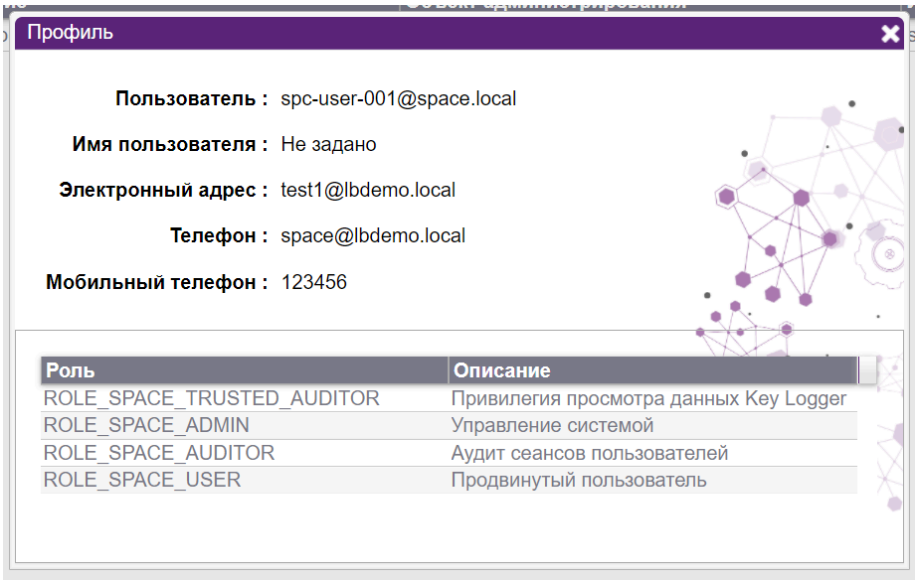


Рисунок 14. *Данные профиля пользователя*

Получение справки

Для получения справки необходимо щелкнуть на пункт **Справка** меню **Настройки системы**. Справочная информация откроется в отдельном окне веб-браузера.

Информация о программе

Для получения информации о программе необходимо кликнуть на пункте **О программе** в меню **Настройки системы**. Откроется окно, в котором содержится номер версии Системы, информация о продукте и производителе.

Выход из системы

Для выхода из Системы щелкните на пункте **Выход** меню **Настройки системы**.

5. ОПИСАНИЕ ОПЕРАЦИЙ

5.1. Вход в Систему

Для входа в Систему необходимо запустить на компьютере совместимый браузер (см. таблицу 2) и ввести в адресной строке адрес Портала Системы, предоставленный администратором.

Для авторизации в Системе необходимо ввести учетные данные пользователя. В первой строке вводится логин в формате тенант:пользователь@домен. Например: main:test-user-001@hq.company.local . Во втором поле вводится пароль пользователя.

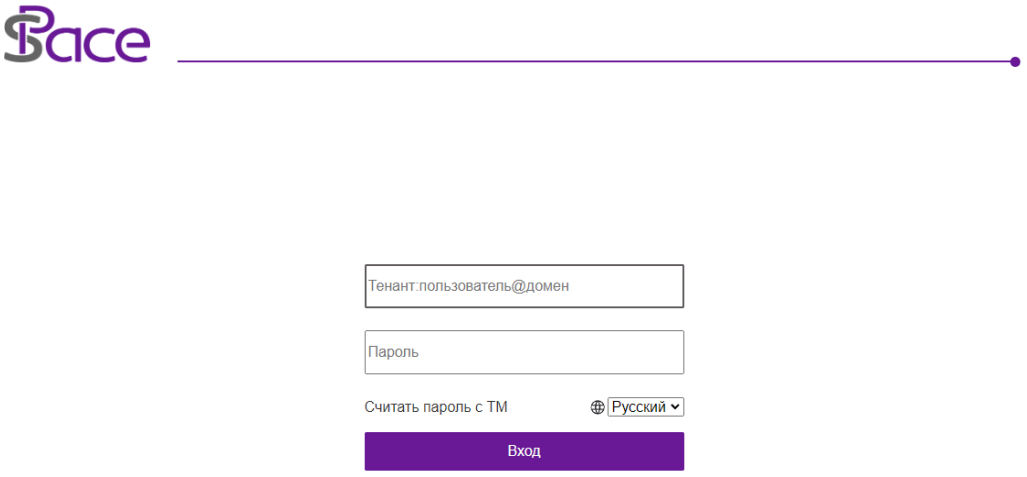


Рисунок 15. *Окно входа в Систему*

Примечание. Учетная запись пользователя должна быть заранее создана и добавлена в соответствующую группу службы каталогов MS Active Directory или же создана во внутреннем домене sPACE. В случае отсутствия учетной записи пользователя или неправильного ввода пароля на экране отобразится сообщение «Ошибка аутентификации».

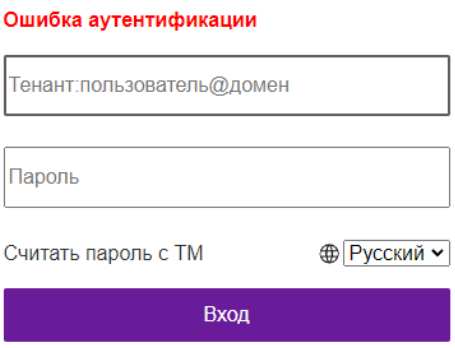


Рисунок 16. *Ошибка аутентификации*

После успешной авторизации на экране отображается главное окно Системы.

5.2. Работа с разделом «Сеансы»

Раздел «Сеансы» содержит в себе 3 основных узла: **Мои сеансы**, **Инфраструктура**, **Наряды-допуски**. Данный раздел позволяет выполнять следующие действия:

- просмотр своих сеансов привилегированного доступа (узел «Мои сеансы»);
- просмотр записей ВСАС своих сеансов привилегированного доступа (узел «Мои сеансы»);
- фильтрация своих сеансов привилегированного доступа (узел «Мои сеансы»);
- запуск нового сеанса привилегированного доступа (узел «Мои Сеансы»);
- просмотр задач на управление объектами администрирования, сгруппированные по объектам администрирования (узел «Инфраструктура»);
- просмотр своих нарядов-допусков (узел «Наряды-допуски»);
- запрос нового наряда-допуска для себя или для другого пользователя, если есть соответствующая роль (узел «Наряды-допуски»);
- согласование нарядов-допусков, если пользователь имеет соответствующую роль (узел «Наряды-допуски»).

Просмотр своих сеансов привилегированного доступа

Для просмотра сеансов привилегированного доступа необходимо щелкнуть на элементе **Мои сеансы** раздела **Сеансы** дерева навигации в левой части экрана. Это окно отображается по умолчанию после авторизации пользователя в Системе. Сеансы привилегированного доступа отображаются в виде таблицы.

Фильтрация своих сеансов привилегированного доступа

Сеансы пользователя могут быть отфильтрованы по следующим категориям:

- **Популярные** – популярные маршруты, сгруппированные по полям «Объект администрирования», «Учетная запись» и отсортированные по количеству запусков;
- **Недавние** – последние 50 сеансов, запущенных пользователем, по умолчанию также сгруппированы по имени объекта администрирования/приложения;
- **Активные** – сеансы, выполняемые в текущий момент;
- **Сегодня** – сеансы, созданные в день фильтрации;
- **За неделю** – сеансы, созданные за последнюю неделю;

- **Все** – все сеансы текущего пользователя.

Для отображения нужной категории сеансов необходимо установить переключатель в соответствующее положение на панели инструментов.

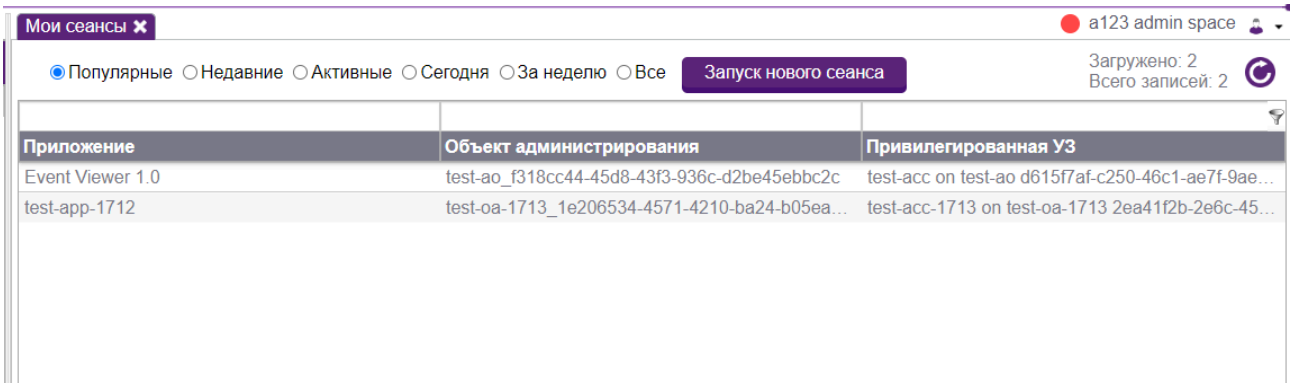


Рисунок 17. *Переключатель установлен на элементе «Популярные»*

Выбрать данные для отображения можно также с помощью элементов дерева навигации, выбрав один из пунктов:

- **Сохраненные;**
- **Активные;**
- **Сегодня**;
- **За неделю.**

Просмотр записей ВСАС своих сеансов привилегированного доступа

Для просмотра скриншотов записи своего сеанса требуется во вкладке **Мои сеансы** выбрать временной промежуток из доступных («Сегодня», «За неделю», «Все») и установить переключатель напротив него, либо выбрать временной промежуток с помощью элементов дерева навигации. После чего выбрать в списке нужный сеанс и нажать на его состояние.

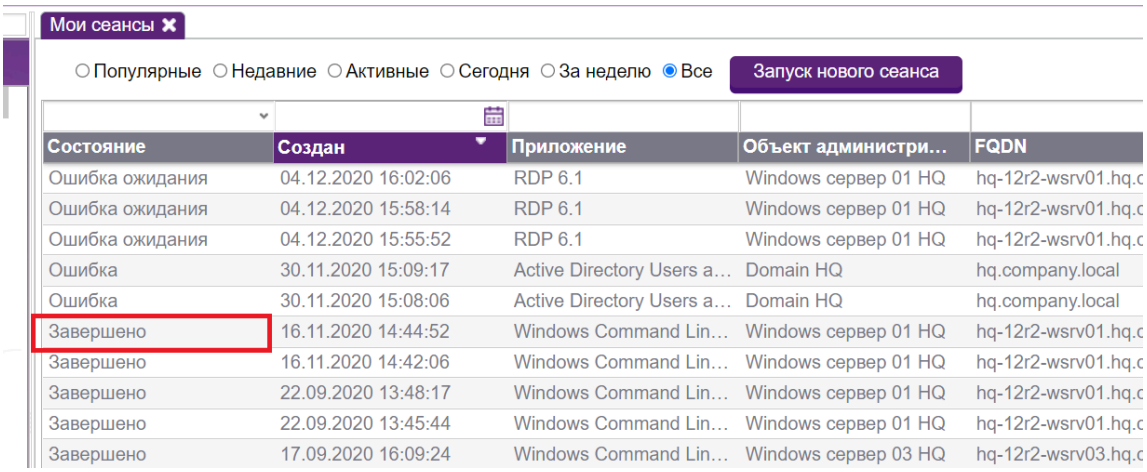


Рисунок 18. *Выбор сеанса для просмотра*

Откроется карточка сеанса, в которой можно посмотреть информацию о запущенном сеансе. Для просмотра записи требуется нажать на кнопку "Просмотр записи сеанса". Также

при необходимости можно скачать скриншоты сеанса, нажав на кнопку "Скачать изображения" (работает только для графических сеансов с подключением RDP).

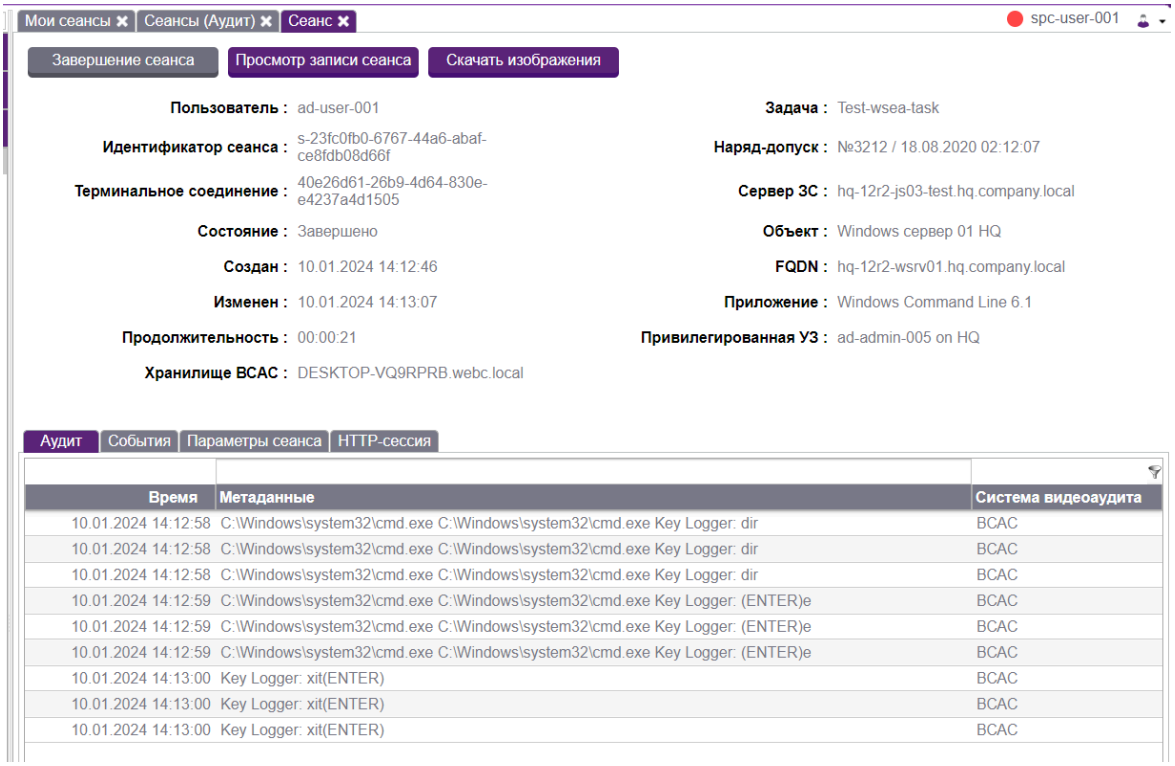


Рисунок 19. *Информация о сеансе*

Откроется окно плеера сеанса, в котором можно просматривать записанные скриншоты.

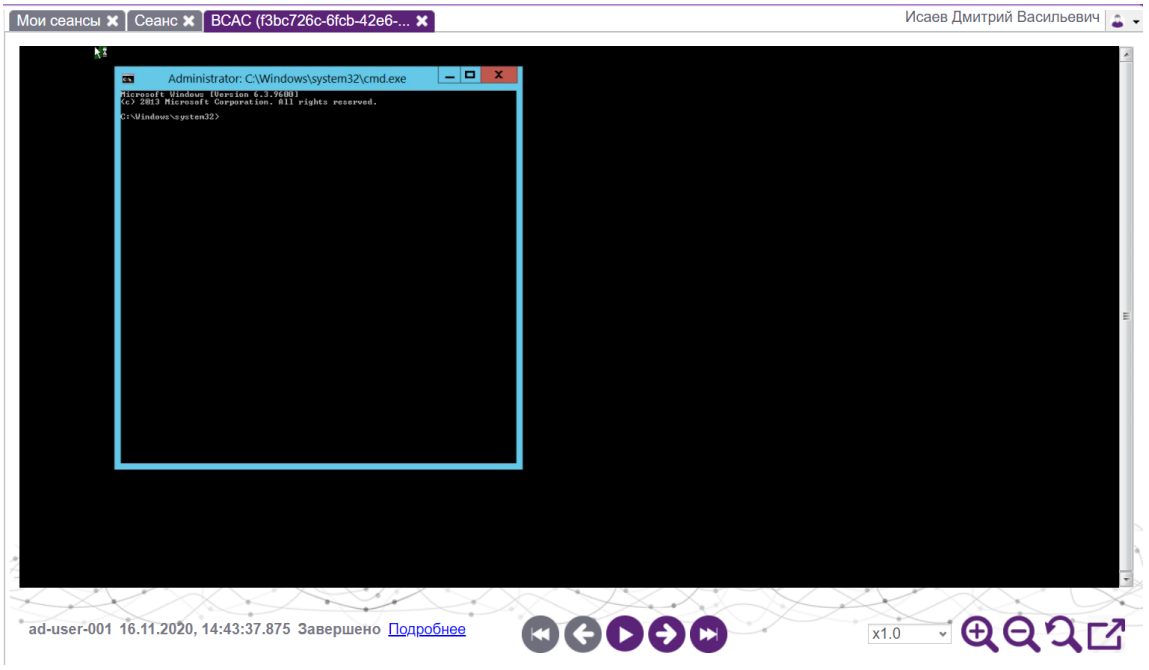


Рисунок 20. *Плеер сеанса*

При помощи кнопок под окном записанного сеанса можно осуществлять последовательную навигацию по записи: переместиться в ее начало, переместиться на

один кадр назад, начать проигрывание записи по порядку с момента, на котором она сейчас остановлена, переместиться на один кадр вперёд, переместиться в конец записи.

Рисунок 21. *Панель управления плеером*

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.

Рисунок 22. *Панель управления отображением скриншотов*

Примечание. В данный момент подробный плеер, описанный выше, доступен только в сеансах с графикой при типе подключения RDP. Если на сервере ЗС выбран тип подключения SSH и сеанс является текстовым, то плеер будет открываться в урезанном формате, только в виде последовательности скриншотов и без панели управления просмотром видеозаписи. Также для этих сессий настройка логирования пока недоступна, она является равной 3 сек.

5.3. Запуск нового сеанса привилегированного доступа

Для запуска нового сеанса необходимо щелкнуть на кнопке **Запуск нового сеанса** в верней части окна **Мои сеансы** и заполнить все поля в появившейся форме **Запуск сеанса**. Каждое поле становится доступным после заполнения предыдущего (пошаговые действия). Для завершения создания формы **Запуск сеанса** необходимо щелкнуть на кнопке **Запустить**, которая становится активной после заполнения всех полей формы.

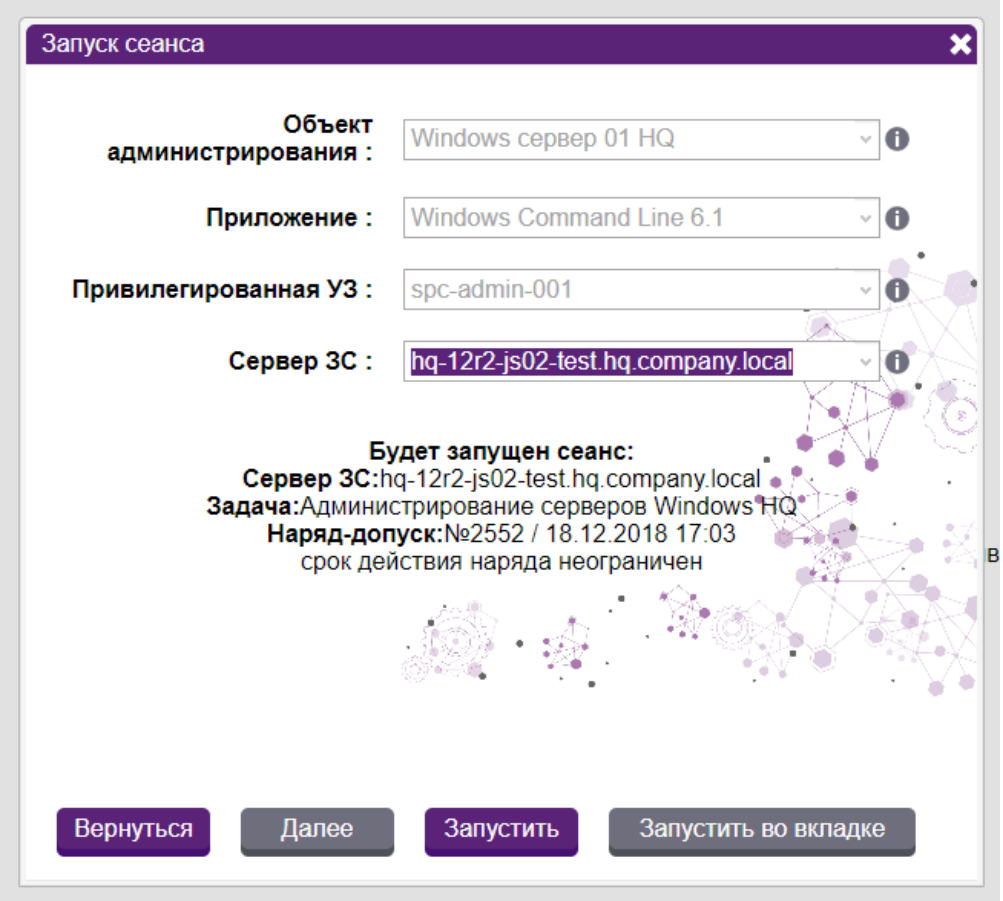


Рисунок 23. *Форма инициации сеанса привилегированного доступа*

Примечание. Для запуска нового сеанса сотрудникам необходимо иметь активные наряды-допуски. В поле **Объект администрирования** отображаются только те объекты администрирования, на управление которыми имеются активные наряды-допуски.

В зависимости от типа ОС рабочей машины пользователя и типа ОС сервера ЗС, на котором будет работать сеанс, процесс дальнейшего запуска немного отличается.

Если машина пользователя на **ОС Windows** и запускается сеанс с графикой (тип подключения RDP), то ему будет предложено скачать rdp-файл, после запуска которого запустится сеанс на удаленной машине. Это происходит независимо от того, к какому типу ОС принадлежит сервер ЗС: к Linux или к Windows.

Если машина пользователя на **ОС Linux** и запускается сеанс с графикой (тип подключения RDP), то ему будет предложена специальная строка, в которой содержится id сеанса. Нужно открыть любой текстовый редактор, скопировать туда следующую строку:

*xfreerdp /u: /cert-ignore /size:100% /v:**IP_АДРЕС_СЗС** /shell:"space_session **ID_СЕАНСА**"*

И подставить в нее нужные данные. Например:

*xfreerdp /u: /cert-ignore /size:100% /v:**192.168.74.195** /shell:"space_session **1625016a-e699-4b50-8243-c218e6b8b138**"*

ID сеанса необходимо скопировать из окошка на портале:

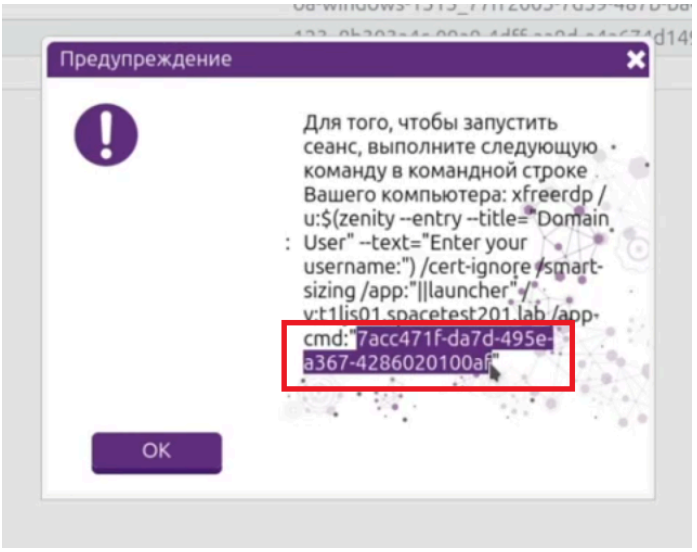


Рисунок 24. ID для запуска сеанса.

Далее полученную команду нужно ввести в Terminal на рабочей машине пользователя. После этого запустится сеанс на удаленном сервере ЗС, который принадлежит к ОС Windows или Linux.

Если машина пользователя на ОС Linux и запускается сеанс без графики (тип подключения SSH), то ему будет предложен ps1-файл. Внутри файла находится команда, которую нужно скопировать и запустить через Terminal.

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

Таблица 3. Связи между типами подключения, файлами подключения и операционными системами рабочих машин

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

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

5.4. Просмотр задач на управление объектами администрирования, сгруппированных по объектам администрирования

Для просмотра задач на управление объектами администрирования необходимо щелкнуть на элементе **Инфраструктура** раздела **Мои сеансы**.

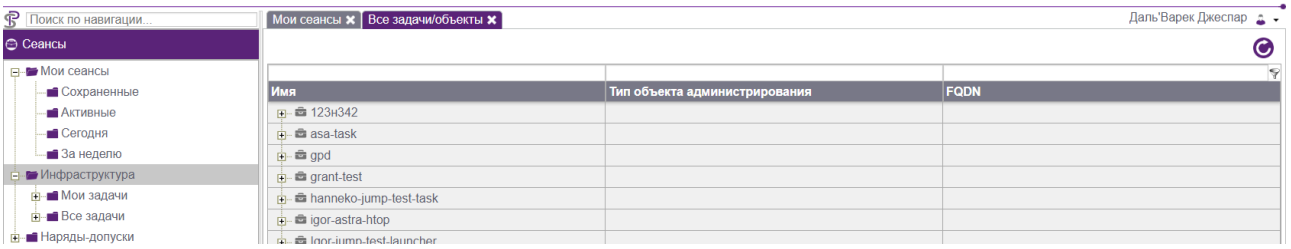


Рисунок 25. *Окно узла «Инфраструктура»*

В окне узла **Инфраструктура** отображаются все объекты инфраструктуры компании, в которых есть объекты администрирования, сгруппированные по задачам. В зависимости от роли пользователя в Системе пользователю доступен просмотр всех задач на управление объектами инфраструктуры, либо только своих задач на управление объектами инфраструктуры.

Дерево навигации узла **Инфраструктура** содержит один или два элемента в зависимости от роли пользователя в Системе:

- Мои задачи;
- Все задачи.

Для просмотра задач текущего пользователя, для которого есть активные наряды-допуски, необходимо щелкнуть на элементе **Мои задачи**. Для просмотра всех задач необходимо щелкнуть на элементе **Инфраструктура** или **Все задачи**.

Для просмотра объектов администрирования, сгруппированных в конкретную задачу, необходимо щелкнуть на названии задачи в дереве навигации или на панели данных.

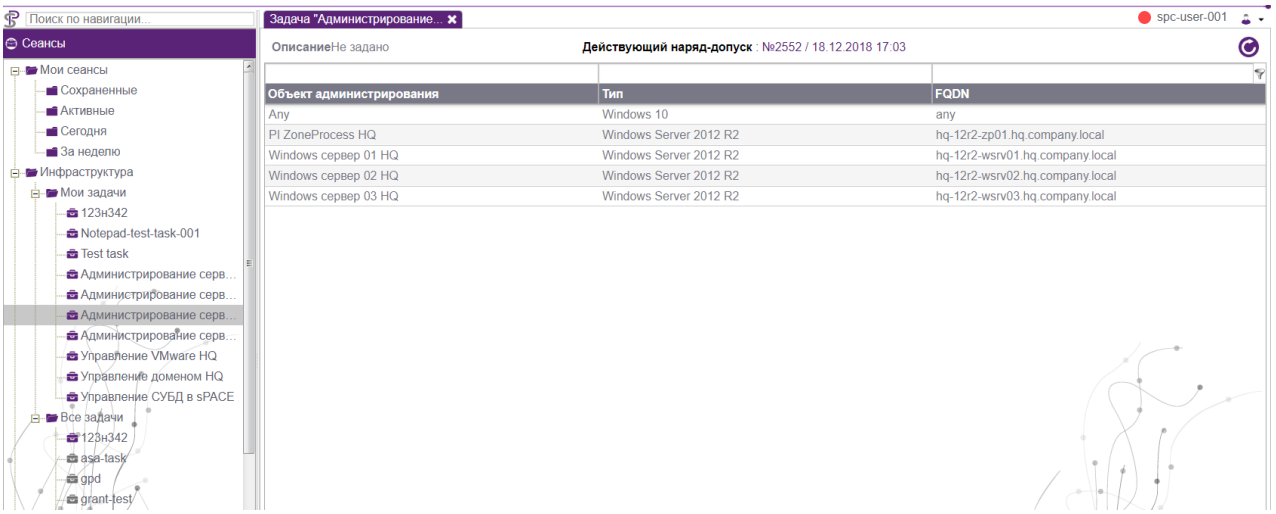


Рисунок 26. *Объекты администрирования, сгруппированные в задачу «Администрирование серверов»*

При двойном щелчке мышью на задаче откроется окно запуска сеанса привилегированного доступа.

Для получения информации о согласованном наряде-допуске для выполнения этой задачи необходимо щелкнуть левой кнопкой мыши на номере наряда-допуска.

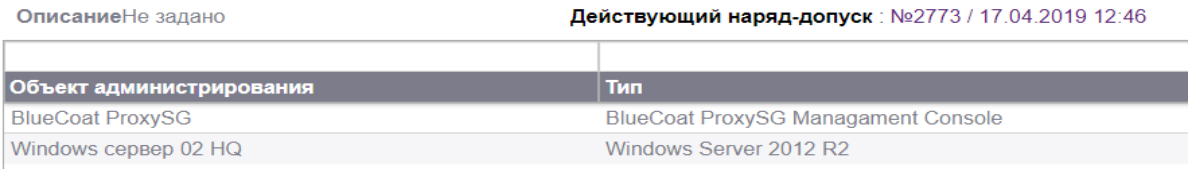


Рисунок 27. *В названии наряда-допуска содержится его номер, дата и время формирования*

5.5. Просмотр нарядов-допусков

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

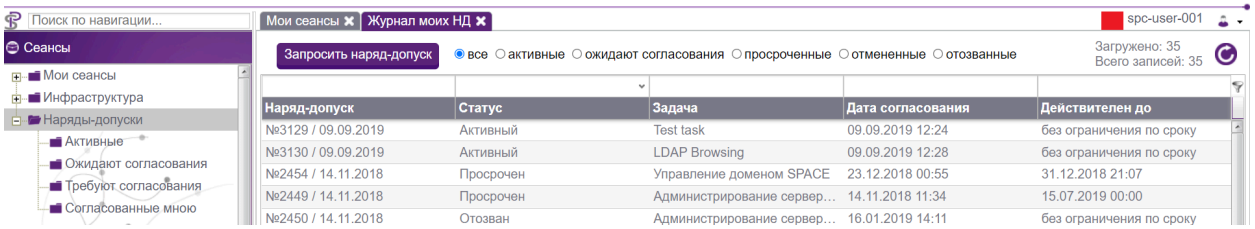


Рисунок 28. *Окно узла «Наряды-допуски»*

Для более удобной навигации по НД дерево навигации содержит в себе четыре подпункта в узле **Наряды-допуски**.

В дереве навигации узла **Наряды-допуски** наряды-допуски сгруппированы следующим образом:

- **Активные** – это согласованные наряды-допуски, срок действия которых не истек;
- **Ожидают согласования** – созданные, но не согласованные наряды-допуски;
- **Требуют согласования** – наряды-допуски, которые должен согласовать пользователь (если он входит в группу согласования нарядов-допусков на управление объектом администрирования);
- **Согласованные мною** – наряды-допуски, которые согласовал данный пользователь (если он входит в группу согласования нарядов-допусков на управление объектом администрирования).

Панель данных этого узла имеет вид таблицы со следующими столбцами.

- **Наряд допуск** – номер наряда-допуска и дата создания;
- **Статус** – наряд-допуск может быть активным, отмененным, отозванным, просроченным, отозванным и ожидать согласования;
- **Задача** – название задачи содержит название объекта администрирования;
- **Дата согласования** – отображается дата согласования или статус «отменен»;
- **Действителен до** – отображается дата окончания срока действия наряда-допуска. Если наряд-допуск был согласован как «бессрочный», то в этом поле указывается значение «без ограничения по сроку».

Отображение нарядов-допусков можно отфильтровать по следующим параметрам:

- **Все** – все наряды-допуски, в которых текущий пользователь указан в поле **Доступ для**;
- **Активные** – согласованные наряды-допуски, срок действия которых не истек;
- **Ожидают согласования** – созданные, но не согласованные наряды-допуски;
- **Просроченные** – наряды-допуски, у которых истек срок действия;

- **Отмененные** – наряды-допуски, которые были созданы и отменены до согласования;
- **Отозванные** – наряды-допуски, отмененные после согласования либо пользователем, либо администратором.

Запрос нового наряда-допуска

Запрос нового наряда-допуска можно осуществить двумя способами – при просмотре задач на управление объектами администрирования в узле **Инфраструктура** и с помощью функционала узла **Наряды-допуски**.

Для создания запроса на новый наряд-допуск с помощью функционала узла **Наряды-допуски** необходимо щелкнуть на кнопке **Запросить наряд-допуск** в верхней части журнала своих нарядов-допусков.

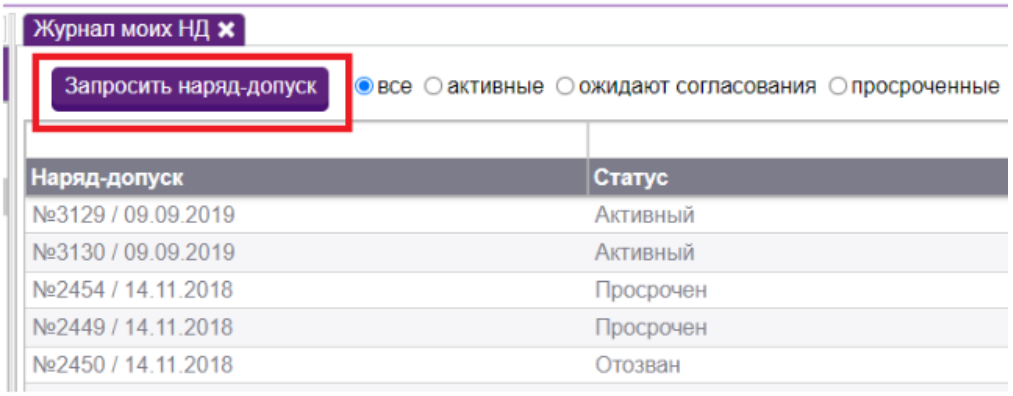


Рисунок 29. *Кнопка «Запросить наряд-допуск»*

Появившаяся форма **Создание наряда-допуска** содержит несколько полей. Поля, выделенные полужирным шрифтом в окне создания наряда-допуска, являются обязательными для заполнения.

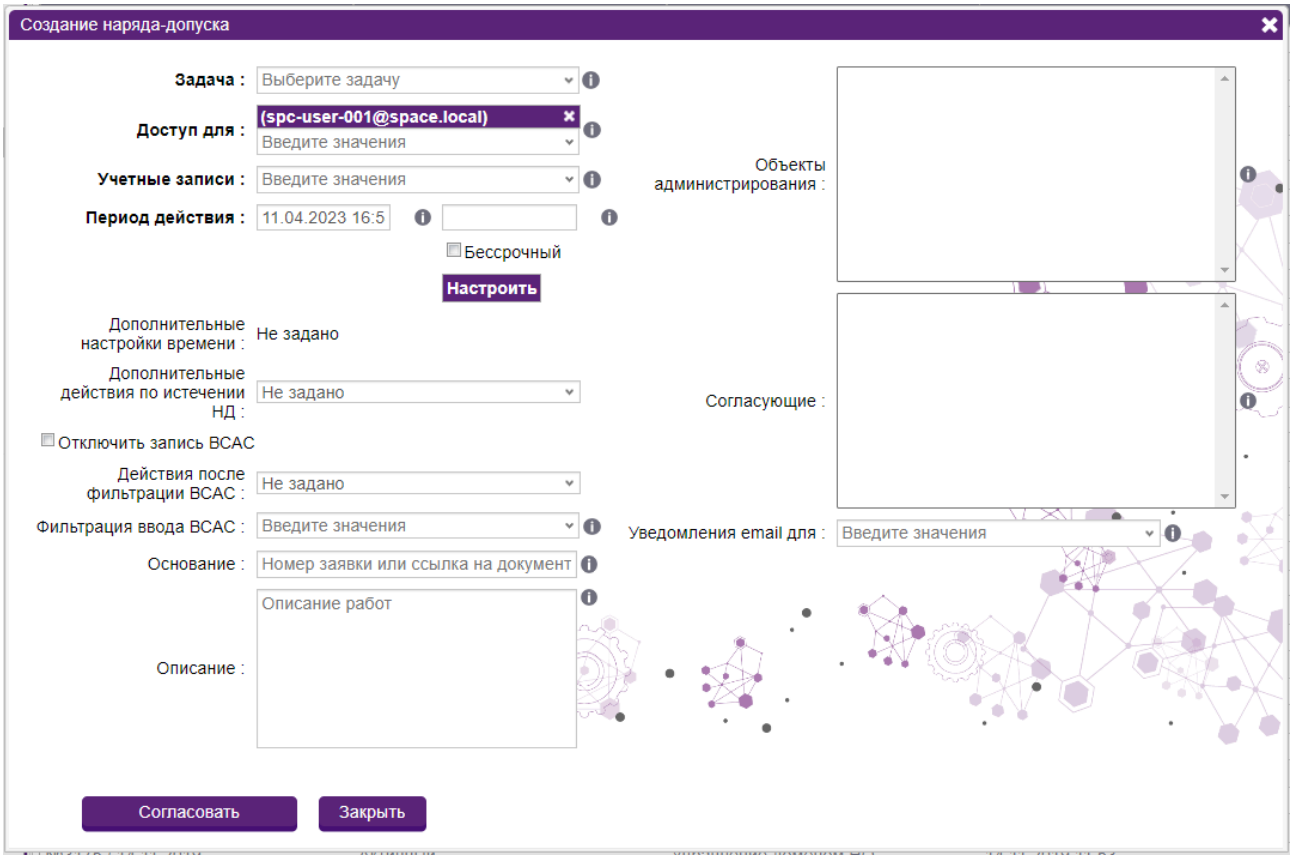


Рисунок 30. *Форма «Создание наряда-допуска»*

Форма **Создание наряда-допуска** содержит следующие поля:

- **Задача** (обязательное поле) – тип задачи, в рамках которой будет осуществляться деятельность в системе;
- **Доступ для** (обязательное поле) – список учетных записей пользователей, для которых требуется предоставить доступ;
- **Учетные записи** (обязательное поле) – список логинов привилегированных учетных записей, для которых требуется предоставить доступ;
- **Период действия** (обязательное поле) – временной интервал, в течение которого будут выполняться работы по запрашиваемому наряду-допуску. Можно поставить галочку и сделать его бессрочным;
- **Дополнительные настройки времени** – при нажатии на кнопку "Настроить" можно задать временные промежутки, в соответствии с которыми данный наряд-допуск будет активен во время недели. Данная настройка не является обязательной, в случае её отсутствия наряд-допуск будет доступен во все дни недели в течение заданного периода;

- **Дополнительные действия по истечении НД** – настроить действия, если в тот момент, когда срок действия наряда-допуска подойдет к концу, будут запущенные сеансы;
- **Отключить запись ВСАС** – действия, производимые в рамках данного сеанса, не будут записываться, в дальнейшем нельзя будет посмотреть их метаданные и скриншоты;
- **Действия после фильтрации ВСАС** – выбор действий, которые будут происходить в том случае, если фильтрация ввода ВСАС найдет какие-либо нарушения;
- **Фильтрация ввода ВСАС** – выбор настраиваемой модели фильтрации ввода ВСАС;
- **Основание** – вид документа, служащий основанием для осуществления запроса наряда допуска;
- **Описание** – описание проводимых типов работ в рамках наряда-допуска;
- **Объекты администрирования** – объекты, с которыми будут проводиться работы в рамках наряда-допуска;
- **Согласующие** – определенная группа пользователей, которые имеют право согласовать задачу;
- **Уведомления email для** – возможность получения уведомлений на e-mail уполномоченным лицом при запуске этого сеанса.

После заполнения всех необходимых полей и нажатия кнопки **Согласовать** новый наряд-допуск будет добавлен в очередь на согласование пользователям, которые входят в группу согласования нарядов-допусков к данному объекту администрирования.

Для запроса нового наряда-допуска с помощью функционала узла **Инфраструктура** необходимо кликнуть мышью на задаче, чтобы получить разрешение на её выполнения. В появившейся форме **Создание наряда-допуска** необходимо заполнить поля, как описано выше.