

**ООО «ВЭБ КОНТРОЛ ДК»**



**sPACE**

**СИСТЕМА УПРАВЛЕНИЯ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ  
SPACE RAM**

ВЕРСИЯ 2.0.2

**КРАТКОЕ РУКОВОДСТВО ДЛЯ ПЕРВИЧНОЙ НАСТРОЙКИ**

**Москва, 2025**

## СОДЕРЖАНИЕ

<b>Об этом документе.....</b>	<b>2</b>
<b>Термины, определения, используемые сокращения.....</b>	<b>4</b>
<b>1. Настройка домена.....</b>	<b>5</b>
1.1. Добавление домена в Систему.....	5
1.2. Настройка групп пользователей.....	8
1.3. Добавление доменных пользователей в Систему.....	10
<b>2. Настройка приложений.....</b>	<b>11</b>
2.1. Настройка сценариев.....	12
2.2. Настройка списков приложений.....	13
<b>3. Создание групп согласования.....</b>	<b>14</b>
<b>4. Добавление привилегированных учетных записей.....</b>	<b>16</b>
<b>5. Создание объектов администрирования.....</b>	<b>19</b>
<b>6. Создание задачи.....</b>	<b>22</b>
<b>7. Наряды-допуски.....</b>	<b>24</b>
7.1. Создать наряд-допуск.....	24
7.2. Согласовать запрошенный наряд-допуск.....	27
<b>8. Настроить внутренний видеоаудит ВСАС.....</b>	<b>29</b>
<b>9. Запуск задачи.....</b>	<b>30</b>
9.1. Запуск задачи на СЗС Windows.....	31
9.2. Запуск задачи на СЗС Linux через SSH.....	33
9.3. Запуск задачи на СЗС Linux через RDP.....	35
<b>10. Проверка функционала аудитора.....</b>	<b>37</b>
10.1. Наблюдение за сеансом в режиме реального времени.....	38
10.2. Управление сессиями.....	40
10.3. Работа с завершенной сессией.....	42

## Об этом документе

Этот документ является кратким руководством для первичной настройки Системы управления привилегированным доступом sPACE RAM (далее Система, «программа», «программный продукт»).

Документ включает в себя главы с пошаговыми инструкциями и пояснениями по основным настройкам функционала Системы.

Документ адресован специалистам, отвечающим за проведение пилотных проектов, внедрение Системы в рабочий процесс, обеспечение работоспособности и настройку Системы.

## Термины, определения, используемые сокращения.

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

# 1. Настройка домена

Залогиньтесь в веб-интерфейсе Системы под пользователем admin.

*Примечание:* Если использовать домен не планируется, переходите к следующему пункту «Настройка приложений».

## 1.1. Добавление домена в Систему

1. Для добавления домена перейдите в раздел «**Управление системой**» > «**Домены**».

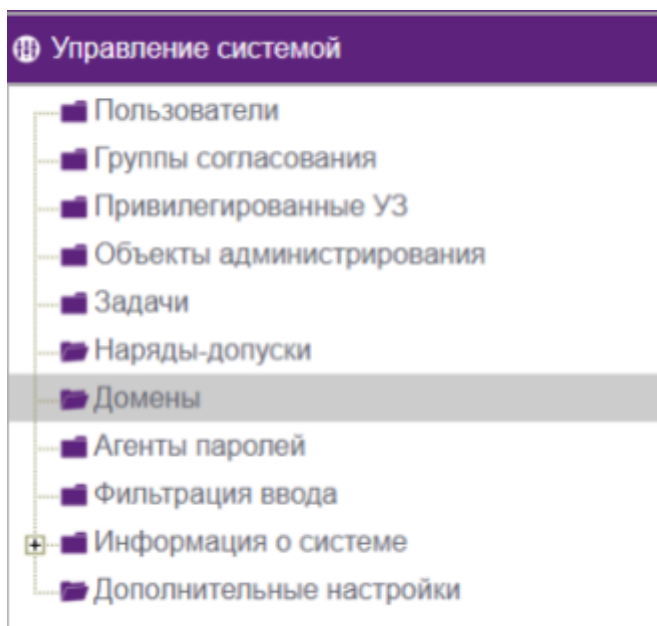


Рис. 1.1. Раздел «Домены»

2. Оказавшись в разделе «**Домены**», нажмите на кнопку «**Добавить**» в верхней панели. Введите полное имя домена, нажмите «**Сохранить**».

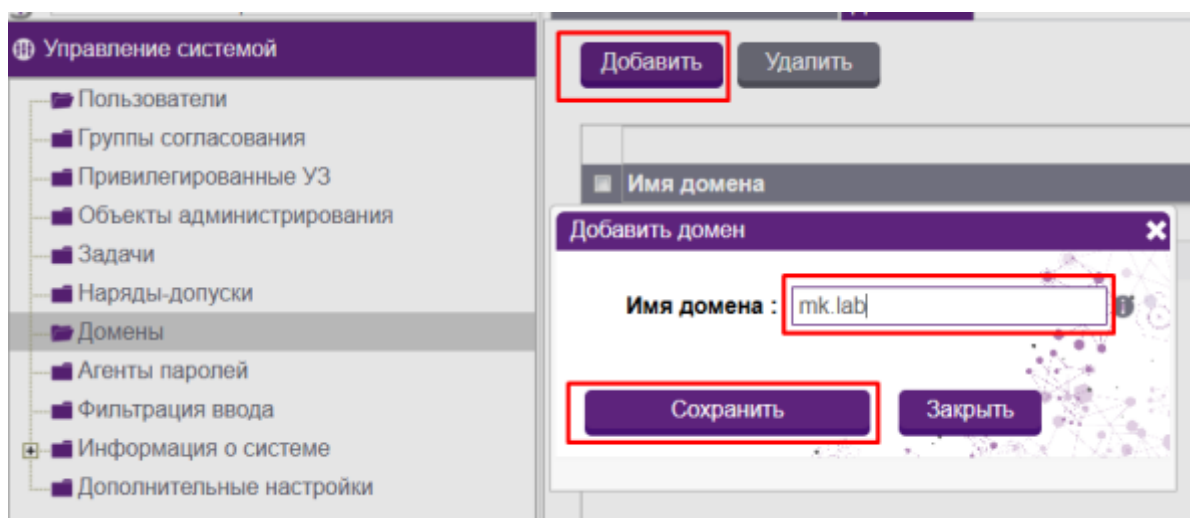


Рис. 1.2. Добавление домена в систему

3. Выберите созданный домен, чтобы отредактировать настройки. В открывшемся окне нажмите «**Настроить LDAP конфигурацию**». Заполните поля по образцу на рисунке.

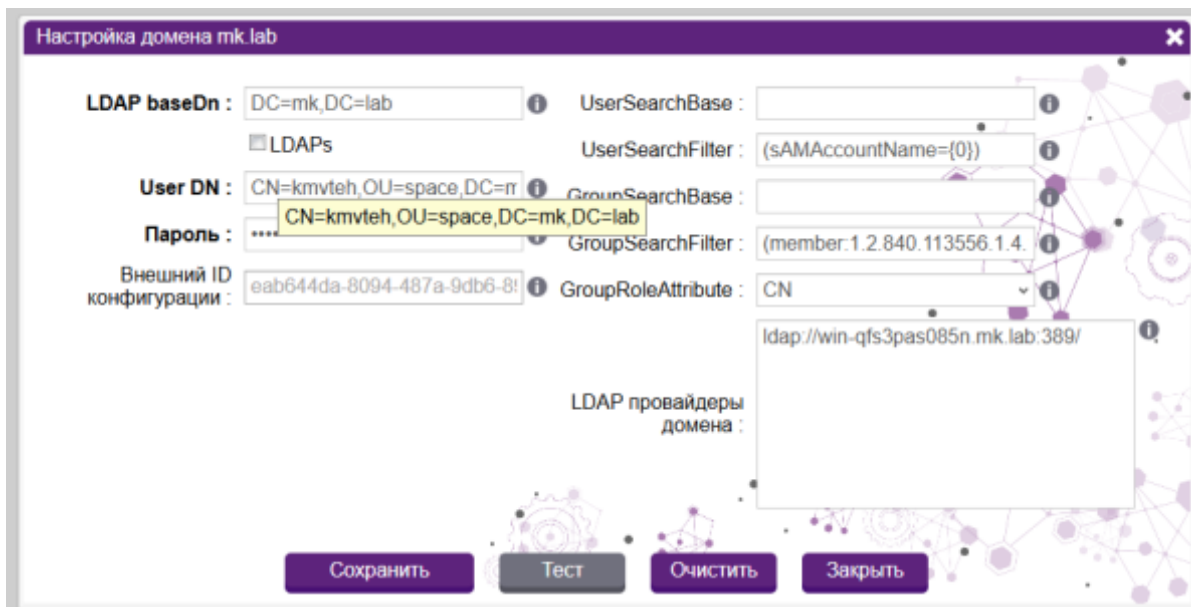


Рис. 1.3. Пример заполнения карточки домена

Примечания: Для настройки подключения к домену (Microsoft AD или другой LDAP каталог) потребуется учетная запись, у которой совпадают поля CN и PN, (пример на рис. 4);

```
PS C:\Users\administrator.SPACEDEMO> Get-AdUser ad-search-user

DistinguishedName : CN=ad-search-user,OU=Users,OU=SPACE,DC=spacedemo,DC=lab
Enabled           : True
GivenName        : ad-search-user
Name             : ad-search-user
ObjectClass      : user
ObjectGUID       : 6123307c-a3e2-40f0-b2c1-726bd49c2456
SamAccountName   : ad-search-user
SID              : S-1-5-21-3480449795-908008138-902860178-1112
Surname          :
UserPrincipalName : ad-search-user@spacedemo.lab
```

Рис. 1.4. Пример проверки идентичности CN и PN

Рекомендуем создать отдельную учетную запись, специально для связи Системы с доменом. Эта учетная запись будет использоваться постоянно, если пароль от неё меняется - в настройках Системы пароль также должен быть изменен на новый.

Пароль от этой учетки не должен содержать следующие специальные символы:

- «/» - воспринимается как разделитель;
- «.» - воспринимается как окончание ввода строки;

Строки «UserSearchBase» и «GroupSearchBase» изначально пустые. Если их не заполнить - поиск будет осуществляться по всему домену. Зону поиска можно ограничить, указав в данных полях OU, соответствующую расположению используемых групп и пользователей;

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

Выберите в строке «**GroupRoleAttribute**» настройку sAMAccountName или CN, sAMAccountName подходит для старых версий типа WinServer 2008-2012, для более современных - CN;

При заполнении поля «LDAP провайдеры домена» можно указать имя домена, IP-адрес, имена контроллеров доменов либо имя одного из контроллеров, если планируется использовать только один из пула. Также при подключении можно использовать облегченный протокол LDAP - подключение по 389 порту, либо защищенную версию LDAPS (LDAP over SSL) - подключение по 636 порту. В случае использования протокола LDAPS убедитесь, что отмечен соответствующий чекбокс (пример на рис. 1.5).

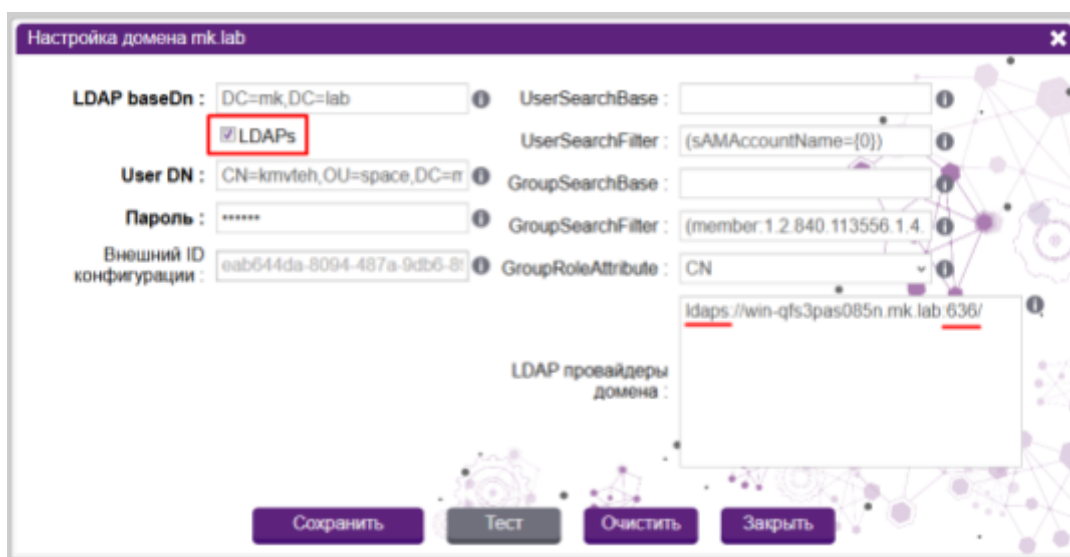


Рис. 1.5. Пример заполнения полей с использованием протокола LDAPS

4. После заполнения нажмите на кнопку «**Сохранить**». Нажатие на кнопку Тест позволяет узнать, являются ли введенные данные верными. Если все

правильно, система выдаст оповещение «**Конфигурация LDAP корректна**», а в статусе домена «Активен» будет отмечен галочкой чекбок.

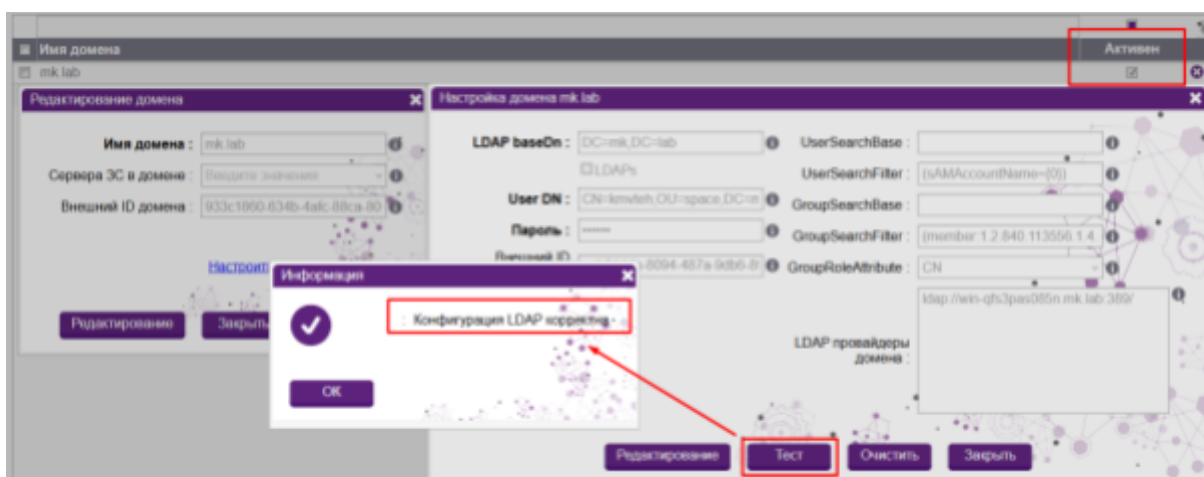


Рис. 1.6. Результат успешного теста

5. В случае обнаружения ошибок домен будет переведён в неактивные, а результат теста укажет, в чем заключается обнаруженная ошибка. Комментарии к распространенным ошибкам можно найти на портале <https://webcontrol.aspro.cloud/hc/3> в разделе «Ошибки при подключении домена».

Подробнее о работе с доменами можно прочитать в Руководстве администратора, раздел 5.7 «Управление доменами».

## 1.2. Настройка групп пользователей

1. Для настройки ролей для доменных групп пользователей перейдите в раздел «**Управление ресурсами**» > «**Пользовательские роли**».

Эта вкладка позволяет настроить пользовательские роли. Можно создать как полностью новую роль (персональную), параметры которой задаёт Технический администратор, так и изменить названия существующих ролей системы sPACE в Active Directory Users and Computers. Каждая группа (включая персональные) должна существовать в Active Directory Users and Computers.



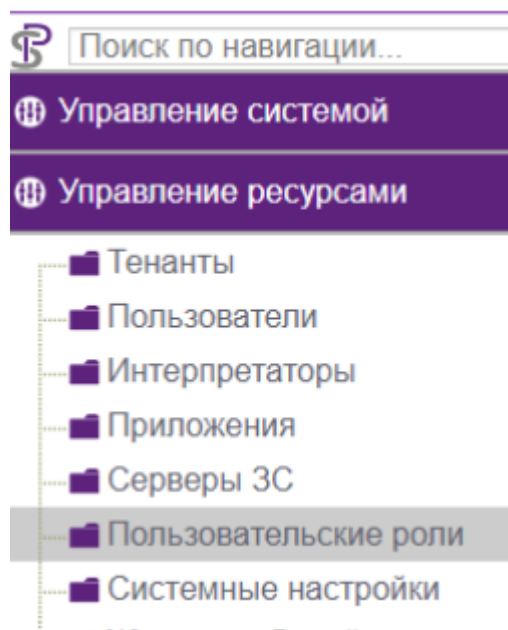


Рис. 1.7. Раздел Пользовательские роли

2. Задать доменной группе пользователей роль в Системе можно двумя путями:

2.1. Создайте в своем домене группы, которые используются системой по умолчанию, и добавьте в них соответствующих пользователей. Список с описанием функционала и названием для доменных групп можно найти в «Руководстве администратора» в разделе 3.5.2 «Перечень функционала, доступного для каждой роли».

В этом случае можно назначать пользователю несколько ролей путем добавления его в соответствующие группы;

 SPACE_ADMINS	Security Group - Global
 SPACE_AUDITORS	Security Group - Global
 SPACE_RESTRICTEDUSERS	Security Group - Global
 SPACE_STANDARDUSERS	Security Group - Global
 SPACE_SUPERADMINS	Security Group - Global
 SPACE_TRUSTED_AUDITORS	Security Group - Global
 SPACE_USERS	Security Group - Global

Рис. 1.8. Группы по умолчанию для домена

2.2. Укажите доменное имя группы для каждой роли. Для этого снимите чекбокс с параметра «**Использовать значение по умолчанию**», впишите доменное имя группы напротив каждой роли. Нажмите «**Сохранить роли**». Система выдаст предупреждение, сохранит изменения, произведет разлогинивание и предложит заново ввести учетные данные для аутентификации.

Таким образом пользователи из уже существующих доменных групп получат соответствующие права в Системе.

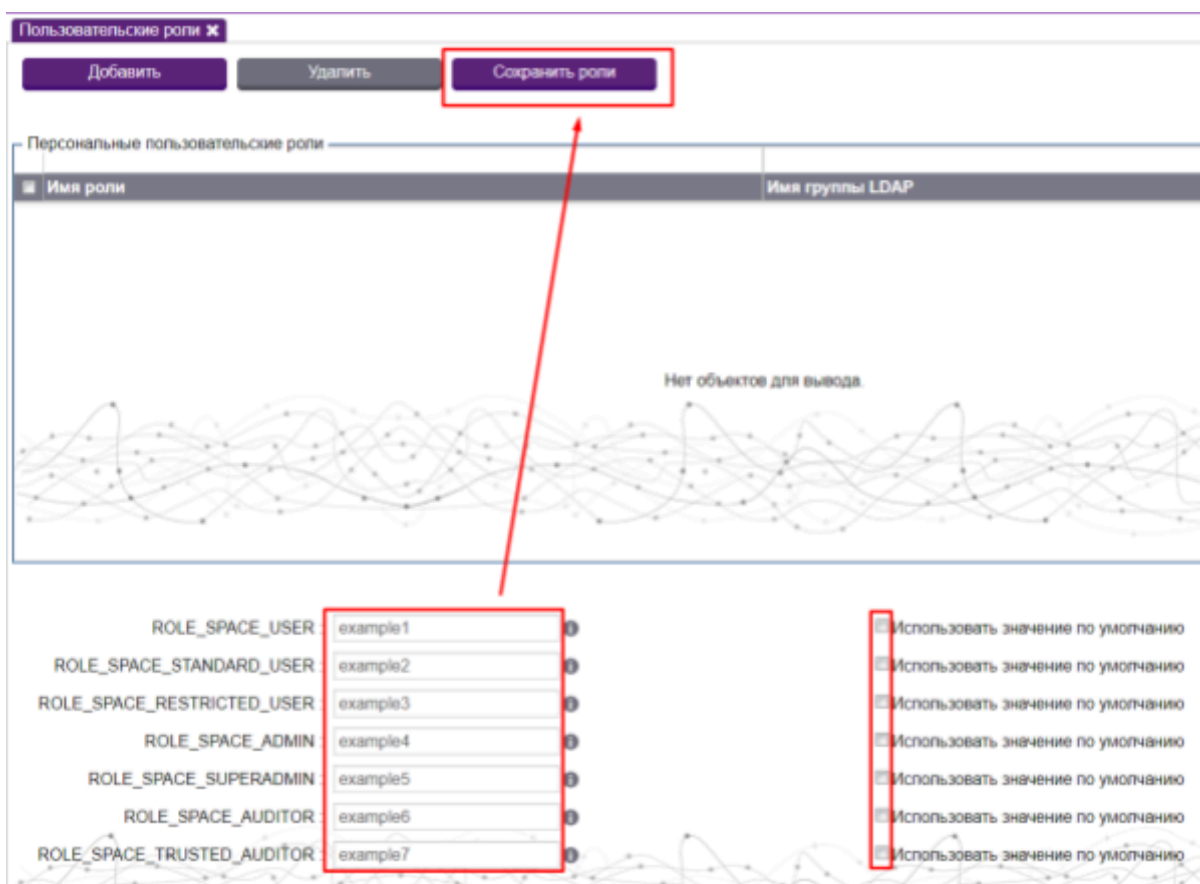


Рис. 1.9. Таблица Пользовательские роли

3. Чтобы добавить новую пользовательскую роль нажмите **«Добавить»** в верхней части вкладки. В открывшейся форме заполните все поля, выберите необходимые роли и нажмите **«Сохранить»**. Система сохранит изменения, произведет разлогинивание и предложит заново ввести учетные данные для аутентификации. Таким образом можно назначать пользователям, состоящим в указанной группе, несколько ролей. Также можно назначать роли пользователям из разных доменов.

Каждый пользователь, имеющий одну из трех ролей «user», должен иметь право доступа к джамп-серверу с использованием протокола mstsc.

### 1.3. Добавление доменных пользователей в Систему

1. Для добавления пользователя из домена перейдите в раздел **«Управление системой» > «Пользователи»**.

2. Нажмите на кнопку **«Добавить»**, откроется окно с формой добавления нового пользователя. Обязательно заполните поля, выделенные

полужирным шрифтом: **Имя пользователя** (в соответствии с доменным именем), **Домен** (выберите только что созданный). В случае добавления доменных пользователей роль выбрать нельзя, она будет присвоена пользователю в соответствии с тем, в какой доменной группе он состоит. Нажмите «**Сохранить**».

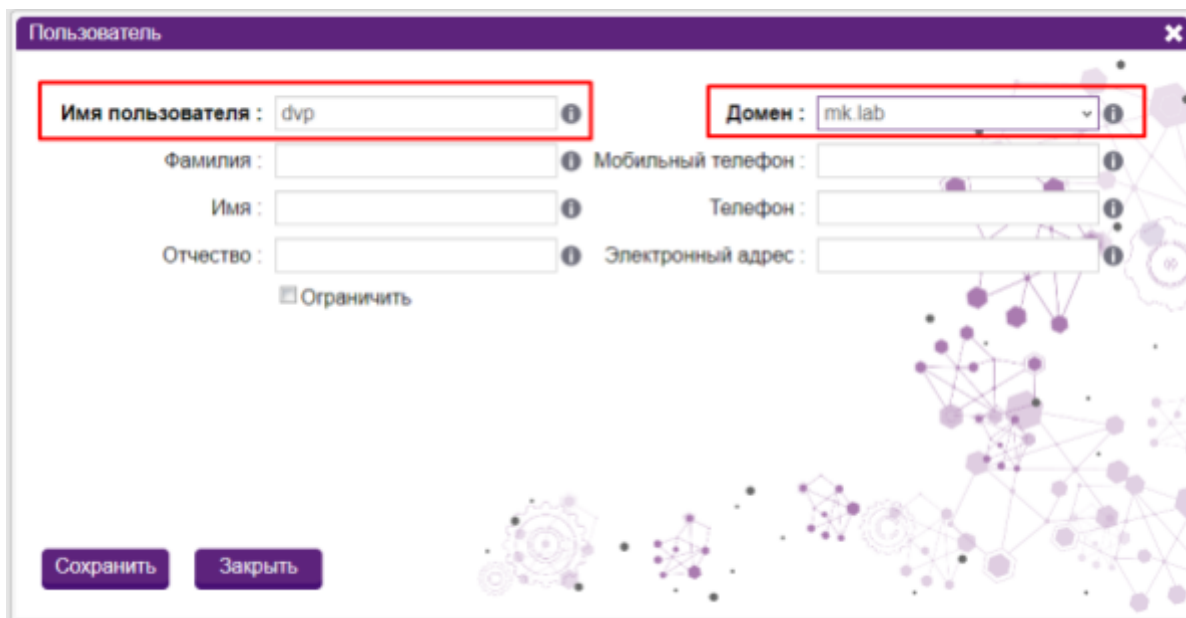


Рис. 1.10. Пример заполнения карточки доменного пользователя

3. Также пользователь домена может залогиниться в систему сразу после настройки домена и доменных групп. В этом случае его учетная запись будет автоматически создана в Системе.

## 2. Настройка приложений

Для настройки приложений перейдите в раздел «**Управление ресурсами**» > «**Приложения**».

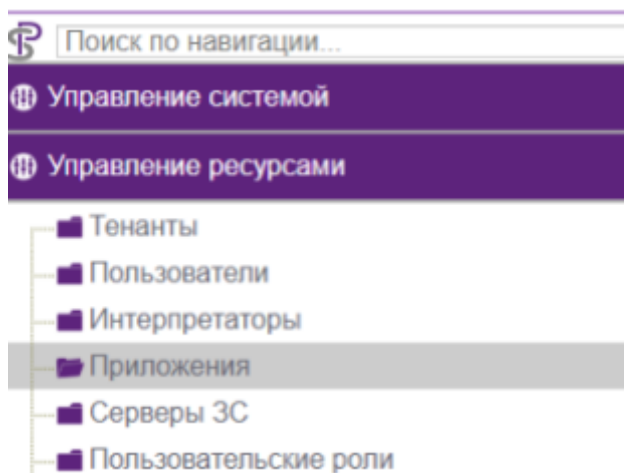
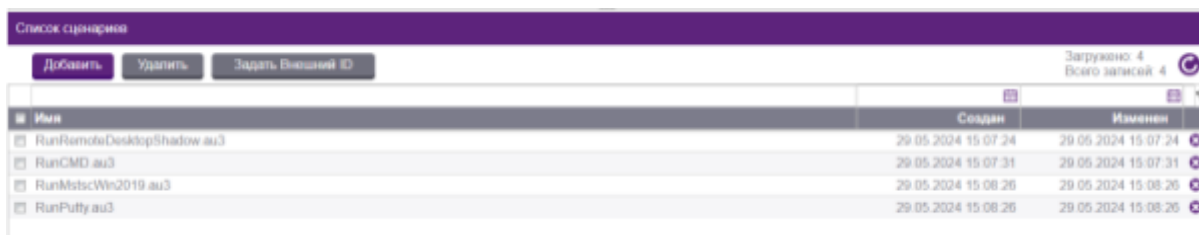


Рис. 2.1. Раздел Приложения

Окно раздела «**Приложения**» содержит две таблицы: Список приложений и Список сценариев.

## 2.1. Настройка сценариев

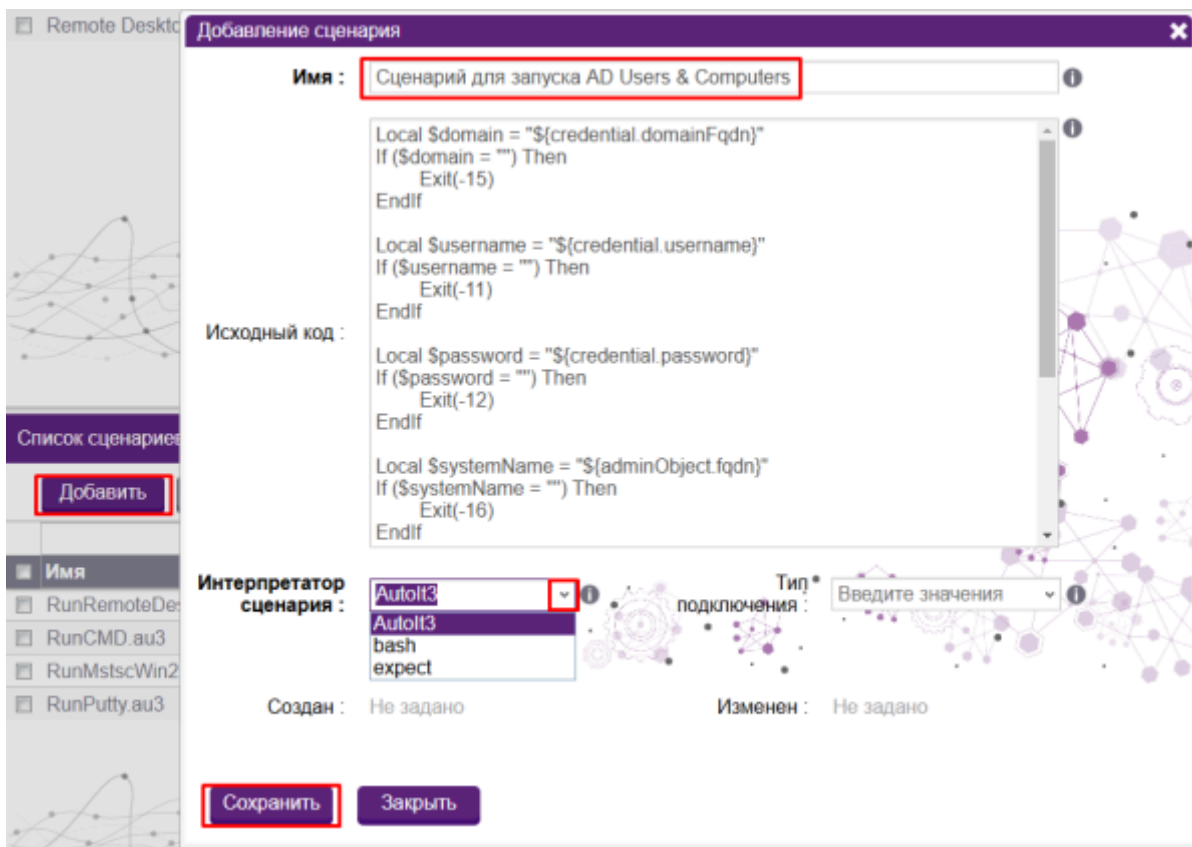
Изначально в систему заложены 4 готовых сценария.



Имя	Создан	Изменен
RunRemoteDesktopShadow.au3	29.05.2024 15:07:24	29.05.2024 15:07:24
RunCMD.au3	29.05.2024 15:07:31	29.05.2024 15:07:31
RunMstscWin2019.au3	29.05.2024 15:08:26	29.05.2024 15:08:26
RunPutty.au3	29.05.2024 15:08:26	29.05.2024 15:08:26

Рис. 2.2. Список сценариев

По мере необходимости сценарии можно добавлять. Чтобы добавить новый сценарий нажмите на кнопку **«Добавить»**, откроется окно с формой добавления нового сценария. Задайте сценарию понятное название, напечатайте или скопируйте текст. Выберите интерпретатор сценария в соответствии с тем, на каком языке написан сценарий. Укажите тип подключения сценария, если для его запуска планируется использовать СЗС с несколькими типами (например, RDP и SSH одновременно). Нажмите **«Сохранить»**.



Имя : Сценарий для запуска AD Users & Computers

```
Local $domain = "${credential.domainFqdn}"
If ($domain = "") Then
    Exit(-15)
EndIf

Local $username = "${credential.username}"
If ($username = "") Then
    Exit(-11)
EndIf

Local $password = "${credential.password}"
If ($password = "") Then
    Exit(-12)
EndIf

Local $systemName = "${adminObject.fqdn}"
If ($systemName = "") Then
    Exit(-16)
EndIf
```

Исходный код :

Интерпретатор сценария : AutoIt3

Тип подключения : Введите значения

Создан : Не задано      Изменен : Не задано

Сохранить      Закреть

Рис. 2.3. Окно добавления сценария

Обратите внимание - в сценариях на языке AutoIt содержится путь запуска приложения. Это тот путь, по которому программа располагается на СЗС Windows. Сравните расположение и замените его на тот, по которому программа

установлена на 3С Windows, если он отличается от указанного. Для этого нажмите кнопку **«Редактировать»**, отредактируйте настройку «Local \$programToLaunch» и нажмите **«Сохранить»**.

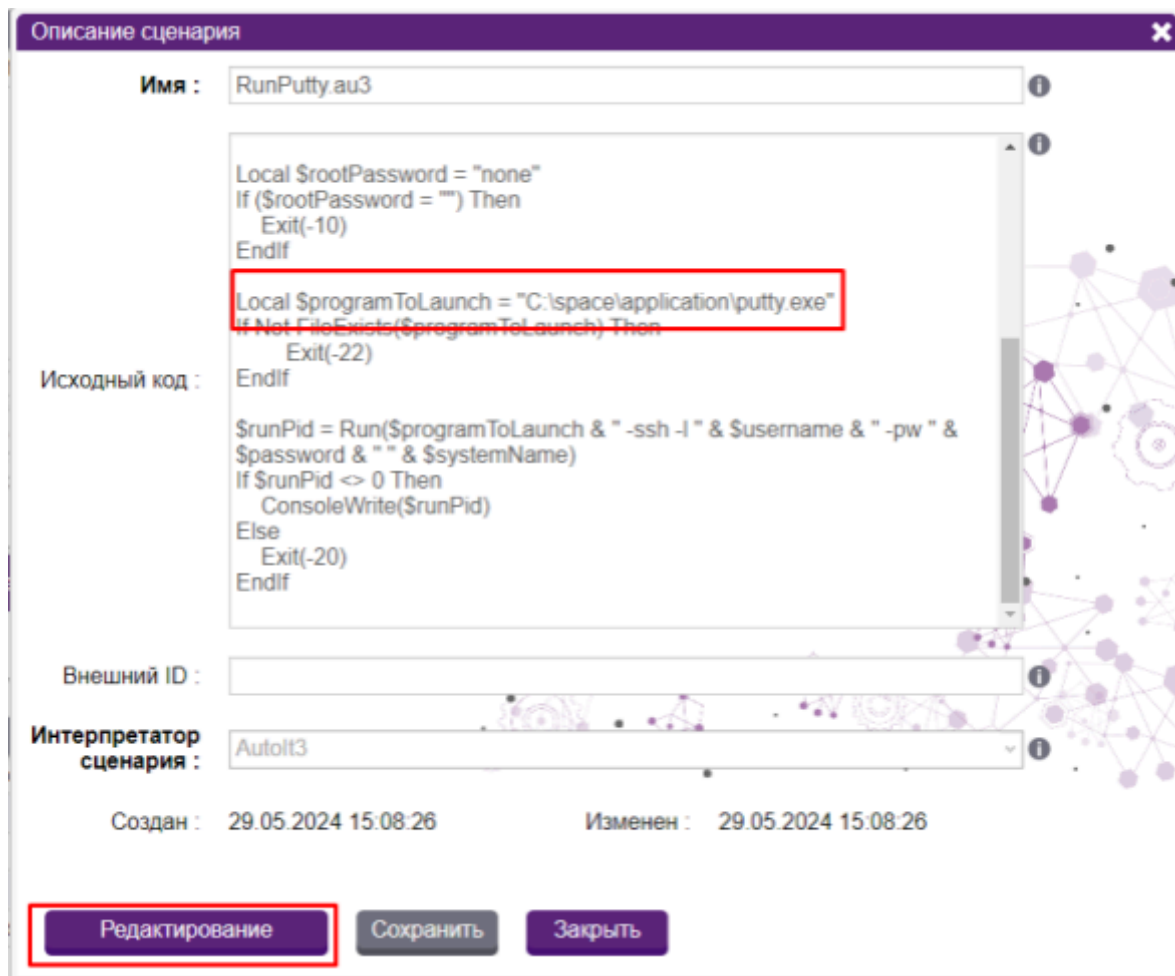


Рис. 2.4. Редактирование пути запуска приложения

После добавления всех нужных сценариев можно переходить к созданию списка приложений.

## 2.2. Настройка списков приложений

1. Чтобы создать приложение нажмите на кнопку **«Добавить»**, откроется окно с формой добавления нового приложения.
2. Введите понятное имя, выберите необходимый сценарий запуска из раскрывающегося списка (например, для RDP - RunMSTSC, для SSH - RunPutty). Для одного приложения можно выбрать только один сценарий.
3. Обязательно выберите Сервер 3С из раскрывающегося списка. Для одного приложения можно выбрать несколько Серверов 3С.
4. После заполнения формы нажмите **«Сохранить»**.

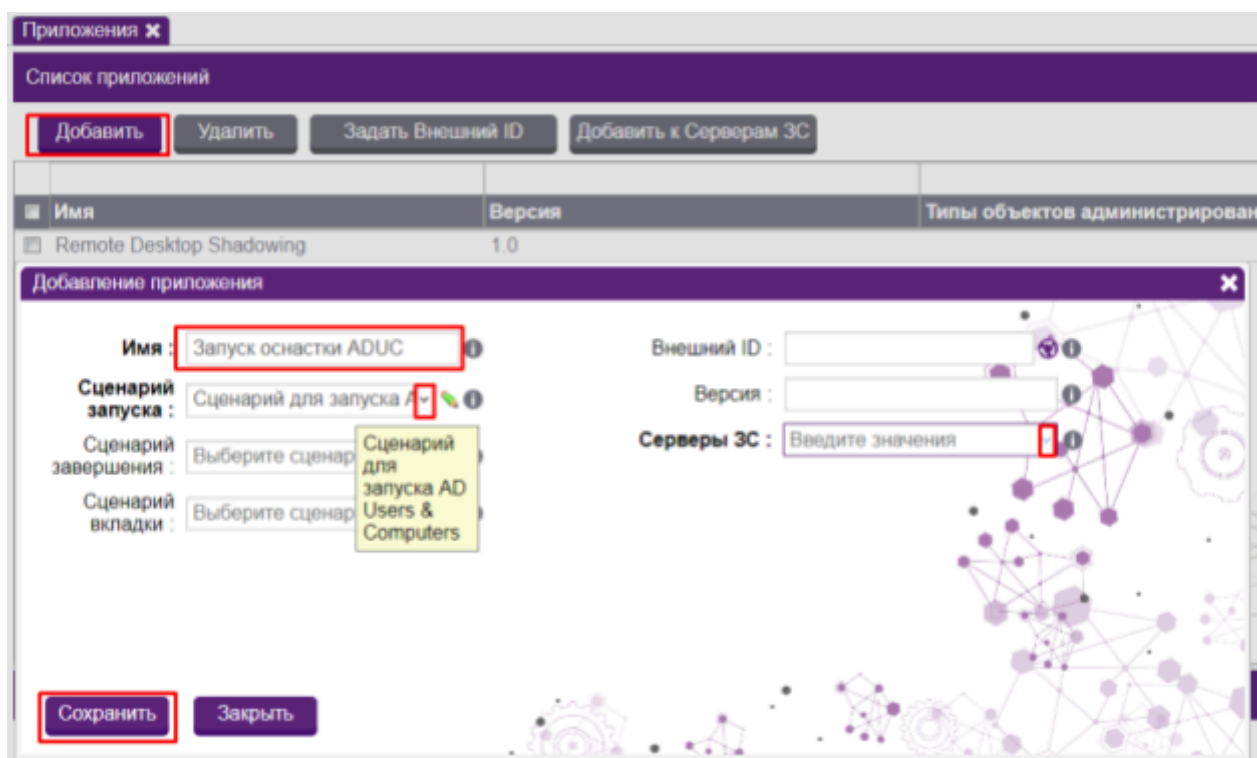


Рис. 2.5. Окно добавления приложения

Сценарии завершения и вкладки являются необязательными полями. Сценарий завершения может быть использован в качестве неинтерактивного сценария для смены пароля сразу после завершения основного сценария.

После того, как были добавлены все нужные приложения, можно переходить к следующему пункту.

### 3. Создание групп согласования

1. Для создания группы согласующих перейдите в раздел **«Управление системой»** > **«Группы согласования»**.

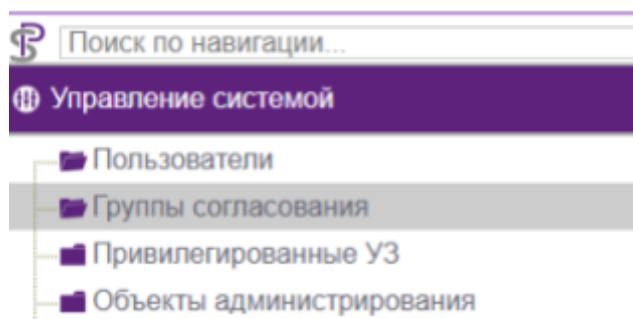


Рис. 3.1. Раздел Группы согласования

2. Нажмите на кнопку «Добавить группу», откроется окно с формой создания группы согласующих.

3. В разделе «Управление группой» в графе «Имя» введите понятное имя и нажмите «**Сохранить**». После сохранения новая группа добавится в список.

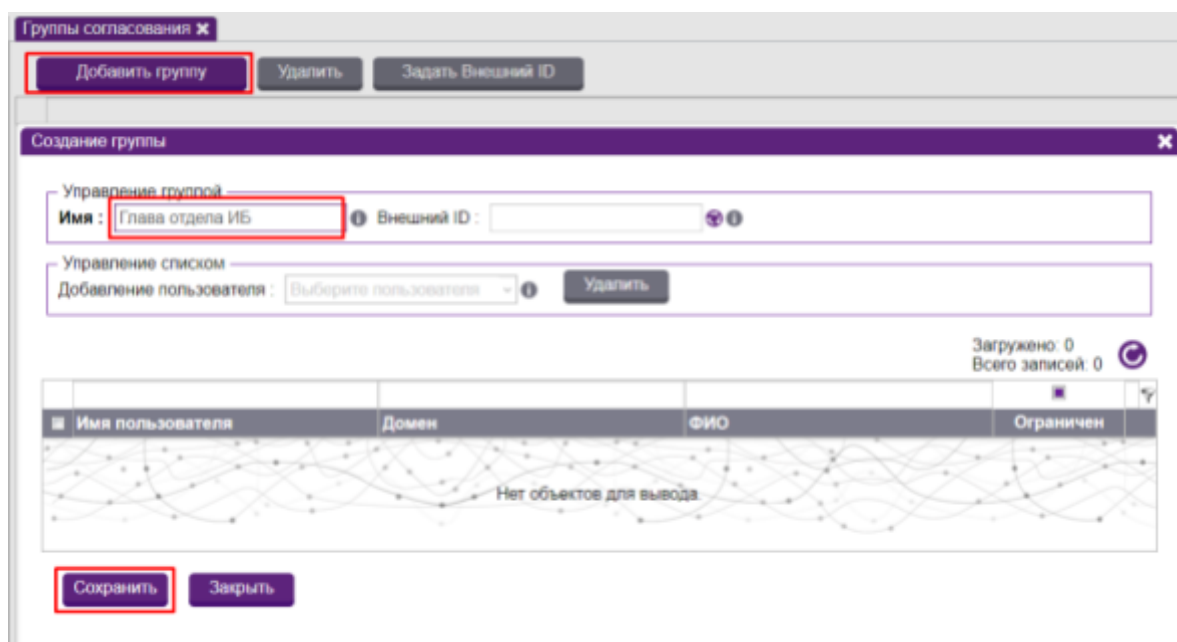


Рис. 3.2. Окно создания группы согласования

4. Далее в этом же окне нажмите «**Редактировать**», в поле «**Управление списком**» в графе «**Добавление пользователя**» выберите одного или нескольких пользователей из раскрывающегося списка. После каждого клика на пользователя Система выдаст сообщение, что пользователь успешно добавлен в группу.

Примечание: Добавить в группу согласующих можно любую учетную запись. Однако, согласовать наряд-допуск могут только учетные записи, обладающие следующими ролями:

- Стандартный пользователь
- Продвинутый пользователь
- Администратор
- Привилегированный администратор

Только у пользователей с перечисленными ролями есть доступ к разделу «**Наряды-допуски**». Остальные пользователи не имеют доступ к этому разделу и не смогут произвести согласование.

Чтобы наряд-допуск перешел в статус «**Согласован**», достаточно получить одобрение от одной из всех учетных записей, входящих в группу согласования.

5. После того как будут добавлены все необходимые согласующие нажмите «**Сохранить**».

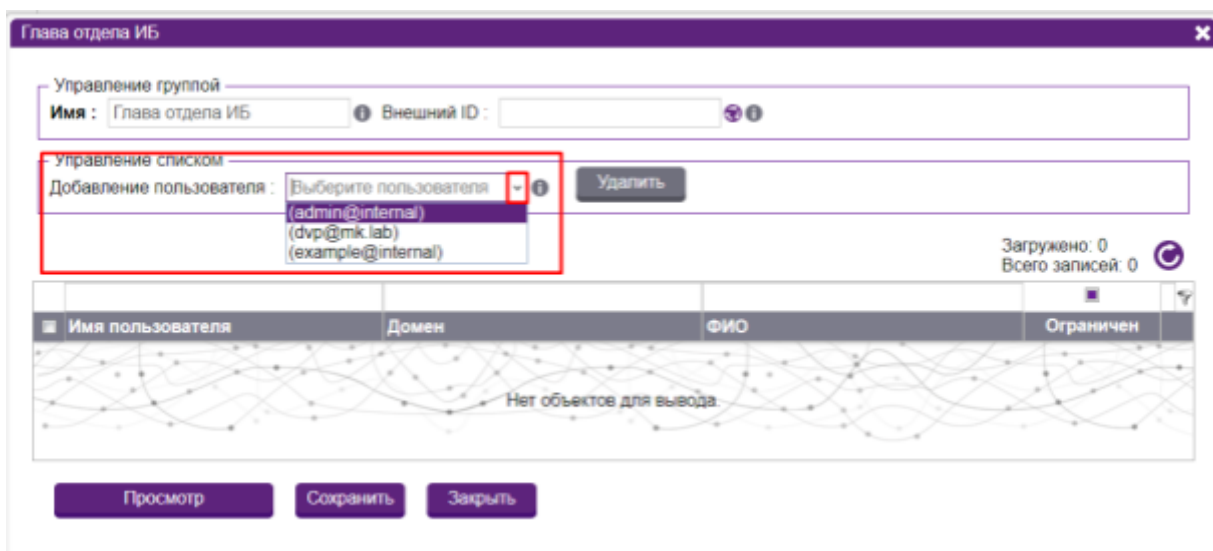


Рис. 3.3. Добавление пользователей в группу согласования

После того как будут созданы все необходимые для согласования группы, можно переходить к следующему пункту.

#### 4. Добавление привилегированных учетных записей

1. Чтобы добавить в Систему привилегированные учетные данные перейдите в раздел **«Управление системой»** > **«Привилегированные УЗ»**.

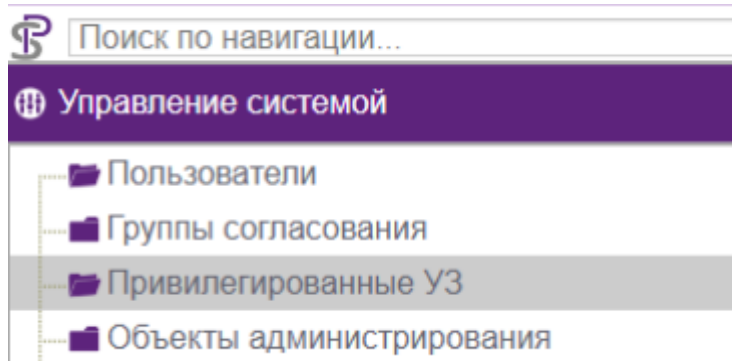


Рис. 4.1. Раздел Привилегированные УЗ

2. Нажмите на кнопку **«Добавить»**.



Рис. 4.2. Форма добавления привилегированных УЗ

Появившаяся форма добавления учетных записей «**Привилегированная УЗ**» (ПУЗ) содержит следующие поля:

- Наименование (обязательное поле) – произвольное наименование ПУЗ в Системе, по которому пользователь может удобным образом обозначить для себя назначение ПУЗ;
- Домен (обязательное поле для доменных учеток) – сокращенное наименование домена, к которому принадлежит учетная запись. Можно выбрать из раскрывающегося списка доменов, добавленных в Систему. Если УЗ является локальной для домена под управлением ОС Windows, то поле можно не заполнять;
- Пользователь (обязательное поле) – указывается логин той привилегированной учетной записи, с которой пользователь системы SPACE получает доступ на конечный объект администрирования;
- FQDN – Fully Qualified Domain Name, имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS. Поле обязательно для заполнения, когда учетная запись используется для работы с объектами под управлением ОС Windows. Если учетная запись является локальной для ОА под управлением ОС Windows, то необходимо указать точку: ".";

- Владелец – владелец (пользователь) данной учетной записи. После выбора владельца учётная запись становится **персонафицированной** - в дальнейшем её можно привязать к задаче, назначенной другому пользователю, но такая задача не запустится. Если владелец не указан, то учетная запись является общедоступной;
- Внешний ID – идентификатор для интеграции внешних систем через API sPACE с данной сущностью;
- Объект администрирования – объекты, с которыми работает пользователь-владелец учетной записи. Если поле остается пустым – учетная запись может быть использована на любом объекте администрирования. Если поле заполнено – использовать данную учетную запись можно только с тем объектом администрирования, который указан в данном поле;
- Агент паролей – тип password agent-а для управления паролем ПУЗ;
- Агент рандомизации паролей – выбор агента рандомизации паролей во вкладке «**Агенты паролей**» для рандомизации паролей ПУЗ ;
- Рандомизация пароля – настройка, показывающая, когда необходимо производить рандомизацию паролей для ПУЗ;
- 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.

3. После заполнения всех необходимых полей нажмите «**Сохранить**».

4. Появится уведомление «**Выбран встроенный агент паролей, задать секрет?**», нажмите «**Задать секрет**».

Примечание: Учетной записи можно задать пароль, либо ввести секретную часть RSA ключа. Публичная часть RSA ключа при этом размещается на конечном объекте администрирования.

Наличие пароля (секрета) является обязательным условием корректной работы Системы с Привилегированной УЗ. Для тех учетных записей, которые используются в сценариях без автоматического ввода пароля, можно указать заведомо неправильный пароль.

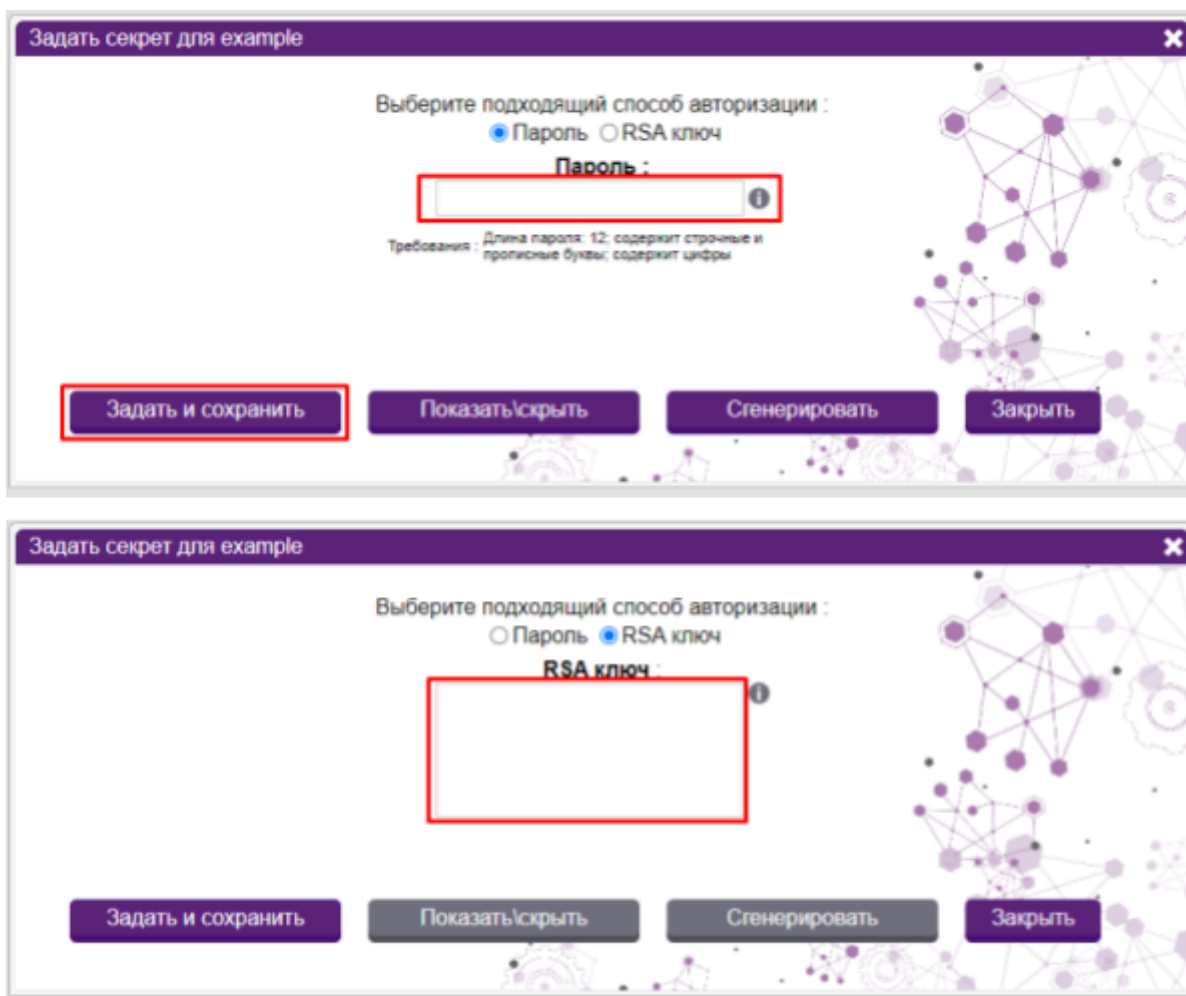


Рис. 4.3. Поле ввода пароля/ключа для привилегированной УЗ

5. После ввода пароля нажмите **«Задать и сохранить»**. Привилегированная учетная запись будет добавлена в систему.

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

6. Добавьте в систему все необходимые привилегированные учетные записи по приведенному образцу. После этого переходите к следующему пункту.

## 5. Создание объектов администрирования

1. Чтобы добавить в Систему объект администрирования перейдите в раздел **«Управление системой»** > **«Объекты администрирования»**.

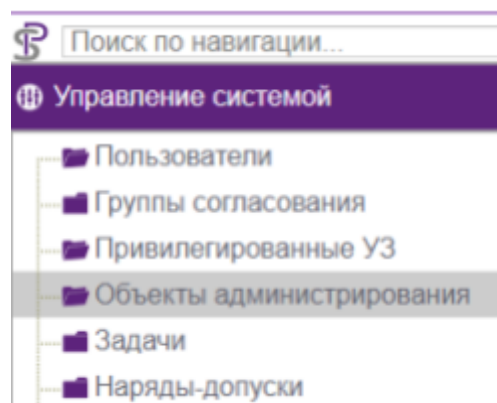


Рис. 5.1. Раздел Объекты администрирования

В этом разделе отображаются две таблицы, **«Список объектов»** и **«Список типов объектов администрирования»**.

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. Например, все объекты, доступ к которым осуществляется по rdp, могут принадлежать к объекту администрирования Windows и использовать сценарий подключения по mstsc.

2. Нажмите на кнопку **«Добавить»** в таблице **«Список типов объектов администрирования»**.

3. В раскрывшемся окне формы создания типа объекта заполните все поля. Введите понятное имя объекта, описание его использования. Из раскрывающегося списка выберите приложение, которое Система будет использовать для подключения к объектам данного типа.

4. Нажмите **«Сохранить»**.

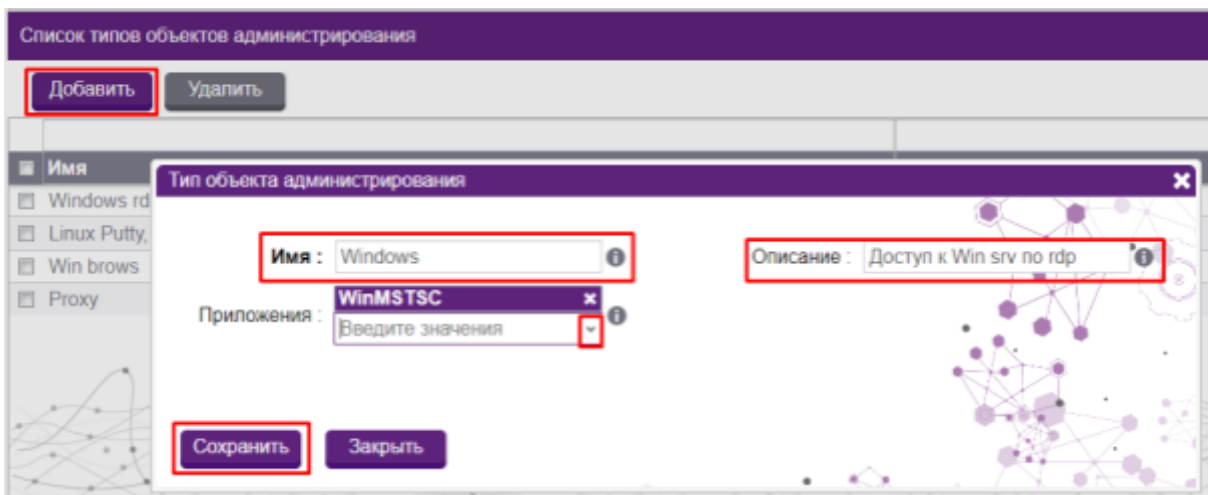


Рис. 5.2. Пример заполнения формы добавления типа объекта администрирования

5. Далее нажмите на кнопку «**Добавить**» в таблице «**Список объектов**».

6. В раскрывшемся окне формы добавления объекта заполните все поля. Введите понятное имя объекта, обязательно укажите его полный FQDN, из раскрывающихся списков выберите тип объекта и джамп сервер, через который будет осуществляться доступ к объекту администрирования.

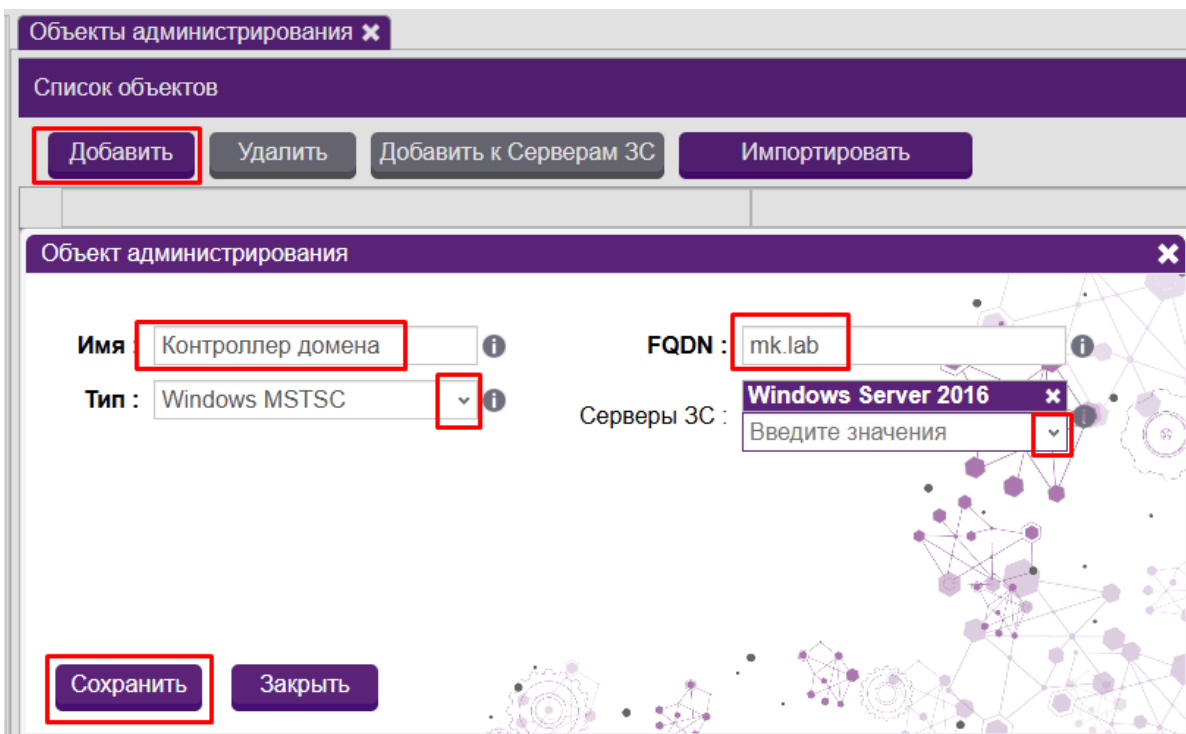


Рис. 5.3. Пример заполнения формы добавления объекта администрирования

7. Нажмите «**Сохранить**». После создания всех необходимых объектов администрирования можно переходить к следующему пункту.

## 6. Создание задачи

1. Чтобы создать Задачу перейдите в раздел «**Управление системой**» > «**Задачи**».

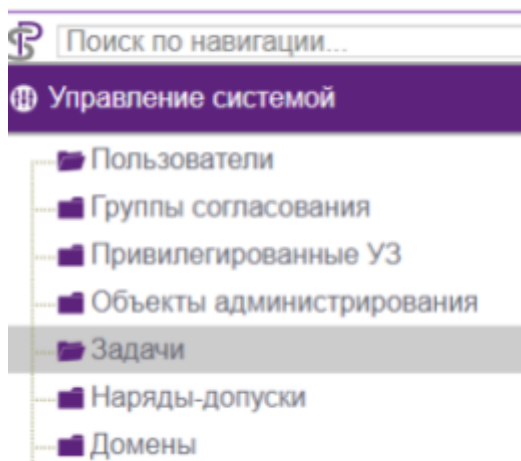


Рис. 6.1. Раздел Задачи

2. Нажмите на кнопку «**Добавить задачу**», в открывшемся окне добавления задачи заполните поля. Введите понятное название, из раскрывающегося списка выберите одну из ранее настроенных групп согласующих, при необходимости добавьте описание.
3. По окончании заполнения нажмите «**Добавить**». Появится оповещение «**Задача добавлена**», откроется форма настройки задачи.

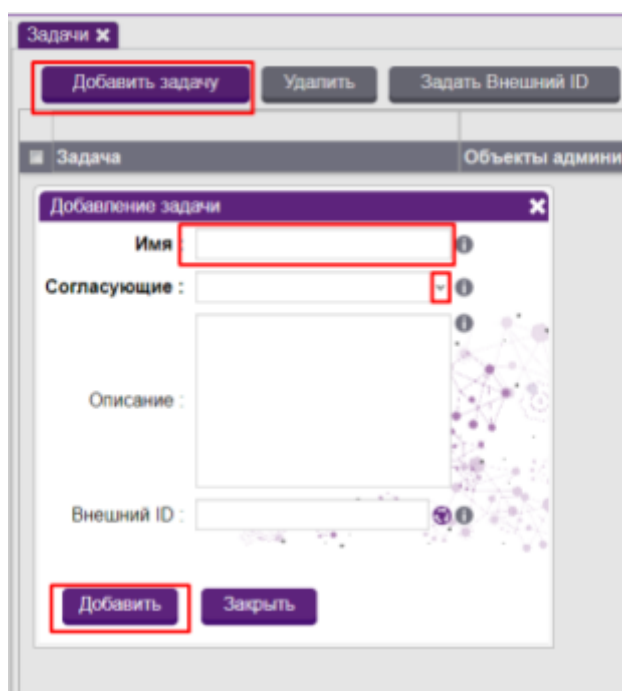


Рис. 6.2. Форма добавления задачи

4. Нажмите на кнопку **«Редактирование»**, в области **«Объекты администрирования»** выберите один из ранее настроенных объектов из раскрывающегося списка.

5. Перейдите в область **«Привилегированные УЗ»** и выберите из раскрывающегося списка те учетные записи, от имени которых будет производиться подключение к выбранному ранее объекту администрирования. Выбранные данные появляются списком в соответствующих полях. Для одной задачи можно выбрать несколько объектов администрирования и привилегированных учетных записей.

6. После того, как все необходимые ОА и ПУЗ выбраны, нажмите **«Сохранить»**.

Объект администрирования	Тип объекта администрирования	FQDN
DC	Windows rdp	mk lab

Полноеимено	Домейн	Полноеимено	Агент паролей
DC test	mk lab	RMS	
DC	mk lab	Administrator	

Рис. 6.3. Форма настройки задачи

7. Повторите данные действия чтобы настроить доступ ко всем нужным объектам в рамках данной задачи.

Настройка задачи завершена. Аналогичным образом настраиваются другие задачи.

Далее требуется выдать пользователям разрешения на запуск этих задач путем настройки соответствующих нарядов-допусков.

## 7. Наряды-допуски

Чтобы у пользователей появился доступ к запуску созданных задач, необходимо оформить для них в Системе наряды-допуски. Это можно сделать несколькими путями:

- пользователь с ролью администратор или супер администратор может создать и согласовать наряд-допуск для любого пользователя с ролью USER;
- пользователь с правом запроса может сам запросить для себя доступ к задаче (стандартный пользователь - ROLE\_SPACE\_STANDARD\_USER);
- пользователь с правом запроса и редактирования может запросить доступ для себя или другого пользователя (продвинутый пользователь - ROLE\_SPACE\_USER).

Подробнее о свойствах каждой роли можно узнать в Руководстве администратора, раздел «Перечень функционала, доступного для каждой роли».

### 7.1. Создать наряд-допуск

#### 7.1.1. Создать наряд-допуск от имени администратора

Чтобы создать наряд-допуск перейдите в раздел «**Управление системой**» > «**Наряды-допуски**».

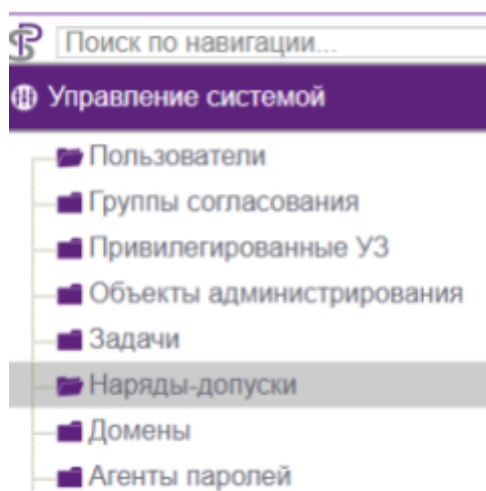


Рис. 7.1. Раздел Наряды-допуски



Нажмите на кнопку «**Добавить наряд-допуск**», выберите из раскрывающихся списков:

- Задача - задачу, к которой оформляется доступ;
- Доступ для - учетку одного или нескольких пользователей с ролью User в Системе;
- Учетные записи - одну или несколько привилегированных учетных записей, которые используются при подключении к целевым объектам администрирования этой задачи.

Рис. 7.2. Пример заполнения формы создания наряда-допуска

Обратите внимание, что поля «**Объекты администрирования**» и «**Согласующие**» заполняются автоматически, в соответствии со сделанными ранее настройками для указанной задачи.

Далее необходимо настроить период действия задачи. Для тестирования мы рекомендуем отметить чекбокс «**Бессрочный**». Для рабочих задач рекомендуем четко ограничивать время действия задачи. Подробнее о настройках периода действия можно прочитать в руководстве пользователя или в справке на портале.

Рис. 7.3. Область настройки периода действия наряда-допуска

После того как выбраны все обязательные настройки нажмите **«Согласовать»**. Согласованный наряд-допуск появится в списке.

### 7.1.2. Запросить наряд-допуск от имени стандартного пользователя

1. Залогиньтесь в Системе под пользователем с ролью STANDARD\_USER по форме username@domainname.

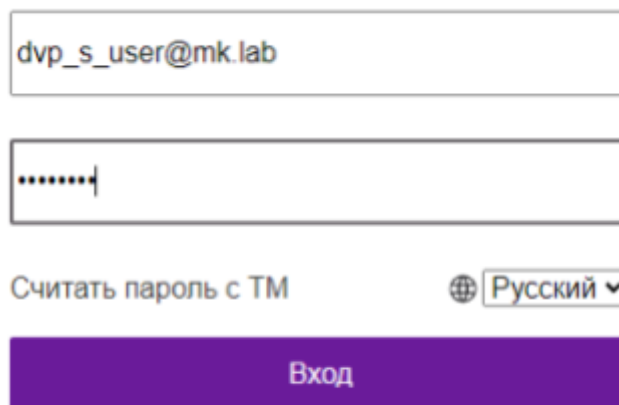


Рис. 7.4. Пример заполнения формы для аутентификации на портале

2. Чтобы запросить новый наряд-допуск перейдите в раздел **«Сеансы»** > **«Наряды-допуски»**.

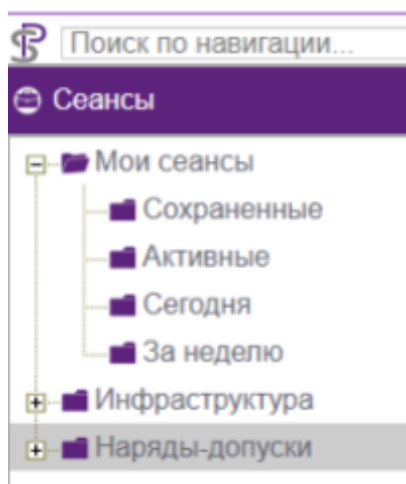


Рис. 7.5. Раздел Наряды-допуски во вкладке Сеансы

3. Нажмите на кнопку **«Запросить наряд-допуск»**, выберите из раскрывающегося списка задачу и привилегированную учетную запись. Обратите внимание, что у стандартного пользователя нет возможности изменить настройку в графе **«доступ для»**. Настройте период действия. Нажмите **«Отправить»**

**запрос».** Новый наряд-допуск появится во вкладке со статусом **«Ожидает согласования».**

Создание наряда-допуска

Задача : DC

Доступ для : ldvp\_s\_user@rnk.lab

Учетные записи : DC test

Период действия : 07.06.2024 19:5

Дополнительные настройки времени : Не задано

Дополнительные действия по истечении НД : Не задано

Основание : Номер заявки или ссылка на документ

Описание работ

Уведомления email для : Введите значения

Объекты администрирования : DC

Согласующие : (admin)

Отправить запрос

Закрыть

Рис. 7.6. Пример заполнения формы для отправки запроса согласования наряда-допуска от имени стандартного пользователя

### 7.1.3. Запросить наряд-допуск от имени продвинутого пользователя

Процесс создания нового наряда-допуска практически идентичен со стандартным пользователем. Различие заключается в том, что продвинутый пользователь может редактировать параметр **«Доступ для»**, указывая любого добавленного в Систему пользователя.

## 7.2. Согласовать запрошенный наряд-допуск

Согласовать наряд-допуск может любой администратор (даже тот, который не входит в группу согласования), или один из участников группы согласующих с ролью стандартного или продвинутого пользователя. Если стандартный пользователь входит в группу согласующих, он сразу может согласовать созданный для себя наряд-допуск самостоятельно.

### 7.2.1. Согласовать от имени администратора

1. Чтобы согласовать наряд-допуск от имени администратора, залогиньтесь в Системе под пользователем admin и перейдите в раздел **«Управление системой» > «Наряды-допуски».**

2. В журнале нарядов-допусков выберите наряд-допуск в статусе **«Ожидает согласования»**.

3. Проверьте выбранные параметры, при необходимости откорректируйте.

4. Нажмите **«Согласовать»/«Изменить и согласовать»**.

5. Наряд-допуск перейдет в статус **«Активный»**. С этого момента у пользователя появляется возможность запустить задачу.

#### **7.2.2. Согласовать от имени пользователя**

1. Чтобы согласовать наряд-допуск от имени пользователя, залогиньтесь в Системе под пользователем с ролью стандартного или продвинутого пользователя, входящего в группу согласования.

2. Перейдите в раздел **«Сеансы» > «Наряды-допуски»**.

3. В журнале нарядов-допусков выберите наряд-допуск в статусе **«Ожидает согласования»**.

4. Проверьте выбранные параметры. У стандартного пользователя нет возможности редактировать параметры. Продвинутый пользователь может изменять основные поля. При необходимости откорректируйте настройки.

5. Нажмите **«Согласовать»/«Изменить и согласовать»**.

6. Наряд-допуск перейдет в статус **«Активный»**. С этого момента у пользователя появляется возможность запустить задачу.

## 8. Настроить внутренний видеоаудит ВСАС

Чтобы включить и отрегулировать настройки ВСАС (внутренняя система аудита сеансов) залогиньтесь в Системе под пользователем admin и перейдите в раздел «**Управление ресурсами**» > «**Внутренний видеоаудит**».

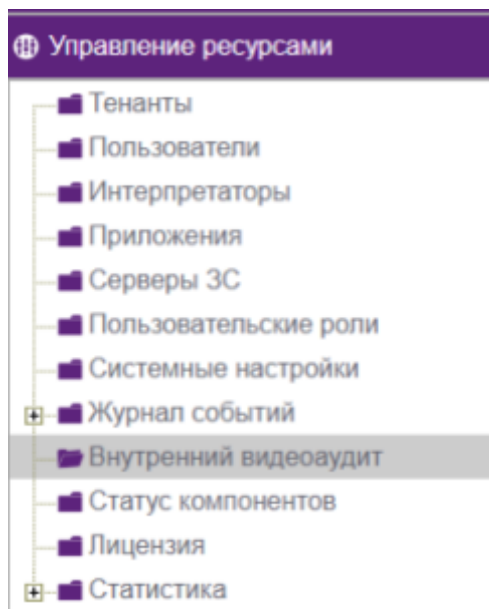


Рис. 8.1. Раздел Внутренний видеоаудит

Отметьте последовательно чекбоксы «**Включить внутренний видеоаудит**», «**Включить запись**» и «**Включить Key Logger**». Настройку «**Интервал регулярной записи**» отредактируйте в зависимости от собственных потребностей в логировании.

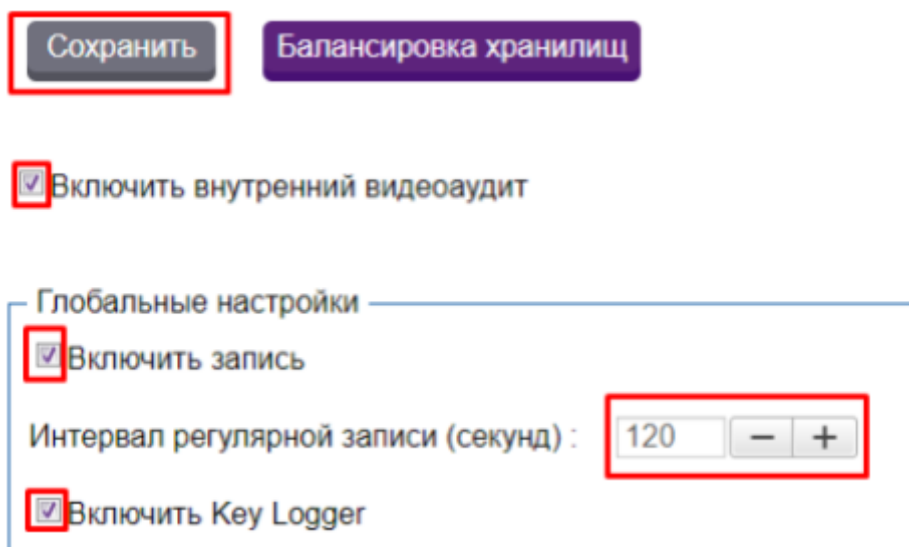


Рис. 8.2. Настройка ВСАС

Чем меньше будет установленный интервал - тем больше места потребуется для сохранения каждой сессии пользователя. Снимки экрана производятся в соответствии с установленным интервалом. Дополнительно снимки создаются на каждое действие пользователя - нажатие клавиш и клики мышью. Таким образом, все действия пользователя сохраняются в Системе независимо от того, какие выставлены настройки для регулярной записи.

В среднем, при стандартном восьмичасовом рабочем дне при разрешении рабочего экрана пользователя FullHD - 1920\*1080 и стандартном интервале регулярной записи - 3 сек, минимально необходимое место на хранилище для одного пользователя на месяц - 20 Гб. Объем меняется в зависимости от продолжительности сессии, размера экрана пользователя, насыщенности цветами внутри самой сессии и интервалов создания скриншотов.

## 9. Запуск задачи

Чтобы запустить задачу залогиньтесь в Системе под пользователем с одной из трех ролей USER, для которого был оформлен и согласован наряд-допуск, по форме username@domainname.

Чтобы увидеть все разрешенные для пользователя задачи перейдите в раздел «**Сеансы**» > «**Инфраструктура**», разверните список «**Мои задачи**».

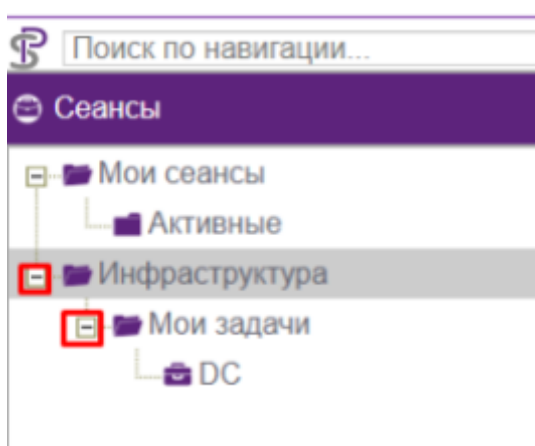


Рис. 9.1. Раздел Инфраструктура (интерфейс базового пользователя)

В этой вкладке отображаются все задачи, разрешенные пользователю. Для запуска щелкните на задачу левой кнопкой мыши (например, сеанс доступа к Windows через mstsc). Откроется окно «**Запуск сеанса**», где нужно выбрать параметры запуска. Если в задаче для каждого пункта настроен один вариант -

все поля будут автоматически заполнены, без доступа к редактированию. Если есть выбор - ненастроенное поле останется пустым. Для каждого такого пункта выберите параметры запуска из раскрывающегося списка. Для перемещения между пунктами используйте клавиши «**Вернуться**» и «**Далее**».

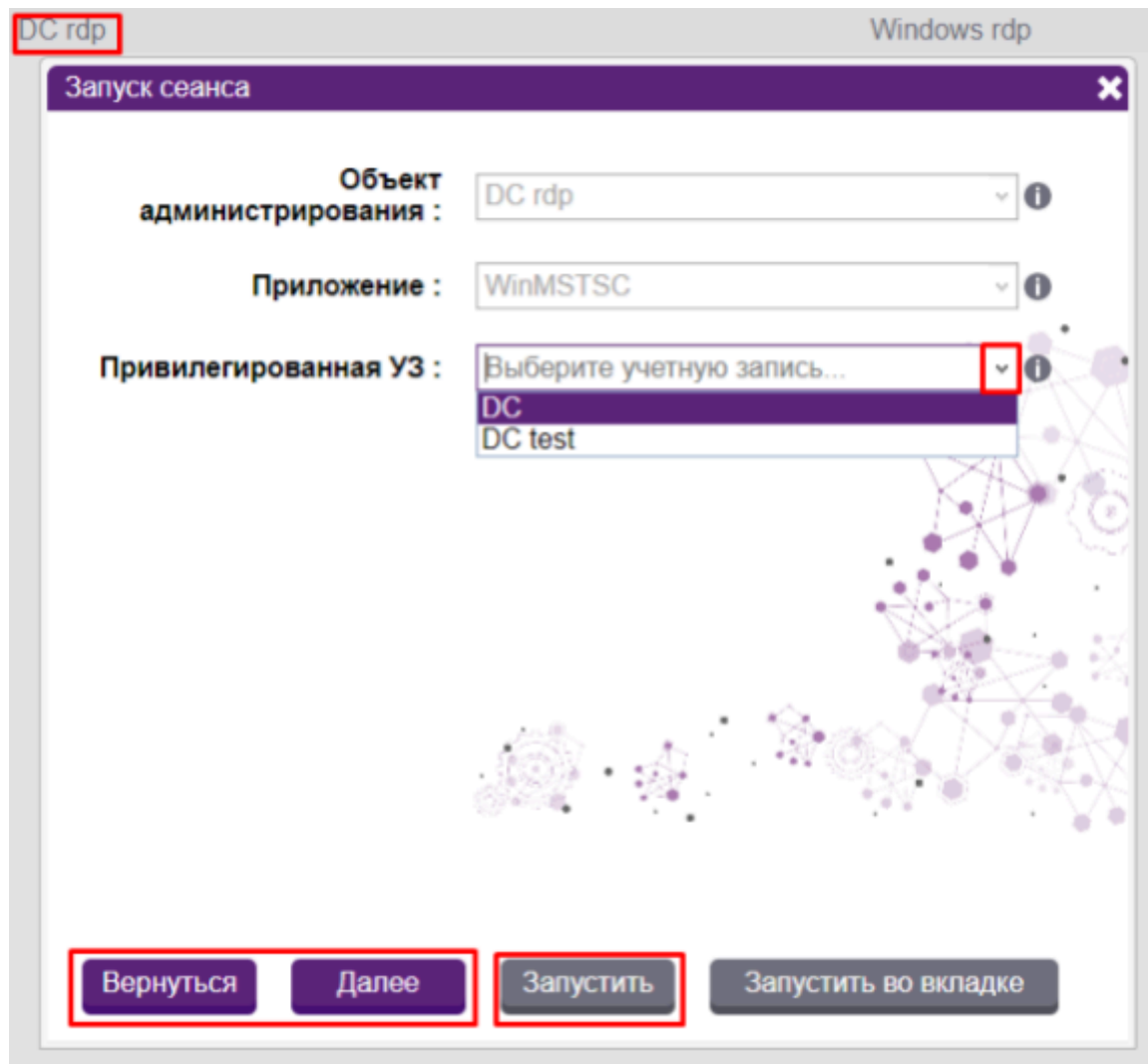


Рис. 9.2. Окно настроек запуска задачи

После того, как все параметры настроены, станет активна кнопка «**Запустить**». Щелкните на нее левой кнопкой мыши.

### 9.1. Запуск задачи на СЗС Windows

Предварительная подготовка не требуется.

После нажатия на кнопку запуска Система сгенерирует и загрузит **rdp-файл** для запуска задачи.

Примечание: Это уникальный файл, время действия которого ограничивается 120 секундами. По истечении этого времени файл станет недействительным, а пользователю будет

выдано окно с ошибкой «Текущий сеанс находится в терминальном состоянии». Файл также является одноразовым, повторно запустить задачу с его помощью нельзя. Если по какой-то причине пользователь не успел воспользоваться файлом в отведенное время, задачу необходимо запустить повторно. При повторном запуске задачи будет сгенерирован новый файл.

Запустите полученный gdr-файл на своей рабочей станции.

На данном этапе Система начнет проброс gdr-соединения между пользовательской рабочей станцией и джамп-сервером. Появится окно авторизации с просьбой ввести учетные данные, при помощи которых пользователь подключается к джамп-серверу.

Доменный пользователь должен ввести те же учетные данные, с которыми аутентифицировался в Системе. Локальный пользователь (с учеткой, созданной во внутреннем домене **internal**) должен ввести логин и пароль доменной или локальной учетной записи, у которой есть права для подключения к джамп-серверу и запуска приложения для ОА из задачи.

Введите учетные данные и нажмите ОК.

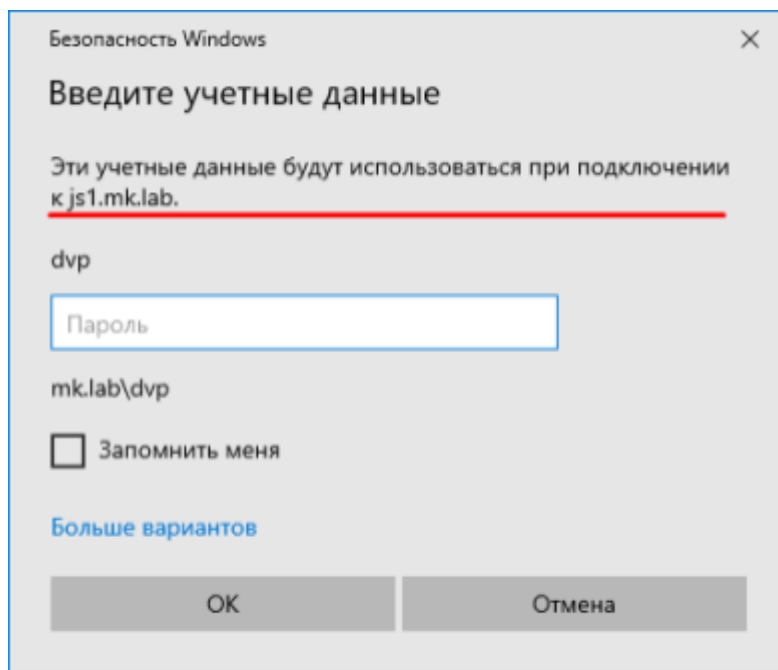


Рис. 9.3. Аутентификация на джамп-сервере

Если в домене настроено sso, этап авторизации на джамп-сервере будет пропущен.



Далее Система запустит нужный инструмент и автоматический ввод всех необходимых для подключения параметров, в том числе привилегированных учетных данных для авторизации на объекте. На этом этапе пользователю ничего не нужно вводить. Дождитесь окончания выполнения сценария. В итоге на рабочей станции появится отдельное окно с запущенной задачей.

Примечание: Если пользователь запускает доступ к задаче с приложением без автоматической подстановки учетных данных, на данном этапе пользователь должен самостоятельно ввести привилегированные учетные данные для подключения.

После того, как будет установлено соединение, вернитесь к списку **«Мои задачи»** и щелкните на другой сеанс (например, доступ к Linux через ssh с использованием Putty). Сразу откроется окно автоматизированного доступа к задаче. В этом случае rdp-файл не генерируется, так как новый сеанс открывается в рамках уже запущенной на джамп-сервере сессии.

Примечание: Последующие задачи будут запускаться в рамках одной сессии до тех пор, пока не будет достигнут предел максимальной нагрузки на джамп-сервер. В этом случае в работу вступит балансировщик - Система автоматически запустит новую сессию на втором (третьем и т.д.), свободном джамп-сервере, в случае его наличия. Если в балансировке нет свободных серверов, система выдаст предупреждение о перегрузке сервера и откажет в запуске нового сеанса.

В результате в рамках одной сессии откроется два сеанса - два окна с доступом к разным инструментам.

## 9.2. Запуск задачи на СЗС Linux через SSH

Перед запуском убедитесь, что используемый СЗС Linux имеет соответствующий тип подключения. Для этого перейдите в раздел **«Управление ресурсами»** > **«Серверы ЗС»** и проверьте настройки сервера, который планируется использовать для запуска задачи. Щелкните на сервер левой кнопкой мыши - откроется окно с настройками. В графе **«Тип подключения:»** должен быть указан **SSH**. Если указан RDP - выберите в раскрывающемся списке SSH.

При этом RDP можно убрать, либо оставить оба типа, если сервер планируется использовать для обоих вариантов подключения. В этом случае при настройке сценариев обязательно указывайте нужный тип подключения.

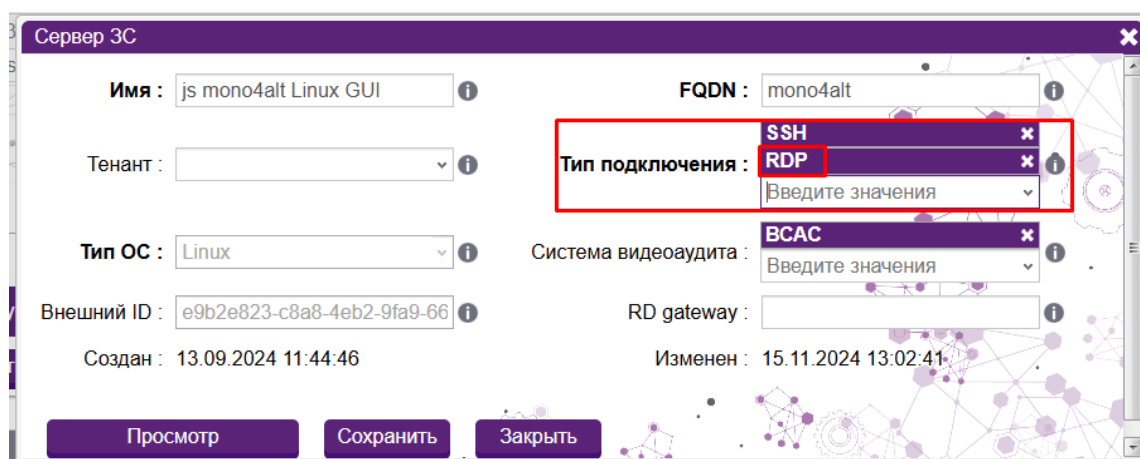


Рис. 9.4. Проверка типа подключения

Чтобы запустить задачу залогиньтесь в Системе под пользователем с одной из трех ролей USER, для которого был оформлен и согласован наряд-допуск, по форме `username@domenname`, перейдите в раздел «**Сеансы**» > «**Инфраструктура**», разверните список «**Мои задачи**».

Щелкните на задачу левой кнопкой мыши (например, сеанс доступа к Linux через ssh). Откроется окно «**Запуск сеанса**», где нужно выбрать параметры запуска.

После того, как все параметры настроены, станет активна кнопка «**Запустить**». Щелкните на нее левой кнопкой мыши.

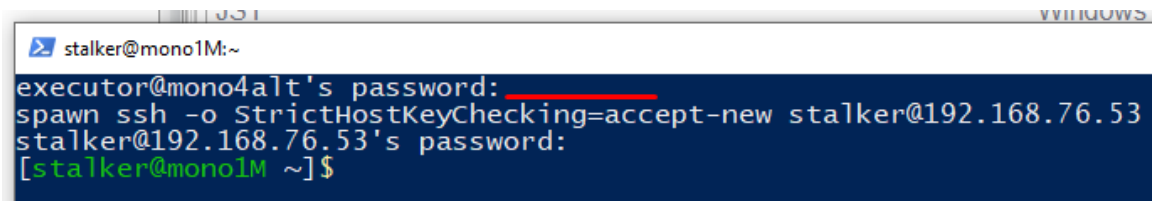
После нажатия Система сгенерирует и загрузит **ps1-файл** для запуска задачи.

Примечание: Это уникальный файл, время действия которого ограничивается 120 секундами. По истечении этого времени файл станет недействительным, а пользователю будет выдано окно с ошибкой «**Текущий сеанс находится в терминальном состоянии**». Файл также является одноразовым, повторно запустить задачу с его помощью нельзя. Если по какой-то причине пользователь не успел воспользоваться файлом в отведенное время, задачу необходимо запустить повторно. При повторном запуске задачи будет сгенерирован новый файл.

Запустите полученный ps1-файл на своей рабочей станции - откройте папку, в которую был загружен файл, щелкните на него правой кнопкой мыши и выберите «**Выполнить с помощью PowerShell**».

На данном этапе Система начнет проброс ssh-соединения между пользовательской рабочей станцией и СЗС Linux. Появится консоль с просьбой ввести пароль для пользователя **executor**, при помощи которого подтверждается

подключение к джамп-серверу. Этой технической учетной записью, единой для всех. Учетные данные создаются автоматически при развертывании дистрибутива на сервере. Введите пароль «**Zaq12wsx**».



```
stalker@mono1M:~  
executor@mono4alt's password: _____  
spawn ssh -o StrictHostKeyChecking=accept-new stalker@192.168.76.53  
stalker@192.168.76.53's password: _____  
[stalker@mono1M ~]$
```

Рис. 9.5. Аутентификация на СЗС Linux

После ввода пароля пользователь **executor** будет авторизован, произойдет проброс соединения до конечной ЦС. Система автоматически подставит привилегированные учетные данные. Дождитесь окончания выполнения сценария. В итоге на рабочей станции появится окно с запущенной задачей.

### 9.3. Запуск задачи на СЗС Linux через RDP

Убедитесь, что используемый СЗС Linux имеет соответствующий тип подключения. Для этого перейдите в раздел «**Управление ресурсами**» > «**Серверы ЗС**» и проверьте настройки сервера, который планируется использовать для запуска задачи. Щелкните на сервер левой кнопкой мыши - откроется окно с настройками. В графе «**Тип подключения:**» должен быть указан **RDP**. Если указан SSH - выберите в раскрывающемся списке RDP.

При этом SSH можно убрать, либо оставить оба типа, если сервер планируется использовать для обоих вариантов подключения. В этом случае при настройке сценариев обязательно указывайте нужный тип подключения.

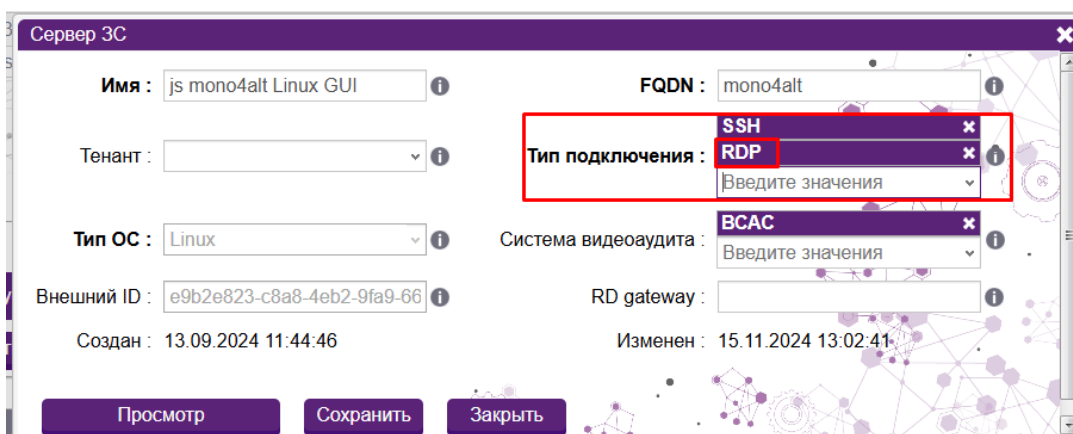


Рис. 9.6. Проверка типа подключения

Чтобы запустить задачу залогиньтесь в Системе под пользователем с одной из трех ролей USER, для которого был оформлен и согласован наряд-допуск на соответствующую задачу, по форме username@domenname.

Щелкните на задачу левой кнопкой мыши (например, доступ к Windows через xfreerdp). Настройте все параметры, станет активна кнопка «**Запустить**». Щелкните на нее левой кнопкой мыши.

После нажатия Система сгенерирует и загрузит **rdp-файл** для запуска задачи.

Примечание: Это уникальный файл, время действия которого ограничивается 120 секундами. По истечении этого времени файл станет недействительным, а пользователю будет выдано окно с ошибкой «**Текущий сеанс находится в терминальном состоянии**». Файл также является одноразовым, повторно запустить задачу с его помощью нельзя. Если по какой-то причине пользователь не успел воспользоваться файлом в отведенное время, задачу необходимо запустить повторно. При повторном запуске задачи будет сгенерирован новый файл.

Удостоверьтесь, что у вас включена английская языковая раскладка и запустите полученный rdp-файл на своей рабочей станции.

На данном этапе Система начнет проброс соединения между пользовательской рабочей станцией и СЗС Linux. Появится окно авторизации с просьбой ввести учетные данные, при помощи которых пользователь проходит аутентификацию в СЗС. Для этих целей используется техническая учетная запись **executor**, единая для всех. Учетные данные для нее создаются автоматически при развертывании дистрибутива на сервере. Введите в графе пользователя «**executor**», в графе пароль «**Zaq12wsx**».



Рис. 9.7. Аутентификация в СЗС

Если в момент запуска файла языковая раскладка будет отличаться от английской, ввести учетные данные не получится. В этом случае закройте соединение и сгенерируйте файл заново повторным запуском сеанса.

Далее Система запустит нужный инструмент и автоматический ввод всех необходимых для подключения параметров, в том числе привилегированных учетных данных для авторизации на объекте. На этом этапе пользователю ничего не нужно вводить. Дождитесь окончания выполнения сценария. В итоге на рабочей станции появится отдельное окно с запущенной задачей.

Примечание: Если пользователь запускает доступ к задаче с приложением без автоматической подстановки учетных данных, на данном этапе пользователь должен самостоятельно ввести привилегированные учетные данные для подключения.

После того, как будет установлено соединение, вернитесь к списку «**Мои задачи**» и щелкните на другой сеанс (например, сеанс доступа к Linux через ssh). Система сгенерирует и загрузит новый **rdp-файл** для запуска новой задачи. На данный момент на СЗС Linux каждая задача запускается в виде отдельной сессии. Повторите ввод технической учетки.

В результате на рабочей станции откроется два окна - две отдельные сессии с доступом к разным инструментам.

## 10. Проверка функционала аудитора

Чтобы проверить функционал аудитора залогиньтесь под пользователем с одной из двух ролей аудитора (space\_auditor или space\_trusted\_auditor), по форме username@domainname. Перейдите в раздел «**Аудит**» > «**Сеансы**», откроется список «**Сеансы(Аудит)**».

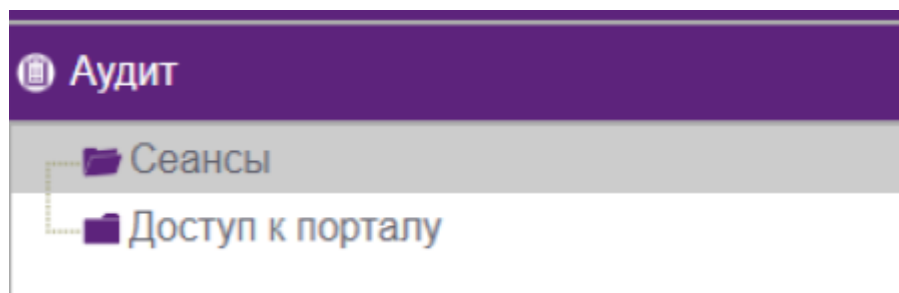
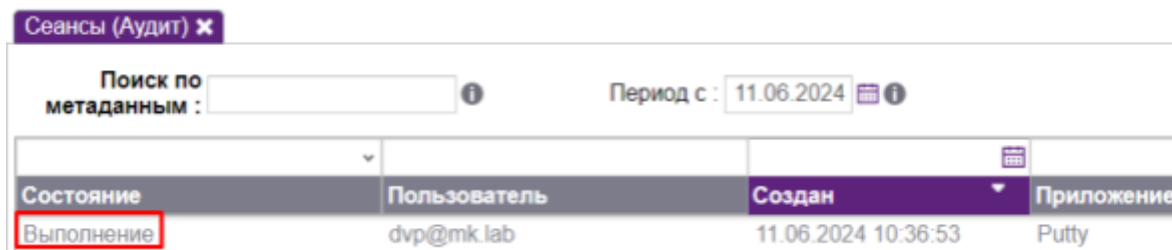


Рис. 10.1. Раздел Сеансы во вкладке Аудит

## 10.1. Наблюдение за сеансом в режиме реального времени

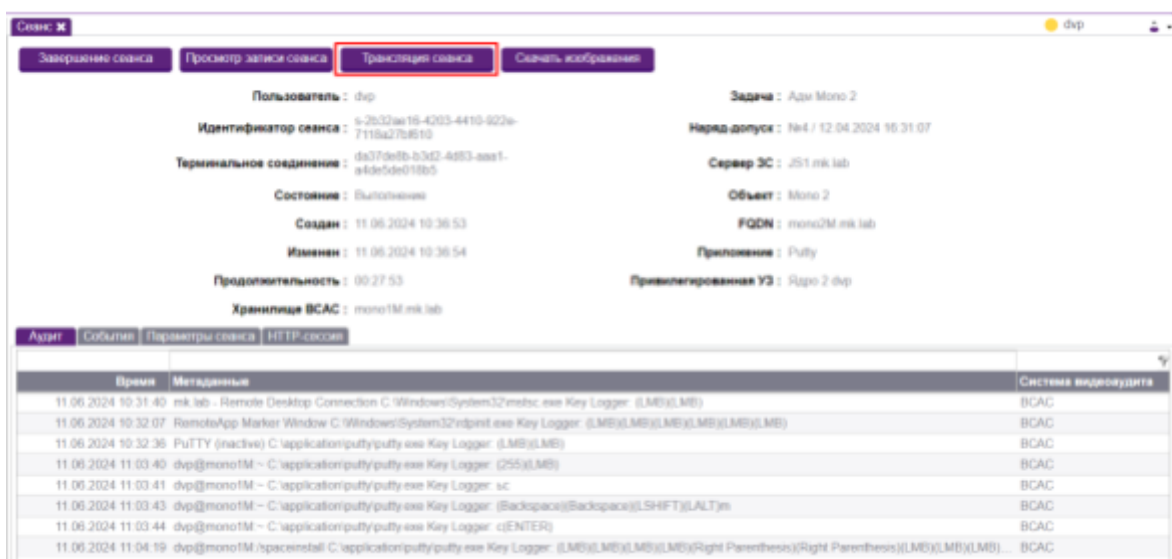
Кликните на запущенный сеанс. Если в списке нет сеансов в состоянии **«Выполнение»**, для отработки следующих пунктов тестирования запустите сеансы доступа по rdp и ssh.



Состояние	Пользователь	Создан	Приложение
Выполнение	dvp@mk.lab	11.06.2024 10:36:53	Putty

Рис. 10.2. Таблица Сеансы (Аудит)

Откроется окно карточки сеанса, где перечислена вся информация о сеансе, и предоставлена возможность наблюдения за сеансом в режиме реального времени. Чтобы запустить режим мониторинга нажмите **«Трансляция сеанса»** в верхней части окна.



Пользователь: dvp  
Идентификатор сеанса: 6-2b32ae15-4203-4410-922b-7118a27b8510  
Терминальное соединение: da379e8b-b3d2-4d53-aaa1-a4de5de018b5  
Состояние: Выполнение  
Создан: 11.06.2024 10:36:53  
Изменен: 11.06.2024 10:36:54  
Продолжительность: 00:27:53  
Хранилище ВСАС: mono1M.mk.lab

Задача: Адм Mono 2  
Наряд допуск: №4 / 12.04.2024 16:31:07  
Сервер ЗС: JS1.mk.lab  
Объект: Mono 2  
FQDN: mono2M.mk.lab  
Приложение: Putty  
Привилегированная УЗ: Ядро 2 dvp

Время	Метаданные	Система видеонаблюдения
11.06.2024 10:31:40	mk.lab - Remote Desktop Connection C:\Windows\System32\mbsc.exe Key Logger (LMB)(LMB)	BCAC
11.06.2024 10:32:07	RemoteApp Marker Window C:\Windows\System32\ripnt.exe Key Logger (LMB)(LMB)(LMB)(LMB)(LMB)(LMB)	BCAC
11.06.2024 10:32:36	PuTTY (inactive) C:\application\putty\putty.exe Key Logger (LMB)(LMB)	BCAC
11.06.2024 11:03:40	dvp@mono1M ~ C:\application\putty\putty.exe Key Logger (255)(LMB)	BCAC
11.06.2024 11:03:41	dvp@mono1M ~ C:\application\putty\putty.exe Key Logger sc	BCAC
11.06.2024 11:03:43	dvp@mono1M ~ C:\application\putty\putty.exe Key Logger (Backspace)(Backspace)(LSHIFT)(LALT)m	BCAC
11.06.2024 11:03:44	dvp@mono1M ~ C:\application\putty\putty.exe Key Logger c(ENTER)	BCAC
11.06.2024 11:04:19	dvp@mono1M /spaceball C:\application\putty\putty.exe Key Logger (LMB)(LMB)(LMB)(LMB)(Right Parenthesis)(Right Parenthesis)(LMB)(LMB)(LMB)	BCAC

Рис. 10.3. Кнопка запуска мониторинга сеанса

Откроется окно наблюдения за сессией.

### 10.1.1. Мониторинг сессии на СЗС Windows и Linux (RDP)

В рамках одной сессии на СЗС Windows пользователем может быть запущено несколько сеансов - все окна с ними будут отображаться в одном окне наблюдения. На СЗС Linux каждый сеанс создает отдельную сессию и отдельное окно наблюдения.

Чтобы убедиться в корректной работе мониторинга, выполните несколько действий внутри запущенных сессий.

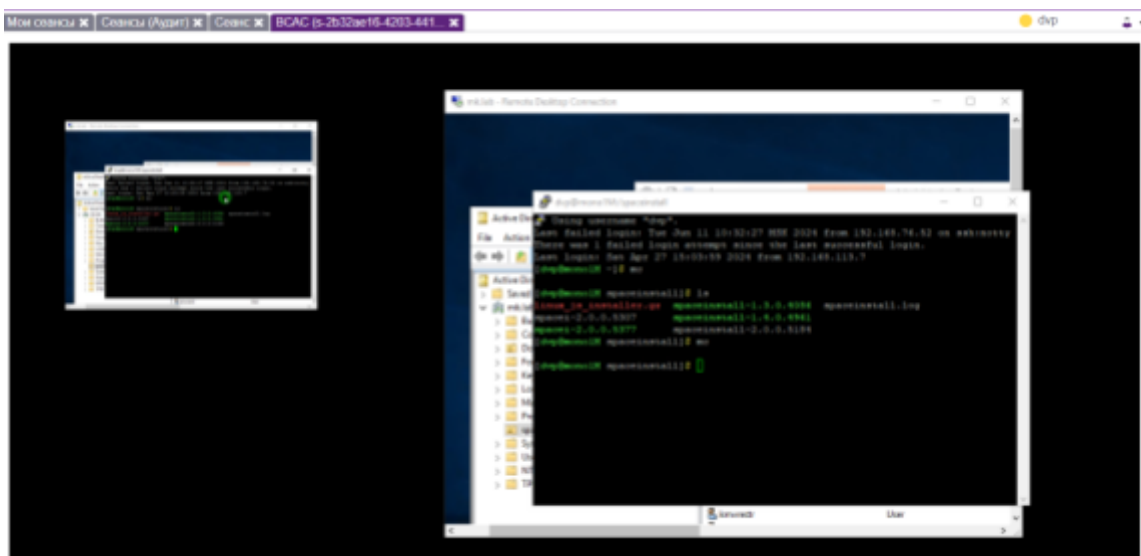


Рис. 10.4. Окно мониторинга сеанса на C3C Windows

### 10.1.2. Мониторинг сессии на C3C Linux (SSH)

На C3C Linux (SSH) может быть запущена только одна сессия - трансляция сеанса развернет текстовое окно, в котором будут отображаться команды, вводимые пользователем с момента начала трансляции.

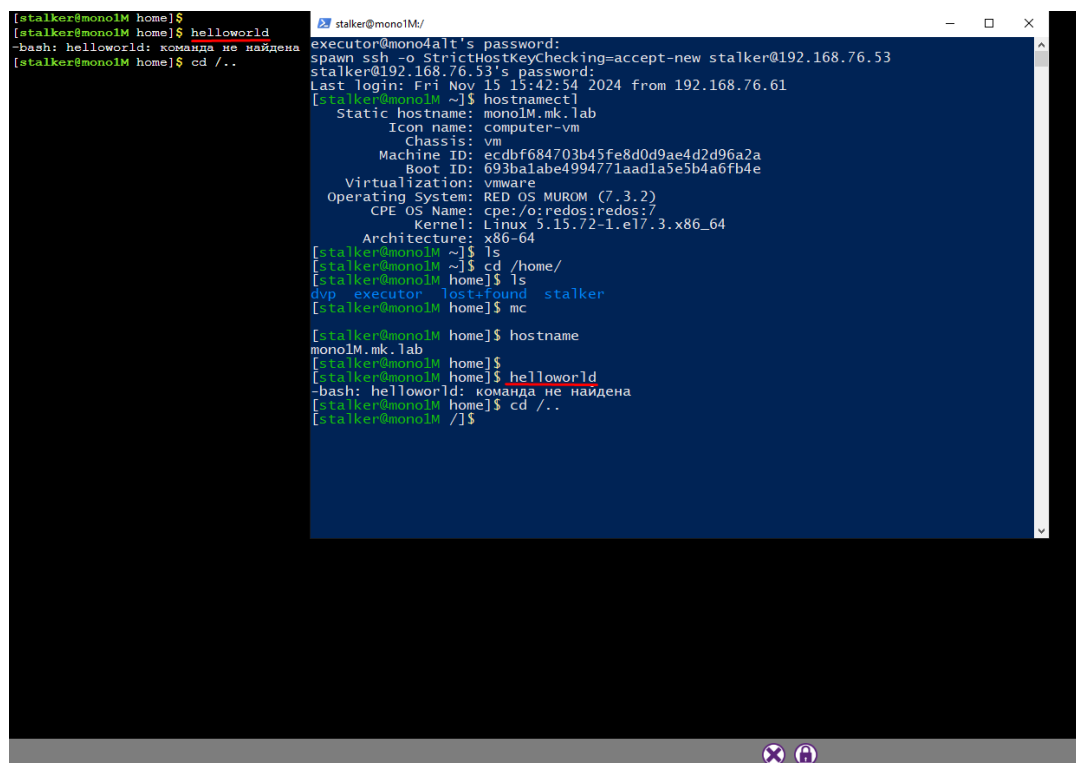


Рис. 10.5. Окно мониторинга сеанса на C3C Linux (SSH)

## 10.2. Управление сессиями

В нижней части окна мониторинга располагается панель активных действий с сессией (для сессии с СЗС Linux (SSH) функционал сильно урезан). Также предоставляется детальная информация о сеансе в рамках открытой сессии по клику на кнопку **«Развернуть»**. Аудитор может осуществлять заморозку/разморозку и завершение сессии путем нажатия на клавиши **«Заблокировать/Разблокировать»** и **«Завершить»**.



Рис. 10.6. Панель инструментов для работы с сессией

### 10.2.1. Блокировка пользовательского ввода

Чтобы проверить работу блокировки пользовательского ввода, нажмите на клавишу **«Заблокировать пользовательский ввод для данного соединения»**. Система выдаст окно с запросом на подтверждение действия в сессии, нажмите **«Да»**. Все сеансы, запущенные в рамках этой сессии, будут заблокированы.

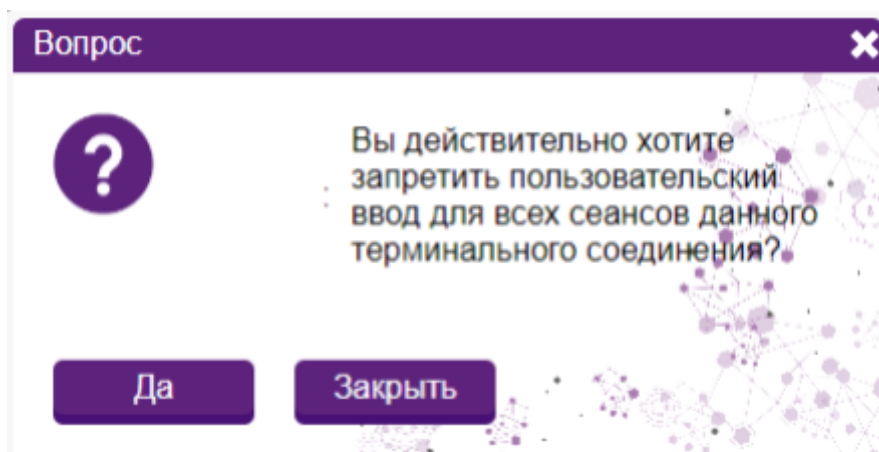


Рис. 10.7. Окно подтверждения действия

Удостоверьтесь, что любые действия в рамках каждого сеанса не имеют эффекта после блокировки. Нажмите **«Разблокировать пользовательский ввод для данного соединения»**. Система выдаст окно с запросом на подтверждение действия, нажмите **«Да»**. Удостоверьтесь, что все сеансы разблокированы и исправно работают.



## 10.2.2. Завершение сеанса и сессии

Чтобы завершить один из сеансов в рамках сессии перейдите на вкладку «Сеанс» и нажмите «**Завершение сеанса**». Система выдаст окно с запросом на подтверждение действия, нажмите «**Да**».

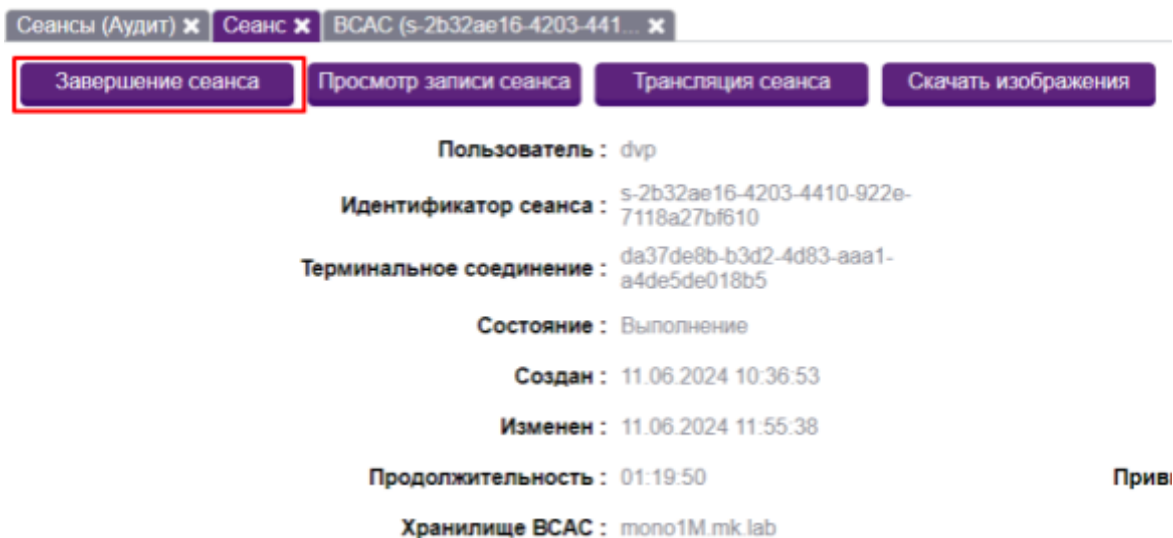


Рис. 10.8. Кнопка завершения сеанса

Система выдаст аудитору оповещение об успешном завершении сеанса. Одновременно Система выдаст пользователю оповещение о принудительном завершении сеанса.

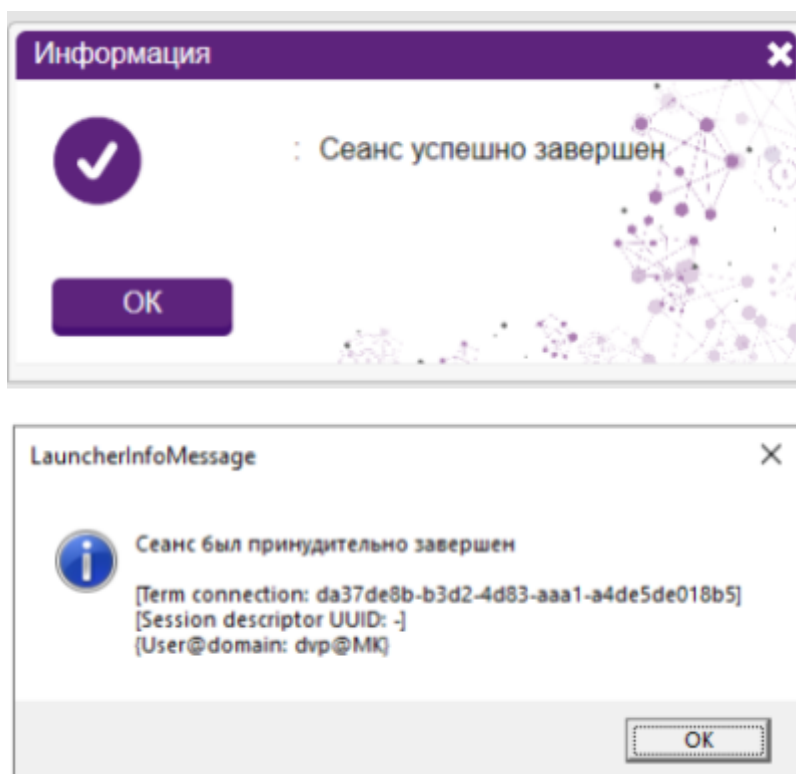


Рис. 10.9. Оповещения о завершении сеанса для аудитора и пользователя

Этот сеанс перейдет в статус **«Завершено»**, остальные сеансы в рамках сессии продолжат свою работу.

Чтобы завершить одновременно все сеансы в рамках сессии перейдите в окно наблюдения за сессией и нажмите **«Завершить все сеансы данного соединения»**. Система выдаст окно с запросом на подтверждение действия, нажмите **«Да»**. Система выдаст пользователю уведомление о принудительном завершении сессии. Одновременно Система выдаст аудитору уведомление об успешном завершении сессии, и предложит открыть сессию во встроенном плеере для просмотра записи, нажмите **«Да»**.

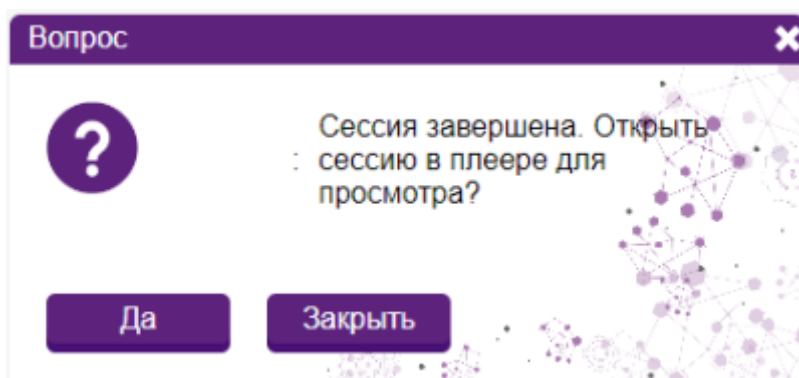


Рис. 10.10. Оповещения о завершении сессии для аудитора

### 10.3. Работа с завершенной сессией

#### 10.3.1. Ретроспективный просмотр действий пользователя

После завершения сессии и перехода к просмотру записи сеанса Система откроет окно встроенного плеера. В этом окне можно запустить последовательный просмотр всех скриншотов сессии. В нижней части окна располагается панель инструментов (для сессии с СЗС Linux (SSH) функционал сильно урезан). С их помощью можно запустить просмотр с нормальной скоростью. Из раскрывающегося списка выбрать скорость воспроизведения, таким образом ускорить или замедлить просмотр. Стрелки позволяют перемещаться между соседними кадрами, перейти в конец и начало сессии. Также можно приблизить или отдалить вкладки в окне сессии, открыть просмотр в отдельной вкладке.







Рис. 10.13. Пример выгруженных скриншотов сеанса

Вне Системы архив можно просматривать в виде отдельных скриншотов, воспроизведение в качестве видео возможно только внутри Системы. Для каждого сеанса в рамках сессии создается свой архив.

Функционал недоступен для сессии с СЗС Linux (SSH).