**Программное обеспечение Джим («Jim»)**

# РУКОВОДСТВО АДМИНИСТРАТОРА

На 38 листах

# Аннотация

В документе приведено руководство администратора программного обеспечения Джим («Jim») (далее – Система).

# Содержание

1 Общие сведения....6
1.1 Назначение Системы....6
1.2 Архитектура Системы....6
1.2.1 Модуль «Ядро»....7
1.2.2 Модуль «Коннекторы»....7
1.2.3 Модуль «API»....7
1.2.4 Модуль «МНП»....7
1.2.5 Модуль «БД»....8
1.3 Основные функции Системы....8
1.4 Краткое описание возможностей....8
1.5 Системные требования....8
1.6 Требования к конфигурации аппаратного обеспечения Системы....9
2 Описание веб-интерфейса Системы....10
2.1 Вход в веб-интерфейс....10
2.1.1 Вход под локальной УЗ....10
2.2 Описание основных элементов интерфейса и общих операций....11
2.2.1 Главное меню....11
2.2.2 Сотрудники....12
2.2.2.1 Создание карточки пользователя....12
2.2.2.2 Карточка пользователя: просмотр и изменение сведений о сотруднике (кадровые данные, роли, учетные записи)....14
2.2.2.2.1 Просмотр и изменение сведений о трудоустройствах сотрудника....14
2.2.2.2.2 Просмотр списка ролей, назначенных сотруднику, и его изменение....14
2.2.2.2.3 Просмотр и изменение УЗ (блокировка/разблокировка учетных записей сотрудника....15
2.2.3 Организационная структура....16
2.2.3.1 Добавление подразделения....17
2.2.3.2 Удаление подразделения....18
2.2.4 Роли....19
2.2.4.1 Просмотр списка ролей....19
2.2.4.2 Создание роли....20
2.2.5 Подключение к ИС....21
2.2.5.1 Просмотр списка подключенных ИС....21
2.2.5.2 Просмотр и редактирование данных в карточке подключения ИС....22
2.2.5.2.1 Вкладка Система....22
2.2.5.2.2 Вкладка Коннектор....23
2.2.5.2.3 Вкладка Свойства подключения....23
2.2.5.2.4 Вкладка Учётные записи....24
2.2.5.3 Подключение новой информационной системы....24
2.2.6 Объекты системы....26
2.2.6.1 Поиск объектов....27
2.2.7 Серверные задачи: управление задачами, выполняемыми на сервере....28
2.2.7.1 Создание задачи....28
2.2.7.2 Редактирование параметров задачи....29
2.3 Отчёты....30
3 Администрирование Системы....31
3.1 Настройка аутентификации....31
3.1.1 Настройка аутентификации с помощью JWT-токена....31

3.1.1.1 Получение JWT-токена....31
3.1.1.2 Запрос к серверу с использованием токена....32
3.2 Общие настройки системы .... 32
3.3 Взаимодействие со смежными ИС .... 33
3.3.1 Настройка взаимодействия с кадровым источником....33
3.3.1.1 Добавление новой задачи ....33
3.3.2 Подключение ИС....33
3.3.2.1 Настройка подключения к ИС....33
3.3.2.1.1 Настройка подключения....35
3.4 Управление УЗ пользователей в целевых системах .... 36
3.4.1 Конфигурирование объектов управляемых систем ....36
3.5 Настройка МНП .... 36
3.5.1 Общая структура модуля....36
3.5.2 Настройка параметров назначения МНП ....37
3.6 Настройка функциональных ролей Системы .... 37
3.7 Настройка уведомлений .... 38

# Перечень терминов и сокращений

| Термин/сокращение | Описание |
|---|---|
| API | Application Programming Interface, программный интерфейс приложений |
| Event Handler | Набор инструкций, которые обрабатывают события и выполняют соответствующие действия при их возникновении. |
| JWT | Json Web Token, ключ аутентификации пользователя. Используется для запросов к защищенным методам API. |
| IDM | Система класса Identity Manager |
| ORM | Object-Relational Mapping, объектно-реляционное отображение, инструмент для работы с реляционными базами данных (СУБД) через объекты языков программирования, вместо написания SQL-запросов вручную. |
| PostgreSQL | Объектно-реляционная система управления базами данных |
| Quartz | Quartz Scheduler, библиотека с открытым исходным кодом для планирования задач в приложениях на языке Java |
| АС | Автоматизированная система |
| БД | База данных |
| Внешний пользователь | Работник, информация о котором отсутствует в источнике кадровых данных |
| ИС | Информационная система |
| МНП | Минимальный набор прав |
| Система | Программное обеспечение Джим («Jim») |
| СУБД | Система управления базами данных |

# 1 Общие сведения

## *1.1 Назначение Системы*

Джим – это программный комплекс, который автоматизирует процесс управления правами доступа работников в информационных системах (далее – ИС) Компании.

Система получает из кадровых источников сведения о работниках и на их основе централизованно управляет учётными записями и правами доступа в различных ИС. Процесс может быть дополнен согласованием, подтверждением прав и другими необходимыми процедурами.

## *1.2 Архитектура Системы*

Архитектура Системы является распределенной и состоит из нескольких модулей:

1) Ядро,
2) МНП,
3) Коннекторы,
4) API,
5) БД.

На Рис. 1 представлена схема архитектуры Системы.

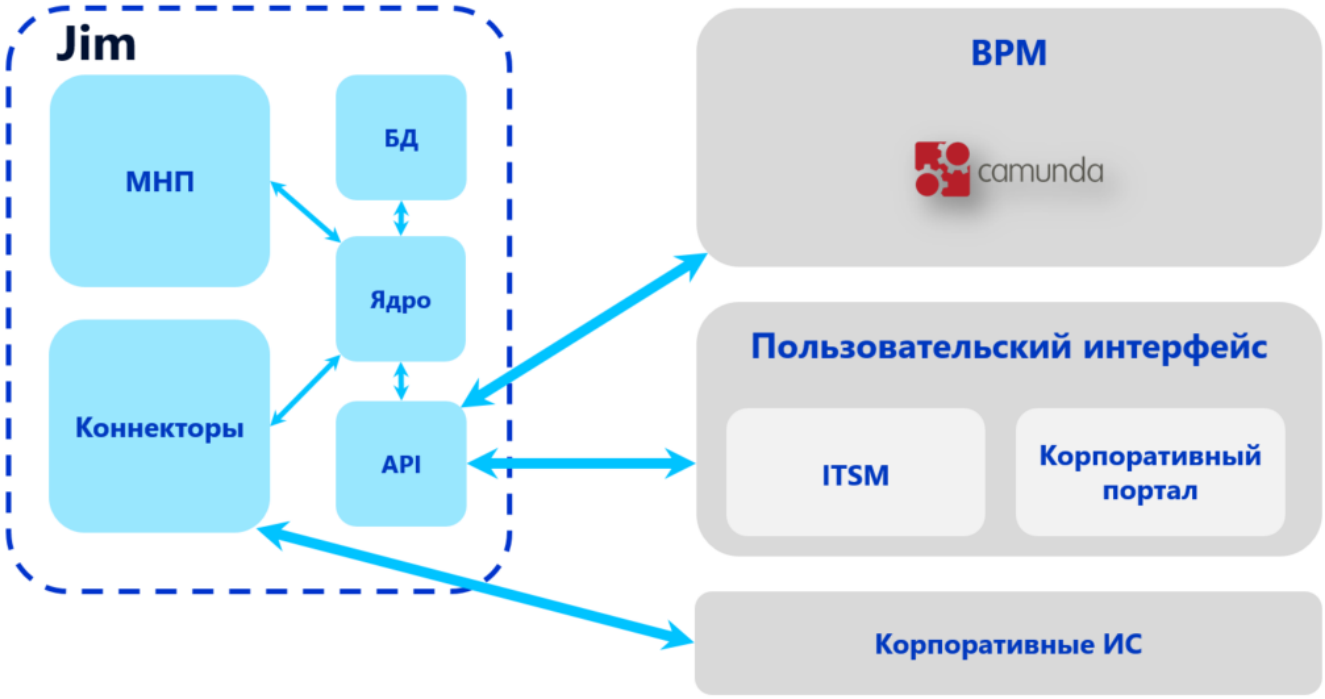


**Рис. 1 Архитектура Системы**

### 1.2.1 Модуль «Ядро»

Это центральный модуль системы, реализующий функциональность работы с объектной моделью и управления других компонентов. Представляет собой java-приложение, реализующее:

- объектный слой системы – представление объектов БД в виде Java-классов,
- функциональность работы с БД (ORM),
- функциональность исполнения задач по расписанию (на базе Quartz),
- функциональность авторизации,
- функциональность Event Handler-ов.

Ядро поддерживает работу в составе нескольких экземпляров, которым могут быть присвоены функциональные роли. Таким образом обеспечивается кластеризация уровня приложения.

### 1.2.2 Модуль «Коннекторы»

Модуль «Коннекторы» обеспечивает синхронизацию данных между Системой и подключенными информационными системами: получает задачи по управлению правами доступа через вызовы со стороны Ядра и обеспечивает их выполнение, взаимодействуя с подключенными ИС при помощи выбранных механизмов взаимодействия.

Коннекторы реализуются на основе стандарта ConnID и исполняются под управлением Сервера коннекторов (Connector Server).

### 1.2.3 Модуль «API»

Это программный интерфейс, обеспечивающий подключение к Системе других внешних систем для получения ими данных из Системы или выполнения операций над объектами Системы.

В качестве таких внешних систем могут выступать:

– ITSM-система, портал, выполняющие роль пользовательского интерфейса для создания и согласования заявок.

– Платформа Camunda для моделирования и автоматизации бизнес-процессов управления правами доступа.

Авторизация при вызове API реализуется внутренней ролевой моделью Системы.

### 1.2.4 Модуль «МНП»

Это механизм, позволяющий настраивать правила, в соответствии с которыми пользователям автоматически назначаются роли в Системе – минимальный набор прав.

Правила формулируются на языке SQL и возвращают набор пар пользователь-роль. Частью модуля также является механизм пересчёта правил, состоящий из очереди пересчёта и

задачи пересчёта, которая исполняется по расписанию и обрабатывает очередь. Интерфейсом данного модуля является «матрица доступа» – таблица пар пользователь-роль, определяющая каким пользователям какие роли должны быть назначены в данный момент времени. При изменении состава данной таблицы срабатывают Event Handler-ы, которые приводят полномочия пользователей к текущему состоянию матрицы путём назначения или отзыва ролей.

#### 1.2.5 Модуль «БД»

БД представляет собой сервер хранения реляционных данных PostgreSQL. Она обеспечивает хранение данных и метаданных, необходимых для функционирования системы. Для БД может быть настроена кластерная конфигурация стандартными средствами.

Модель данных является расширяемой, в рамках внедрения продукта в БД могут быть добавлены таблицы или столбцы.

## *1.3 Основные функции Системы*

Основными функциями Системы являются:

– Автоматическое управление правами доступа пользователей в подключенных к Системе ИС в зависимости от информации по работникам, получаемой из источника кадровых данных.

– Создание и согласование заявок на предоставление и отзыв прав доступа в подключенных к Системе ИС.

– Формирование отчетов по данным пользователей и их правам доступа в подключенных ИС.

– Ведение данных по работникам, информация о которых отсутствует в источнике кадровых данных, но которым требуется доступ в ИС Компании (далее – внешние пользователи).

– Управление правами доступа в подключенных к Системе ИС для внешних пользователей.

– Автоматическое создание рабочих заданий на ручное исполнение в ITSM-системе в рамках реализованных в Системе бизнес-процессов.

## *1.4 Краткое описание возможностей*

Пользователь с ролью «Администратор» имеет доступ ко всем функциям Системы (1.3), в том числе возможность создавать и настраивать роли для других пользователей Системы.

## *1.5 Системные требования*

Для работы Администратора Системы необходимы:

– Дистрибутив операционной системы;

– Веб-браузер для работы с Системой;

– Доступ к сети.

## *1.6 Требования к конфигурации аппаратного обеспечения Системы*

Минимальная конфигурация представлена в документе «2. Функциональные характеристики ПО JIM».

# 2 Описание веб-интерфейса Системы

## *2.1 Вход в веб-интерфейс*

Администратору доступна аутентификация в интерфейсе Системы под локальной УЗ – вход в Систему с обязательным вводом логина и пароля (раздел 2.1.1).

### 2.1.1 Вход под локальной УЗ

Для входа в веб-интерфейс Системы следует в адресной строке браузера ввести адрес Системы после установки. Отобразится окно авторизации (Рис. 2).

Для входа в Систему необходимо в соответствующие поля ввести учетные данные (логин и пароль) и нажать кнопку Войти (Рис. 2).

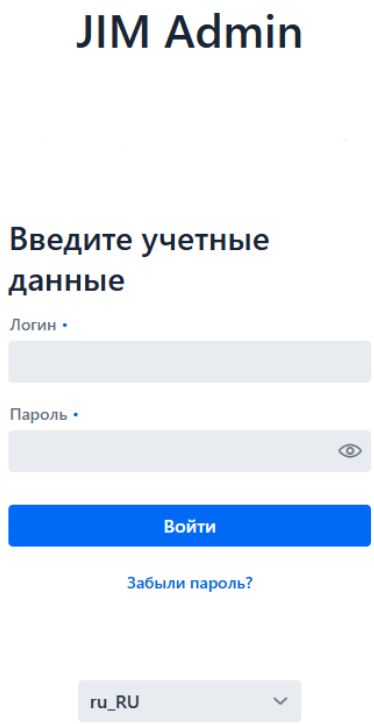


**Рис. 2 Вход в систему**

При вводе неверных данных вход в Систему выполнен не будет, а на экране отобразится сообщение: «Ошибка авторизации, неверный логин и/или пароль».

После успешного входа в Систему на экране отобразится главное меню панели администрирования (Рис. 3).

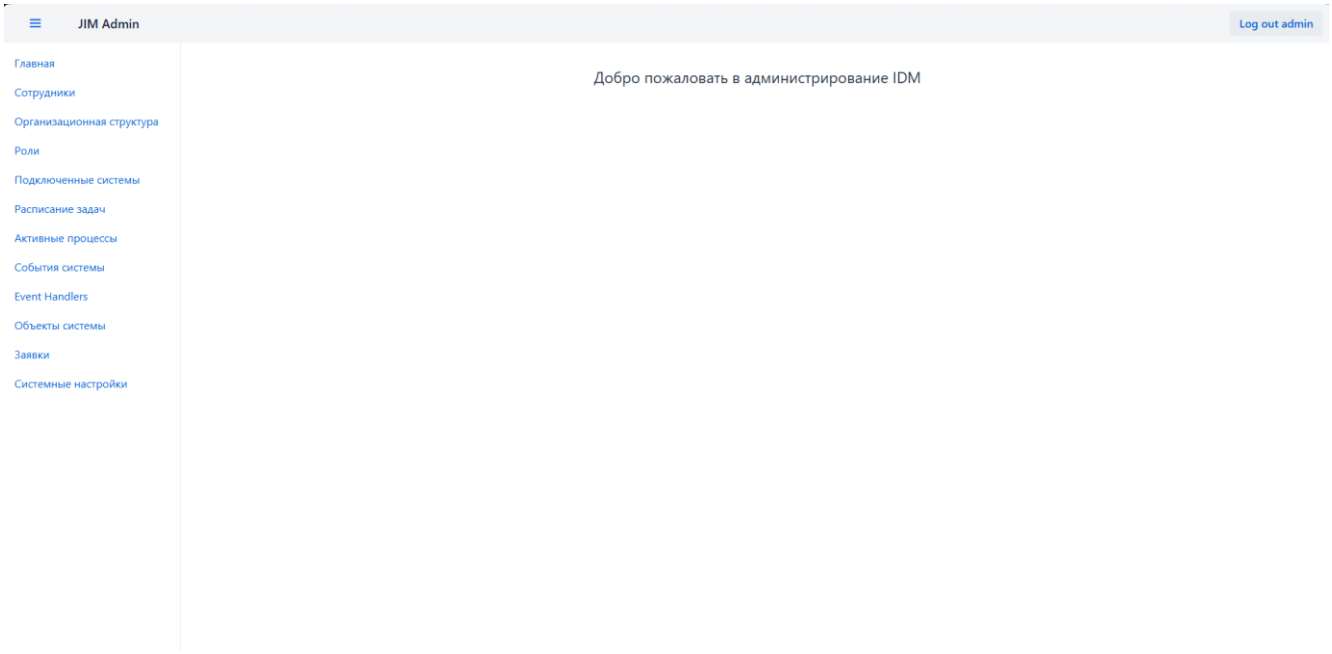


**Рис. 3 Главное меню панели администрирования IDM**

## *2.2 Описание основных элементов интерфейса и общих операций*

Каждая страница веб-интерфейса Системы содержит необходимый для выполнения конкретных задач набор стандартных элементов управления и отображения, таких как меню, панель навигации, кнопка, флажок, поле со списком, поле ввода данных, переключатель, список объектов, таблица, вкладка и т. д.

### 2.2.1 Главное меню

Навигация по разделам интерфейса выполняется с помощью меню, расположенного в левой части страницы. Чтобы раскрыть или свернуть меню, необходимо нажать на  в области меню (Рис. 4).

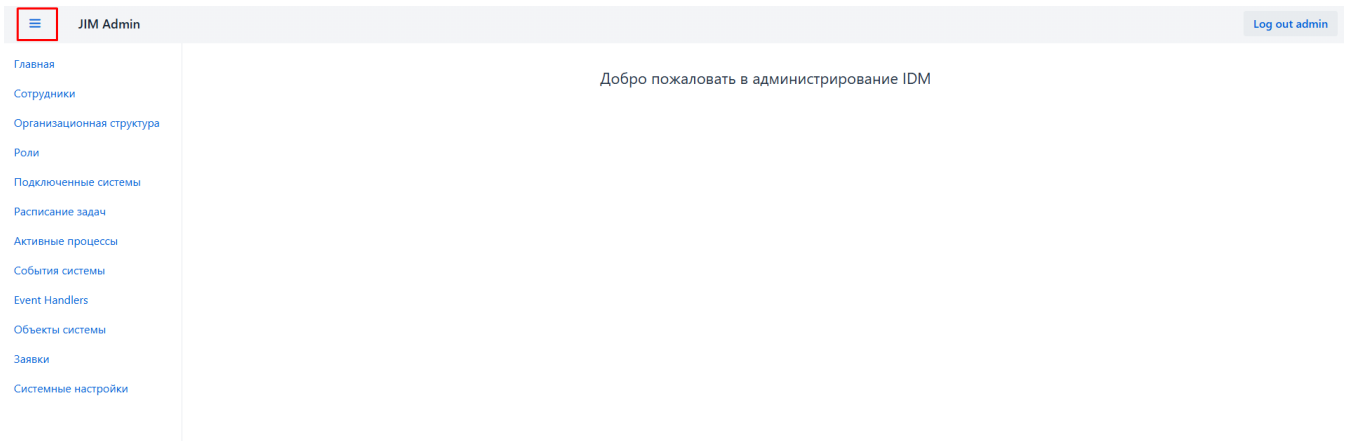


**Рис. 4 Главное меню, управление меню навигации**

В меню при нажатии на конкретный пункт отображается блок ссылок на соответствующие разделы интерфейса. Описание разделов меню приведены в Табл. 1.

**Табл. 1 Описание разделов главного меню**

| Раздел интерфейса | Описание |
|---|---|
| Сотрудники | Раздел с данными пользователей Системы |
| Организационная структура | Раздел, предназначенный для управления организационно-штатной структурой |
| Роли | Раздел с перечнем всех ролей в Системе |
| Подключенные системы | Раздел, предназначенный для управления подключенными ИС |
| Расписание задач | Раздел, предназначенный для управления и настройки задач по заданному расписанию; |
| Активные процессы | Раздел, предназначенный для просмотра процессов Системы, включая имя, дату запуска, статус и шаги |
| События системы | Раздел, предназначенный для просмотра перечня событий системы, связанных с созданием и изменениям объектов, включая ошибки |
| Event Handlers | Раздел, предназначенный для просмотра обработчиков, которые запускаются по событию Системы |
| Объекты системы | Раздел, предназначенный для просмотра, изменения, удаления объектов Системы |
| Заявки | Разделы, предназначенные для работы с заявками пользователей |
| Системные настройки | Раздел, предназначенный для работы с техническими параметрами Системы |

### 2.2.2 Сотрудники

Вся информация о сотрудниках Компании (ФИО, подразделение, должность, логин и др.), а также сведения о его правах доступа к ИС Компании содержится в карточке пользователя.

Карточки пользователей в Системе создаются автоматически при синхронизации данных из кадрового источника. В Системе предусмотрена возможность создания карточки пользователя вручную в интерфейсе Системы.

#### *2.2.2.1 Создание карточки пользователя*

Для создания карточки пользователя следует:

1) Перейти в раздел Сотрудники (Рис. 5).

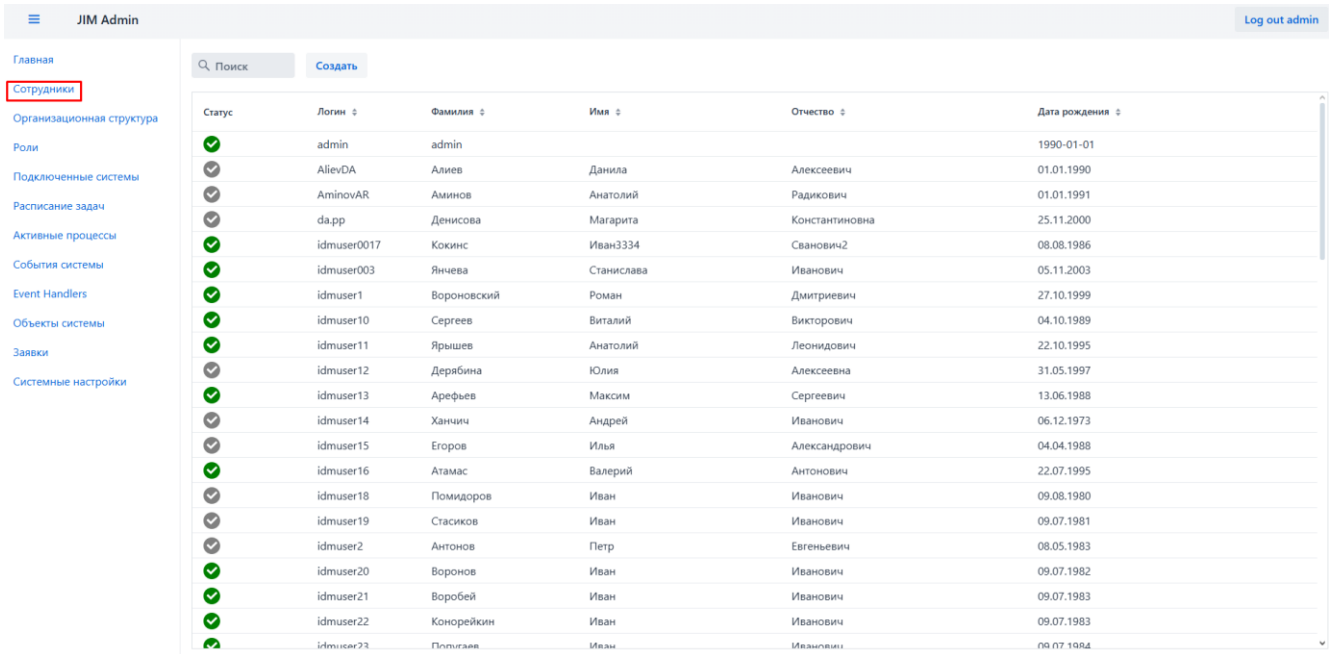


**Рис. 5 Раздел Сотрудники**

2) В разделе Сотрудники нажать кнопку **Создать**, появится панель создания нового сотрудника.

3) В открывшейся панели заполнить необходимые поля на вкладке **Основные данные** и нажать кнопку **Сохранить (**Рис. 6**)**. Далее перейти к следующей вкладке **Трудоустройства.**

4) На вкладке Трудоустройства нажать кнопку **Создать**, заполнить поля и нажать на кнопку **Сохранить** (Рис. 7).

5) После нажатия кнопки **Сохранить** будет создан новый сотрудник. Откроется карточка созданного сотрудника.

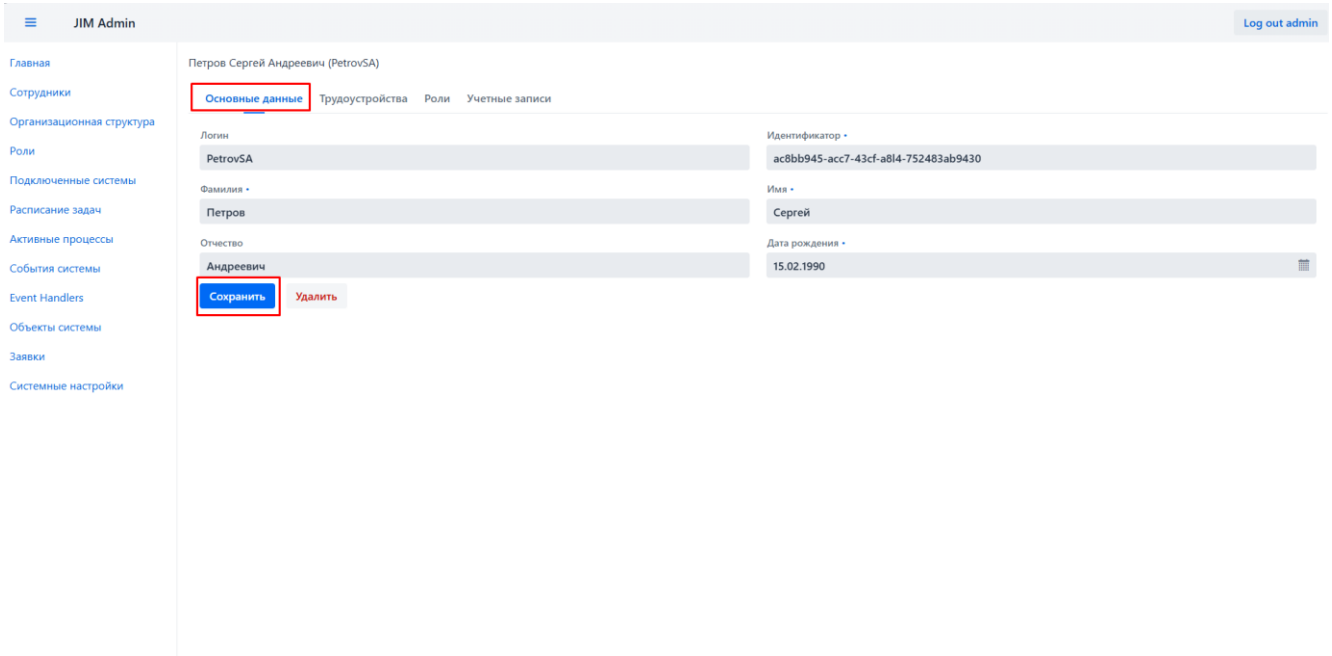


**Рис. 6 Добавление нового сотрудника – Основные данные**

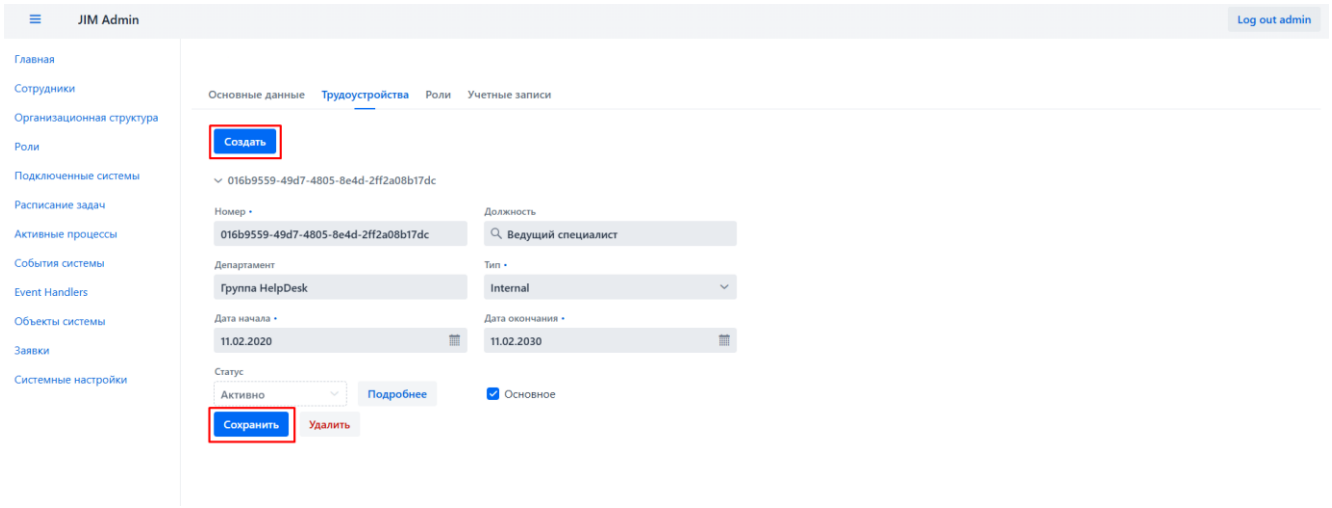


**Рис. 7 Добавление нового сотрудника – Трудоустройства**

#### *2.2.2.2 Карточка пользователя: просмотр и изменение сведений о сотруднике (кадровые данные, роли, учетные записи)*

Сведения о сотруднике (основные данные, кадровые данные, роли и учётные записи) можно просмотреть, открыв его карточку. Для этого следует:

1) В главном меню перейти в раздел **Сотрудники**.
2) В списке сотрудников нажать на строку с ФИО сотрудника.

##### 2.2.2.2.1 Просмотр и изменение сведений о трудоустройствах сотрудника

Трудоустройство – это сущность, которая хранит кадровую информацию о месте работы сотрудника (должность, подразделение, дата начала работы/увольнения и т.п.).

Для просмотра информации о трудоустройствах сотрудника необходимо в Карточке пользователя перейти на вкладку Трудоустройства (Рис. 7).

Информация о каждом трудоустройстве отображается в отдельной панели. В панели содержатся сведения о должности сотрудника и подразделении компании, где работает сотрудник, а также дата начала и окончания работы (при наличии). В самой панели, помимо вышеуказанных сведений, отображается различная кадровая информация: табельный номер, кадровый статус («Работает», «Уволен», «В отпуске» и т.д.), тип трудоустройства (например, «Штатный», «Внешний») и т.д.

##### 2.2.2.2.2 Просмотр списка ролей, назначенных сотруднику, и его изменение

Для просмотра информации о ролях сотрудника необходимо в Карточке пользователя перейти на вкладку Роли (Рис. 8).

В ячейках таблицы отображается следующая информация:

1) Название – название роли в Компании.
2) Тип – бизнес роль, одиночная роль, внутренняя и т.д.

3) Отображаемое наименование – отображение роли.

4) Описание – описание роли.

5) Тип назначения – основание для назначения роли.

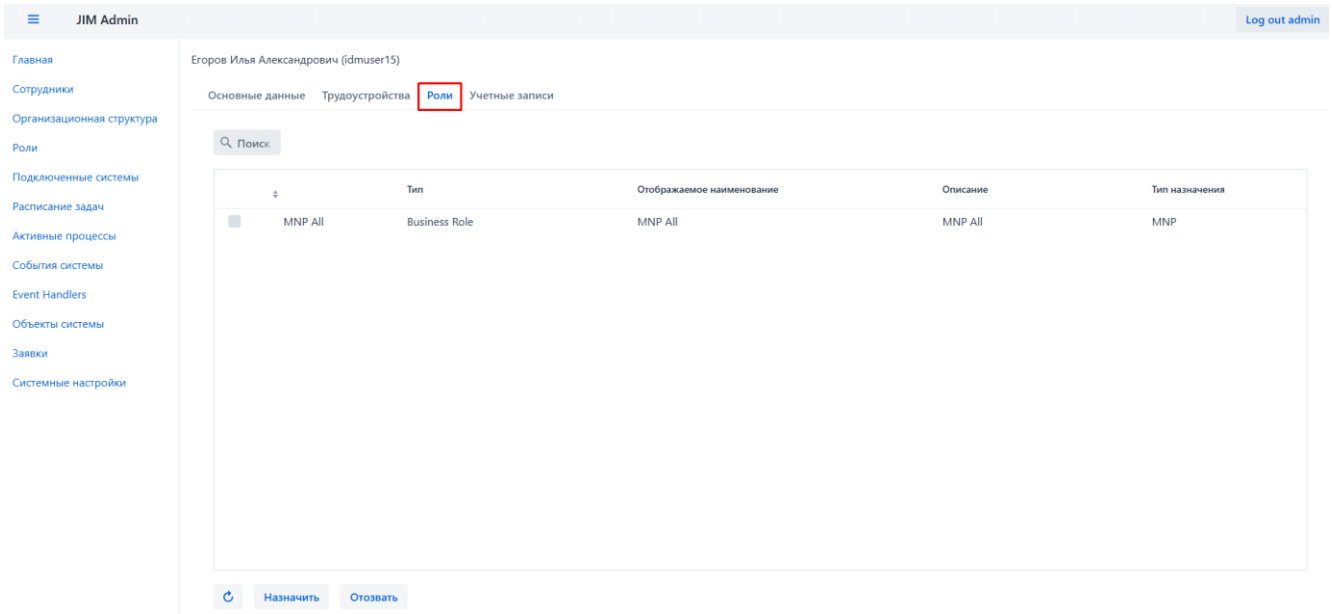


**Рис. 8 Просмотр карточки сотрудника – Роли**

### 2.2.2.2.3 Просмотр и изменение УЗ (блокировка/разблокировка учетных записей сотрудника

Для просмотра информации об учетных записях сотрудника необходимо в Карточке пользователя перейти на вкладку Учетные записи (Рис. 9).

В таблице отображается следующая информация:

1) Статус;

2) Имя;

3) Идентификатор;

4) Тип;

5) Система.

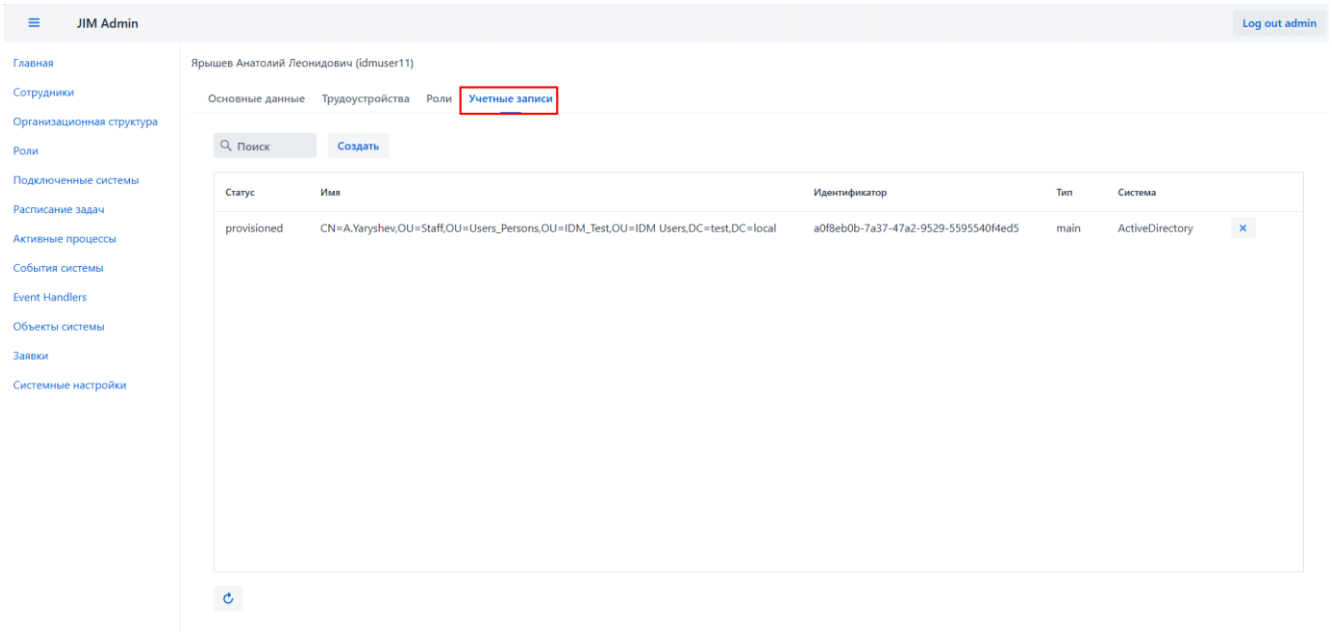


**Рис. 9 Просмотр карточки сотрудника – Учётные записи**

Нажав на строку учётной записи, можно просмотреть подробную информацию об УЗ: перечень атрибутов УЗ в информационной системе и их значения.

### 2.2.3 Организационная структура

Как правило, организационная структура в Системе создается автоматически при импорте данных из кадрового источника. В Системе также предусмотрена возможность создания и редактирования узлов структуры вручную в интерфейсе Системы.

Для просмотра и изменения организационной структуры компании необходимо перейти в раздел **Организационная структура** (Рис. 10).

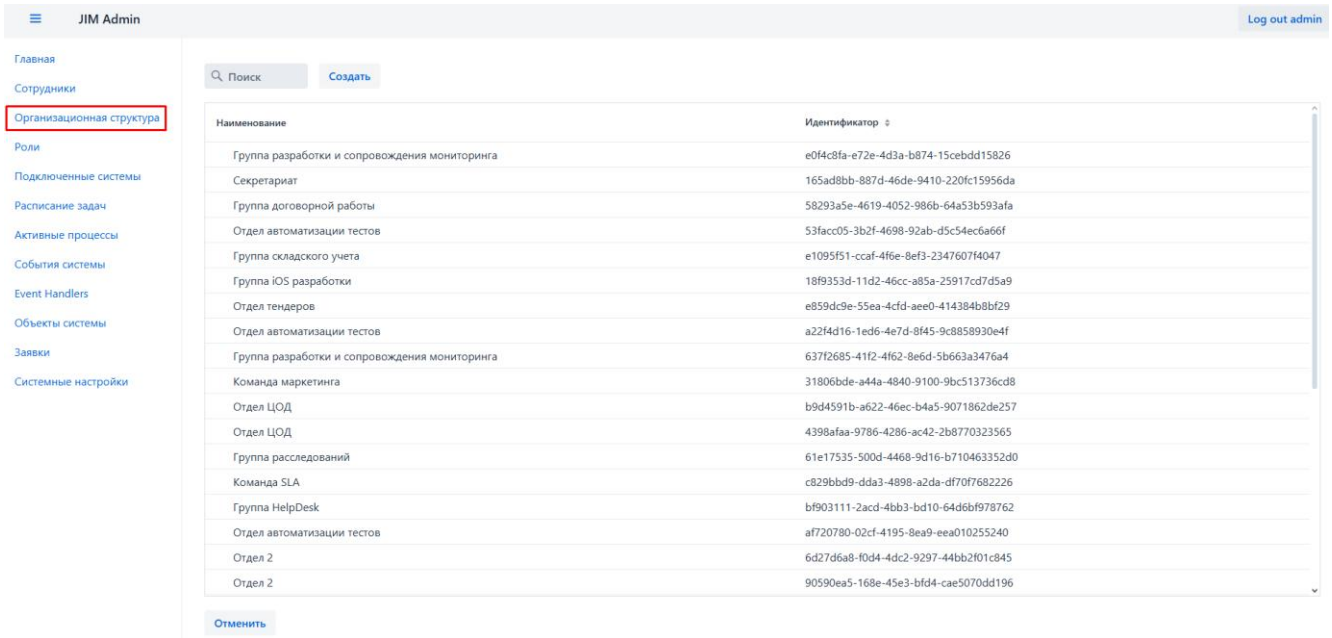


**Рис. 10 Раздел Организационная структура**

Раздел Организационная структура – структура с вложенностью всех существующих в системе узлов орг. структуры: корневых подразделений, дочерних подразделений и должностей.

Доступно выполнение следующих операций:

1) просмотр карточки подразделения;

2) добавление, редактирование и удаление узлов орг. структуры, а также их поиск.

При необходимости в разделе Организационная структура можно воспользоваться поиском любого узла по его названию. Для этого следует в поле поиска ввести название искомого узла (Рис. 11).

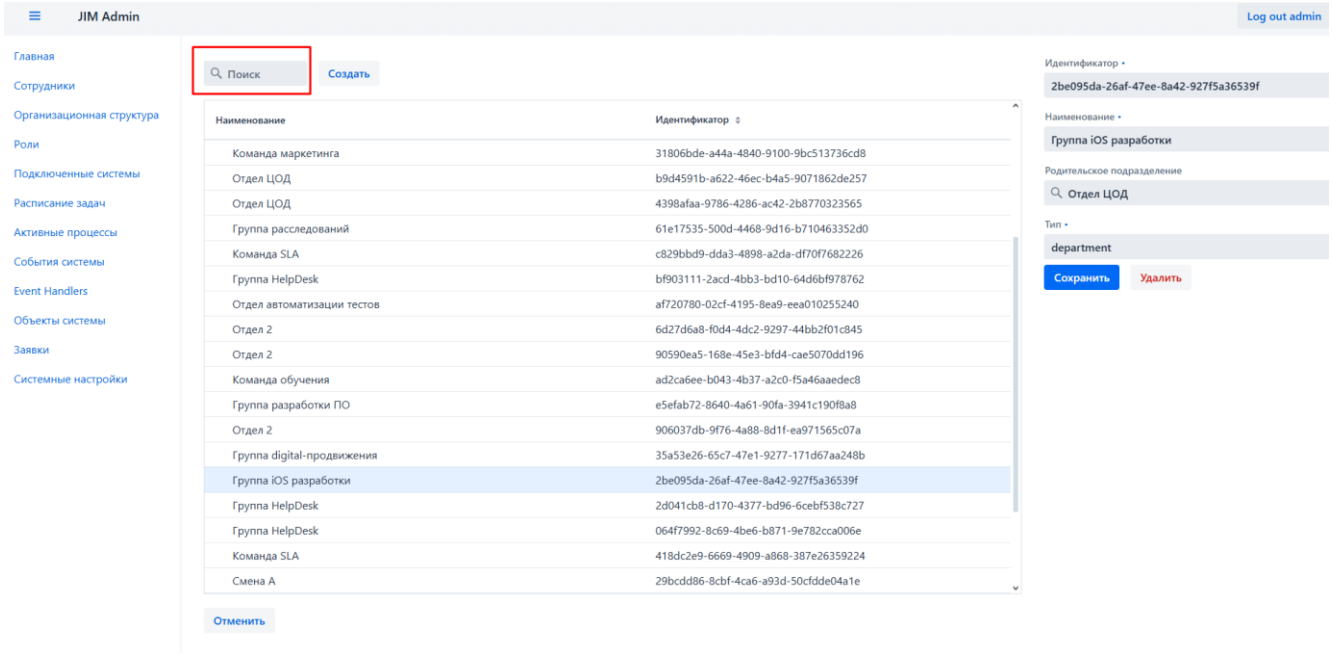


**Рис. 11 Орг. структура – поиск**

### *2.2.3.1 Добавление подразделения*

Для добавления узла ОШС следует:

1. В разделе Организационная структура нажать кнопку **Создать** (Рис. 12). Откроется панель создания нового структурного подразделения (Рис. 13).

2. Ввести название подразделения и тип. При необходимости следует заполнить необязательные атрибуты нового подразделения.

3. Для завершения добавления записи нового подразделения нажать кнопку **Сохранить** (Рис. 13).

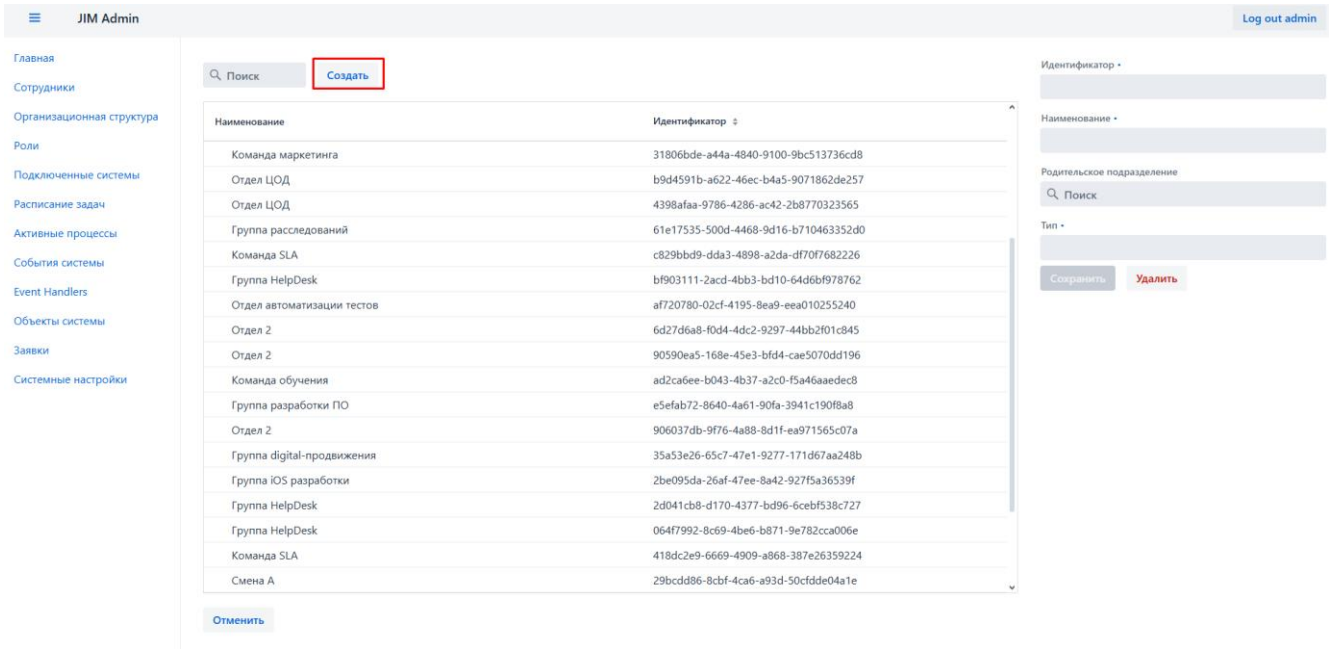


**Рис. 12 Орг. структура – создание**

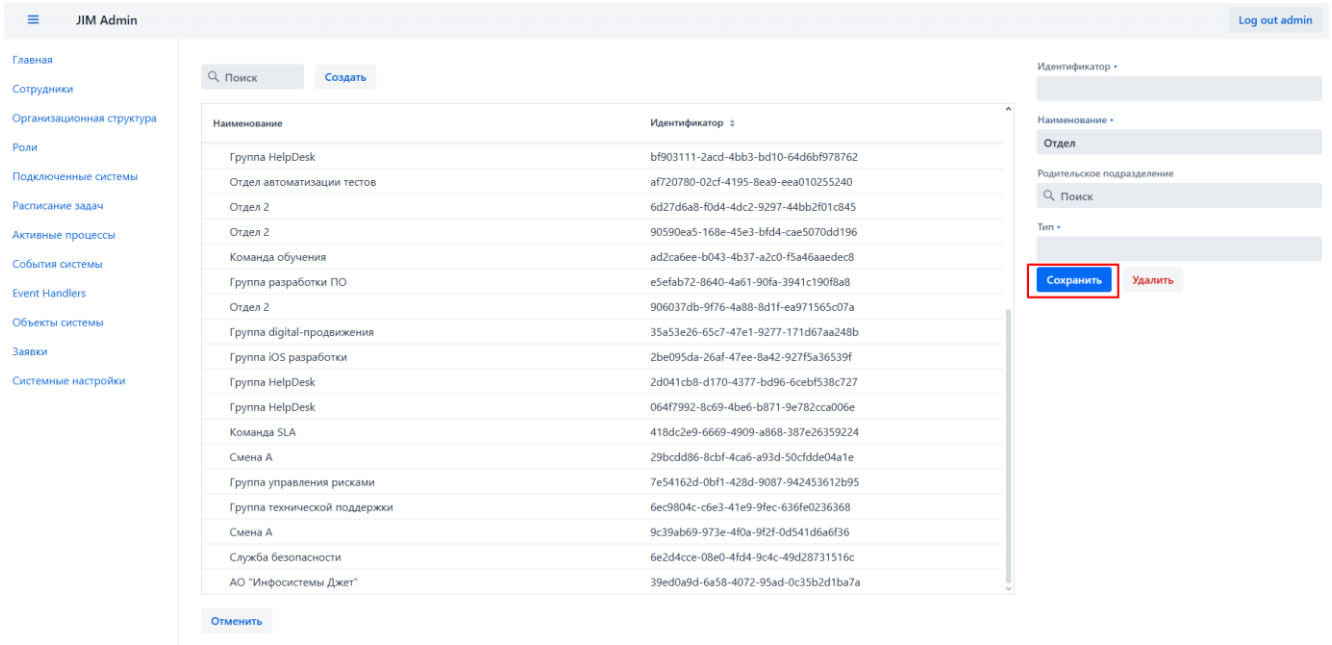


**Рис. 13 Орг. структура – сохранение нового подразделения**

### *2.2.3.2 Удаление подразделения*

Для удаления подразделения следует:

1) В разделе Организационная структура в иерархическом списке узлов выбрать требуемый узел;

2) Нажать кнопку Удалить (Рис. 14). Удалять можно только пустой узел, то есть узел, у которого нет дочерних узлов.

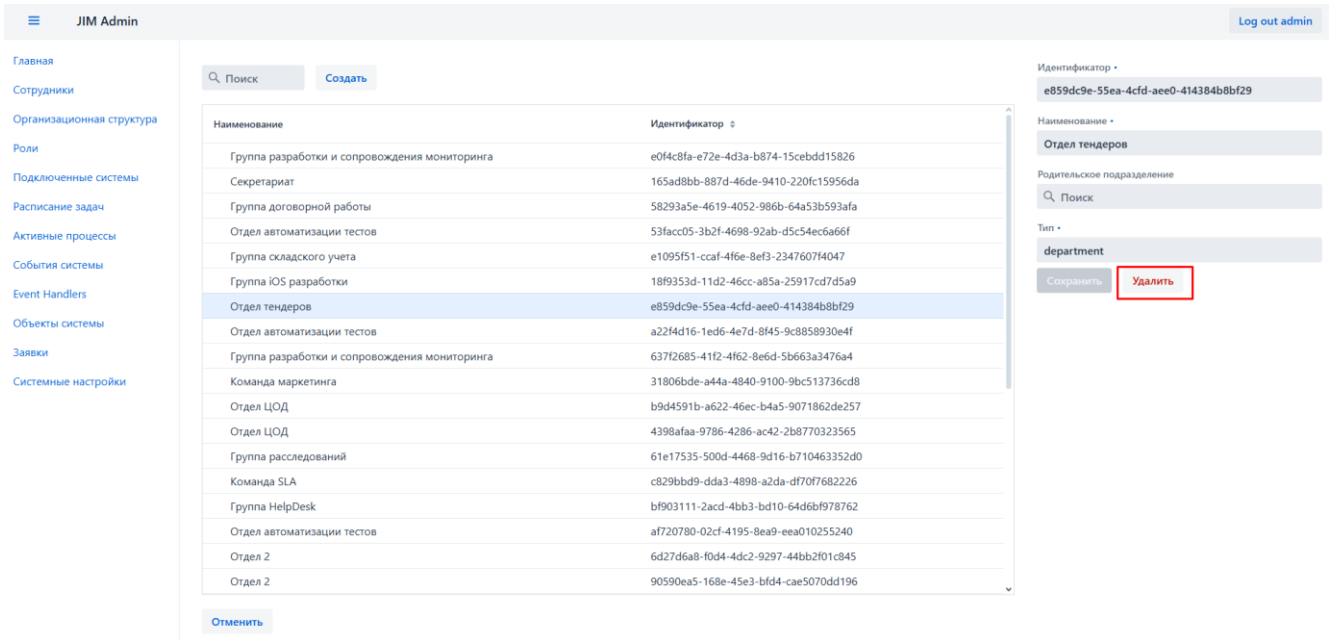


**Рис. 14 Орг. структура – удаление подразделения**

### 2.2.4 Роли

Роль – набор прав доступа, который назначается пользователю, в результате чего пользователь получает полномочия на выполнение некоторых действий.

#### *2.2.4.1 Просмотр списка ролей*

Для просмотра списка ролей необходимо перейти в раздел **Роли** (Рис. 15). В таблице с ролями отображается следующая информация:

1) Наименование – техническое имя роли в Системе.
2) Тип – бизнес роль, одиночная роль, внутренняя и т.д.
3) Отображаемое наименование – отображение роли.
4) Описание – описание роли.

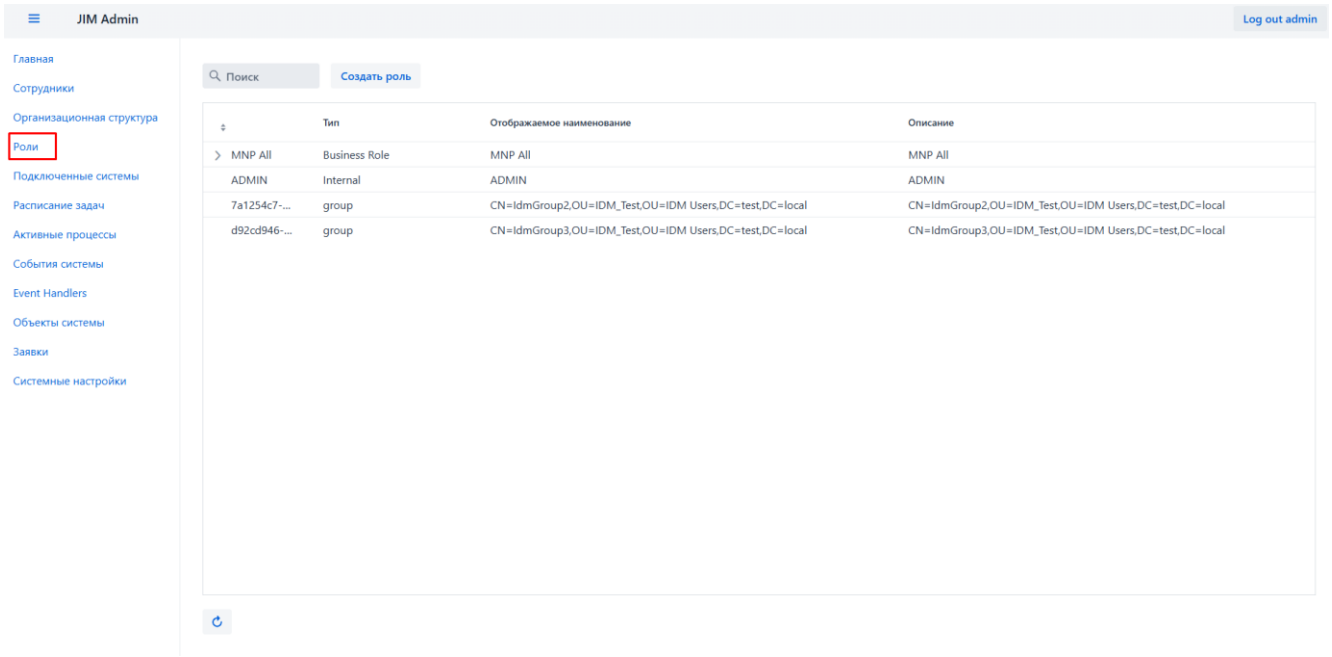


**Рис. 15 Раздел Роли**

### *2.2.4.2 Создание роли*

Для создания роли следует:

1) Нажать кнопку **Создать роль** (Рис. 16).
2) В отобразившейся панели заполнить необходимые поля.
   - Наименование – название роли в Компании.
   - Тип – бизнес роль, одиночная роль, внутренняя и т.д.
   - Отображаемое наименование – отображение роли.
   - Описание – описание роли.
3) Для завершения создания новой роли нажать кнопку **Сохранить** (Рис. 16).

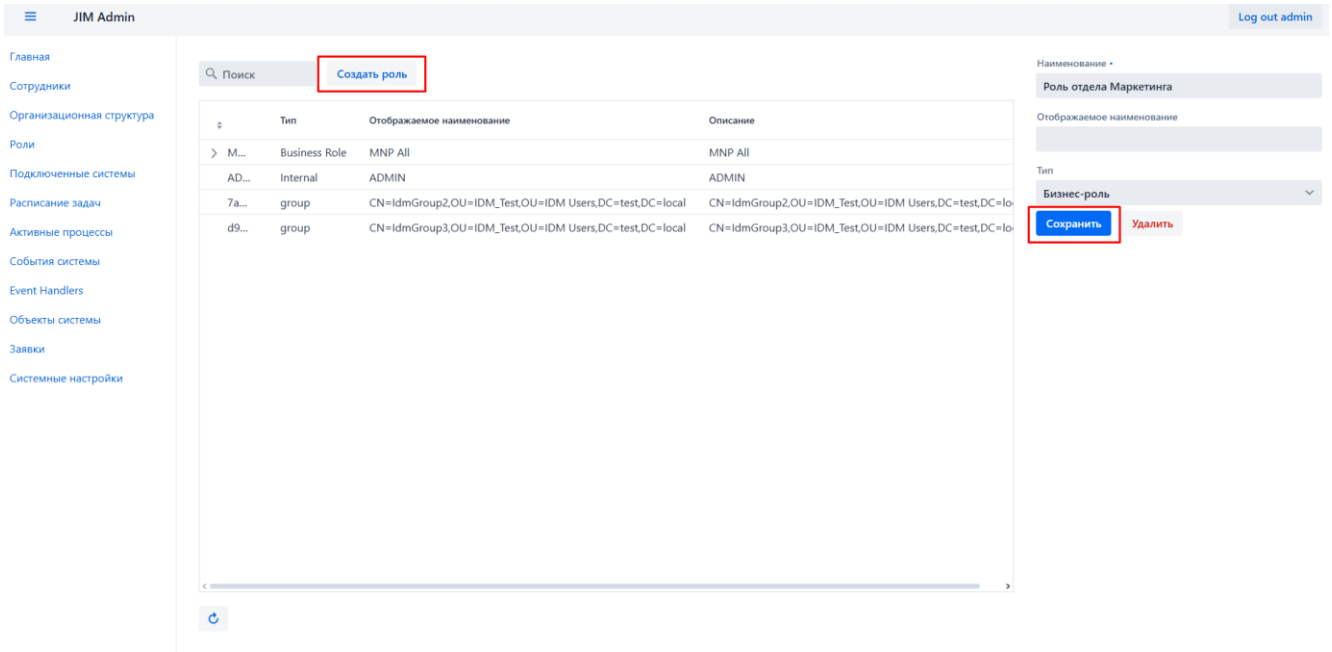


**Рис. 16 Роли – создание новой роли**

### 2.2.5 Подключение к ИС

Карточка ИС – это объект, определяющий настройки соединения и правила взаимодействия Системы и подключаемой ИС.

#### *2.2.5.1 Просмотр списка подключенных ИС*

Для просмотра карточек ИС следует:

1) Перейти в раздел Подключенные системы. Отобразится список всех карточек ИС (Рис. 17);

2) Выбрать необходимую ИС из списка, нажав на ее название. Откроется карточка ИС (Рис. 18).

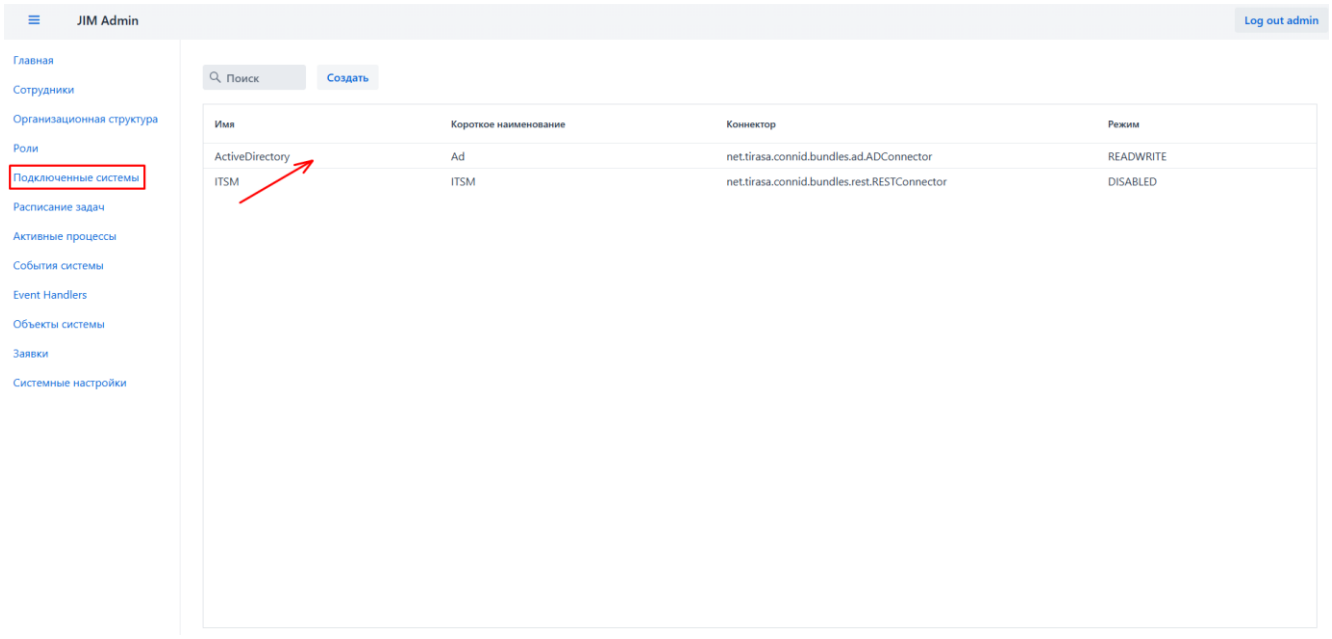


**Рис. 17 Раздел Подключенные системы**

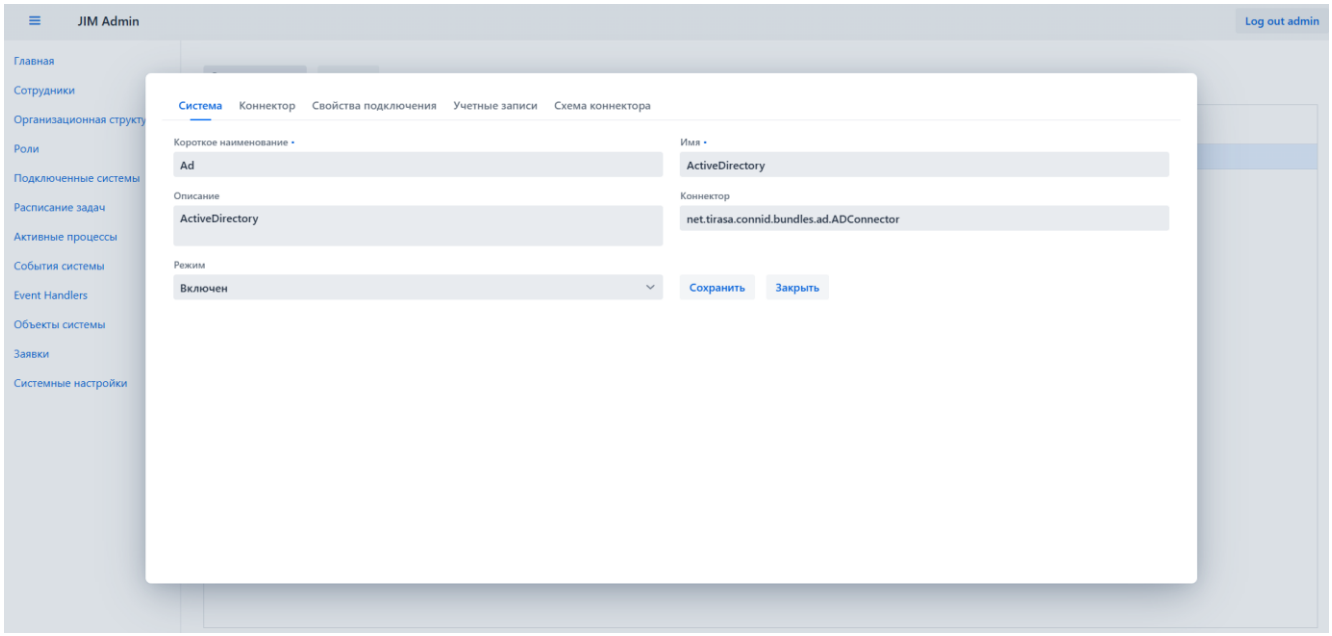


**Рис. 18 Подключенные системы – просмотр карточки ИС**

### *2.2.5.2 Просмотр и редактирование данных в карточке подключения ИС*

#### 2.2.5.2.1 Вкладка Система

На вкладке Система представлены общие данные о подключении (Рис. 18). На вкладке можно отредактировать наименование и описание системы, а также режим взаимодействия с системой – включен, выключен или доступен только для чтения. После внесения изменений необходимо нажать на кнопку **Сохранить**.

#### 2.2.5.2.2 Вкладка Коннектор

На вкладке Коннектор представлены параметры Коннектора, с помощью которого осуществляется взаимодействие с ИС. При внесении изменений необходимо нажать кнопку **Сохранить** (Рис. 19).

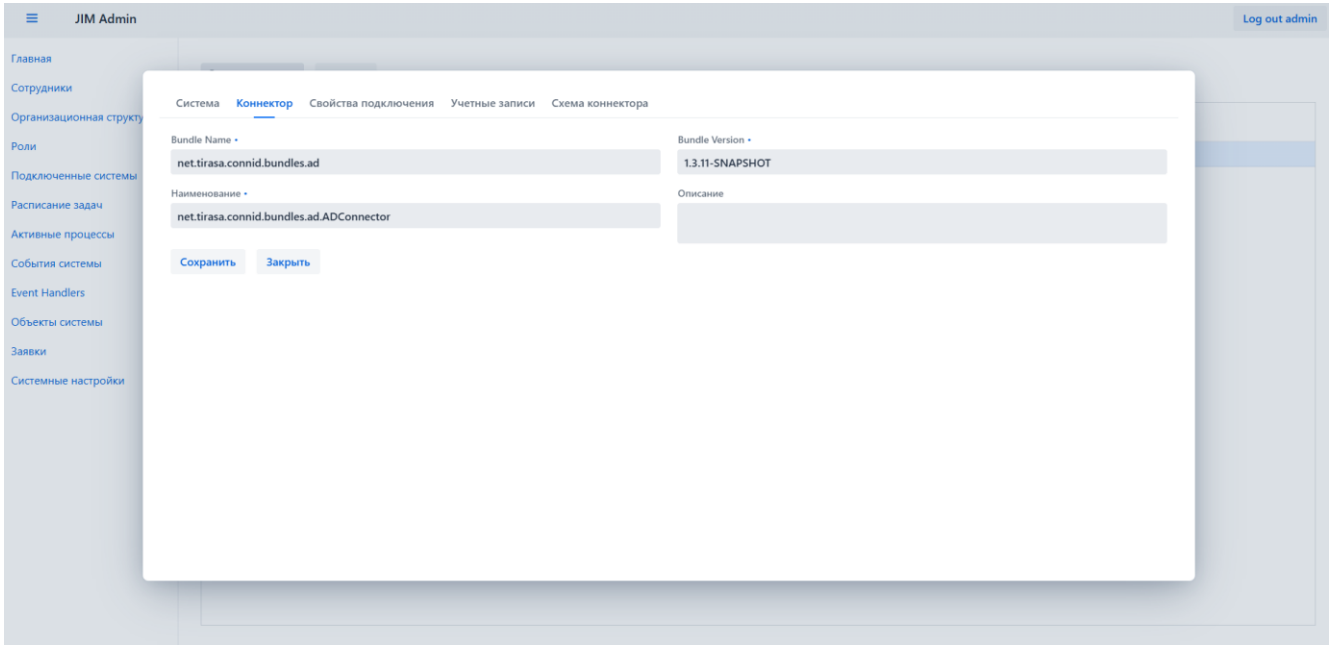


**Рис. 19 Подключенные системы – карточка ИС, коннектор**

#### 2.2.5.2.3 Вкладка Свойства подключения

На вкладке Свойства подключения представлены атрибуты подключения к ИС, доступные для редактирования.

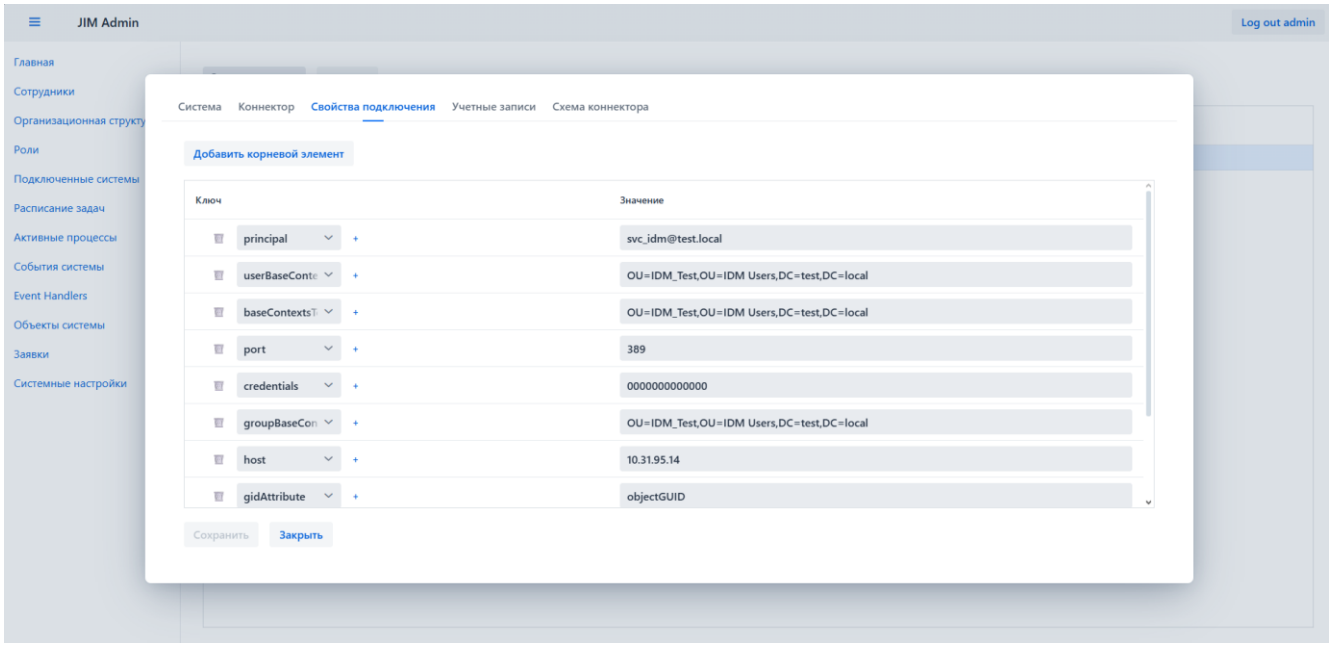


**Рис. 20 Подключенные системы – карточка ИС, свойства подключения**

#### 2.2.5.2.4 Вкладка Учётные записи

На вкладке Учётные записи представлен перечень учётных записей ИС, включая идентификаторы и статусы (синхронизирована, в процессе или ошибка синхронизации).

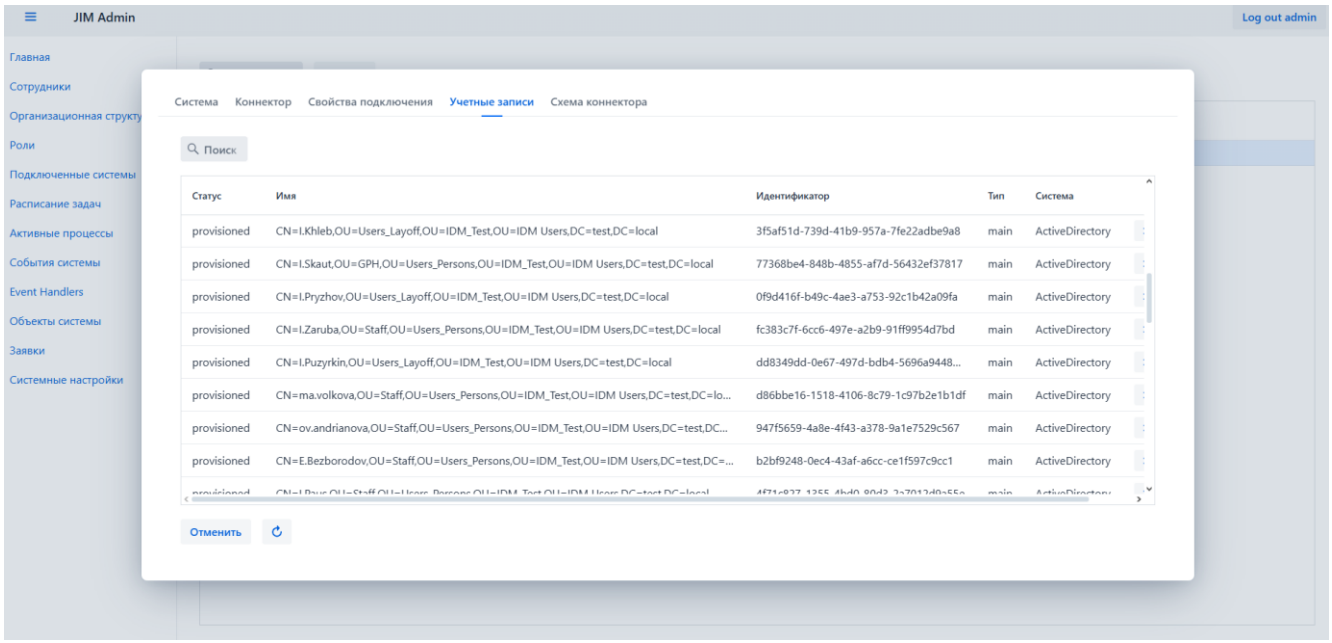


**Рис. 21 Подключенные системы – карточка ИС, Учётные записи**

### *2.2.5.3 Подключение новой информационной системы*

Для подключения новой ИС следует:

1) Перейти в раздел Подключенные системы и нажать кнопку Создать (Рис. 22). В отобразившемся окне заполнить поля «наименование» и «описание системы», а также режим взаимодействия с системой – включен, выключен или доступен только для чтения.

2) В поле Коннектор выбрать необходимый коннектор. Если требуемый коннектор отсутствует в Системе, следует нажать кнопку **Создать**, заполнить атрибуты в соответствии с 2.2.5.2.2, нажать кнопку Сохранить (Рис. 24).

3) После внесения изменений необходимо нажать на кнопку **Сохранить** (Рис. 23).

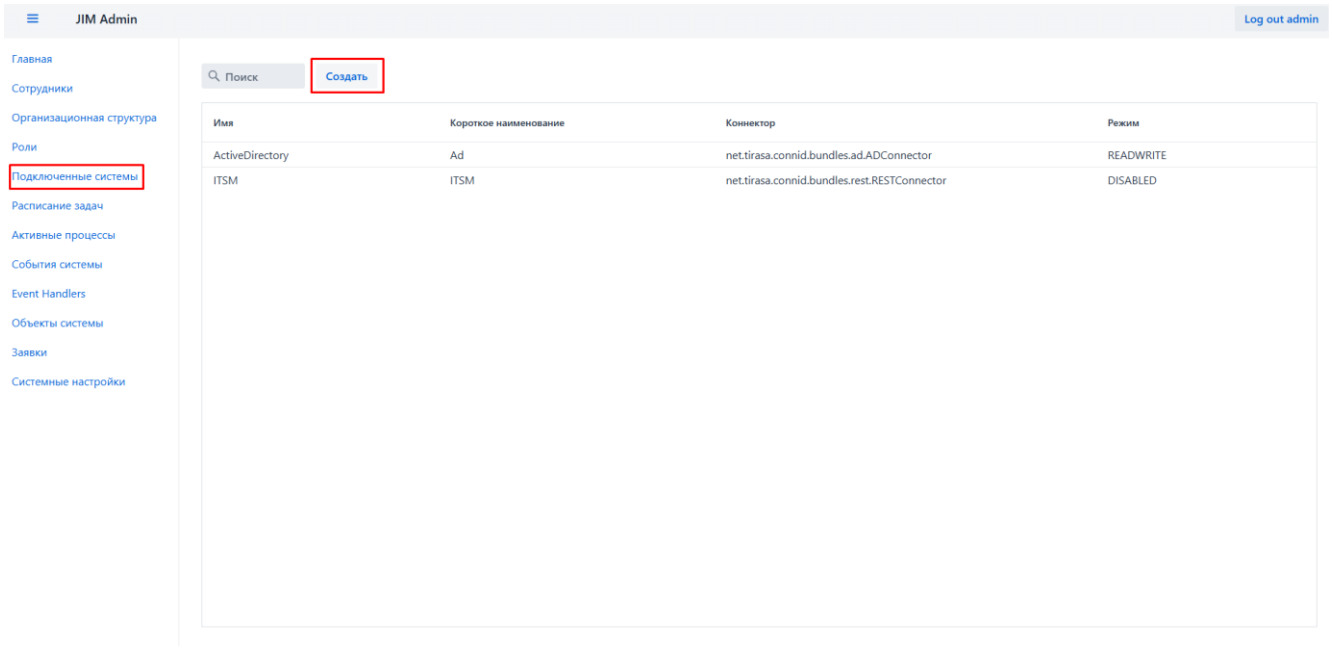


**Рис. 22 Подключенные системы – новая ИС**

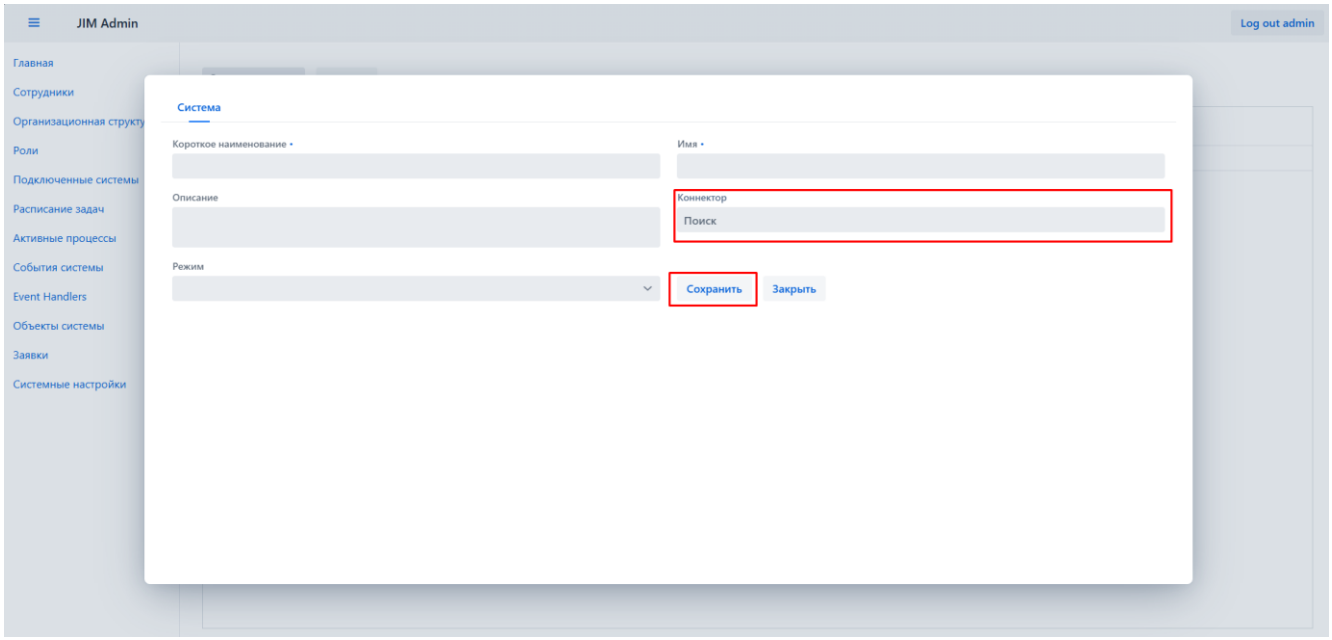


**Рис. 23 Подключенные системы – новая ИС, заполнение атрибутов**

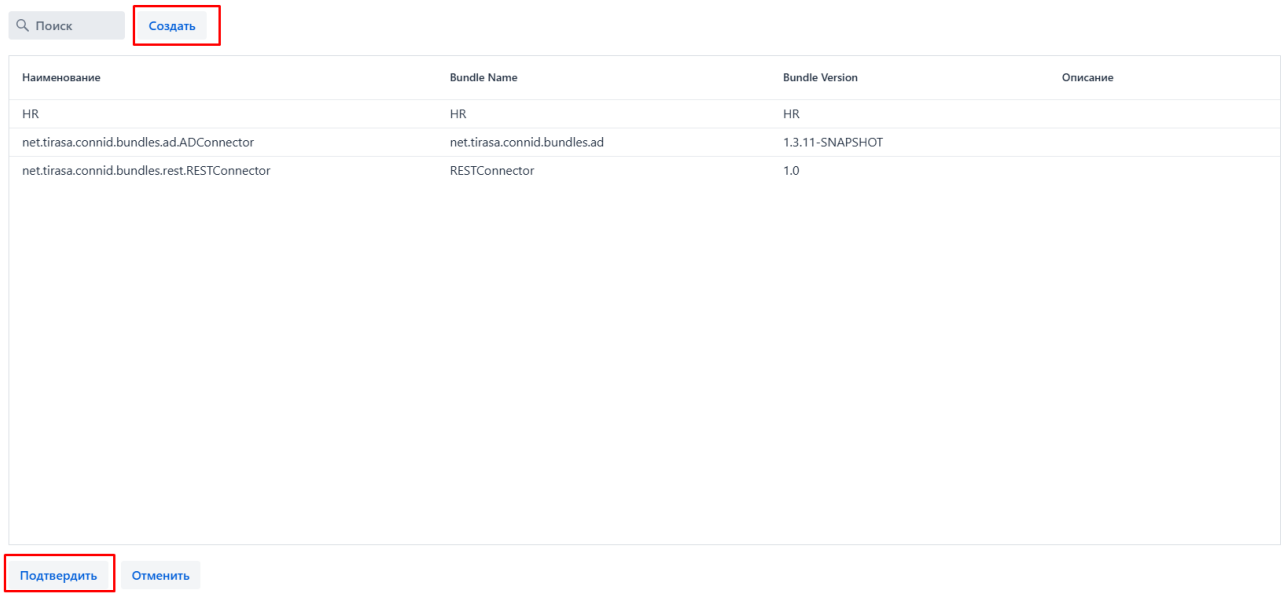


**Рис. 24 Подключенные системы – новая ИС, создание нового коннектора**

### 2.2.6 Объекты системы

Администратор может просматривать, создавать, редактировать и удалять объекты, находящиеся в хранилище Системы. Указанные операции выполняются в разделе Объекты системы. Для перехода в этот раздел необходимо в главном меню выбрать пункт Объекты системы (Рис. 25).

В Системе предусмотрены следующие типы объектов:

– Пользователь;
– Трудоустройство;
– Роль;
– Каталог;
– Подразделение;
– Должность;
– Заявка;
– Маршрут согласования;
– Назначение;
– Системная конфигурация;
– Объект конфигурации;
– Уведомление;
– Шаблон объекта;
– Информационная система;
– Шаблон интеграции;

– Коннектор;

– Серверная задача.

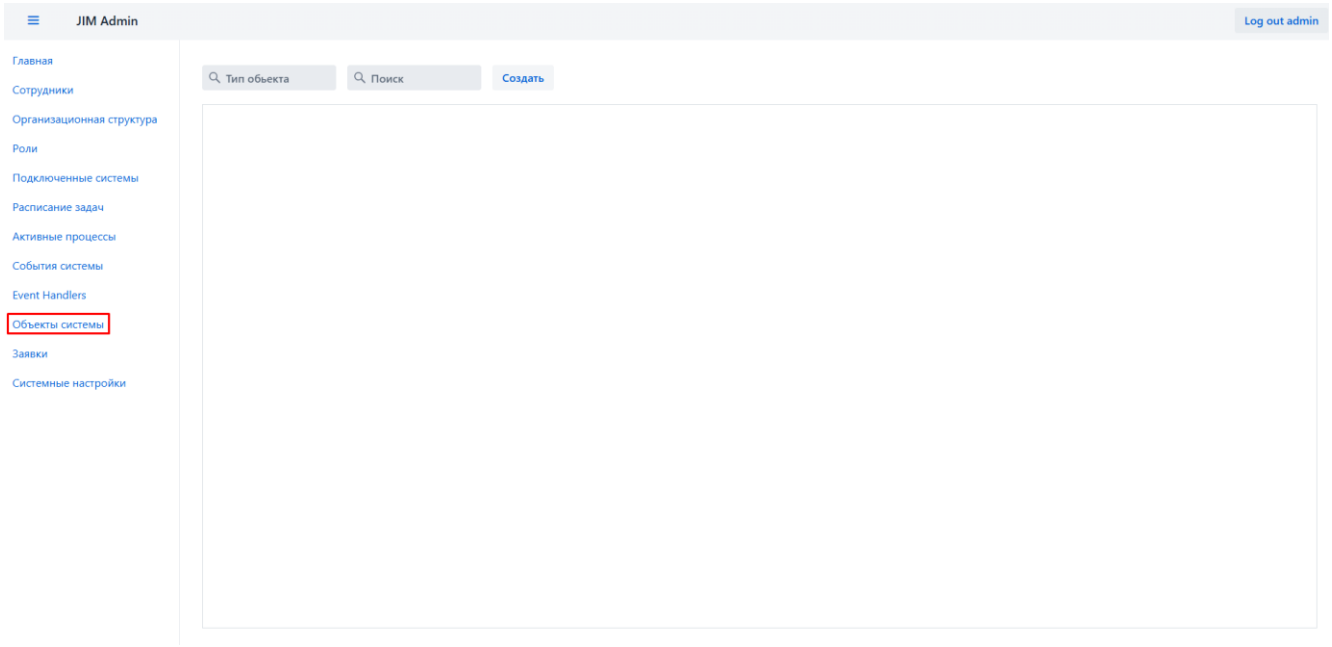


**Рис. 25 Раздел Объекты системы**

### *2.2.6.1 Поиск объектов*

Для отображения объекта определенного типа, необходимо нажать на поле Тип объекта и выбрать требуемый тип (Рис. 26).

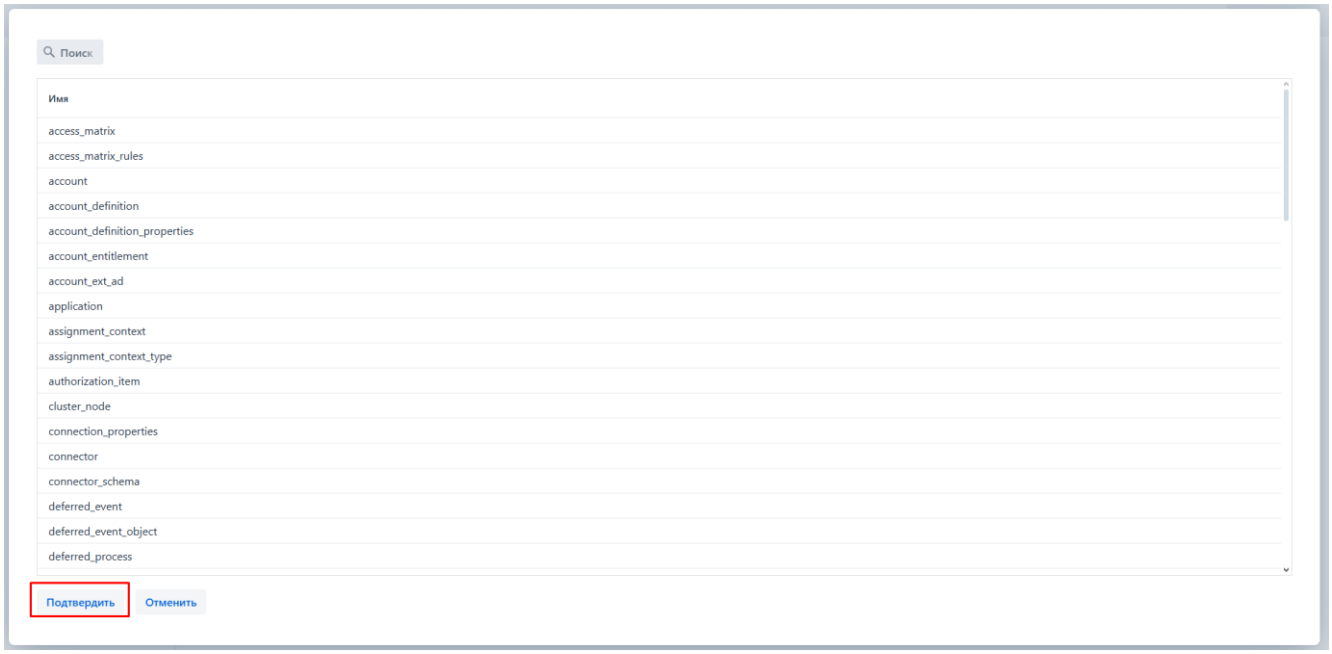


**Рис. 26 Объекты системы – Выбор типа объекта**

Для поиска требуемого объекта необходимо нажать на поле **Поиск** и начать заполнять поле искомым наименованием объекта. По мере заполнения поиска Система будет предлагать

наиболее релевантные результаты до того момента, пока не останется единственный искомый объект – используется предиктивный ввод.

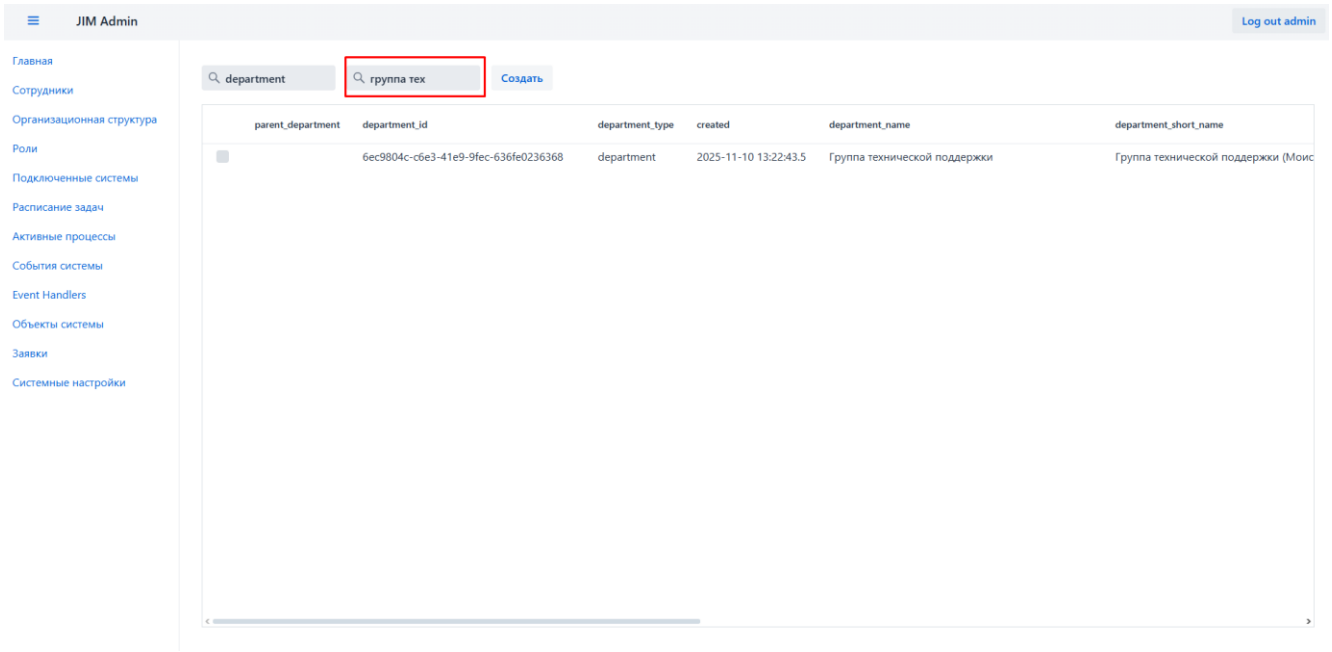


**Рис. 27 Объекты системы – Поиск объекта**

### 2.2.7 Серверные задачи: управление задачами, выполняемыми на сервере

Серверные задачи выполняются на сервере Системы в фоновом режиме. К таким задачам можно отнести, например, синхронизацию и реконсиляцию данных. При создании и настройке серверных задач администратор может указать, например, период времени, через который требуется запустить синхронизацию данных.

#### *2.2.7.1 Создание задачи*

Для создания серверной задачи следует:

1) В главном меню перейти в раздел Расписание задач.

2) Нажать на кнопку **Создать** (Рис. 28). Откроется раздел создания новой серверной задачи.

3) Заполнить параметры новой задачи.

- Пул – выбор приоритета запуска.
- Группа – вхождение в группу задач, например, в кадровую.
- Имя – название серверной задачи.
- Класс – выбрать класс объектов из выпадающего списка.
- Cron-расписание – задать даты, в которые выполняется задача, с указанной частотой.
- Флажок «Запустить по настроенному расписанию» – снять флажок, если задачи создаются в остановленном состоянии (не запускать сразу после создания);

4) Нажать кнопку **Сохранить** (Рис. 29).

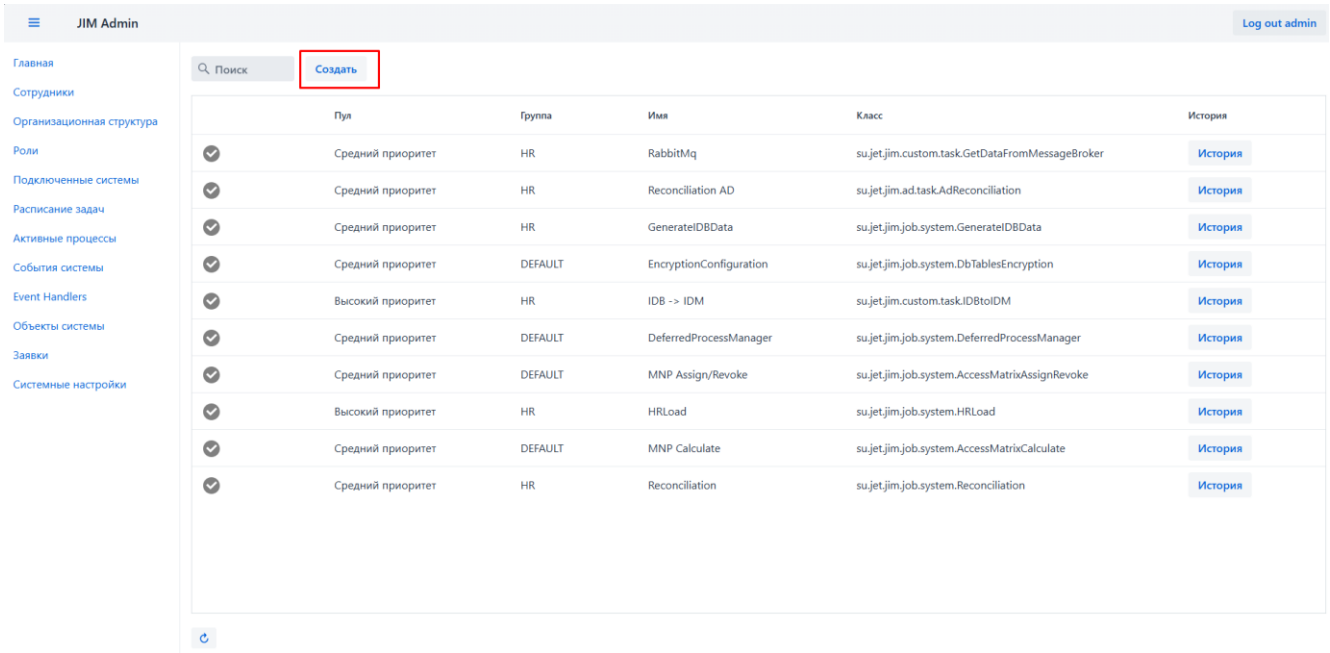


**Рис. 28 Серверные задачи – Создание задачи**

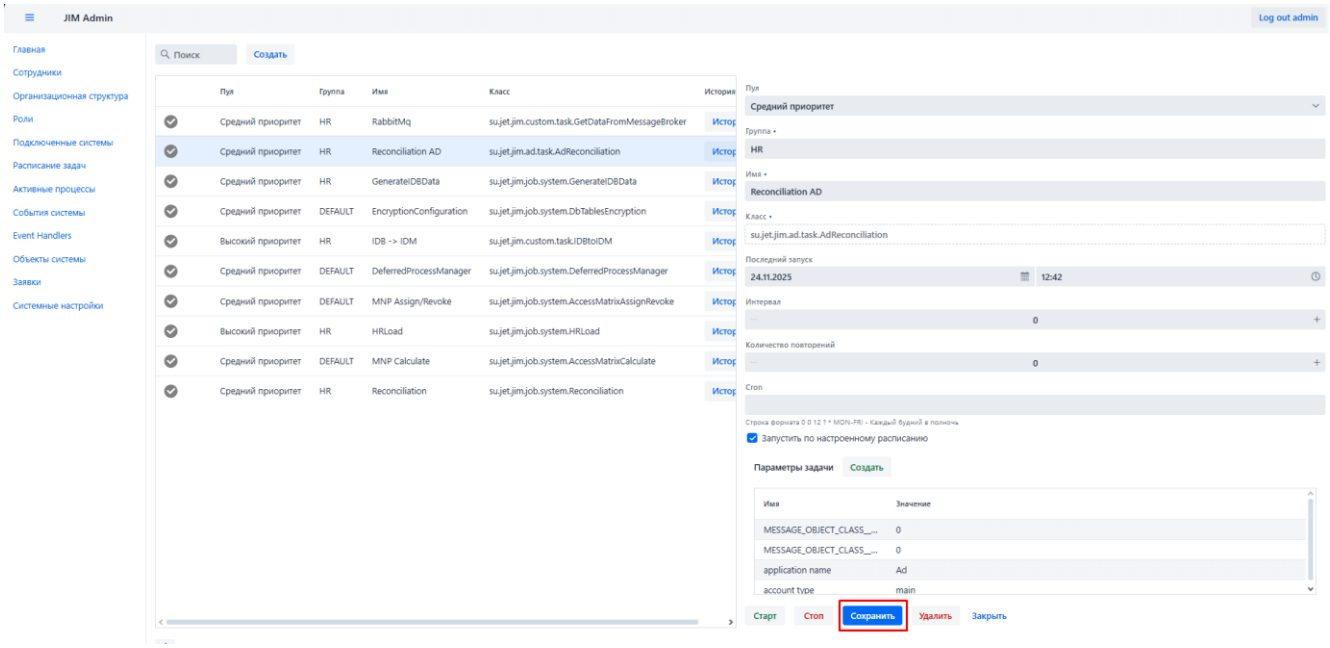


**Рис. 29 Серверные задачи – Создание задачи, заполнение параметров**

### *2.2.7.2 Редактирование параметров задачи*

Для редактирования параметров серверной задачи следует:

1) В разделе Расписание задач выбрать серверную задачу, которую необходимо изменить. Откроется карточка серверной задачи.

2) В карточке задачи внести необходимые изменения и нажать Сохранить (Рис. 29).

## *2.3 Отчёты*

Администратор может создавать отчёты, используя любой GUI БД Jim, экспортируя результат запросов в формат xlsx, csv.

# 3 Администрирование Системы

Администрирование системы предполагает различные операции, выполнение которых требует понимания процесса взаимодействия Системы с подключёнными ИС.

## *3.1 Настройка аутентификации*

### 3.1.1 Настройка аутентификации с помощью JWT-токена

JWT (Json Web Token) – ключ аутентификации пользователя. Используется для запросов к защищенным методам API.

Процесс аутентификации и авторизации с JWT-токеном между клиентом и веб-приложением выглядит следующим образом:

1) Клиент отправляет запрос серверу Системы с логином и паролем (basic auth).

2) Сервер проверяет логин и пароль. Если они верны, то сервер автоматически генерирует JWT-токен и отправляет его клиенту. При генерации JWT-токена веб-приложение ставит подпись секретным ключом, который хранится на сервере. Время жизни токена ограничено.

3) Клиент сохраняет JWT-токен и отправляет его вместе с каждым запросом в приложение.

4) Приложение проверяет JWT-токен. Если он верный, позволяет выполнять действия от имени авторизованного пользователя.

Токен состоит из 3 частей, разделенных точкой:

– header – содержит информацию об алгоритме шифрования и типе токена (JWT)

– payload – данные токена.

– signature – строка, полученная из частей токена (header + payload) при помощи шифрования RS256.

#### *3.1.1.1 Получение JWT-токена*

Запрос токена аутентификации Системы производится на основании известных логина и пароля УЗ.

Клиент должен выполнить POST запрос, передать логин и пароль в теле запроса:

```
POST [url]
Headers {
      "Content-Type" = "application/json"
      "X-Role" = "default"}
Body '{"username":"admin", "password":"admin"}'
```

При положительном ответе сервера (код 200) будет сформирован json следующего вида:

```
{
```

```
"token":
"eyJraWQiOiJpbnJpZ2h0cyIsImFsZyI6IlJTMjU2In0.eyJzdWIiOiJpbnJpZ2h0c0FjY2VzcyIsImF
1ZCI6ImEuYWFhIiwiaXNzIjoiaW5yaWdodHNBcHAiLCJleHAiOjE2ODUwOTY3MTZ9.BOvKTrO6J6s2WzMK
dLGfFFDVrNoYWT0MsQG_JehhhdjNcx47qA7rQ_UzppRWEPPrBTGRHQgXAORA_0zT2bws_sdCd_qzMsZEv5
EEKroBZLQghPdy9qBku9dJIFg0s2bhWWmSu5o9MrLRYsI4jSmVYaIG3zA70ngUcmYjEDNjwQJ2yghHb7LH
9nVlWm9RvNJohrilyijNiNFIOm9ofHi_5tZ6yvUIvCcv0vudf00lSbrUR_inVnFXt5dQk5_gi4NJw5zDc-
nV6AzF1veh_GeIwYxXL243BUSzFcdrw4sF99SpA5P5z6yU2Yx-IVeg37WHK7SsffohnAf_NFqUDOSVw"
}
```


### 3.1.1.2 Запрос к серверу с использованием токена

Полученным токеном необходимо сопровождать запросы к API Системы, и они будут выполнены в сессии от лица пользователя.

При формировании запросов следует учитывать, что время жизни токена ограничено. При получении кода 401 (не авторизован) при попытке выполнить запрос клиент должен выполнить повторный запрос токена у сервера Системы

## 3.2 Общие настройки системы

Для доступа к общим настройкам необходимо перейти в раздел Системные настройки (Рис. 30).

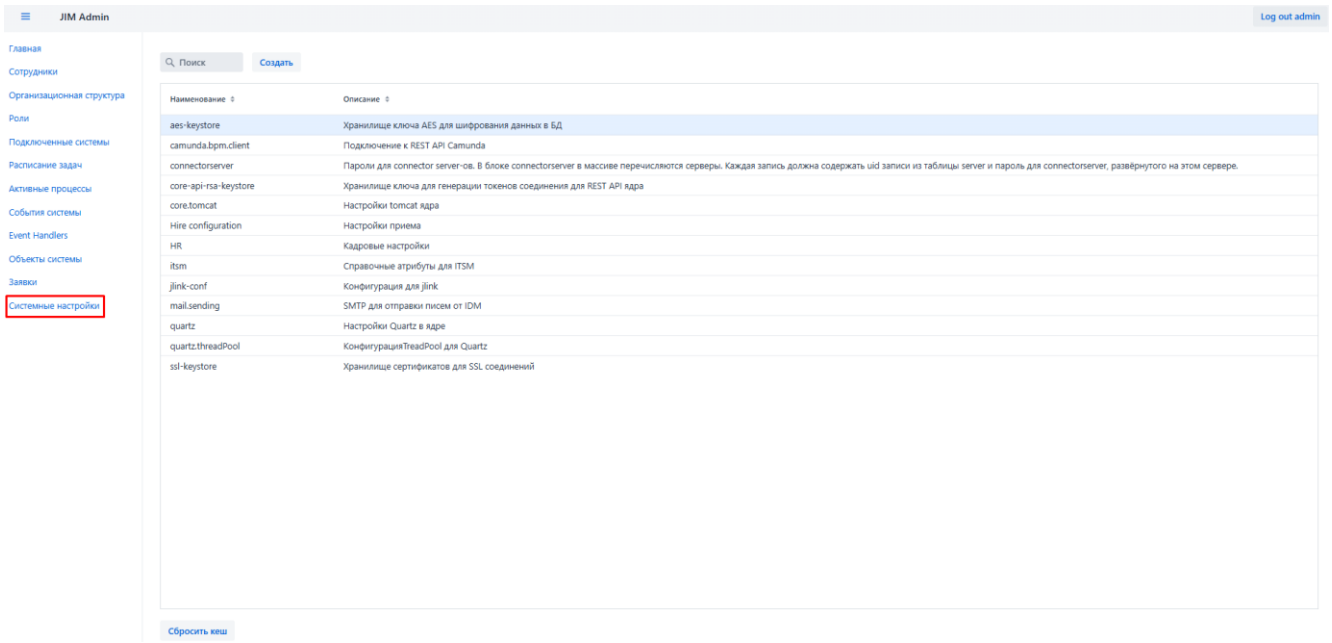


**Рис. 30 Раздел Системные настройки**

В разделе доступны к созданию (просмотру, изменению, удалению) такие настройки Системы, как параметры подключения к ИС, пути к хранилищам сертификатов, конфигурации и функциональности исполнения задач по расписанию.

## *3.3 Взаимодействие со смежными ИС*

### 3.3.1 Настройка взаимодействия с кадровым источником

Взаимодействие IDM и источника кадровых данных осуществляется с целью автоматизации получения информации об организационно-штатной структуре и сотрудниках, их трудоустройствах и изменении кадровых данных, которые являются триггером для запуска операций по управлению учетными записями пользователей и их правами доступа в подключенных к IDM информационных системах.

За вычитывание, обработку и сохранение из кадрового источника отвечают серверные задачи по расписанию. Независимо от типа кадрового источника, задачи по расписанию обрабатывают и сохранят кадровые данные в промежуточную базу данных (далее – ПБД).

#### *3.3.1.1 Добавление новой задачи*

Описание создания новой серверной задачи описано в разделе 2.2.7.1.

### 3.3.2 Подключение ИС

При подключении новой ИС задаются значения конфигурационных параметров, набор которых зависит от того, к какому внешнему ресурсу выполняется подключение.

Необходимым предусловием выполнения подключения является наличие установленного модуля «Коннекторы».

Коннекторы – специальные модули, которые являются каналами передачи данных между Системой и подключаемыми ИС.

В общем случае коннектор – это независимый модуль, предоставляющий интерфейс определенного вида для доступа к функциям внешней системы.

#### *3.3.2.1 Настройка подключения к ИС*

Для подключения ИС следует:

1) Перейти в раздел Подключенные системы и нажать кнопку **Создать** (Рис. 31). В отобразившемся окне заполнить поля «наименование» и «описание системы», а также режим взаимодействия с системой – включен, выключен или доступен только для чтения.

2) В поле Коннектор выбрать коннектор (Рис. 32, Рис. 33). Если требуемый коннектор отсутствует в Системе, следует нажать кнопку **Создать**, заполнить атрибуты в соответствии с 2.2.5.2.2, нажать кнопку **Сохранить** (Рис. 34).

3) После внесения изменений необходимо нажать на кнопку **Сохранить** (Рис. 32).

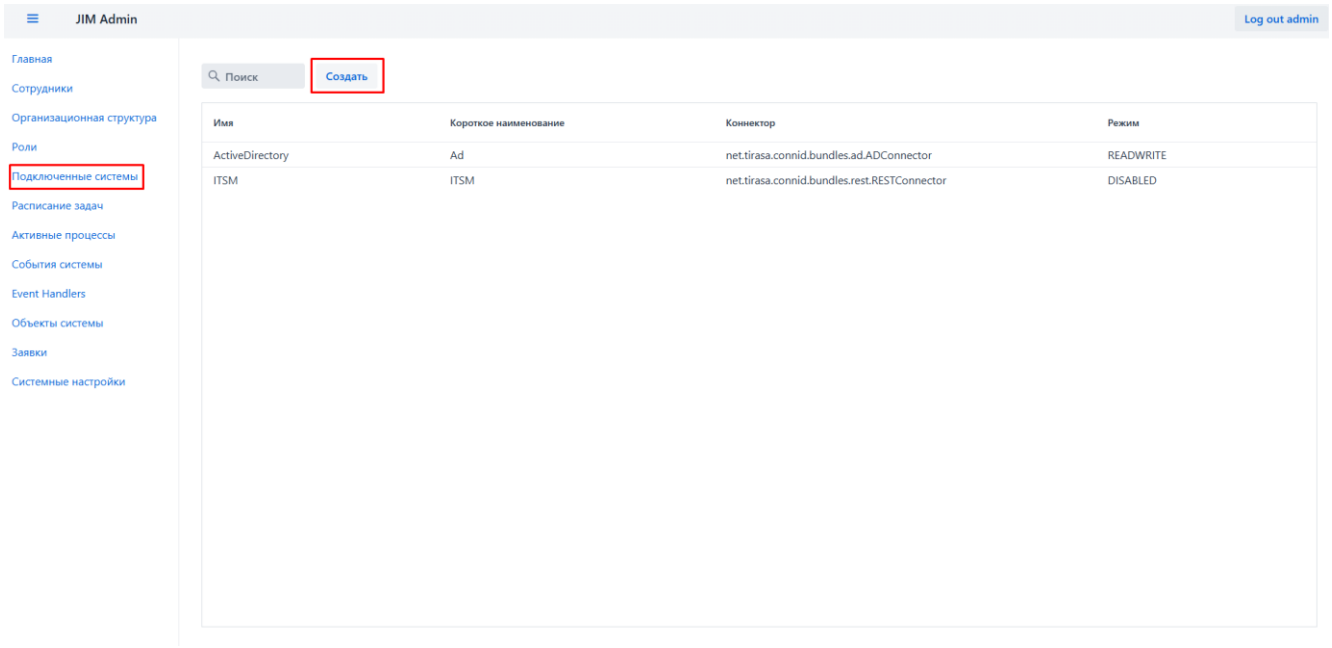


**Рис. 31 Подключенные системы – новая ИС**

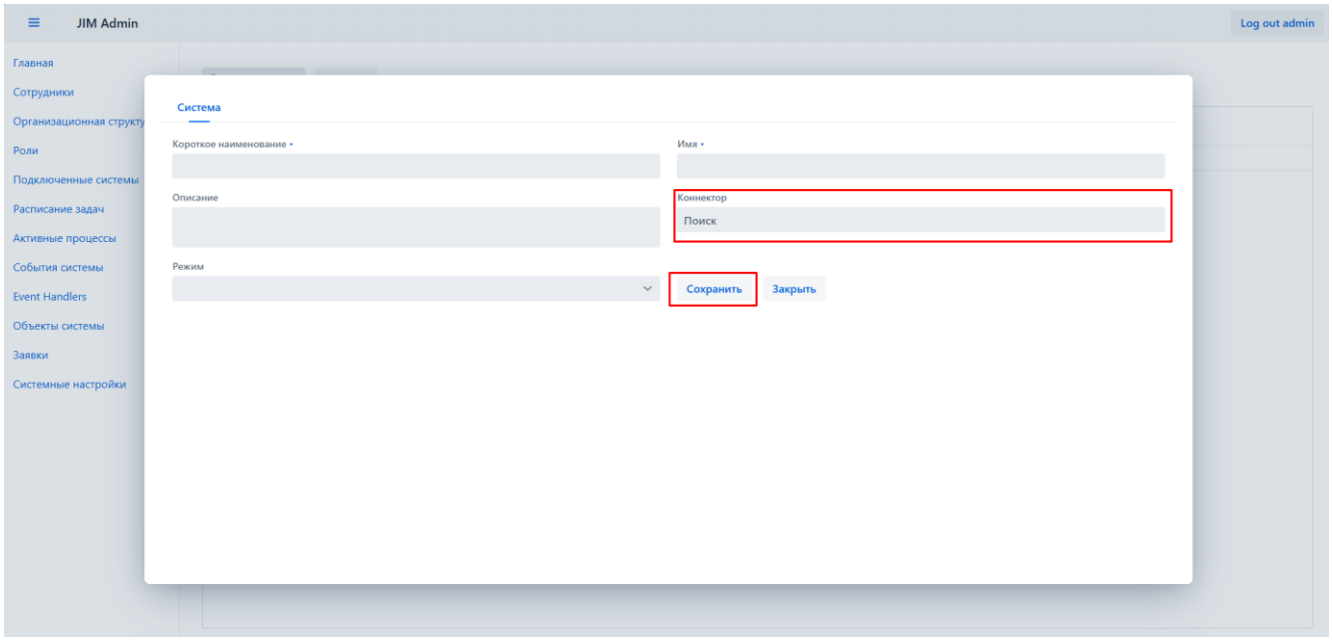


**Рис. 32 Подключенные системы – новая ИС, заполнение атрибутов**

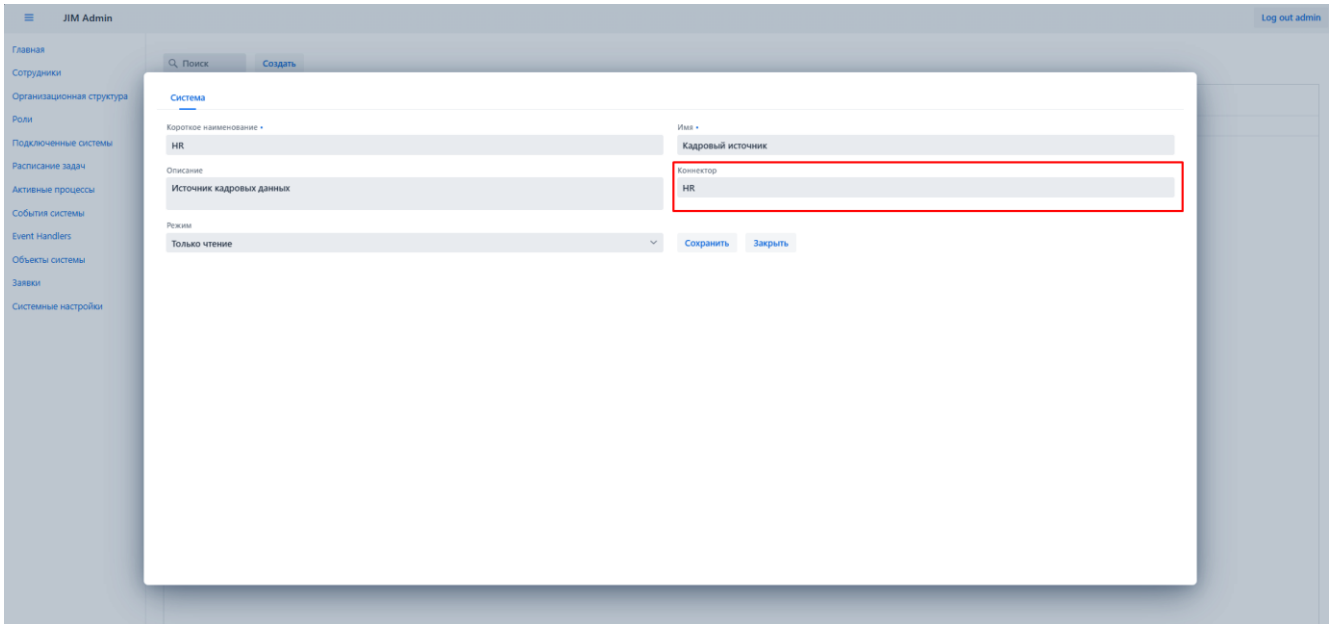


**Рис. 33 Подключенные системы – новая ИС, выбор коннектора**

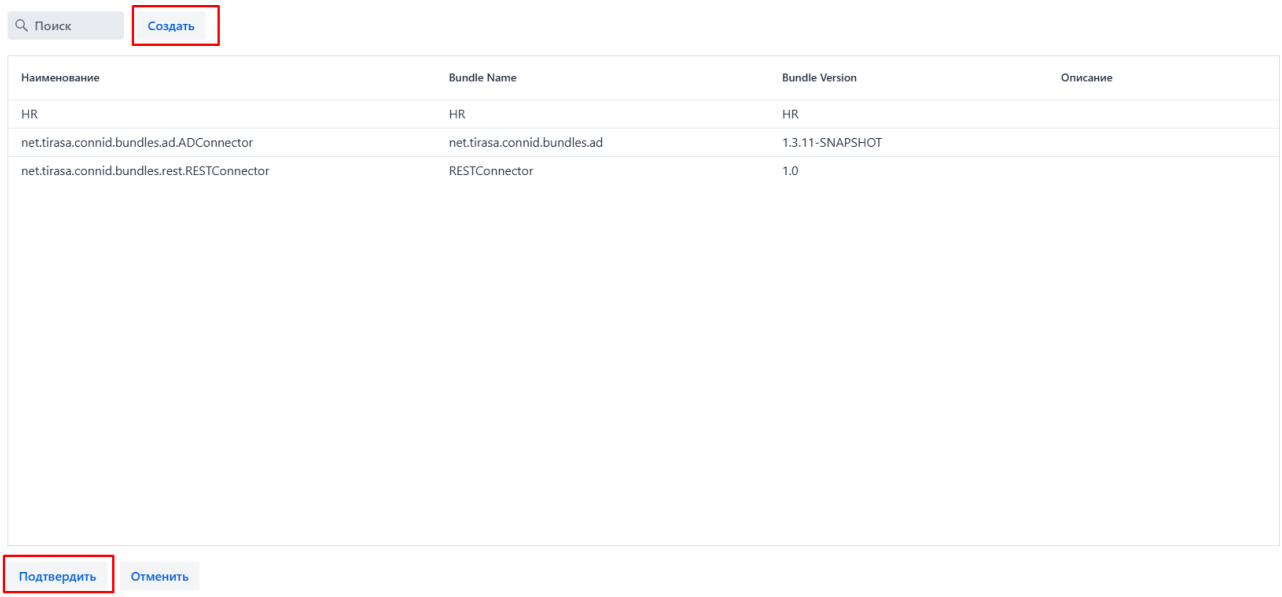


**Рис. 34 Подключенные системы – новая ИС, создание нового коннектора**

#### 3.3.2.1.1 Настройка подключения

1) Перейти в раздел Подключенные системы и выбрать из списка ИС.
2) Перейти на вкладку Свойства подключения, выбрать необходимый параметр и внести изменения и нажать кнопку **Сохранить** (Рис. 35).

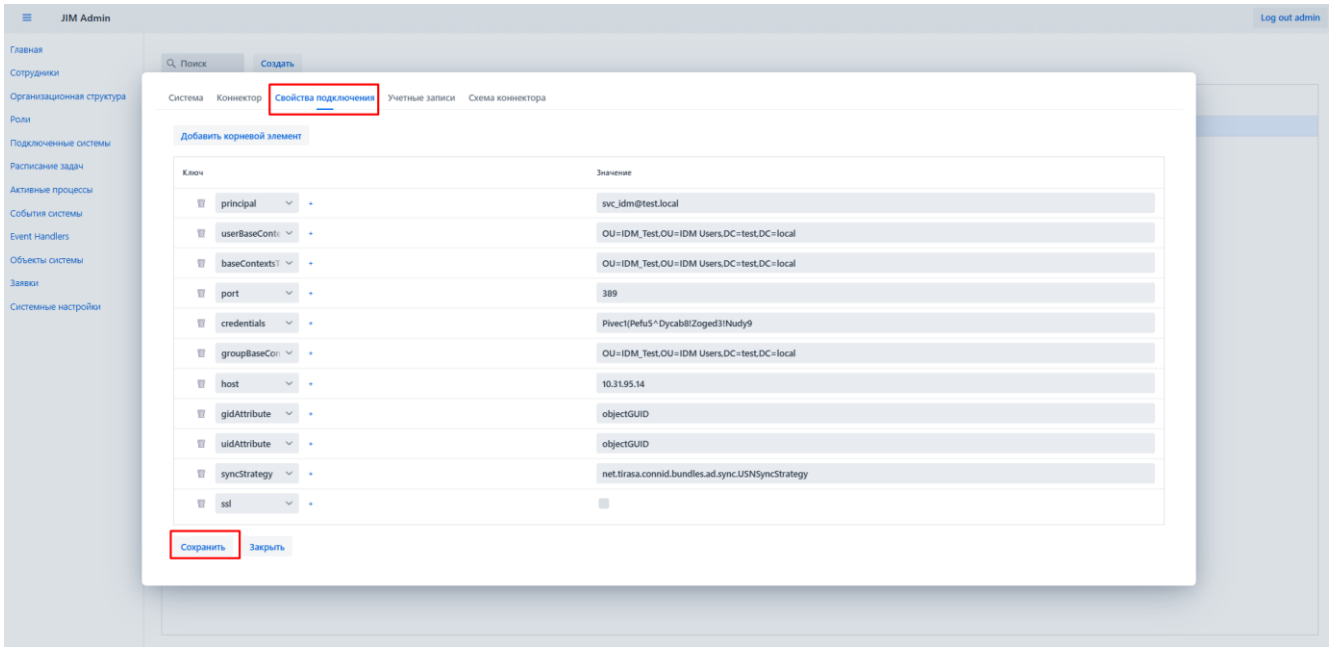


**Рис. 35 Подключенные системы – настройка свойств подключения ИС**

## *3.4 Управление УЗ пользователей в целевых системах*

Модуль «Коннекторы» обеспечивает синхронизацию данных между Системой и подключенными информационными системами: получает задачи по управлению правами доступа через вызовы со стороны Ядра и обеспечивает их выполнение, взаимодействуя с подключенными ИС при помощи выбранных механизмов взаимодействия.

Коннекторы реализуются на основе стандарта ConnID и исполняются под управлением Сервера коннекторов (Connector Server).

### 3.4.1 Конфигурирование объектов управляемых систем

Конфигурирование объектов информационных систем осуществляется на платформе с BPM-движком (например, Camunda) при настройке бизнес-процессов управления правами доступа. Конфигурирование включает настройку и связывание учётных записей и прав доступа управляемых ИС с УЗ и ролями в Системе.

## *3.5 Настройка МНП*

### 3.5.1 Общая структура модуля

Предоставление МНП реализовано через назначение пользователям ролей Системы. Администратор может включить в роли Системы доступы целевых ИС, УЗ и другие роли.

Модуль МНП состоит из следующих компонентов:

1) Механизм назначения/отзыва ролей – это задача по расписанию, которая выполняет назначение или отзыв ролей на основе информации из матрицы доступа.

2) Матрица доступа – таблица БД, содержащая информацию о пользователях Системы (Трудоустройство) и ролях Системы, которые должны быть назначены этим пользователям в данный момент времени.

3) Rules (далее – набор правил) – является таблицей в БД, состоящей из правил. Правило представляет собой код запроса на языке SQL. Правила определяют, какие роли Системы каким пользователям Системы должны быть назначены.

4) Механизм вычисления правил – механизм, позволяющий запускать пересчёт указанного правила, исполняющий код правила (SQL-запрос) и сохраняющий полученный результат в матрицу доступа. На выходе – таблица пар ID трудоустройства и ID роли.

5) Очередь пересчёта правил – таблица БД, в которую добавляются задания на пересчёт правил. Задания содержат информацию о том, какие правила нужно пересчитать, обрабатываются методом FIFO (первый вошёл – первый вышел) и через механизм вычисления правил инициируют их пересчёт.

6) Обработчик очереди пересчёта правил – задача по расписанию, обрабатывающая очередь заданий на пересчёт правил.

7) Интерфейс добавления заданий – внутренний API ядра, являющийся интерфейсом для работы с модулем МНП. Позволяет внешним модулям:

а) Добавить в очередь задание на пересчёт определённых правил.

б) Получить информацию о текущем состоянии матрицы МНП. В т.ч. с применением фильтров по пользователю и роли.

### 3.5.2 Настройка параметров назначения МНП

Для настройки параметров МНП необходимо перейди в раздел **Набор правил** из главного меню.

Для настройки нового правила необходимо:

1) Нажать кнопку **«Добавить»**.
2) Заполнить атрибуты нового правила.
3) Добавить роли, которые должны быть назначены по текущему правилу.
4) После добавления информации необходимо нажать кнопку **Сохранить**.

## *3.6 Настройка функциональных ролей Системы*

Для управления доступом к объектам и операциям в Системе используются функциональные роли. По умолчанию в Системе применяется политика «Всё, что не разрешено явно – то запрещено». Поэтому чтобы иметь возможность выполнять в Системе ту или иную

операцию над каким-либо объектом, необходима функциональная роль, которая явно разрешает доступ к такой операции.

Каждая функциональная роль содержит набор авторизаций. Авторизации позволяют явно указать множество объектов и операции над ними, к которым конкретная авторизация предоставляет доступ.

## *3.7 Настройка уведомлений*

Система предоставляет возможность отправлять уведомления пользователям о каких-либо системных событиях.

Шаблоны уведомлений хранятся в модуле «БД», организация отправки осуществляется с помощью модуля «API» посредством вызова интерфейса из внешней системы (например, BPM-системы).

Администратору доступно ведение шаблонов уведомлений в интерфейсе администрирования IDM.

Чтобы настроить шаблоны уведомлений:

1) Перейдите в раздел **Шаблоны уведомлений**. На экране отобразится перечень групп, по которым распределены шаблоны уведомлений.
2) Выберите группу, в которой находится шаблон.
3) В группе выберите шаблон, который нужно отредактировать.
4) Внесите необходимые изменения в шаблон.
5) После внесения изменений нажмите кнопку **Сохранить**.