Приложение 6

Подсистема управления доступом

Оглавление

[1. Общие сведения 3](#_Toc47607244)

[2. Управление пользователями 3](#_Toc47607245)

[2.1. Управление списком пользователей 3](#_Toc47607246)

[2.1.1. Создание нового пользователя 4](#_Toc47607247)

[2.1.2. Добавление пользователя из внешней системы управления учетными записями 5](#_Toc47607248)

[2.2. Редактор учетной записи 6](#_Toc47607249)

[2.2.1. Управление персональной информацией и блокировка пользователя 6](#_Toc47607250)

[2.2.2. Управление ролями пользователя 7](#_Toc47607251)

[2.2.3. Настройка способа аутентификации пользователя 8](#_Toc47607252)

[2.2.4. Настройка факторов аутентификации пользователя 14](#_Toc47607253)

[2.3. Аутентификация пользователя 14](#_Toc47607254)

[2.4. Хранение персональной информации пользователей 16](#_Toc47607255)

[3. Управление группами пользователей 16](#_Toc47607256)

[3.1. Управление списком групп пользователей 17](#_Toc47607257)

[3.2. Создание новой группы пользователей 17](#_Toc47607258)

[3.3. Редактор группы пользователей 18](#_Toc47607259)

[3.3.1. Редактирование общей информации о группе пользователей 19](#_Toc47607260)

[3.3.2. Редактирование доступа к решениям 20](#_Toc47607261)

[3.3.3. Редактирование доступа к приложениям 20](#_Toc47607262)

[3.3.4. Редактирование списка связанных ролей 20](#_Toc47607263)

[4. Управление ролевой моделью 22](#_Toc47607264)

[4.1. Управление списком ролей 22](#_Toc47607265)

[4.2. Создание новой роли 23](#_Toc47607266)

[4.3. Редактор роли 23](#_Toc47607267)

[4.3.1. Настройка общей информации о роли 24](#_Toc47607268)

[4.3.2. Настройка состава пользователей роли 25](#_Toc47607269)

[4.3.3. Настройка иерархии ролей 28](#_Toc47607270)

[4.3.4. Просмотр схемы иерархии ролей 29](#_Toc47607271)

[4.3.5. Управление группами пользователей, связанными с ролью 30](#_Toc47607272)

[4.3.6. Настройка доступа к решениям 31](#_Toc47607273)

[4.3.7. Настройка доступа к сущностям 41](#_Toc47607274)

[4.3.8. Импорт и синхронизация групп MS Active Directory 42](#_Toc47607275)

# Общие сведения

Подсистема управления доступом содержит полный набор функций аутентификации и авторизации пользователей, включая ведение собственной базы данных пользователей и использование внешней системы аутентификации, ведения ролевой модели, назначения пользователям ролей, согласно выполняемых ими должностным обязанностям, разграничения доступа и конфигурации для пользователей их рабочего пространства в рамках прикладной системы, выполняемой на Платформе.

# Управление пользователями

Работа с инструментами и модулями Платформы возможна только после прохождения процедуры аутентификации. При разворачивании экземпляра Платформы автоматически создается пользователь «admin», обладающий полными административными правами.

Доступ к функциям управления пользователями имеет пользователь с правами «Управление пользователями».

## Управление списком пользователей

Управление списком пользователей осуществляется на странице управления пользователями (Рис. 1). Для перехода к странице в главном меню выберите пункт «Безопасность» → «Пользователи».

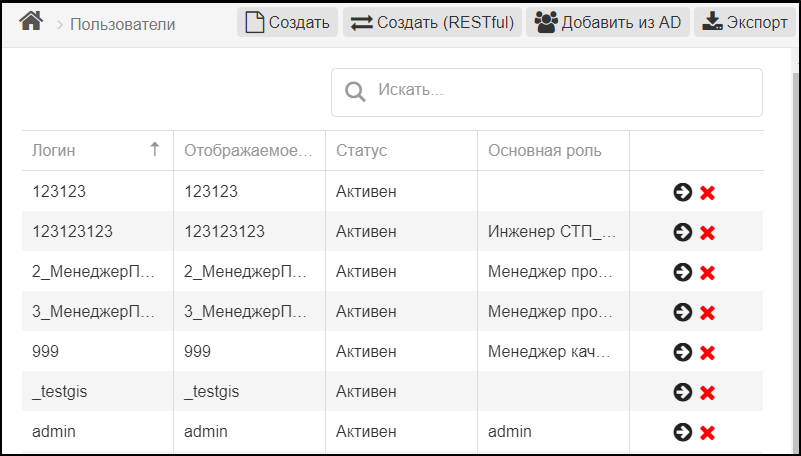


Рис. 1. Список пользователей

Страница содержит список всех пользователей, определенных для данного экземпляра Платформы.

В последнем столбце таблицы расположены следующие пиктограммы:

*  — переход к редактору учетной записи пользователя (см. раздел 2.2. Редактор учетной записи);
*  — удаление пользователя из данного экземпляра Платформы.

В верхней части страницы расположена навигационная панель. В левой ее части отображается путь к странице. В правой части расположены кнопки для добавления пользователей и экспорта матрицы доступа пользователей.

Пользователи создаются в рамках данного экземпляра Платформы или могут быть добавлены из внешней системы управления учетными записями пользователей MS Active Directory, с которой настроено взаимодействие экземпляра Платформы.

При нажатии на кнопку «Экспорт» в навигационной панели формируется файл Excel, содержащий список пользователей. Для каждого пользователя отображается его логин, отображаемое имя, комментарий и список ролей пользователя.

### Создание нового пользователя

Для создания нового пользователя:

1. На странице управления пользователями в навигационной панели нажмите на кнопку «Создать». Откроется всплывающее окно «Создание пользователя» (Рис. 2).



Рис. 2. Создание пользователя

1. В поле «Логин» введите уникальный логин создаваемого пользователя.
2. При необходимости установите флаг в поле «Создать локальный способ входа». Во всплывающем окне отобразятся два новых поля: «Пароль для первого входа» и «Подтвердите пароль для первого входа». В данные поля необходимо ввести одноразовый пароль для пользователя и подтвердить его. При первом входе пользователь должен будет изменить введенный одноразовый пароль на постоянный. Данное действие не является обязательным и может выполниться позже в редакторе данных пользователя.
3. Нажмите на кнопку «Создать». Новый пользователь будет создан, для него откроется окно редактора данных пользователя (см. раздел 2.2. Редактор учетной записи). Пользователю отобразится всплывающее сообщение с текстом «Назначьте роль для <логин>, чтобы он смог зайти в систему».

### Добавление пользователя из внешней системы управления учетными записями

Для добавления пользователя из MS Active Directory:

1. На странице управления пользователями в навигационной панели нажмите на кнопку «Добавить из AD». Откроется всплывающее окно «Поиск пользователей в AD» (Рис. 3).

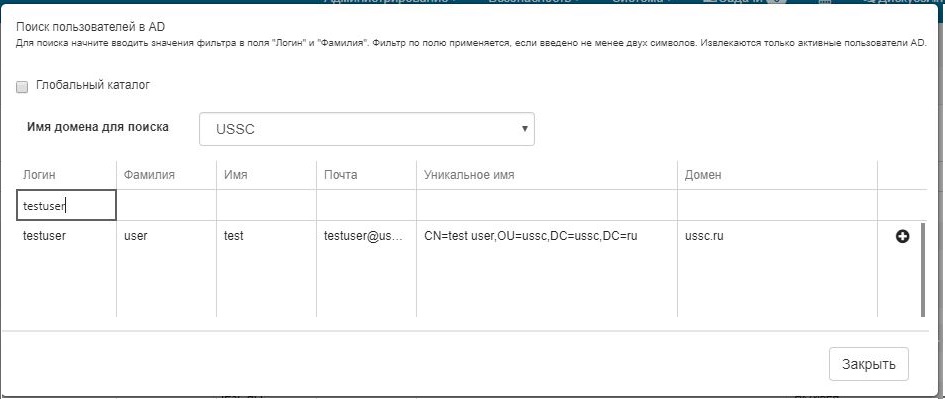


Рис. 3. Добавление пользователя из MS Active Directory

1. При необходимости установите флаг в поле «Глобальный поиск». При установленном флаге поиск будет производиться по всем доменам. При снятом флаге поиск будет производиться по выбранному домену.
2. В соответствующем столбце введите поисковое значение (логин, фамилия и пр.). Будет сформирован список пользователей, удовлетворяющих заданным условиям поиска.
3. Нажмите на пиктограмму  для импорта пользователя. Учетная запись выбранного пользователя будет импортирована.
4. Для добавления нескольких пользователей последовательно нажмите на пиктограмму для каждого из них. Учетные записи выбранных пользователей будут импортированы.
5. Нажмите на кнопку «Закрыть». Всплывающее окно закроется.

## Редактор учетной записи

Редактирование параметров учетной записи пользователя производится в редакторе учетной записи (Рис. 4). Переход к редактору осуществляется с помощью пиктограммы  в списке пользователей на странице управления пользователями.

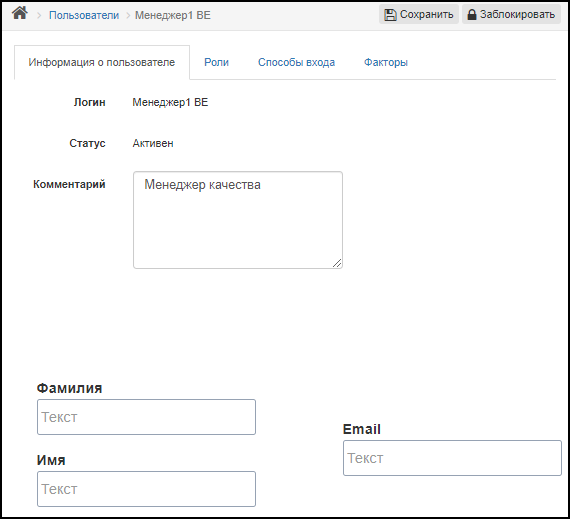


Рис. 4. Редактор учетной записи

Редактор учетной записи содержит следующие вкладки:

* «Информация о пользователе». Управление персональной информацией пользователя, а также блокировка пользователя.
* «Роли». Управление списком ролей, в которые входит пользователь.
* «Способы входа». Настройка способа аутентификации пользователя.
* «Факторы». Настройка двухфакторной аутентификации пользователя.

### Управление персональной информацией и блокировка пользователя

Управление персональной информацией пользователя производится на вкладке «Информация о пользователе» редактора учетной записи (см. Рис. 4).

В верхней части вкладки отображаются логин и статус пользователя, а также поле для ввода произвольного комментария об учетной записи пользователя.

В нижней части страницы расположена форма для ввода персональных данных пользователя. Структура информации и форма редактирования может быть изменена администратором Платформы. Форма редактирования информации о пользователе создается отдельно в любом решении и затем подключается в настройках Платформы. Информация о пользователях хранится в системном приложении «Пользователи», структура которого доступна для редактирования администратору Платформы.

В верхней части страницы расположена навигационная панель. В левой ее части отображается путь к странице. В правой части расположена кнопка «Заблокировать/Разблокировать», позволяющая включить или отключить временную блокировку учетной записи пользователя, а также кнопка «Сохранить», позволяющая сохранить введенный комментарий к учетной записи пользователя.

*Примечание: кнопка «Сохранить» в навигационной панели сохраняет только поле «Комментарий». Для сохранения изменений, внесенных в форму для ввода персональных данных пользователя, расположенную в нижней части страницы, необходимо добавить на форму кнопку с действием «Сохранить».*

### Управление ролями пользователя

Пользователю может быть назначено несколько ролей. Одна из ролей является основной, т.е. после прохождения процесса аутентификации пользователь попадает в окружение, определенное для этой роли.

#### Управление списком ролей пользователя

Управление списком ролей пользователя производится на вкладке «Роли» редактора учетной записи (Рис. 5).

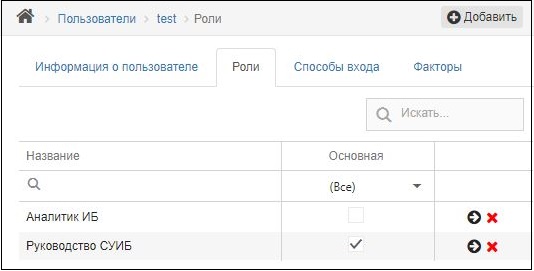


Рис. 5. Список ролей для пользователя

На вкладке отображается список ролей, в которые входит пользователь. В последнем столбце таблицы расположены следующие пиктограммы:

*  — переход к редактору роли (см. раздел 4.3. Редактор роли);
*  — удаление роли из числа ролей, в которые входит пользователь.

Во втором столбце расположен флаг, позволяющий назначить выбранную роль основной для данного пользователя.

В верхней части страницы расположена навигационная панель. В левой ее части отображается путь к странице. В правой части расположена кнопка, позволяющая добавить новую роль для пользователя.

#### Добавление роли для пользователя

Для добавления новой роли для пользователя:

1. На вкладке «Роли» редактора учетной записи в навигационной панели нажмите на кнопку «Добавить». Откроется всплывающее окно «Добавление роли»   
   (Рис. 6).



Рис. 6. Добавление роли пользователю

1. В раскрывающемся списке «Роль» выберите роль, которую необходимо добавить пользователю. Для добавления нескольких ролей для пользователя последовательно повторите выбор роли в раскрывающемся списке необходимое число раз.
2. Нажмите на кнопку «Добавить». Выбранные роли будут добавлены в число ролей пользователя и отобразятся в списке ролей на вкладке «Роли» редактора учетной записи.

#### Назначение основной роли для пользователя

Одна из ролей пользователя является основной. Для назначения основной роли установите флаг в столбце «Основная» таблицы в строке с данной ролью.

### Настройка способа аутентификации пользователя

В текущей версии Платформы существует три способа аутентификации пользователей:

* *Local.* Информация о пользователе и его пароль хранятся локально в БД Платформы;
* *Windows*. Проверка пароля пользователя производится средствами MS Active Directory, к которой подключен экземпляр Платформы;
* *Certificate*. Аутентификация происходит с помощью смарт-карты или электронного токена. При выборе «Сопоставление в Active Directory» совместно с аутентификацией по электронному ключу проводится проверка на наличие пользователя с такими данными в MS Active Directory.

Возможно использование нескольких способов аутентификации для одного пользователя.

Настройка способа аутентификации пользователя производится на вкладке «Способы входа» редактора учетной записи (Рис. 7).

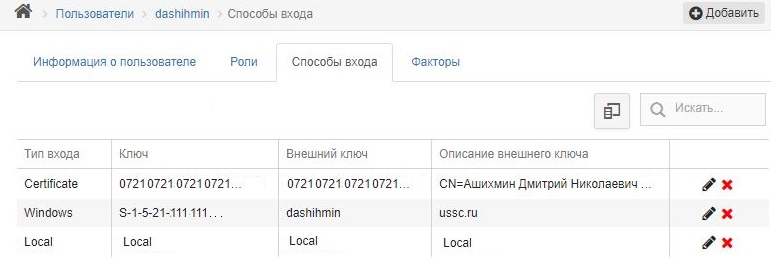


Рис. 7. Определение способа входа для пользователя

На вкладке отображается список всех настроенных для пользователя способов входа. В последнем столбце таблицы расположены следующие пиктограммы:

*  — переход к окну редактирования способа входа (см. раздел 2.2.3.3. Смена пароля для локального способа входа);
*  — удаление способа входа для пользователя.

В верхней части страницы расположена навигационная панель. В левой ее части отображается путь к странице. В правой части расположена кнопка, позволяющая добавить новый способ входа для пользователя.

#### Добавление способа входа для пользователя через Windows

Для добавления способа входа типа *Windows* для пользователя:

1. На вкладке «Способы входа» редактора учетной записи нажмите на кнопку «Добавить». Откроется всплывающее окно «Добавление способа входа»   
   (Рис. 8).

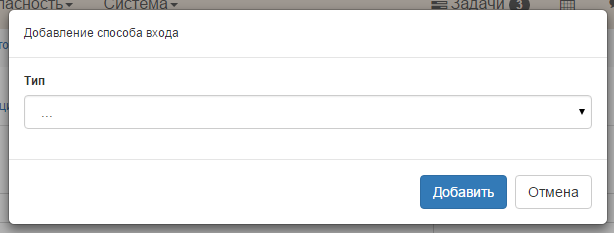


Рис. 8. Добавление способа входа

1. В раскрывающемся списке «Тип» выберите «Вход через Windows». Откроются поля для поиска пользователей в MS Active Directory.

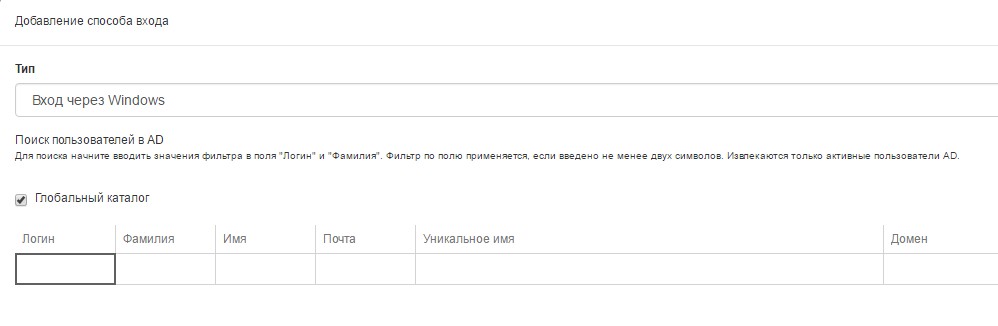


Рис. 9. Поиск пользователя в MS Active Directory

1. В соответствующем столбце введите поисковое значение (логин, фамилия и пр.). Будет сформирован список пользователей, удовлетворяющих заданным условиям поиска.
2. Выберите учетную запись пользователя, которая будет использоваться для входа.
3. Нажмите на кнопку «Добавить». Будет добавлен способ входа по логину и паролю выбранной учетной записи.

#### Добавление локального способа входа для пользователя

Для добавления типа входа *Local* для пользователя:

1. На вкладке «Способы входа» редактора учетной записи нажмите на кнопку «Добавить». Откроется всплывающее окно «Добавление способа входа»   
   (см. Рис. 8).
2. В раскрывающемся списке «Тип» выберите «Локальный вход». Откроются поля для настройки параметров локального входа (Рис. 10).

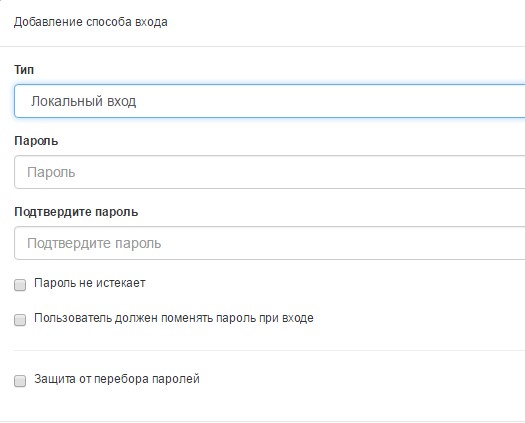


Рис. 10. Настройка параметров локального входа

1. В поле «Пароль» введите пароль доступа пользователя к Платформе.
2. В поле «Подтвердите пароль» введите пароль повторно.
3. Установите флаг «Пароль не истекает» если необходимо, чтобы пароль имел неограниченный срок действия.
4. Установите флаг «Пользователь должен поменять пароль при входе» если необходимо, чтобы при первом входе пользователь сменил пароль на собственный.
5. Установите флаг «Защита от перебора паролей» если необходимо производить блокировку действий текущего пользователя в случае превышения заданного количества попыток ввода пароля. Количество попыток ввода пароля и время блокировки задаются в настройках системы (см. документ «Приложение 9. Подсистема управления, мониторинга и контроля» раздел «Настройки безопасности»).
6. Нажмите на кнопку «Добавить». Будет добавлен локальный способ входа с указанным паролем для выбранной учетной записи.

#### Смена пароля для локального способа входа

Для смены пароля при локальном способе входа:

1. На вкладке «Способы входа» редактора учетной записи воспользуйтесь пиктограммой . Откроется всплывающее окно «Редактирование способа входа» (Рис. 11).

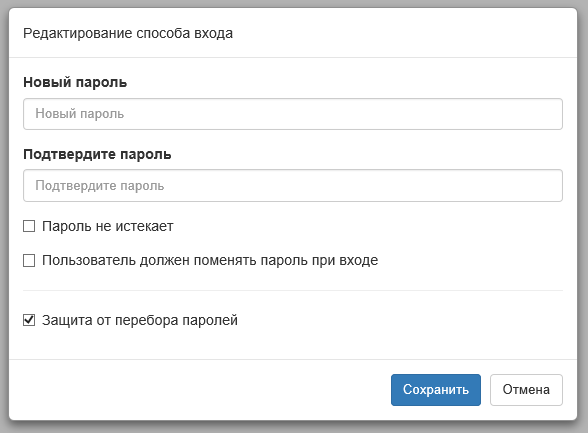


Рис. 11. Смена пароля для способа входа типа *локальный*

1. В поле «Новый пароль» введите новый пароль для способа входа.
2. В поле «Подтвердите пароль» введите новый пароль повторно.
3. При необходимости измените положение флагов (описание см. выше).
4. Нажмите на кнопку «Сохранить». Пароль для выбранного способа входа будет изменен.

#### Добавление способа входа через пользовательский сертификат

Для добавления способа входа типа *Certificate* для пользователя:

1. На вкладке «Способы входа» редактора учетной записи нажмите на кнопку «Добавить». Откроется всплывающее окно «Добавление способа входа»   
   (см. Рис. 8).
2. В раскрывающемся списке «Тип» выберите «Вход через пользовательский сертификат». Откроются поля для настройки параметров входа (Рис. 12).

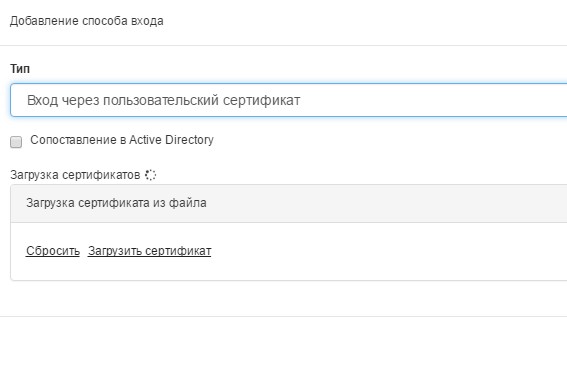


Рис. 12. Настройка параметров входа типа *Certificate*

1. В раскрывающемся списке «Выберите сертификат» выберите сертификат, установленный на компьютере.
2. Для загрузки сертификата из файла нажмите на кнопку «Загрузить сертификат». Откроется всплывающее окно выбора файла сертификата в файловой системе. Выберите нужный сертификат и нажмите на кнопку «Открыть». Всплывающее окно закроется, в области «Загрузка сертификата из файла» появятся сведения о выбранном сертификате и его владельце.
3. Установите флаг «Сопоставление в Active Directory», если необходимо дополнительно к аутентификации по электронному ключу проводить проверку на наличие пользователя с такими данными в MS Active Directory.
4. Нажмите на кнопку «Добавить». Настроенный способ входа будет добавлен пользователю.

При наличии нескольких способов входа, настроенных для пользователя, нужно выбрать какой из них будет использоваться для входа.

|  |
| --- |
| *Внимание!*  *Для работы с сертификатом необходимо установить ПО CryptoPro CSP для Windows, а также плагины CAPICOM и CadesCOM.* |

### Настройка факторов аутентификации пользователя

Настройка факторов аутентификации пользователя производится на вкладке «Факторы» редактора учетной записи пользователя (Рис. 13).

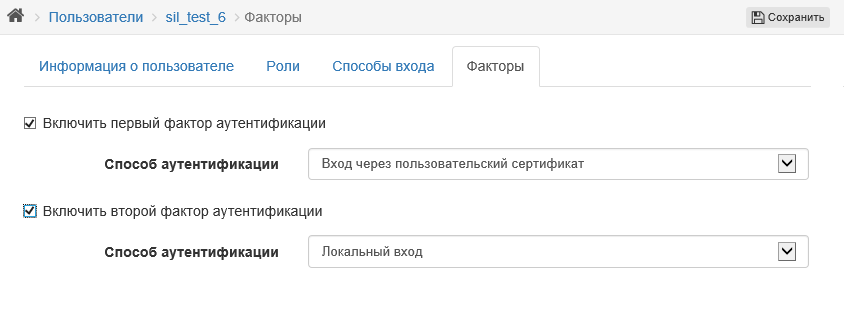


Рис. 13. Настройка двухфакторной аутентификации пользователя

При создании способа входа для пользователя, автоматически включается первый фактор аутентификации. При наличии нескольких настроенных для пользователя способов входа необходимо выбрать, какой из них будет использоваться для входа в случае однофакторной аутентификации. Для этого:

1. Выберите нужный способ входа в раскрывающемся списке «Способ аутентификации».
2. Нажмите на кнопку «Сохранить» в навигационной панели.

Для повышения защищенности системы возможна настройка двухфакторной аутентификации пользователя, т.е. совместное использование двух способов входа. Для настройки двухфакторной аутентификации:

1. Установите флаг «Включить второй фактор аутентификации».
2. В раскрывающемся списке «Способ аутентификации» выберите способ входа, который будет использоваться в качестве второго фактора.
3. Нажмите на кнопку «Сохранить» в навигационной панели.

## Аутентификация пользователя

После того как пользователь создан, добавлен в необходимые роли, для него настроен способ входа, он может начать работать с Платформой, пройдя процесс аутентификации.

Для аутентификации пользователь должен ввести логин и пароль, соответствующие его учетной записи в поля формы аутентификации (Рис. 14).



Рис. 14. Форма аутентификации пользователя

При установке флага «Расширенные опции» отображается раскрывающийся список, содержащий все возможные для системы способы входа.

Пользователь может получить доступ к своей персональной информации в редакторе профиля своей учетной записи (Рис. 15). Для перехода к странице профиля в главном меню выберите пункт «Имя пользователя» → «Профиль».

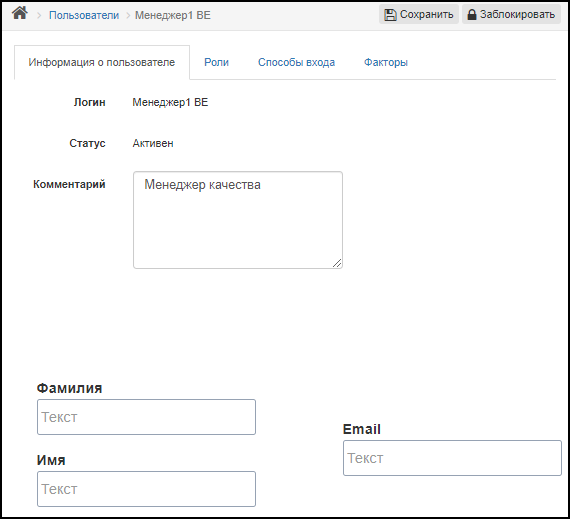


Рис. 15. Редактор профиля пользователя

Редактор профиля пользователя аналогичен редактору учетной записи пользователя (см. раздел 2.2. Редактор учетной записи). Для редактирования пользователю доступны вкладки «Информация о пользователе» и «Способы входа». Остальные вкладки доступны только для чтения.

## Хранение персональной информации пользователей

Как отмечалось выше, персональная информация пользователей хранится в системном приложении «Пользователи» (Рис. 16. Структура приложения «Пользователи»), структура которого может быть изменена администратором Платформы.

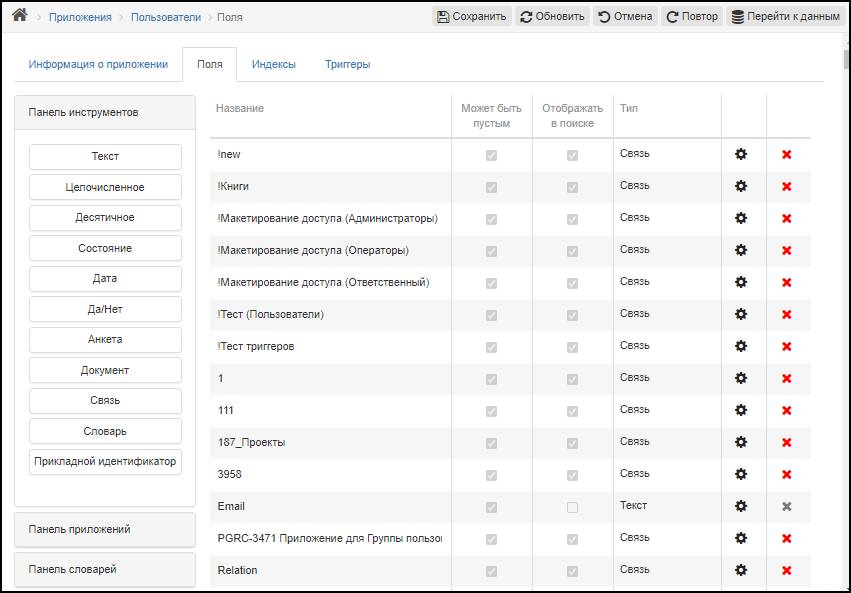


Рис. 16. Структура приложения «Пользователи»

# Управление группами пользователей

Группы пользователей предназначены для динамического объединения пользователей с различными ролями с целью решения ими общих задач в рамках бизнес-процесса. Группы пользователей используются для назначения общих задач, групповых рассылок сообщений, организации форумов, процесса обучения и пр.

Один из вариантов использование групп – доступ комиссии к проекту. Как только текущий пользователь хотя бы раз упоминается в связях с проектами, он становится участником группы. Далее, в настройках условных привилегий, конкретизируется уровень доступа текущего пользователя к проектам: может он редактировать все проекты, или те, в которые включен.

Для группы могут быть предоставлены временные (на время выполнения задачи, связанной с группой, или этапа процесса) права на объекты решения: приложения, формы, отчеты, импорт и пр. Настройка доступа зависит от условных привилегий, заданных для приложений или доступа к объектам.

Группа создается на основе приложения, имеющего поле связи с системным приложением «Пользователи». Так же для группы пользователей обязательно должна быть указана роль, от которой наследуются права доступа. Группа пользователей, не связанная с ролью, работать не будет.

Для включения в группу пользователей у пользователя должна быть одна или несколько ролей, связанных с данной группой.

## Управление списком групп пользователей

Управление списком групп пользователей осуществляется на странице управления группами пользователей (Рис. 17). Для перехода к странице в главном меню выберите пункт «Безопасность» → «Группы пользователей».

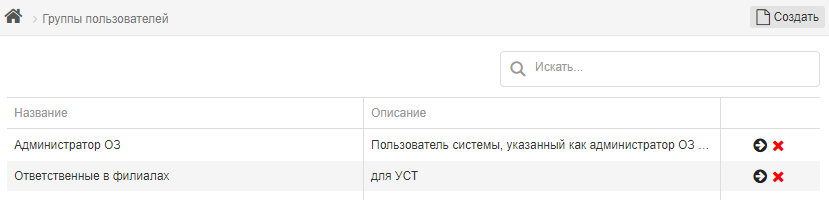


Рис. 17. Список групп пользователей

На странице отображается список всех групп пользователей, определенных для данного экземпляра Платформы. В последнем столбце таблицы расположены следующие пиктограммы:

*  — переход к редактору группы пользователей (см. раздел 3.3. Редактор группы пользователей);
*  — удаление группы пользователей.

В верхней части страницы расположена навигационная панель. В левой ее части отображается путь к странице. В правой части расположена кнопка «Создать» для создания новой группы пользователей.

## Создание новой группы пользователей

Для создания новой группы пользователей:

1. На странице управления группами пользователей в навигационной панели нажмите на кнопку «Создать». Откроется всплывающее окно «Создание группы пользователей» (Рис. 18).

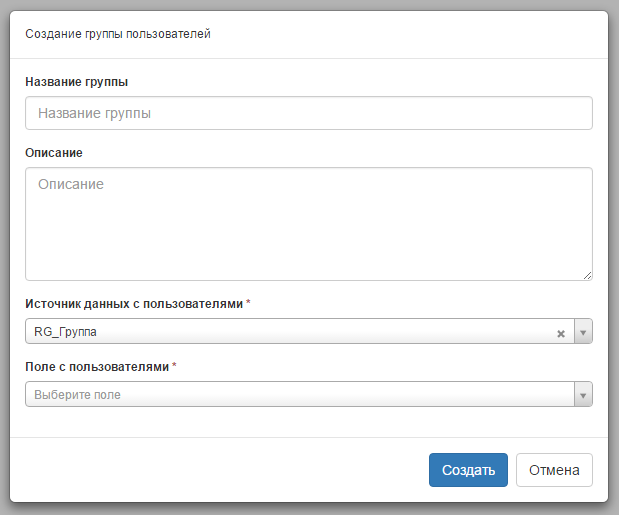


Рис. 18. Создание новой группы пользователей

1. В поле «Название группы» введите уникальное название группы пользователей.
2. В поле «Описание» введите, при необходимости, описание группы пользователей.
3. В раскрывающемся списке «Источник данных с пользователями» выберите источник данных, в котором хранятся данные пользователей, входящих в группу.
4. В появившемся после выбора источника данных раскрывающемся списке «Поле с пользователями» выберите поле источника данных, связанное с системным приложением «Пользователи».
5. Нажмите на кнопку «Создать». Группа пользователей будет создана, для данной группы откроется окно редактора группы пользователей (см. ниже).

## Редактор группы пользователей

Для перехода к редактору группы пользователей (Рис. 19) воспользуйтесь кнопкой перехода () на странице управления списком групп пользователей (см. раздел 3.1. Управление списком групп пользователей).

При создании новой группы пользователей редактор откроется автоматически после заполнения основных параметров.

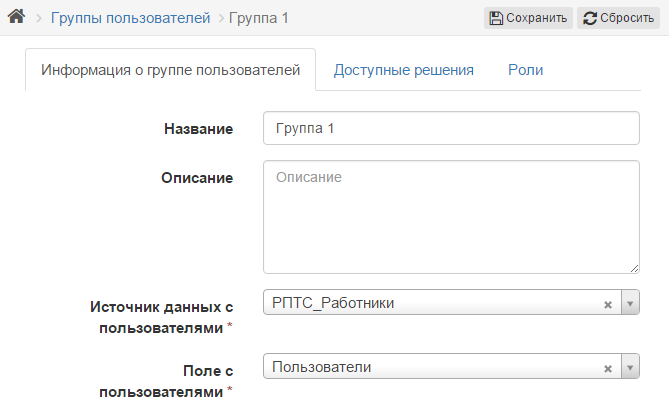


Рис. 19. Редактор группы пользователей

Редактор группы пользователей содержит следующие вкладки:

* «Информация о группе пользователей». Редактирование общих свойств группы пользователей;
* «Доступные решения». Настройка для участников группы доступа к решениям и их компонентам;
* «Роли». Управление списком ролей, с которыми связана группа пользователей.

### Редактирование общей информации о группе пользователей

Вкладка «Информация о группе пользователей» редактора группы пользователей (Рис. 19) предназначена для редактирования общих свойств группы пользователей. Вкладка содержит следующие поля:

* *Название*. Редактирование названия группы пользователей;
* *Описание*. Редактирование описания группы пользователей;
* *Источник данных с пользователями*. Изменение источника данных, в котором находятся сведения о пользователях, входящих в группу;
* *Поле с пользователями*. Изменение поля источника данных, связанного с системным приложением «Пользователи».

В верхней части страницы расположена навигационная панель. В левой ее части отображается путь к странице. В правой части расположены кнопки для сохранения и сброса внесенных изменений.

### Редактирование доступа к решениям

По умолчанию группа пользователей наследует права доступа от связанной роли (ролей). Для каждого конкретного пользователя из группы пользователей права доступа наследуются только от тех связанных с группой пользователей ролей, в которые включен данный пользователь. При необходимости можно изменить параметры доступа для группы пользователей.

Редактирование доступа участников группы пользователей к решениям и их компонентам выполняется на вкладке «Доступные решения». Настройка доступа к решениям для группы пользователей аналогична настройке доступа к решениям для роли (см. раздел 4.3.6. Настройка доступа к решениям).

### Редактирование доступа к приложениям

Для редактирования доступа к приложениям создайте провайдер данных, связанный с приложением и содержащий ссылку на системное приложение «Пользователи».

Для приложения указывается фильтр с использованием этого провайдера и условием «Идентификатор пользователя = Текущий пользователь».

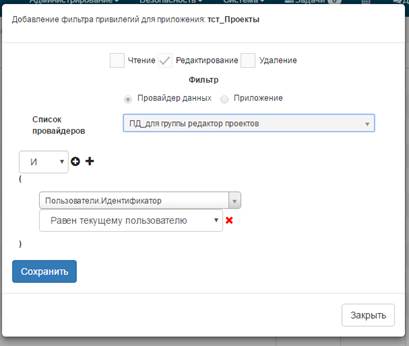


Рис. 20. Настройка доступа для пользователя группы

В настройках полей отмечаются поля, которые пользователь должен редактировать.

### Редактирование списка связанных ролей

На вкладке «Роли» выполняется редактирование списка ролей, с которыми связана группа пользователей.

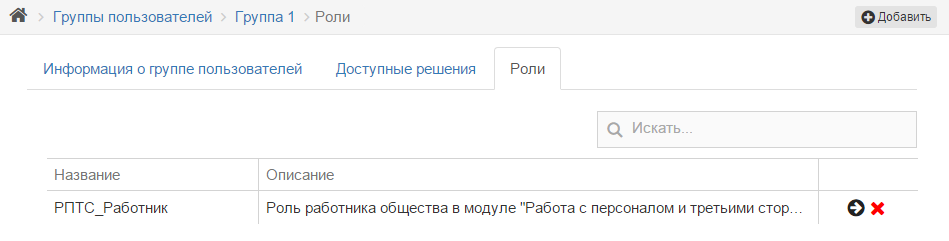


Рис. 21. Список ролей, с которыми связана группа пользователей

На вкладке отображается список ролей, связанных с группой пользователей.

В последнем столбце таблицы расположены следующие пиктограммы:

*  — переход к редактору роли (см. раздел 4.3. Редактор роли);
*  — удаление роли из списка ролей, связанных с группой пользователей.

В верхней части страницы расположена навигационная панель. В левой ее части отображается путь к странице. В правой части расположена кнопка для добавления ролей, связанных с группой пользователей.

|  |
| --- |
| *Внимание!*  *Для корректной работы группа пользователей обязательно должна быть связана с ролью.* |

#### Добавление роли, связанной с группой пользователей

Для добавления роли, связанной с группой пользователей:

1. На вкладке «Роли» редактора групп пользователей нажмите на кнопку «Добавить». Откроется окно «Добавление ролей» (Рис. 22).

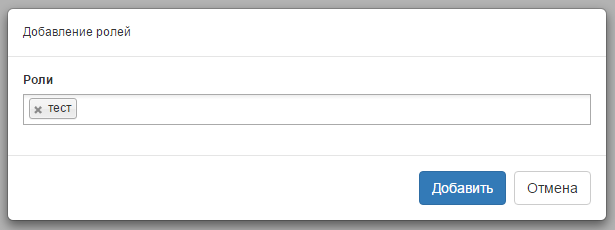


Рис. 22. Добавление ролей, связанных с группой пользователей

1. В раскрывающемся списке «Роли» выберите роль, связанную с группой пользователей. Можно последовательно добавить несколько ролей.
2. Нажмите на кнопку «Добавить». Группа пользователей будет связана с выбранной ролью (ролями).

# Управление ролевой моделью

Ролевая модель прикладной системы должна отражать набор бизнес-функций, выполняемых пользователями в рамках своих должностных обязанностей.

Ролевая модель предназначена для:

* разграничения прав доступа пользователя к объектам прикладной системы/прикладного модуля (решения);
* создания инструментальной среды, обеспечивающей наиболее эффективное выполнение пользователем своих должностных обязанностей.

В Платформе реализована иерархическая ролевая модель. Для роли можно указать произвольное количество родительских ролей. В этом случае данная роль наследует права родительских ролей. Если для роли назначено более одного родителя, то данная роль получает доступ ко всем разрешенным хотя бы в одной родительской роли объектам.

## Управление списком ролей

Управление списком ролей осуществляется на странице управления ролевой моделью (Рис. 23). Для перехода к странице в главном меню выберите пункт «Безопасность» → «Роли».

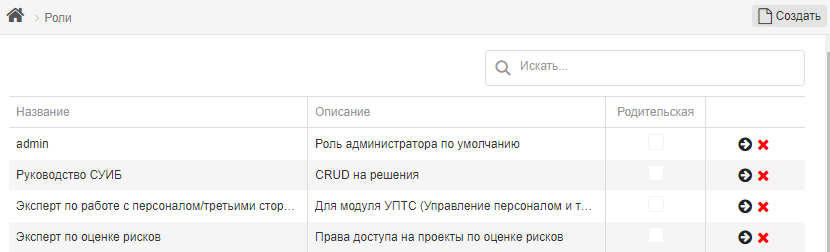


Рис. 23. Список ролей

На странице отображается список всех ролей, определенных для данного экземпляра Платформы. Для каждой роли указывается название, описание, признак родительской роли. В последнем столбце таблицы расположены следующие пиктограммы:

*  — переход к редактору роли (см. раздел 4.3. Редактор роли);
*  — удаление роли.

В верхней части страницы расположена навигационная панель. В левой ее части отображается путь к странице. В правой части расположена кнопка «Создать» для создания новой роли.

## Создание новой роли

Для создания новой роли:

1. На странице управления ролевой моделью в навигационной панели нажмите на кнопку «Создать». Откроется всплывающее окно «Создание роли»   
   (Рис. 24).

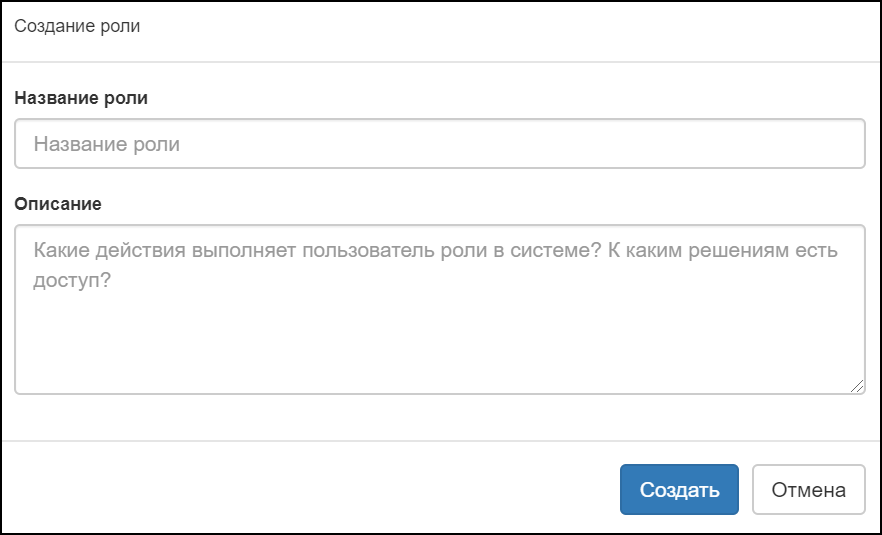


Рис. 24. Создание новой роли

1. В поле «Название роли» введите уникальное название роли.
2. В поле «Описание» введите, при необходимости, описание роли. Если нет необходимости в текстовом описании роли, оставьте поле пустым.
3. Нажмите на кнопку «Создать». Роль будет создана, для данной роли откроется окно редактора роли (см. ниже).

## Редактор роли

Редактор роли позволяет производить полную настройку всех параметров роли: общие свойства роли, состав пользователей, родительские роли и роли-наследники, доступ к решениям и сущностям.

Для перехода к редактору роли (Рис. 25) воспользуйтесь пиктограммой перехода   
() для выбранной роли в списке ролей на странице управления ролевой моделью   
(см. раздел 4.1. Управление списком ролей).

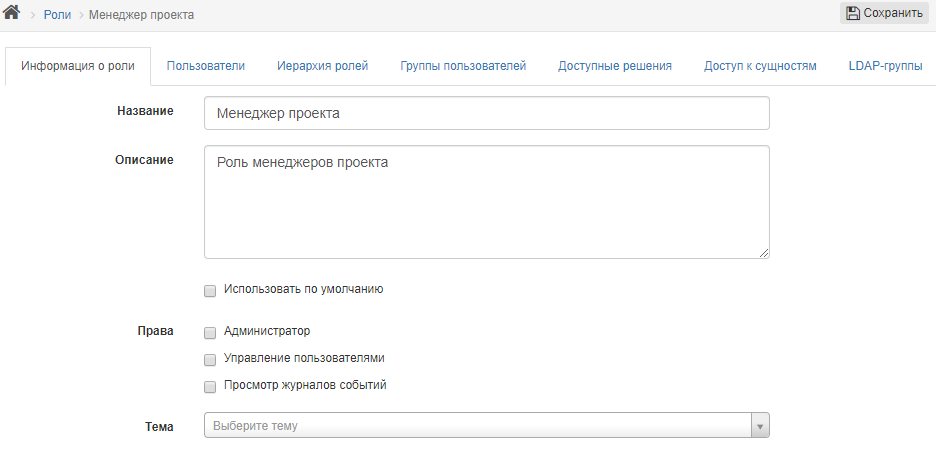


Рис. 25. Редактор роли

Редактор роли содержит следующие вкладки:

* «Информация о роли». Редактирование общих свойств роли;
* «Пользователи». Управление составом пользователей, входящих в роль;
* «Иерархия ролей». Управление списком родительских ролей и просмотр иерархии ролей в графическом виде;
* «Группы пользователей». Управление списком групп пользователей;
* «Доступные решения». Управление доступом роли к прикладным модулям;
* «Доступ к сущностям». Настройка доступа к задачам;
* «LDAP-группы». Импорт и синхронизация групп MS Active Directory.

### Настройка общей информации о роли

Вкладка «Информация о роли» редактора роли (Рис. 25) предназначена для редактирования общих свойств роли. Вкладка содержит следующие поля (группы полей):

* *Название*. Редактирование названия роли;
* *Описание*. Редактирование описания роли;
* *Использовать по умолчанию*. Признак, логическое значение «Да» которого означает, что данная роль автоматически будет назначаться для нового пользователя;
* *Права*. Признак «Администратор», логическое значение «Да» которого устанавливает для роли полные права на управление всеми объектами Платформы. Признак «Управление пользователями», логическое значение «Да» которого устанавливает для роли полные права на управление пользователями Платформы. Признак «Просмотр журналов событий», логическое значение «Да» которого устанавливает для роли права на просмотр протоколов работ (разделы «Безопасность», «Действия пользователей» и «Импорт/экспорт»);
* *Тема.* Выбор темы визуального оформления. Выбранная тема визуального оформления по умолчанию устанавливается для всех пользователей с данной ролью (подробнее о темах визуального оформления см. документ «Приложение 3. Подсистема визуализации» раздел «Настройка внешнего вида платформы»).

В верхней части страницы расположена навигационная панель. В левой ее части отображается путь к странице. В правой части расположены кнопка для сохранения внесенных изменений.

### Настройка состава пользователей роли

Вкладка «Пользователи» редактора роли (Рис. 26) обеспечивает возможность управления составом пользователей, входящих в роль.

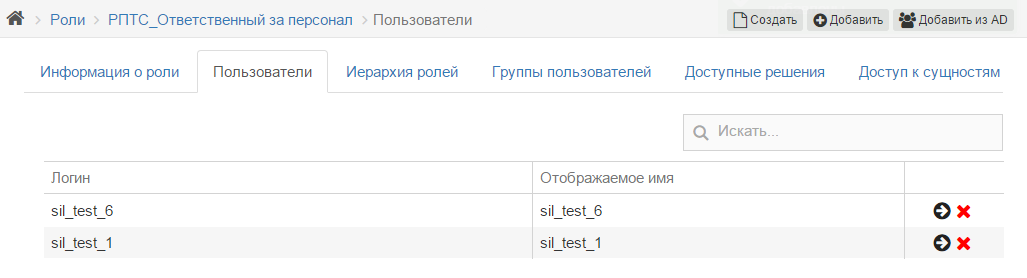


Рис. 26. Список пользователей в роли

Вкладка содержит список пользователей, добавленных в роль. В последнем столбце таблицы расположены следующие пиктограммы:

*  — переход к редактору учетной записи пользователя (см. раздел 2.2. Редактор учетной записи);
*  — удаление пользователя из числа пользователей роли.

В верхней части страницы расположена навигационная панель. В левой ее части отображается путь к странице. В правой части расположены кнопки для добавления пользователей.

В роль могут быть добавлены существующие локальные пользователи (определенные в рамках Платформы) или пользователи из внешней системы управления учетными записями пользователей, например, MS Active Directory. Кроме того, может быть создан новый пользователь, который будет сразу добавлен в роль.

#### Добавление локального пользователя

Для добавления локального пользователя:

1. На вкладке «Пользователи» редактора роли нажмите на кнопку «Добавить». Откроется всплывающее окно «Добавление пользователя» (Рис. 27).

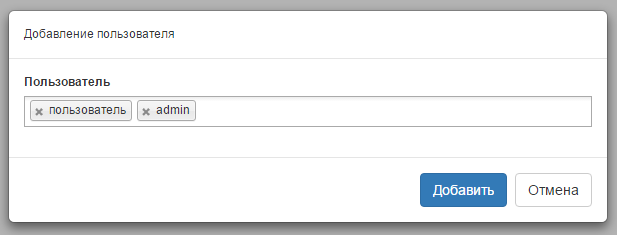


Рис. 27. Добавление локального пользователя

1. В раскрывающемся списке «Пользователь» выберите наименование учетной записи пользователя. Можно последовательно выбрать несколько учетных записей.
2. Нажмите на кнопку «Добавить». Выбранные пользователи будет добавлены в число пользователей роли и отобразятся в списке пользователей на вкладке «Пользователи» редактора роли.

#### Добавление пользователя из внешней системы управления учетными записями

Для добавления пользователя из MS Active Directory:

1. На вкладке «Пользователи» редактора роли нажмите на кнопку «Добавить из AD». Откроется всплывающее окно «Поиск пользователей в AD» (Рис. 28).

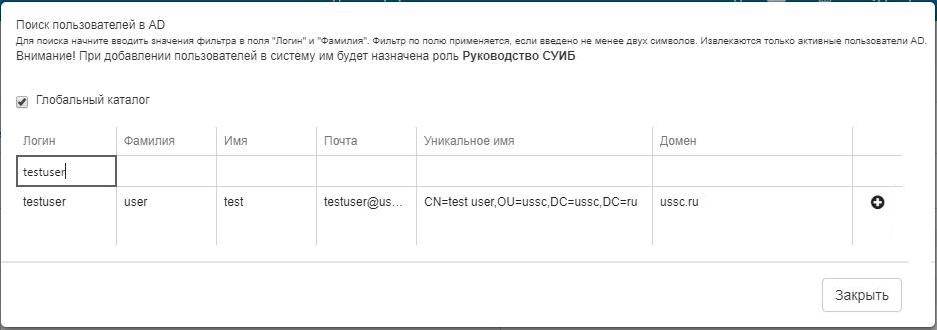


Рис. 28. Добавление пользователя из MS Active Directory

1. В соответствующем столбце введите поисковое значение (логин, фамилия и пр.). Будет сформирован список пользователей, удовлетворяющих заданным условиям поиска.
2. Нажмите на пиктограмму  для импорта пользователя. Для добавления нескольких пользователей последовательно нажмите на пиктограмму для каждого из них.
3. Нажмите на кнопку «Закрыть». Выбранные пользователи будут добавлены в число пользователей роли и отобразятся в списке пользователей на вкладке «Пользователи» редактора роли.

#### Создание нового пользователя

Для создания нового пользователя:

1. На вкладке «Пользователи» редактора роли нажмите на кнопку «Создать». Откроется всплывающее окно «Создание пользователя» (Рис. 29).



Рис. 29. Создание пользователя

1. В поле «Логин» введите уникальный логин создаваемого пользователя.
2. При необходимости установите флаг в поле «Создать локальный способ входа». Во всплывающем окне отобразятся два новых поля: «Пароль для первого входа» и «Подтвердите пароль для первого входа». В данные поля необходимо ввести одноразовый пароль для пользователя и подтвердить его. При первом входе пользователь должен будет изменить введенный одноразовый пароль на постоянный. Данное действие не является обязательным и может выполниться позже в редакторе данных пользователя.
3. Нажмите на кнопку «Создать». Новый пользователь будет создан, добавлен в число пользователей роли и отобразится в списке пользователей на вкладке «Пользователи» редактора роли.

### Настройка иерархии ролей

Для каждой роли может быть назначено произвольное количество родительских ролей. При задании родительских ролей текущая роль унаследует их права. Если для роли назначено более одного родителя, то данная роль получает доступ ко всем разрешенным хотя бы в одной родительской роли объектам.

Управление составом родительских ролей производится на вкладке «Иерархия ролей» редактора роли (Рис. 30).

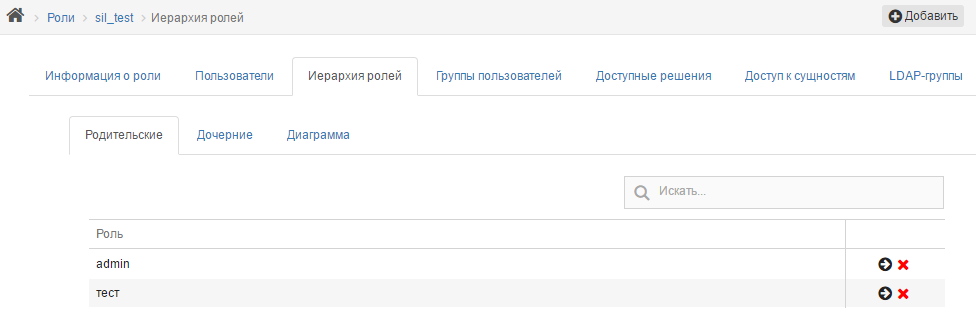


Рис. 30 Список родительских ролей

Вкладка содержит три вкладки:

* *Родительские*. Вкладка содержит список всех родительских ролей текущей роли. В последнем столбце таблицы расположена пиктограмма , позволяющая удалить выбранную роль из числа родительских ролей;
* *Дочерние*. Вкладка содержит список всех дочерних ролей текущей роли. В последнем столбце таблицы расположена пиктограмма , позволяющая удалить выбранную роль из числа дочерних ролей;
* *Диаграмма*. На вкладке отображается схема иерархии ролей в графическом виде.

В верхней части страницы расположена навигационная панель. В левой ее части отображается путь к странице. В правой части расположена кнопка для добавления родительских/дочерних ролей.

#### Добавление родительской/дочерней роли

Для добавления родительской/дочерней роли:

1. На вкладке «Родительские» или «Дочерние» вкладки «Иерархия ролей» редактора роли в навигационной панели нажмите на кнопку «Добавить». Откроется всплывающее окно «Добавление роли» (Рис. 31).

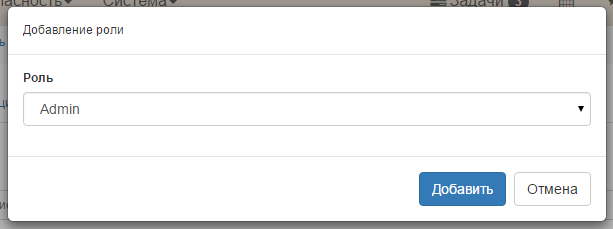


Рис. 31. Добавление роли

1. В раскрывающемся списке «Роль» выберите роль, которая будет назначена родительской/дочерней для текущей роли. Можно последовательно выбрать несколько ролей.
2. Нажмите на кнопку «Добавить». Выбранная (выбранные) роль будет добавлена и отобразится в списке родительских/дочерних ролей на соответствующей вкладке вкладки «Иерархия ролей» редактора роли.

### Просмотр схемы иерархии ролей

Для просмотра схемы иерархии ролей в графическом виде (Рис. 32) на вкладке «Иерархия ролей» редактора роли выберите вкладку «Диаграмма».

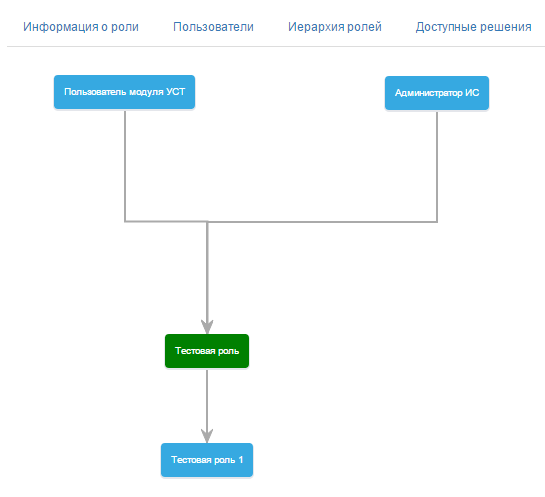


Рис. 32. Иерархия ролей

На странице отображается схема иерархии ролей. Можно увидеть место текущей роли в иерархии, ее родительские и дочерние роли. Роли на схеме можно перетаскивать с помощью мышки с целью более удобного отображения схемы.

### Управление группами пользователей, связанными с ролью

Вкладка «Группы пользователей» редактора роли позволяет управлять списком групп пользователей, связанных с ролью (Рис. 33).

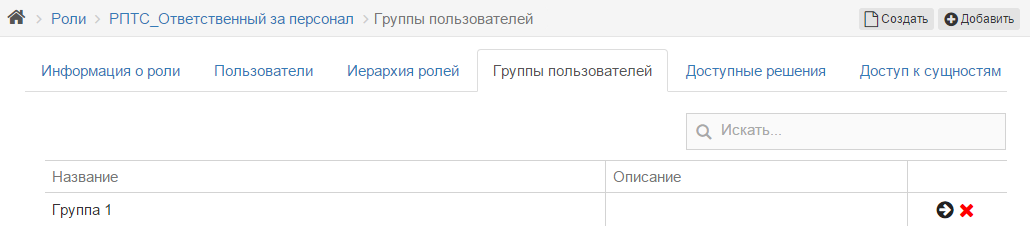


Рис. 33. Список групп пользователей, связанных с ролью

На вкладке отображается список групп пользователей, связанных с ролью.

В последнем столбце таблицы расположены следующие пиктограммы:

*  — переход к редактору группы пользователей (см. раздел 3.3. Редактор группы пользователей);
*  — удаление группы пользователей из списка групп пользователей, связанных с ролью.

В верхней части страницы расположена навигационная панель. В левой ее части отображается путь к странице. В правой части расположены кнопки для добавления связанной группы пользователей из числа имеющихся групп и для создания новой группы пользователей, связанной с ролью.

#### Добавление связанной группы пользователей

Для добавления существующей группы пользователей в список групп пользователей, связанных с ролью:

1. На вкладке «Группы пользователей» редактора роли в навигационной панели нажмите на кнопку «Добавить». Откроется всплывающее окно «Добавление группы пользователей» (Рис. 34).

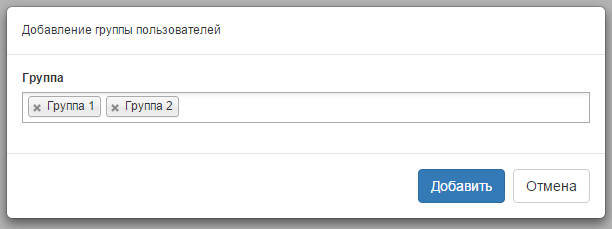


Рис. 34. Добавление существующей группы пользователей

1. В раскрывающемся списке «Группа» выберите группу пользователей, которую нужно добавить в список. Можно последовательно добавить несколько групп.
2. Нажмите на кнопку «Добавить». Выбранные группы пользователей будут добавлены в список групп пользователей, связанных с ролью.

#### Создание группы пользователей, связанной с ролью

Для создания группы пользователей, связанной с ролью, на вкладке «Группы пользователей» редактора роли в навигационной панели нажмите на кнопку «Создать». Откроется всплывающее окно «Создание группы пользователей». Создание группы пользователей, связанной с ролью, аналогично созданию несвязанной группы пользователей (см. раздел 3.2. Создание новой группы пользователей).

### Настройка доступа к решениям

Вкладка «Доступные решения» редактора роли позволяет управлять доступом роли к прикладным модулям (Рис. 35).

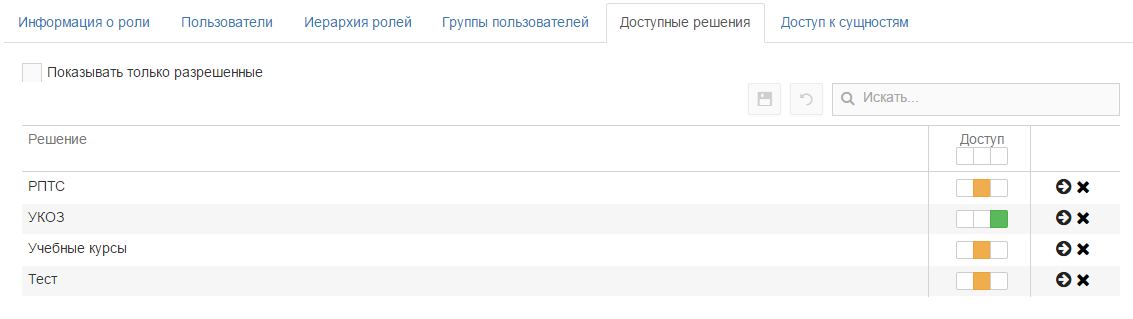


Рис. 35. Список доступных для роли прикладных модулей

На вкладке отображается список всех прикладных модулей текущего экземпляра Платформы.

В последнем столбце таблицы расположены следующие пиктограммы:

*  — переход к редактору настройки прав доступа к элементам решения: источникам данных, формам, отчетам, интеграциям (см. разделы 4.3.6.2 –4.3.6.6);
*  — сброс произведенных настроек доступа к приложениям на значения по умолчанию (желтое значение индикатора — наследование прав доступа от родительских ролей).

В верхней части страницы расположен флаг «Показывать только разрешенные». При установленном флаге в списке отображаются только решения, к которым у данной роли есть доступ.

#### Настройка прав на доступ к решению

Права на доступ к решению задаются с помощью индикатора-светофора в последнем столбце таблицы. Установка индикатора в шапке таблицы настраивает выбранный вариант предоставления доступа для всех решений.

Индикатор-светофор принимает следующие значения:

* *Красный*. Запрет на доступ к решению;
* *Желтый*. Права на доступ к решению наследуются от родительских ролей. В случае их отсутствия устанавливается запрет на доступ к решению;
* *Зеленый*. Разрешение на доступ к решению.

После установки требуемых индикаторов необходимо сохранить изменения. Для этого нажмите на кнопку сохранения ().

Доступ к решению обозначает, что данное решение будет отображаться в левом меню пользователя. Доступ к отдельным компонентам решения: источникам данных, формам, отчетам, шаблонам импорта/экспорта настраивается отдельно (см. ниже).

#### Настройка прав доступа к приложениям

Для каждого приложения, входящего в решение, можно настроить отдельные права доступа, в том числе права доступа к отдельным полям и записям приложения.

Настройка прав доступа к приложениям решения осуществляется на вкладке «Доступные приложения» (Рис. 36) редактора настройки прав доступа к элементам решения. Переход к редактору осуществляется с помощью пиктограммы  в списке решений на вкладке «Доступные решения» редактора роли.

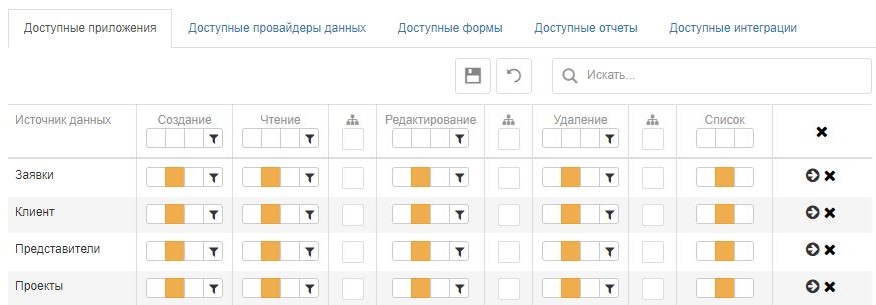


Рис. 36. Настройка доступа к приложениям

На вкладке отображается список всех приложений, входящих в выбранное решение.

В последнем столбце таблицы расположены следующие пиктограммы:

*  — переход к редактору привилегий к полям приложения;
*  — сброс произведенных настроек доступа к приложениям на значения по умолчанию (желтое значение индикатора — наследование прав доступа от родительских ролей). Нажатие на пиктограмму в шапке прав доступа сбрасывает все настроенные права доступа для данного решения.

Имеется возможность настроить следующие виды доступа к приложениям:

* создание;
* чтение;
* редактирование;
* удаление;
* список — отображение в левом меню. Запрет на доступ к элементу блокирует возможность отображения элемента в левом меню.

Права на различные виды доступа задаются с помощью индикатора-светофора. Установка индикатора в шапке столбца настраивает выбранный вариант предоставления доступа для всех приложений.

Индикатор-светофор принимает следующие значения:

* *Красный*. Запрет на выбранный вид доступа к приложению;
* *Желтый*. Права на выбранный вид доступа к приложению наследуются от родительских ролей. В случае их отсутствия устанавливается запрет на выбранный вид доступа;
* *Зеленый*. Разрешение на выбранный вид доступа к приложению;
* — переход к редактору фильтра доступа к приложению (см. раздел. Настройка фильтра привилегий к приложению и его полям).



Для видов доступа чтение, редактирование и удаление имеется возможность использовать дополнительный признак «каскад», который устанавливается с помощью флага в столбце, расположенном справа от выбранного вида доступа и обозначенном пиктограммой . Логическое значение «Да» признака означает, что для данного приложения будет учитываться только значение соответствующего индикатора, и не будут учитываться настройки прав доступа, заданные для отдельных полей приложения. Флаг, установленный в шапке столбца, настраивает значение признака для всех приложений.

##### Редактирование привилегий к полям приложения

Настройка прав доступа к отдельным полям приложения выполняется в окне «Редактирование привилегий к полям приложения» (Рис. 37). Переход к окну осуществляется с помощью пиктограммы  в списке приложений на вкладке «Доступные приложения».

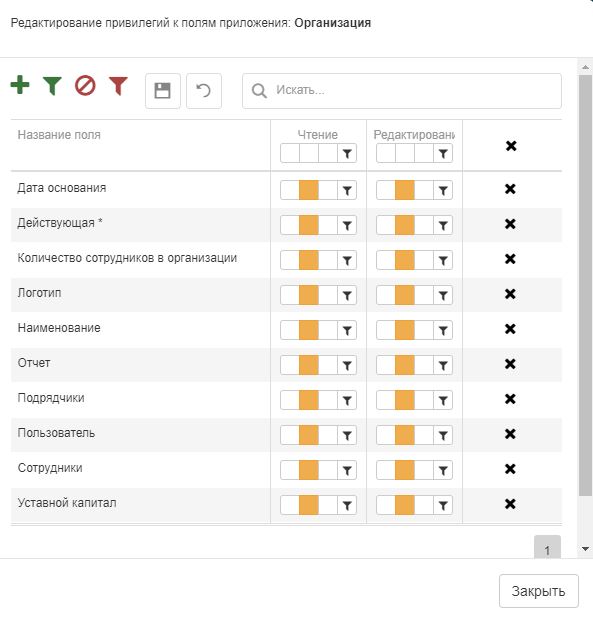


Рис. 37. Редактирование прав доступа к полям приложения

В окне отображается список всех полей, входящих в приложение. В последнем столбце таблицы расположена пиктограмма , позволяющая сбросить настройки доступа для выбранного поля на значения по умолчанию (желтый индикатор — права доступа наследуются от родительских ролей). При нажатии на пиктограмму в шапке таблицы сбрасываются права доступа для всех полей данного приложения.

Поля, указанные как обязательные в редакторе полей приложения, отмечены в списке полей звездочкой. При настройке прав доступа обратите внимание на эти поля и учитывайте обязательность при настройке прав доступа к полям приложения.

Для каждого поля можно настроить права на чтение и редактирование. Права задаются с помощью индикатора-светофора. Установка индикатора в шапке столбца настраивает выбранный вариант предоставления доступа для всех полей приложения.

Индикатор-светофор принимает следующие значения:

* *Красный*. Запрет на выбранный вид доступа к полю приложения;
* *Желтый*. Права на выбранный вид доступа к полю приложения наследуются от родительских ролей. В случае их отсутствия устанавливается запрет на выбранный вид доступа;
* *Зеленый*. Разрешение на выбранный вид доступа к полю приложения;
*  — переход к редактору фильтра доступа к полю приложения (см. раздел. Настройка фильтра привилегий к приложению и его полям).

Над таблицей расположены управляющие кнопки:

*  — добавление фильтра ко всем полям приложения (см. раздел. Настройка фильтра привилегий к приложению и его полям);
*  — добавление фильтра к выбранным полям приложения (см. раздел. Настройка фильтра привилегий к приложению и его полям);
*  — удаление фильтров для всех полей приложения;
*  — удаление фильтров для выбранных полей приложения;
*  — сохранение внесенных изменений;
*  — отмена всех несохраненных изменений;
* поле для поиска информации.

##### Настройка фильтра привилегий к приложению и его полям

Настройка фильтра к приложению, ко всем или к выбранным его полям выполняется в окне «Добавление фильтра привилегий для приложения» (Рис. 38).

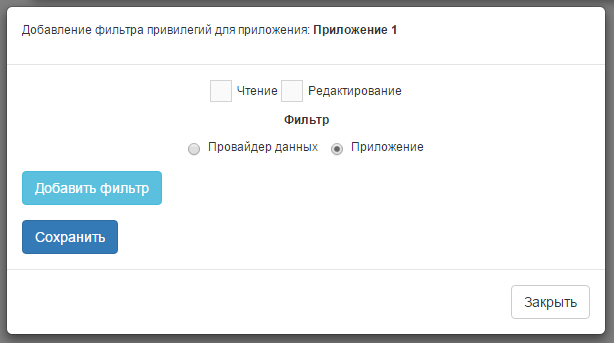


Рис. 38. Редактирование фильтра привилегий к приложению

В верхней части окна выбирается для какого вида действий с записями приложения настраивается фильтр: создание, чтение, редактирование или удаление. Набор флагов зависит от места, из которого вызвано окно настройки фильтра.

Фильтр можно настраивать по записям текущего приложения либо по записям связанного приложения с использованием существующего (созданного ранее) провайдера данных. Вариант задания фильтра определяется с помощью установки соответствующего флага в средней части окна.

Для настройки фильтра:

1. Установите флаги, определяющие, для какого вида действий с записями приложения настраивается фильтр: создание, чтение, редактирование или удаление.
2. Выберите вариант настройки фильтра:

* по записям текущего приложения;
* по записям связанного приложения с использованием существующего (созданного ранее) провайдера данных. При выборе этого варианта отобразится раскрывающийся список для выбора нужного провайдера данных.

1. Нажмите на кнопку «Добавить фильтр».
2. Задайте необходимые условия фильтрации.
3. Нажмите на кнопку «Сохранить». Настройки фильтра будут сохранены.
4. После завершения всех настроек нажмите на кнопку «Закрыть». Всплывающее окно будет закрыто.

*Пример*

*Фильтр на создание записей в приложении работает для отношения многие-к-одному. Для настройки фильтра используется провайдер данных. Поля провайдера должны содержаться в создаваемой записи – при сохранении происходит проверка на пересечение данных в провайдере и новой записи.*

*Например, приложение «Проекты» связано с приложением «Документы» связью с типом «многие-к-одному». Для настройки фильтрации на вставку записей:*

1. *Создайте провайдер данных, с источником данных — приложением «Проекты», и полем «Идентификатор проекта».*
2. *Вызовите окно настройки фильтра для приложения «Документы».*
3. *Установите флаги «Создание» и «Провайдер данных».*
4. *Нажмите на кнопку «Добавить фильтр» и задайте условие, например: состояние проекта принимает значение «Новый».*

*В результате при вставке данных пользователю будет доступно добавление документов, связанных с проектами только в состоянии «Новый».*

Примечание: настройки фильтров привилегий к приложению или его полям не применяются к редактированию записей приложения, отображаемых с помощью элементов «Таблица» и «Связь». Для данных элементов формы применимы только прямые привилегии.

#### Настройка прав доступа к провайдерам данных

Отображение записей в провайдере данных зависит от настроенных разрешений на чтение для приложений, поэтому настройки доступа на чтение провайдера данных не задаются.

Для каждого провайдера данных, входящего в решение, можно настроить отдельные права доступа на отображение в левом меню провайдеров данных.

Настройка прав доступа к провайдерам данных решения осуществляется на вкладке «Доступные провайдеры данных» (Рис. 39) редактора настройки прав доступа к элементам решения. Переход к редактору осуществляется с помощью пиктограммы  в списке решений на вкладке «Доступные решения» редактора роли.

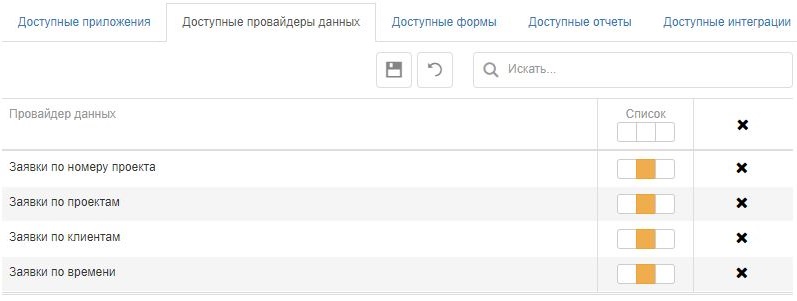


Рис. 39. Настройка доступа к провайдерам данных

На вкладке отображается список всех провайдеров данных, входящих в выбранное решение. В последнем столбце таблицы расположена пиктограмма , позволяющая сбросить настройки доступа для выбранного провайдера данных на значения по умолчанию (желтый индикатор — права доступа наследуются от родительских ролей). Нажатие на пиктограмму в шапке сбрасывает права доступа для всех провайдеров данных.

Для провайдеров данных настраивается только один тип доступа — Список, определяющий отображение провайдера данных в левом меню. Права задаются с помощью индикатора-светофора. Установка индикатора в шапке столбца настраивает выбранный вариант предоставления доступа для всех провайдеров данных.

Индикатор-светофор принимает следующие значения:

* *Красный*. Запрет на отображение провайдера данных в левом меню;
* *Желтый*. Права на отображение провайдера данных в левом меню наследуются от родительских ролей. В случае их отсутствия устанавливается запрет на отображение;
* *Зеленый*. Разрешение на отображение провайдера данных в левом меню.

После окончания всех настроек нажмите на кнопку сохранения ().

#### Настройка прав доступа к формам

Для каждой формы, входящей в решение, можно настроить отдельные права доступа.

Настройка прав доступа к формам решения осуществляется на вкладке «Доступные формы» (Рис. 40) редактора настройки прав доступа к элементам решения. Переход к редактору осуществляется с помощью пиктограммы  в списке решений на вкладке «Доступные решения» редактора роли.

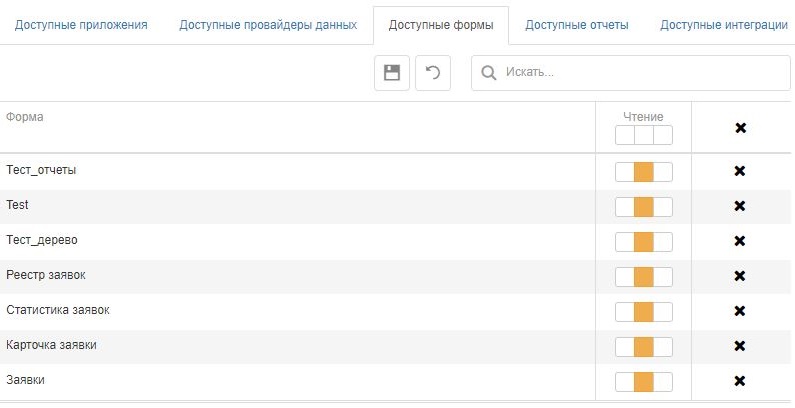


Рис. 40. Настройка доступа к формам

На вкладке отображается список всех форм, входящих в выбранное решение. В последнем столбце таблицы расположена пиктограмма , позволяющая сбросить настройки доступа для выбранной формы на значения по умолчанию (желтый индикатор — права доступа наследуются от родительских ролей). Нажатие на пиктограмму в шапке сбрасывает права доступа для всех форм решения.

Права доступа к формам задаются с помощью индикатора-светофора. Установка индикатора в шапке столбца настраивает выбранный вариант предоставления доступа для всех форм.

Индикатор-светофор принимает следующие значения:

* *Красный*. Запрет на доступ к форме;
* *Желтый*. Права на доступ к форме наследуются от родительских ролей. В случае их отсутствия устанавливается запрет на доступ;
* *Зеленый*. Разрешение на доступ к форме.

После окончания всех настроек нажмите на кнопку сохранения ().

#### Настройка прав доступа к отчетам

Для каждого отчета, входящего в решение, можно настроить отдельные права доступа.

Настройка прав доступа к отчетам решения осуществляется на вкладке «Доступные отчеты» (Рис. 41) редактора настройки прав доступа к элементам решения. Переход к редактору осуществляется с помощью пиктограммы  в списке решений на вкладке «Доступные решения» редактора роли.

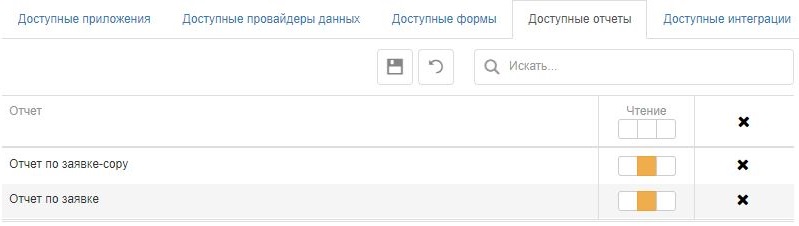


Рис. 41. Настройка доступа к отчетам

На вкладке отображается список всех отчетов, входящих в выбранное решение. В последнем столбце таблицы расположена пиктограмма , позволяющая сбросить настройки доступа для выбранного отчета на значения по умолчанию (желтый индикатор — права доступа наследуются от родительских ролей). Нажатие пиктограммы в шапке сбрасывает права доступа ко всем отчетам решения.

Права на доступ к отчетам задаются с помощью индикатора-светофора. Установка индикатора в шапке столбца настраивает выбранный вариант предоставления доступа для всех отчетов.

Индикатор-светофор принимает следующие значения:

* *Красный*. Запрет на доступ к отчету;
* *Желтый*. Права на доступ к отчету наследуются от родительских ролей. В случае их отсутствия устанавливается запрет на доступ;
* *Зеленый*. Разрешение на доступ к отчету.

После окончания всех настроек нажмите на кнопку сохранения ().

#### Настройка прав доступа к шаблонам импорта/экспорта данных

Для каждого шаблона импорта/экспорта данных, входящего в решение, можно настроить отдельные права доступа.

Настройка прав доступа к шаблонам импорта/экспорта данных осуществляется на вкладке «Доступные интеграции» (Рис. 42) редактора настройки прав доступа к элементам решения. Переход к редактору осуществляется с помощью пиктограммы  в списке решений на вкладке «Доступные решения» редактора роли.

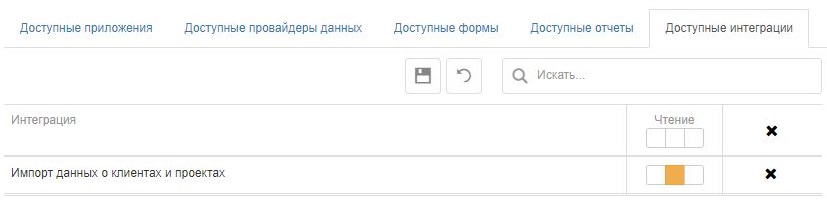


Рис. 42. Настройка доступа к интеграциям

На вкладке отображается список всех шаблонов импорта/экспорта данных, входящих в выбранное решение. В последнем столбце таблицы расположена пиктограмма , позволяющая сбросить настройки доступа для выбранного шаблона на значения по умолчанию (желтый индикатор — права доступа наследуются от родительских ролей). Нажатие на пиктограмму в шапке сбрасывает права доступа ко всем интеграциям решения.

Права на доступ к шаблонам импорта/экспорта данных задаются с помощью индикатора-светофора. Установка индикатора в шапке столбца настраивает выбранный вариант предоставления доступа для всех шаблонов.

Индикатор-светофор принимает следующие значения:

* *Красный*. Запрет на доступ к шаблону;
* *Желтый.* Права на доступ к шаблону наследуются от родительских ролей. В случае их отсутствия устанавливается запрет на доступ;
* *Зеленый*. Разрешение на доступ к шаблону.

После окончания всех настроек нажмите на кнопку сохранения ().

### Настройка доступа к сущностям

Настройка доступа роли к сущностям Платформы выполняется на вкладке «Доступ к сущностям» (Рис. 43). В текущей версии Платформы доступ настраивается только к сущности «Задачи».

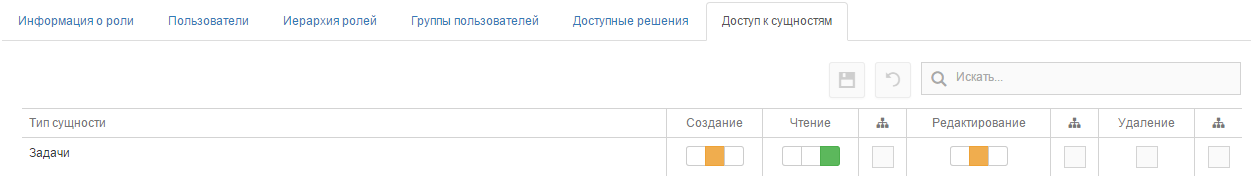


Рис. 43. Настройка доступа к сущностям

Имеется возможность настроить следующие виды доступа к сущности «Задачи»:

* создание;
* чтение;
* редактирование;
* удаление.

Права на различные виды доступа задаются с помощью индикатора-светофора.

Индикатор-светофор принимает следующие значения:

* *Красный*. Запрет на выбранный вид доступа к сущности «Задачи»;
* *Желтый*. Права на выбранный вид доступа к сущности «Задачи» наследуются от родительских ролей. В случае их отсутствия устанавливается запрет на выбранный вид доступа;
* *Зеленый*. Разрешение на выбранный вид доступа к сущности «Задачи».

После окончания всех настроек нажмите на кнопку сохранения ().

### Импорт и синхронизация групп MS Active Directory

В Платформе предусмотрена возможность массового добавления в роль пользователей из MS Active Directory, входящих в одну группу.

Настройка импорта и синхронизации групп MS Active Directory выполняется на вкладке «LDAP-группы» (Рис. 44).

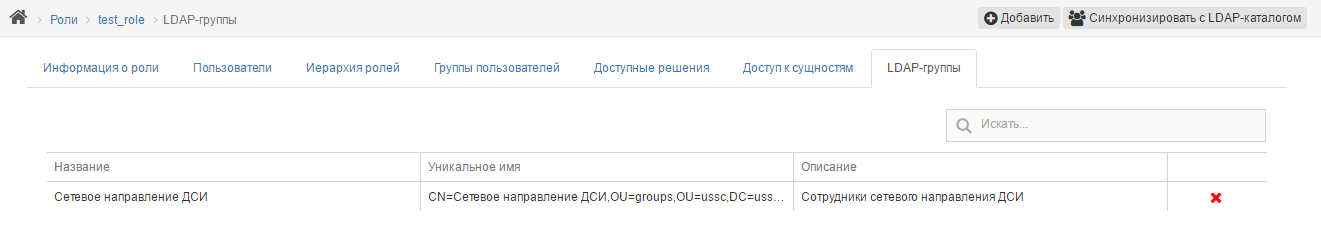


Рис. 44. Настройка импорта и синхронизации групп MS Active Directory

Вкладка содержит список групп MS Active Directory, добавленных в роль. В последнем столбце таблицы расположена пиктограмма , позволяющая удалить LDAP-группу из роли.

В верхней части страницы расположена навигационная панель. В левой ее части отображается путь к странице. В правой части расположены кнопки для добавления LDAP-группы и синхронизации.

#### Добавление группы MS Active Directory в роль

Для добавления группы MS Active Directory в роль:

1. На вкладке «LDAP-группы» редактора роли нажмите на кнопку «Добавить». Откроется всплывающее окно поиска групп в AD (Рис. 45).

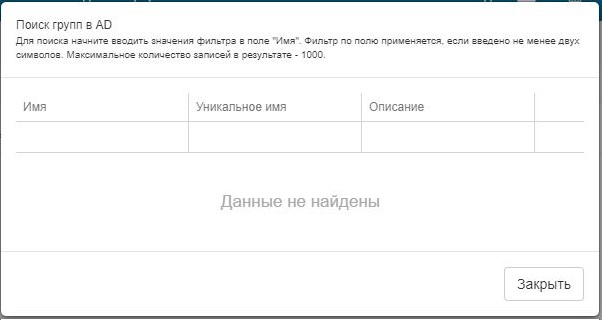


Рис. 45. Добавление LDAP-группы

1. В соответствующем столбце введите поисковое значение (имя, уникальное имя и пр.). Будет сформирован список групп пользователей, удовлетворяющих заданным условиям поиска.
2. Нажмите на пиктограмму  для импорта группы. Выбранная группа будет импортирована в роль.
3. Для добавления нескольких групп последовательно нажмите на пиктограмму для каждой из них. Выбранные группы будут импортированы.
4. Нажмите на кнопку «Закрыть». Всплывающее окно закроется.

|  |
| --- |
| *Внимание!*  *Добавление LDAP-группы в роль не влечет за собой добавления и обновления пользователей. Для этого необходимо выполнить синхронизацию с LDAP-каталогом.* |

#### Синхронизация с LDAP-каталогом

При синхронизации с LDAP-каталогом выполняется импорт/обновление списка пользователей:

* если пользователь, входящий в LDAP-группу, не зарегистрирован в Платформе, для него создается учетная запись;
* если пользователь зарегистрирован в Платформе, выполняется обновление его атрибутов;
* если в Active Directory пользователь заблокирован, выполняется блокировка его учетной записи в Платформе;
* если пользователь удален из LDAP-группы, его учетная запись блокируется в Платформе (если пользователь не включен ни в одну LDAP-группу, связанную с его ролями).

Синхронизация может выполнятся вручную или автоматически по заданному расписанию.

Для синхронизации с LDAP-каталогом вручную на вкладке «LDAP-группы» редактора роли нажмите на кнопку «Синхронизировать с LDAP-каталогом». Подтвердите свое действие во всплывающем окне, информирующем о том, что синхронизация может занять некоторое время. После завершения синхронизации появится системное сообщение об успешной синхронизации с указанием числа пользователей.

Включение автоматической синхронизации и настройка ее расписания выполняется на странице системных настроек. Подробнее см. документ «Приложение 9. Подсистема управления, мониторинга и контроля» раздел «Настройка LDAP-синхронизации».