Программа для ЭВМ

Analytic Workspace «ДатаМед»

Документация, содержащая информацию, необходимую для эксплуатации экземпляра программного обеспечения

2022

Содержание

Перечень терминов и сокращений

Термин, сокращение	Определение
Apache Airflow	Открытое программное обеспечение для создания, мониторинга и оркестрации сценариев обработки данных
API	Application Programming Interface – интерфейс программирования приложений – набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) для использования во внешних программных продуктах
BI	Business Intelligence – инструменты для поиска, анализа, моделирования и доставки информации, необходимой для принятия решения
ClickHouse	Колоночная аналитическая СУБД с открытым кодом, позволяющая выполнять аналитические запросы в режиме реального времени на структурированных больших данных
CPU	Central processing unit – центральное процессорное устройство
csv	Comma – Separated Values – текстовый формат, предназначенный для представления табличных данных
DAG	Структура данных в виде однонаправленного графа, где ни один элемент не может считаться дочерним
DevOps	Development & operations – методология активного взаимодействия специалистов по разработке со специалистами по информационно-технологическому обслуживанию и взаимная интеграция их рабочих процессов друг в друга для обеспечения качества продукта
Drag-and-drop	Способ оперирования элементами интерфейса в интерфейсах пользователя (как графическим, так и текстовым) при помощи манипулятора «мышь» или сенсорного экрана
Elasticsearch	Масштабируемая утилита полнотекстового поиска и аналитики, которая позволяет быстро в режиме реального времени хранить, искать и анализировать большие объемы данных
ETL	Один из основных процессов в управлении хранилищами данных, который включает в себя: извлечение данных из внешних источников, их трансформацию и загрузку в хранилище данных
GET	Метод запроса для получения информации от web-сервера, используемый HTTP протоколом сети Интернет, передает данные через ссылку (в URL) в виде пар «имя-значение»
GUI	Graphical User Interface – графический интерфейс пользователя
ID	Уникальный признак объекта, позволяющий отличать его от других объектов
IP	Internet Protocol – маршрутизируемый протокол сетевого уровня стека TCP/IP

Термин, сокращение	Определение
IP-адрес	Internet Protocol Address – уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP
JOIN	Оператор языка SQL, который является реализацией операции соединения реляционной алгебры
JSON	JavaScript Object Notation – простой формат обмена данными, удобный для чтения и написания как человеком, так и компьютером
LDAP	Lightweight Directory Access Protocol – протокол прикладного уровня для доступа к службе каталогов X.500. LDAP – протокол, использующий TCP/IP и позволяющий производить операции аутентификации, поиска и сравнения, а также операции добавления, изменения или удаления записей
OAuth	Открытый протокол (схема) авторизации, который позволяет предоставить третьей стороне ограниченный доступ к защищенным ресурсам пользователя без необходимости передавать ей (третьей стороне) логин и пароль
OIDC	OpenID Connect – расширение, предназначенное для обеспечения идентификации и аутентификации пользователя посредством протокола OAuth 2.0
OpenID	Система единого входа (авторизации) на сайты, порталы, блоги и форумы
PHP	Hypertext Preprocessor – язык программирования, специально разработанный для написания web-приложений
POST	Один из многих методов запроса, поддерживаемых HTTP протоколом, используемым в сети Интернет, предназначен для запроса, при котором web-сервер принимает данные, заключенные в тело сообщения, для хранения. Он часто используется для загрузки файла или представления заполненной web-формы
PostgreSQL	Свободная объектно-реляционная система управления базами данных
RAM, ОЗУ	Random Access Memory – оперативное запоминающее устройство – оперативная память – энергозависимая часть системы компьютерной памяти, в которой во время работы компьютера хранится выполняемый машинный код (программы), а также входные, выходные и промежуточные данные, обрабатываемые процессором
REST	Representational State Transfer — архитектурный стиль взаимодействия компонентов распределенного приложения в сети
SQL	Structured Query Language (язык структурированных запросов) – язык программирования, предназначенный для управления данными в системах управления реляционными базами данных
SSD	Solid State Drive – накопитель информации, основанный на чипах энергонезависимой памяти, которые сохраняют данные после отключения питания
SSO	Single Sign-On – технология, при использовании которой пользователь переходит из одного раздела портала в другой без повторной аутентификации

Термин, сокращение	Определение
Swagger	Набор инструментов для разработчиков API от SmartBear Software
UNION	Объединение. В языке SQL операция UNION применяется для объединения двух наборов строк, возвращаемых SQL-запросами
UNION ALL	Оператор SQL для объединения результирующего набора данных нескольких запросов, данный оператор выведет абсолютно все строки, даже дубли
URL	Uniform Resource Locator – стандартизированный способ записи адреса ресурса в сети Интернет
VM	Виртуальная машина
Администратор, администратор Системы	Сотрудник, наделенный полномочиями управления Системой
Алиас	Alias – псевдоним – альтернативное наименование
БД	База данных
Виджет	Элемент графического интерфейса
Дамп	Файл с полным или частичным содержимым памяти компьютера или базы данных в момент создания этого файла
ИА	Система идентификации, аутентификации и авторизации
Интерактивная панель (Дашборд)	Инструмент для визуализации и анализа информации о бизнес-процессах и их эффективности
ООО «НОВОСОФТИМ»	Общество с ограниченной ответственностью «НОВОСОФТИМ»
ОС	Операционная система
ПК	Персональный компьютер
Система	Программа для ЭВМ «ДатаМед»
СУБД	Система управления базами данных
ФИО	Фамилия, имя, отчество

1 Введение

1.1 Область применения

Программа для ЭВМ «ДатаМед» (далее – Система) Система предназначена для анализа первичной информации, возникающей в процессе оказания медицинских услуг.

1.2 Краткое описание возможностей

Система предназначена для решения следующих задач:

- **работа с разными источниками данных:**
  - интерфейс работы со списками источников данных;
  - настройка подключения к доступным источникам данных посредством диалога через GUI:
    - настройка параметров подключения к источнику данных;
    - проверка успешности подключения к источнику данных.
  - регистрация подключения к источнику данных в Системе (успешно подключенных) посредством диалога через GUI;
  - просмотр физических моделей данных в подключенном источнике данных посредством диалога через GUI:
    - просмотр списка доступных пользователю таблиц выбранного источника данных;
    - контекстный поиск таблиц по имени в выбранном источнике данных;
    - просмотр структуры выбранной таблицы (названия столбцов и их типы) и данные (первые несколько строк) в табличном представлении;
    - сортировка данных выбранной таблицы по убыванию или возрастанию.

- клонирование источника данных;
- удаление источника данных;
- управление доступом к источнику данных.
    - Предусмотрена возможность использования источников данных стороннего реляционного хранилища под управлением СУБД PostgreSQL, Oracle, Microsoft SQL, ClickHouse, Greenplum, MariaDB, Vertica, а также загрузка данных из файлов форматов Excel, CSV, JSON, XML.

- **работа с моделями данных:**
    - создание/редактирование логических структур данных (набор логических таблиц данных) на основе доступных физических структур данных из состава подключенных источников данных посредством диалога через GUI:
        - просмотр физических моделей из состава подключенных источников данных;
        - подбор таблиц физической модели для включения в логическую модель данных;
        - подбор отдельных полей из физической структуры данных для включения в логическую модель;
        - настройка дополнительных синтетических полей таблицы логической модели (вычисляемых полей и иерархий);
        - создание/редактирование логических моделей на основе выбранных физических таблиц и полей в них;
        - переход в интерфейс Apache Airflow для просмотра деталей процесса загрузки данных.

- управление составом зарегистрированных логических моделей данных посредством диалога через GUI;
- управление процедурами загрузки данных посредством диалога через GUI:
    - синхронизация логических моделей;
    - синхронизация данных в логических моделях и данных в физических источниках;
    - планировщик синхронизации данных логической модели с источником данных;
    - настройка инкрементальной загрузки данных.
- клонирование модели;
- удаление модели;
    - управление доступом к модели.

- **работа с визуальными элементами (виджеты):**
    - управление настройками элемента визуального представления посредством диалога через GUI:
        - подключение логических моделей и ее элементов к визуальному элементу;
        - выбор типа визуального элемента:
            - таблица;
            - столбчатая диаграмма (вертикальная);
            - столбчатая диаграмма с накоплением (вертикальная);

        - столбчатая диаграмма (горизонтальная);
        - столбчатая диаграмма с накоплением (горизонтальная);
        - линейный график;
        - радар;
        - круговая диаграмма;
        - кольцевая диаграмма;
        - полярная диаграмма;
        - тренд;
        - карта;
        - древовидная карта;
        - тепловая карта;
        - сводная таблица.
    - предварительный просмотр визуального элемента;
    - управление составом настроенных визуальных элементов;
    - условное форматирование в таблицах;
    - управление цветом в графических виджетах;
    - агрегация данных в таблицах.
- отображение визуальных элементов с данными:

- сортировка данных в визуальном элементе (включая скрытую сортировку по уровням вложенности);
- фильтрация данных в визуальном элементе;
- агрегация, настройка итоговых и промежуточных значений;
- условное форматирование в визуальном элементе;
- группировка данных на визуальном элементе (если математический смысл визуального элемента это допускает).

- доступ к виджету по прямой ссылке (в режиме просмотра);
- выгрузка архива в формате .zip с данными в формате .cvs, выведенными в визуальном элементе. В случае выгрузки большого объема данных в Системе предлагается фоновая выгрузка данных;
- клонирование элемента визуального представления;
- удаление элемента визуального представления;
- управление доступом к визуальному элементу.

- **работа с интерактивными панелями:**
  - интерфейс работы со списком информационных панелей;
  - добавление, редактирование, клонирование и удаление информационных панелей;
  - добавление и настройка аналитических виджетов:
    - вывод на одном экране информации нескольких виджетов;
    - настройка отображения элементов аналитических виджетов.

- настройка связи между виджетами, построенными на базе разных моделей;
- добавление и настройка виджетов – полей фильтрации с типом:
  - «Список»;
  - «Множественный выбор»;
  - «Календарь»;
  - «Двойной календарь»;
  - «Ползунок»;
  - «Поле ввода».
- экспорт необходимого виджета информационной панели в формате .csv;
- экспорт данных информационной панели в файлы формата .pdf и .png;
- доступ к информационной панели по прямой ссылке (в режиме просмотра);
- управление доступом к информационной панели.

- **работа с панелью управления администратора:**
  - отображение списка зарегистрированных в Системы пользователей;
  - регистрация, редактирование, блокировка учетных записей пользователей;
  - создание, редактирование, удаление групп пользователей;
  - просмотр прав доступа пользователей к объектам Системы. Каждый объект содержит независимую настройку доступа с правом ее редактирования автором объекта;

- просмотр прав доступа группы пользователей к объектам Системы. Каждый объект содержит независимую настройку доступа с правом ее редактирования автором объекта;
- управление доступом пользователей к объектам Системы;
- управление доступом групп пользователей к объектам Системы;
- просмотр активности пользователей, в том числе просмотр даты и времени входа в программу для ЭВМ и выхода пользователей из Системы;
- просмотр, добавление, редактирование и удаление атрибутов схемы доступа;
- просмотр, добавление, редактирование и удаление провайдеров;
- выгрузка краткой информации о параметрах Системы в файл формата .csv;
- внесение изменений в поле ввода адреса официального сайта Системы.

1.3 Уровень подготовки пользователей

Пользователи Системы – аналитики и BI-разработчики с базовыми знаниями SQL. Пользователи должны обладать навыками работы с ОС Microsoft Windows или любой версией Linux, а также навыками работы с web-браузером (например, Microsoft Internet Explorer, Opera, Mozilla Firefox). Перед началом работы с Системой пользователи, не обладающие такими навыками, должны пройти соответствующие курсы.

1.4 Перечень эксплуатационной документации, с которой необходимо ознакомиться пользователю

Для работы с Системой ознакомьтесь с данным руководством.

2 Назначение и условия применения

2.1 Виды деятельности и автоматизируемые функции в Системе

Система создана как многопользовательский инструмент для интерактивной визуализации и анализа данных, в том числе для автоматизации функций:

- добавления, изменения, клонирования и удаления источников данных;
- создания, изменения, клонирования и удаления модели данных;
- создания, изменения, клонирования и удаления виджета, фильтрации, сортировки, форматирования и агрегации выводимых им данных;
- создания, изменения, клонирования и удаления информационных панелей.

2.2 Условия применения

2.2.1 Требования к техническому обеспечению

Аппаратное обеспечение должно соответствовать типу используемого web-браузера для комфортной работы с сетью Интернет.

2.2.1.1 Аппаратные требования по размещению Системы

Заданные показатели назначения и надежности Системы должны осуществляться при условии выполнения следующих аппаратных требований по размещению Системы (Таблица 1). Допустима виртуализация мощностей.

Таблица 1 – Требования к вычислительным мощностям

№	Назначение	Количество VM (виртуальных машин), шт	CPU, шт	Минимальная тактовая частота, ГГц	RAM, ГБ	SSD, ГБ	Минимальные требования к сетевому интерфейсу
1	Сервер (назначение: Сервер приложения, Сервер	1	4	2	64	500	2x1 Гбит/с

№	Назначение	Количество VM (виртуальных машин), шт	CPU, шт	Минимальная тактовая частота, ГГц	RAM, ГБ	SSD, ГБ	Минимальные требования к сетевому интерфейсу
	балансировки, СУБД)						
Итого		1	4	2	64	500	2x1 Гбит/с

2.2.1.2 Требования к обеспечению каналами связи

Для связи между всеми серверами приложения: web -приложение, БД, файловое хранилище, балансировщики и т.д., должен использоваться канал с пропускной способностью не менее 1 Гбит/сек.

Требования к характеристикам каналов связи для пользователей представлены в таблице ниже (Таблица 2).

Таблица 2 – Каналы связи

Требования к количеству пользователей, подключенных к каналу связи	Требования к каналам связи между клиентскими машинами и севером приложений
От 1 до 50 пользователей	Канал связи: 1 Гбит/сек
От 50 до 100 пользователей	Канал связи: 1 Гбит/сек
От 100 до 200 пользователей	Канал связи: 1 Гбит/сек
От 200 пользователей	Канал связи: 1 Гбит/сек
Примечание – Подразумевается стабильный канал связи	

2.2.1.3 Требования к техническому обеспечению клиентских машин

Для клиентских машин устанавливаются следующие минимальные технические требования:

- процессор Intel Core i3-2330M 2,2 ГГц;
- ОЗУ – 4 ГБ;
- объем жесткого диска – 100 ГБ, объем свободного места на диске – не менее 5 ГБ;
- сетевая карта 1 ГБ/с;

- монитор, поддерживающий разрешение не менее 1920x1080;
- клавиатура, манипулятор типа «мышь».

2.2.2 Требования к программному обеспечению

Для функционирования Системы необходимо следующее программное обеспечение:

- CentOS, версия 7 и выше – сервер приложения;
- Docker, версия 20.10.1 и выше – контейнеризация.

Требования к обеспечению клиентских рабочих мест:

- web-браузеры:
  - Microsoft Edge версии 12 или выше;
  - Google Chrome версии 64 или выше;
  - Mozilla Firefox версии 52 или выше;
  - Safari версии 11 или выше;
  - Opera версии 43 или выше;
  - Яндекс.Браузер версии 19.6.1 и выше.
- одна из следующих ОС: Microsoft Windows, Linux (Unix), MacOS, IOS и других, поддерживающих работу указанных web-браузеров.

2.3 Языки программирования

Используемые в Системе языки программирования:

- Golang;

- PHP;
- Python.

3 Функциональная архитектура Системы

Общая функциональная архитектура Системы представлена на рисунке (Рисунок 1).

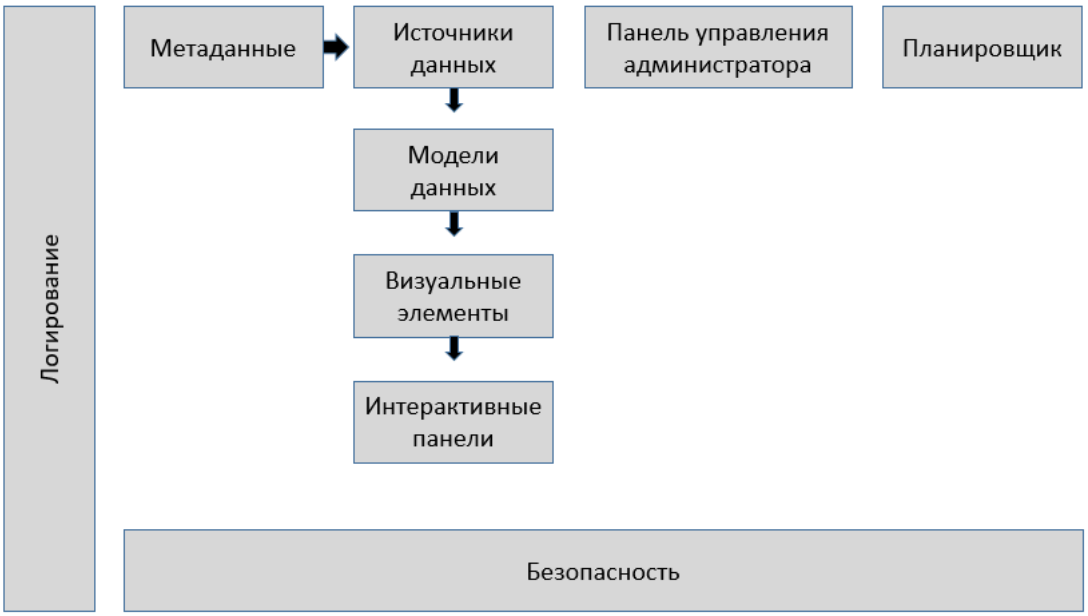


Рисунок 1 – Общая функциональная архитектура Системы

Система состоит из следующих подсистем:

- «Источники данных»;
- «Модели данных»;
- «Визуальные элементы (виджеты)»;
- «Интерактивные панели (дашборды)»;
- «Панель управления администратора».

3.1 Источники данных

Модуль предоставляет следующие функциональные возможности:

- интерфейс работы со списками источников данных;

- настройка подключения к доступным источникам данных посредством диалога через GUI:
  - настройка параметров подключения к источнику данных;
  - проверка успешности подключения к источнику данных.
- регистрация подключения к источнику данных в Системе (успешно подключенных) посредством диалога через GUI;
- просмотр физических моделей данных в подключенном источнике данных посредством диалога через GUI:
  - просмотр списка доступных пользователю таблиц выбранного источника данных;
  - контекстный поиск таблиц по имени в выбранном источнике данных;
  - просмотр структуры выбранной таблицы (названия столбцов и их типы) и данные (первые несколько строк) в табличном представлении;
  - сортировка данных выбранной таблицы по убыванию или возрастанию.
- клонирование источника данных;
- удаление источника данных;
- управление доступом к источнику данных.
- Предусмотрена возможность использования источников данных стороннего реляционного хранилища под управлением СУБД PostgreSQL, Oracle, Microsoft SQL, ClickHouse, Greenplum, MariaDB, Vertica, а также загрузка данных из файлов форматов Excel, CSV, JSON, XML.

3.2 Модели данных

Модуль предоставляет следующие функциональные возможности:

- создание/редактирование логических структур данных (набор логических таблиц данных) на основе доступных физических структур данных из состава подключенных источников данных посредством диалога через GUI:
  - просмотр физических моделей из состава подключенных источников данных;
  - подбор таблиц физической модели для включения в логическую модель данных;
  - подбор отдельных полей из физической структуры данных для включения в логическую модель;
  - настройка дополнительных синтетических полей таблицы логической модели (вычисляемых полей и иерархий);
  - создание/редактирование логических моделей на основе выбранных физических таблиц и полей в них;
  - переход в интерфейс Apache Airflow для просмотра деталей процесса загрузки данных.
- управление составом зарегистрированных логических моделей данных посредством диалога через GUI;
- управление процедурами загрузки данных посредством диалога через GUI:
  - синхронизация логических моделей;
  - синхронизация данных в логических моделях и данных в физических источниках;

- планировщик синхронизации данных логической модели с источником данных;
- настройка инкрементальной загрузки данных.

- клонирование модели;
- удаление модели;
- управление доступом к модели.

3.3 Визуальные элементы (Виджеты)

Модуль предоставляет следующие функциональные возможности:

- управление настройками элемента визуального представления посредством диалога через GUI:
  - подключение логических моделей и ее элементов к визуальному элементу;
  - выбор типа визуального элемента:
    - таблица;
    - столбчатая диаграмма (вертикальная);
    - столбчатая диаграмма с накоплением (вертикальная);
    - столбчатая диаграмма (горизонтальная);
    - столбчатая диаграмма с накоплением (горизонтальная);
    - линейный график;
    - радар;

        - круговая диаграмма;
        - кольцевая диаграмма;
        - полярная диаграмма;
        - тренд;
        - карта;
        - древовидная карта;
        - тепловая карта;
        - сводная таблица.
    - предварительный просмотр визуального элемента;
    - управление составом настроенных визуальных элементов;
    - условное форматирование в таблицах;
    - управление цветом в графических виджетах;
    - агрегация данных в таблицах.
- отображение визуальных элементов с данными:
    - сортировка данных в визуальном элементе (включая скрытую сортировку по уровням вложенности);
    - фильтрация данных в визуальном элементе;
    - агрегация, настройка итоговых и промежуточных значений;
    - условное форматирование в визуальном элементе;

- группировка данных на визуальном элементе (если математический смысл визуального элемента это допускает).
- доступ к виджету по прямой ссылке (в режиме просмотра);
- выгрузка архива в формате .zip с данными в формате .cvs, выведенными в визуальном элементе. В случае выгрузки большого объема данных в Системе предлагается фоновая выгрузка данных;
- клонирование элемента визуального представления;
- удаление элемента визуального представления;
- управление доступом к визуальному элементу.

3.4 Интерактивные панели (дашборды)

Модуль предоставляет следующие функциональные возможности:

- интерфейс работы со списком информационных панелей;
- добавление, редактирование, клонирование и удаление информационных панелей;
- добавление и настройка аналитических виджетов:
  - вывод на одном экране информации нескольких виджетов;
  - настройка отображения элементов аналитических виджетов.
- настройка связи между виджетами, построенными на базе разных моделей;
- добавление и настройка виджетов – полей фильтрации с типом:
  - «Список»;

- «Множественный выбор»;
- «Календарь»;
- «Двойной календарь»;
- «Ползунок»;
- «Поле ввода».

- экспорт необходимого виджета информационной панели в формате .csv;
- экспорт данных информационной панели в файлы формата .pdf и .png;
- доступ к информационной панели по прямой ссылке (в режиме просмотра);
- управление доступом к информационной панели.

3.5 Панель управления администратора

Панель управления администратора предназначена для управления правами доступа к аналитической СУБД и управления доступа к объектам и функциям модулей Системы.

Панель управления администратора предоставляет следующие функциональные возможности:

- отображение списка зарегистрированных в Системы пользователей;
- регистрация, редактирование, блокировка учетных записей пользователей;
- создание, редактирование, удаление групп пользователей;
- просмотр прав доступа пользователей к объектам Системы. Каждый объект содержит независимую настройку доступа с правом ее редактирования автором объекта;

- просмотр прав доступа группы пользователей к объектам Системы. Каждый объект содержит независимую настройку доступа с правом ее редактирования автором объекта;
- управление доступом пользователей к объектам Системы;
- управление доступом групп пользователей к объектам Системы;
- просмотр активности пользователей, в том числе просмотр даты и времени входа в программу для ЭВМ и выхода пользователей из Системы;
- просмотр, добавление, редактирование и удаление атрибутов схемы доступа;
- просмотр, добавление, редактирование и удаление провайдеров;
- выгрузка краткой информации о параметрах Системы в файл формата .csv;
- внесение изменений в поле ввода адреса официального сайта Системы.

4 Подготовка к работе

4.1 Запуск Системы

Для начала работы с Системой:

- запустите web-браузер двойным нажатием левой кнопки мыши по его ярлыку на рабочем столе или нажмите на кнопку «Пуск» и в открывшемся меню выберите пункт, соответствующий используемому web-браузеру;
- в адресной строке введите адрес Системы;
- в окне авторизации пользователя введите логин и пароль и нажмите на кнопку «Войти» (Рисунок 2).

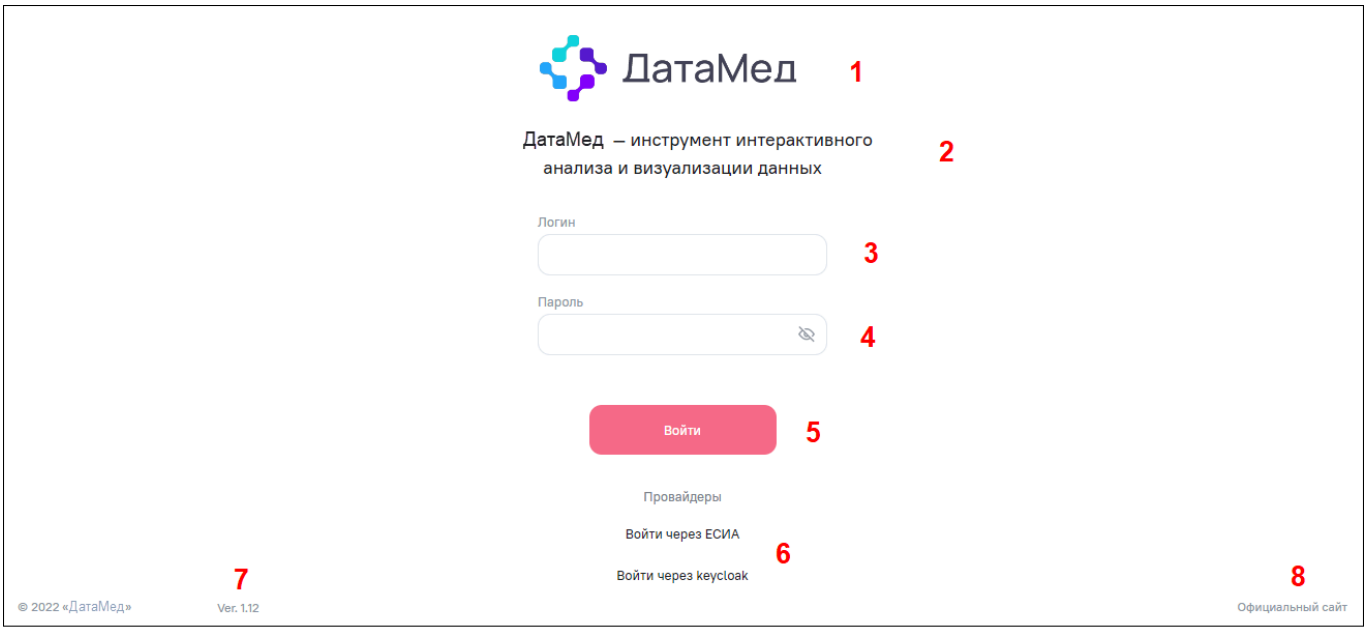


Рисунок 2 – Окно авторизации

Окно авторизации состоит из следующих элементов (см. Рисунок 2):

1) логотип Системы;
2) наименование Системы;
3) поле для ввода логина;
4) поле для ввода пароля;
5) кнопка «Войти» для входа в Систему;

6) кнопки входа через внешние провайдеры. Кнопки отображаются, если внешние провайдеры настроены администратором Системы;
7) номер версии Системы;
8) ссылка на официальный сайт Системы. Для перехода на официальный сайт Системы нажмите на ссылку «Официальный сайт» или на логотип Системы.

Примечание – В целях защиты обратной связи при вводе аутентификационной информации Система не отображает вводимые символы в поле пароля.

Доступен вход в Систему через провайдеры, если они настроены администратором Системы. При нажатии на кнопку провайдера происходит переадресация на страницу аутентификации провайдера.

Откроется окно Системы (Рисунок 3). Слева отображается главное меню.

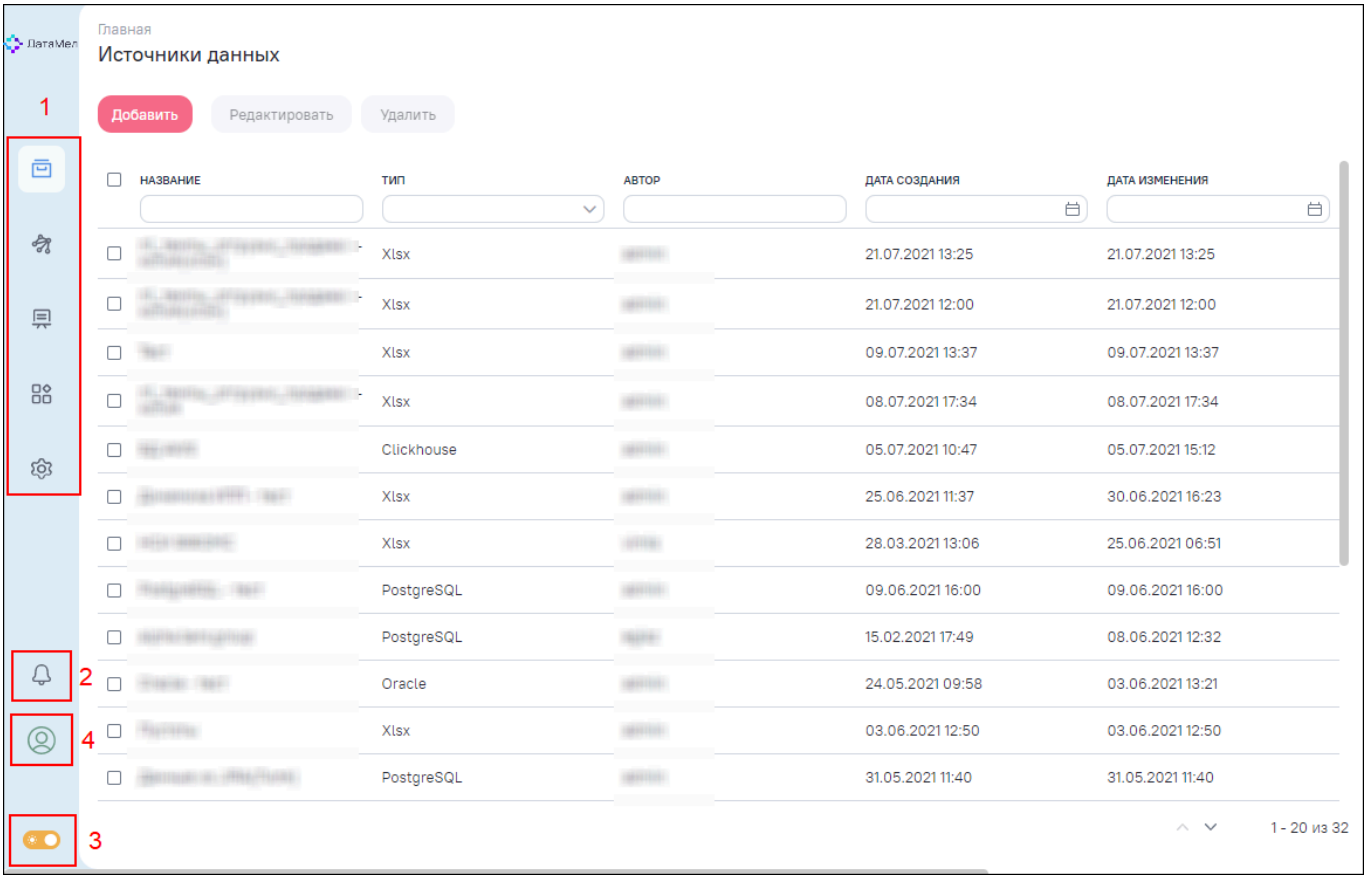


Рисунок 3 – Окно Системы

Примечание – Панель главного меню отображается на каждой странице Системы.

Чтобы перейти в другие разделы Системы, нажмите на соответствующую разделу кнопку (см. 1, Рисунок 3). Откроется окно выбранного раздела, цвет фона окна в каждом разделе различается.

Чтобы посмотреть уведомления, нажмите на кнопку  (см. 2, Рисунок 3). Откроется окно просмотра уведомления (Рисунок 4).

Примечание – Возле пиктограммы отображается число новых уведомлений (при их наличии).

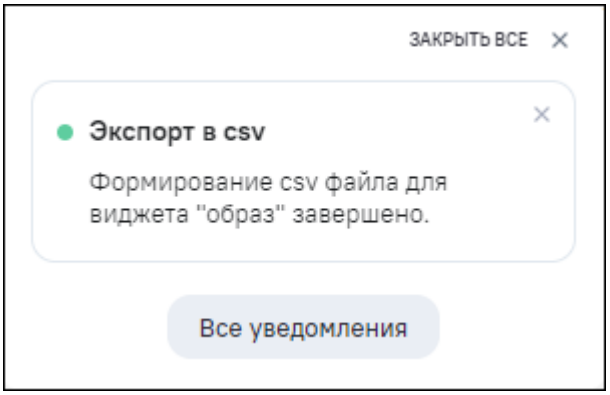
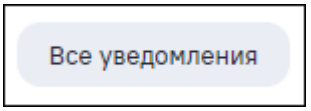


Рисунок 4 – Окно просмотра уведомления

После просмотра уведомления нажмите на кнопку 

, чтобы закрыть окно, или на кнопку 

, чтобы перейти в раздел «Центр уведомлений» (Рисунок 5).

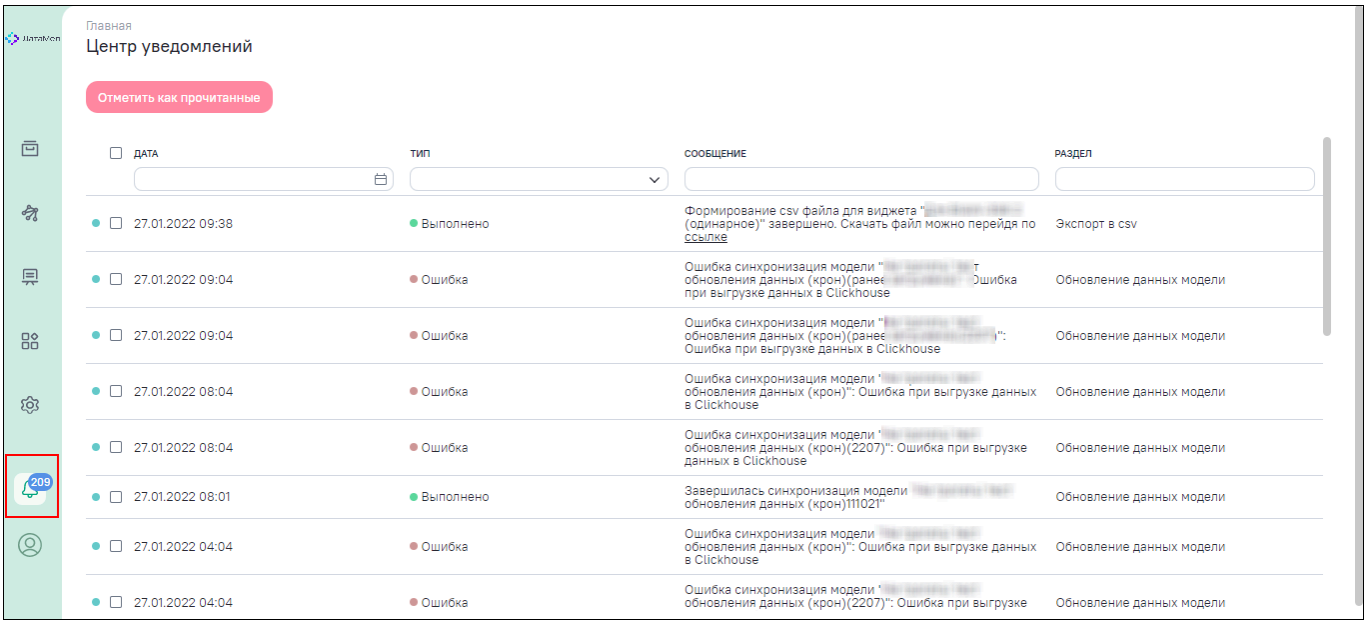


Рисунок 5 – Окно «Центр уведомлений»

Чтобы сменить тему Системы, нажмите на кнопку  (см. 3, Рисунок 6).

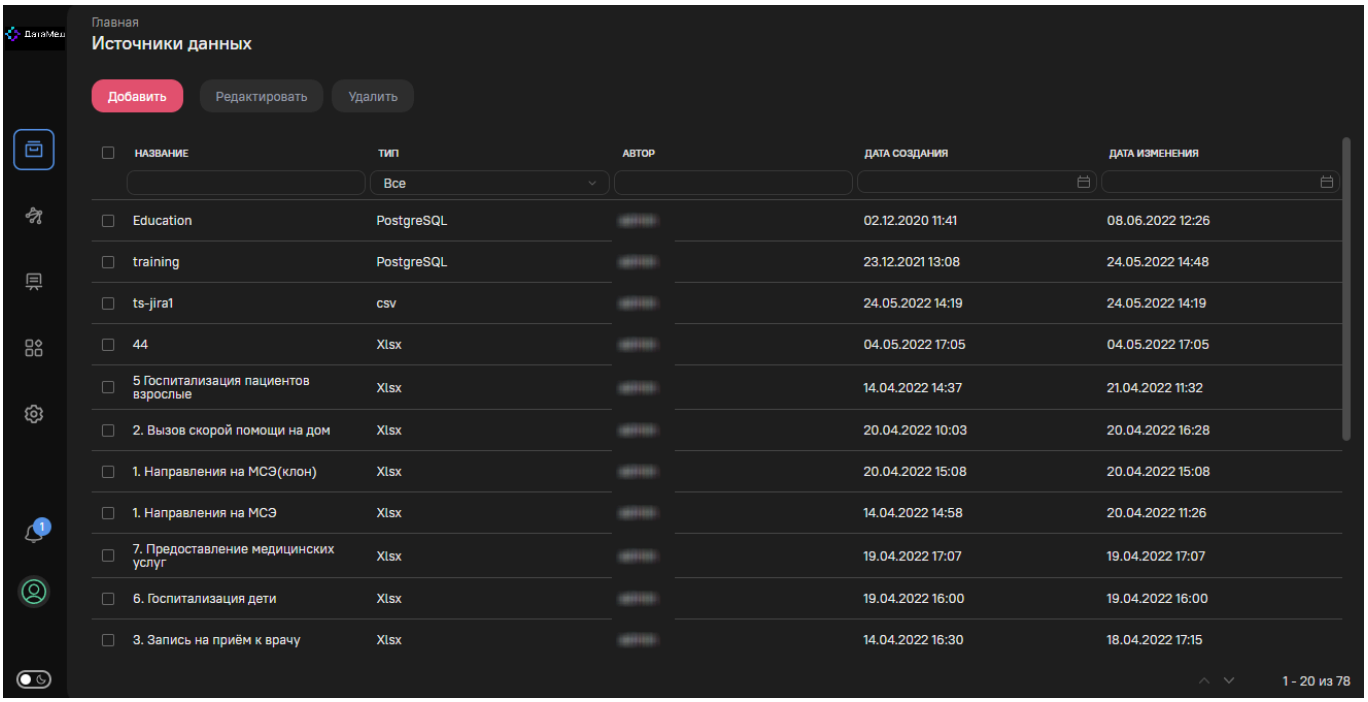


Рисунок 6 – Темная тема Системы

4.2 Выход из Системы

Чтобы выйти из Системы, нажмите на поле (см. 4, Рисунок 3) с аватаром в главном меню и выберите значение «Выход» (Рисунок 7).

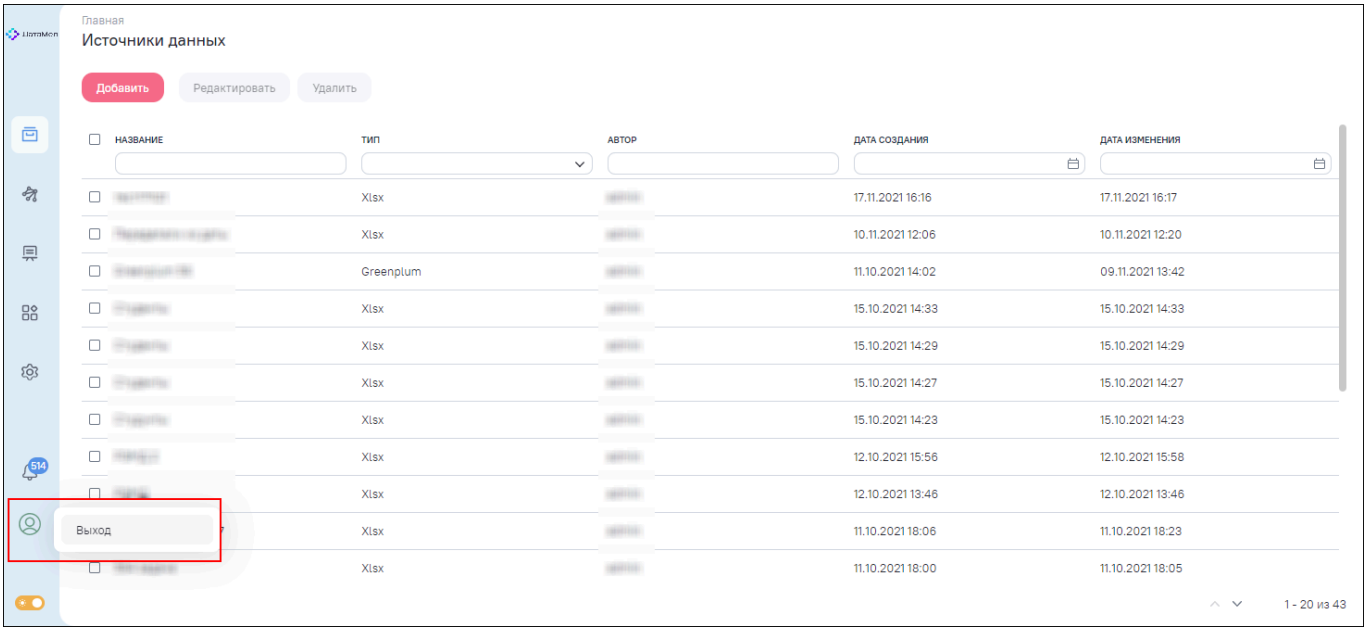


Рисунок 7 – Выход из Системы

5 Администрирование Системы

5.1 Состав администраторов Системы

В Системе есть встроенная учетная запись «admin» (главный администратор Системы), а также пользователи, наделенные административными правами через встроенную системную группу «Администратор». Данным пользователям доступны интерфейс блока администрирования и функции администратора Системы.

Управление доступом к конкретным объектам Системы может выполнять пользователь, не являющийся администратором Системы. Доступно управление доступом:

- к тем объектам, которые пользователь создал самостоятельно;
- к тем объектам, на которые создавший их пользователь выдал разрешение на администрирование.

5.2 Функции администратора Системы

В функции администратора Системы входят задачи управления:

- общими настройками;
- пользователями;
- группами пользователей (предназначены для массового присвоения пользователям стандартных наборов разрешений);
- активностью пользователей;
- схемами доступов;
- провайдерами.

В Системе действует разрешительная модель доступа пользователей к функциям и данным других пользователей. Доступ ко всему по умолчанию запрещен. Для созданных

(своих объектов) пользователь получает доступ сразу (в рамках своих прав доступа к функциям). Пользователь может предоставить свои объекты в доступ другим пользователям и группам пользователей.

Пользовательский интерфейс блока администрирования построен в соответствии с указанным выше набором функций и имеет следующий вид (Рисунок 8).

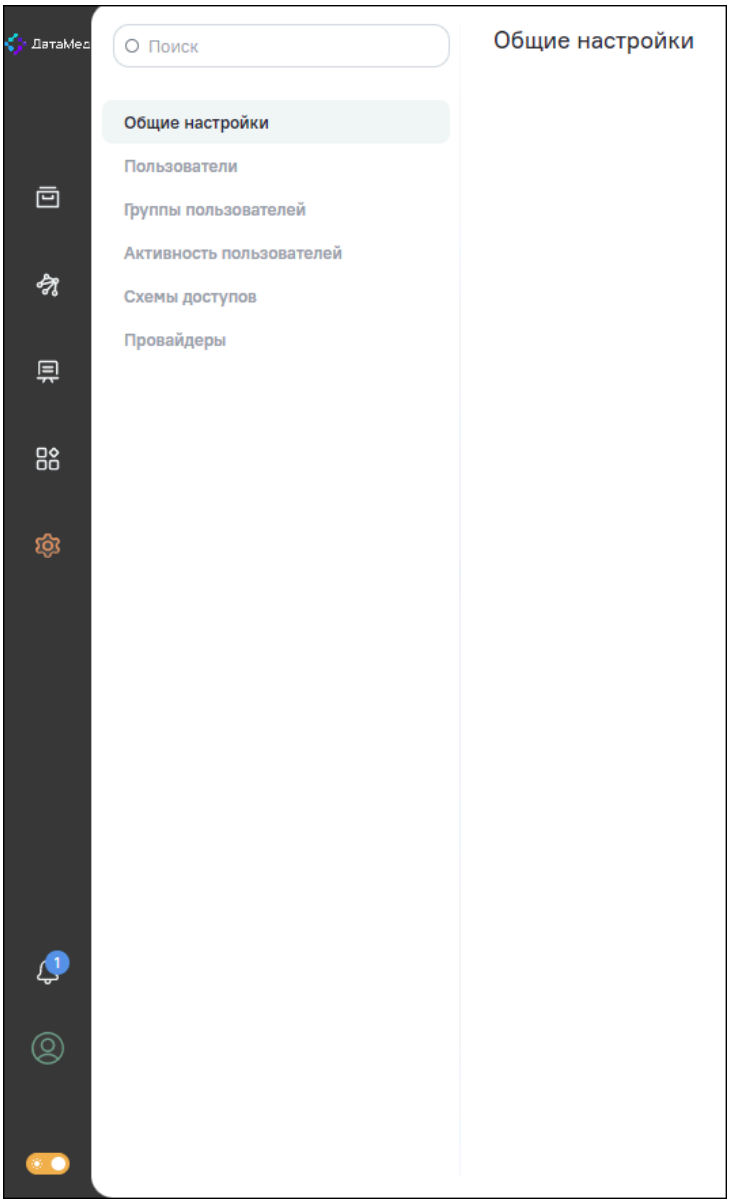


Рисунок 8 – Пользовательский интерфейс блока администрирования

5.2.1 Управление пользователями

Интерфейс управления пользователями (Рисунок 9) позволяет выполнять:

- создание пользователей Системы (кнопка «Добавить»);

- редактирование пользователей Системы;

- блокировку пользователей Системы.

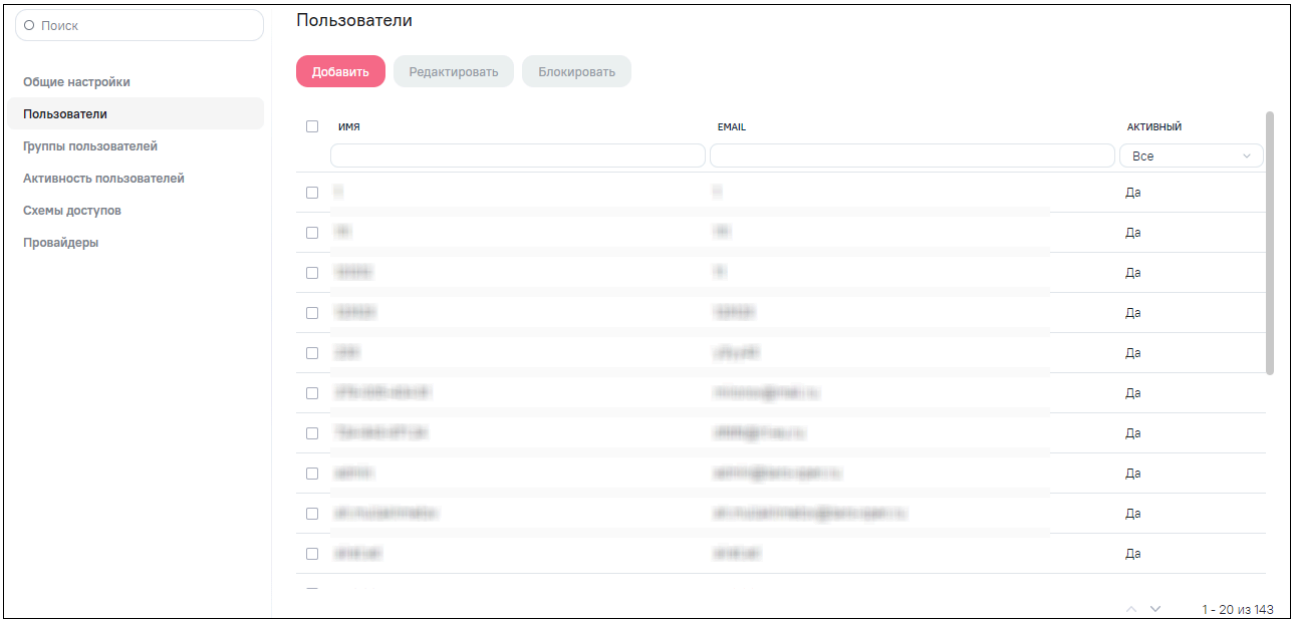


Рисунок 9 – Интерфейс управления пользователями

По всем столбцам реализована сортировка по возрастанию/убыванию. Нажмите на наименование необходимого столбца, список пользователей отсортируется по возрастанию. Повторно нажмите на наименование столбца, список пользователей отсортируется по убыванию. Нажмите на наименование столбца в третий раз, список пользователей отобразится без сортировки, и скроется кнопка сортировки.

5.2.1.1 Создание пользователей Системы

Окно создания нового пользователя приведено на рисунке (Рисунок 10). Для добавления пользователя укажите его:

- логин (целое слово без пробелов латинскими буквами);

- электронную почту;

- пароль (с подтверждением);

- установите «флажок» в поле «Активный». При создании нового пользователя «флажок» установлен автоматически.

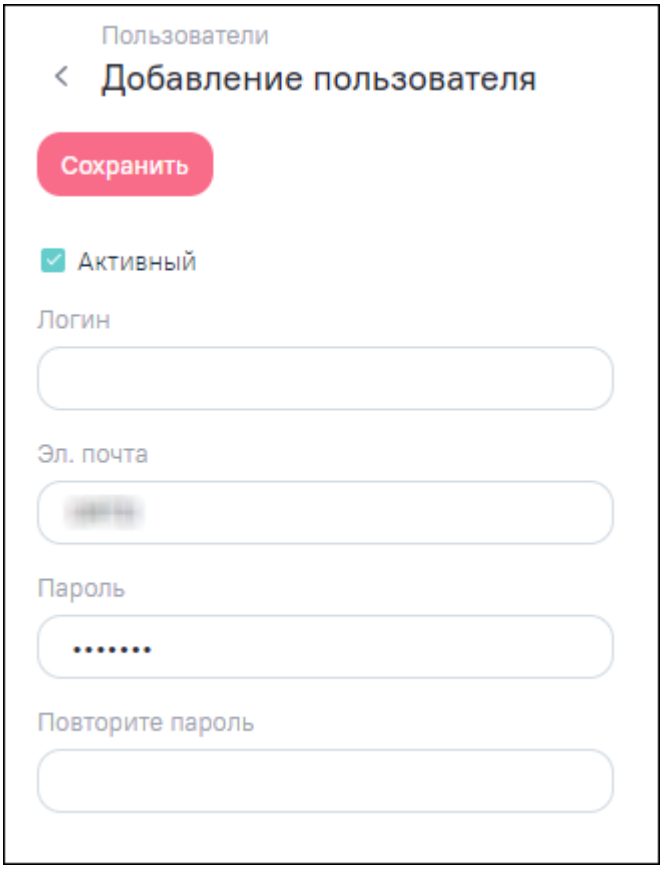
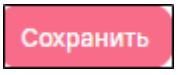
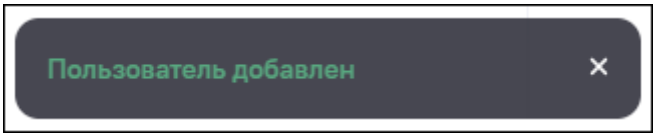


Рисунок 10 – Окно создания нового пользователя

Нажмите на кнопку «Сохранить» 

.

В случае успешного сохранения отобразится уведомление о внесенных изменениях 

.

Поле «Активный» позволяет временно отключить возможность входа в Систему для созданного пользователя, не удаляя его совсем (снимите «флажок» или нажмите на кнопку «Блокировать пользователя»).

5.2.1.2 Редактирование пользователей Системы

Операции изменения параметров и прав для существующего пользователя со стороны администратора Системы включают возможности:

- изменения:
  - логина;
  - адреса электронной почты;
  - пароля.
- блокировки или разблокировки пользователя (поле «Активный»);
- просмотра и управления его правами через принадлежность к группам пользователей (описано ниже в п. 5.2.1.2.1).

5.2.1.2.1 Добавление доступа пользователю к группам и объектам

Данные операции доступны как для созданного (нового) пользователя, так и для изменяемого существующего. Переход к ним выполняется через меню редактирования выбранного пользователя.

Для существующего (созданного) пользователя в интерфейсе редактирования отображаются вкладки «Группы» и «Объекты доступа».

5.2.1.2.1.1 Вкладка «Группы»

Вкладка содержит интерфейс просмотра и настройки групп, к которым отнесен данный пользователь, с целью передачи пользователю назначенных группе разрешений.

По умолчанию созданные пользователи включаются в те группы, которые указаны в качестве базовых групп в карточке соответствующего провайдера (см. п. 5.2.5).

Для включения пользователя в группы нажмите на кнопку «Добавить». В открывшемся окне поиска начните вводить название группы, которой предоставляются права (Рисунок 11). В выпадающем списке отобразятся группы согласно параметрам поиска. Необходимую группу выберите нажатием кнопки мыши или клавишами навигации и клавишей <Enter>.

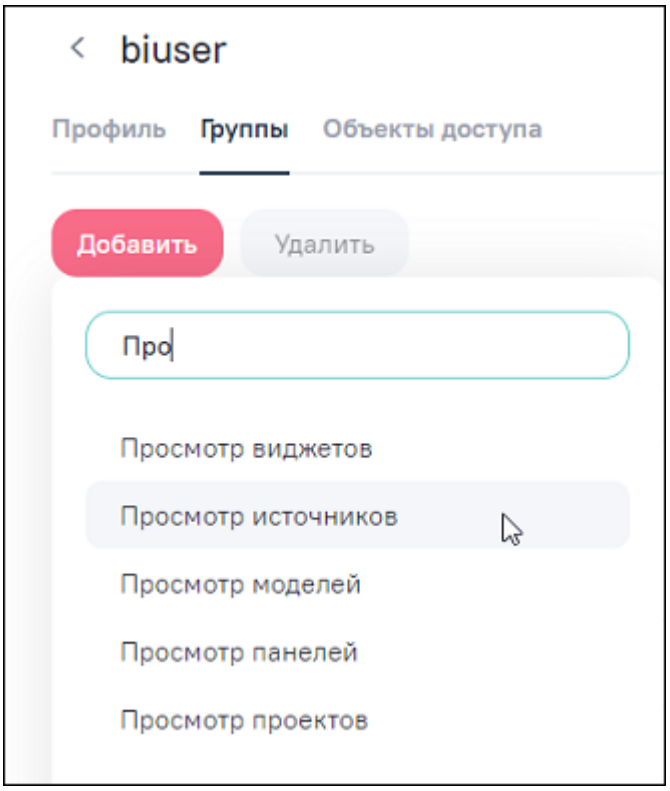


Рисунок 11 – Добавление пользователя в группы

Добавленная группа отображается в общем списке групп данного пользователя. Пользователь получает все назначенные группе разрешения. Для удаления пользователя из групп выберите их в данном списке (Рисунок 12) и нажмите на кнопку «Удалить».

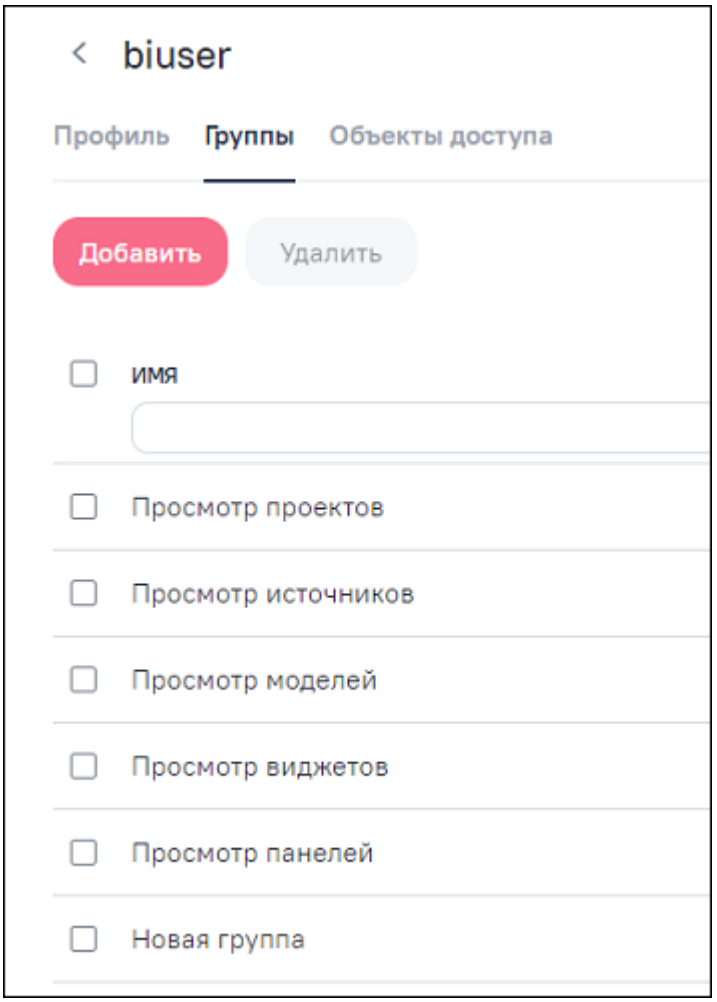


Рисунок 12 – Вкладка «Группы» – управление списком групп пользователя

5.2.1.2.1.2 Вкладка «Объекты доступа»

Пользователь получает права доступа к объектам Системы, если:

- они созданы им;
- права на них предоставлены ему другими пользователями – владельцами (создателями) объектов или имеющими права на их «Администрирование»;
- права на них предоставлены ему администратором Системы.

Предоставление данных прав доступа выполняется в контексте конкретного объекта и описано ниже в п. 5.3.

Вкладка «Объекты доступа» (Рисунок 13) содержит интерфейс только для просмотра списка фактически установленных данному пользователю прав доступа к объектам Системы. Данный список содержит поля:

- «Наименование» – наименование объекта, к которому предоставлен доступ;
- «Тип» – тип объекта Системы;
- «Дата создания» – дата и время создания объекта;
- «Дата изменения» – дата и время изменения объекта.

Для удобства поиска прав в списке он содержит возможности фильтрации выводимой информации по всем перечисленным выше полям.

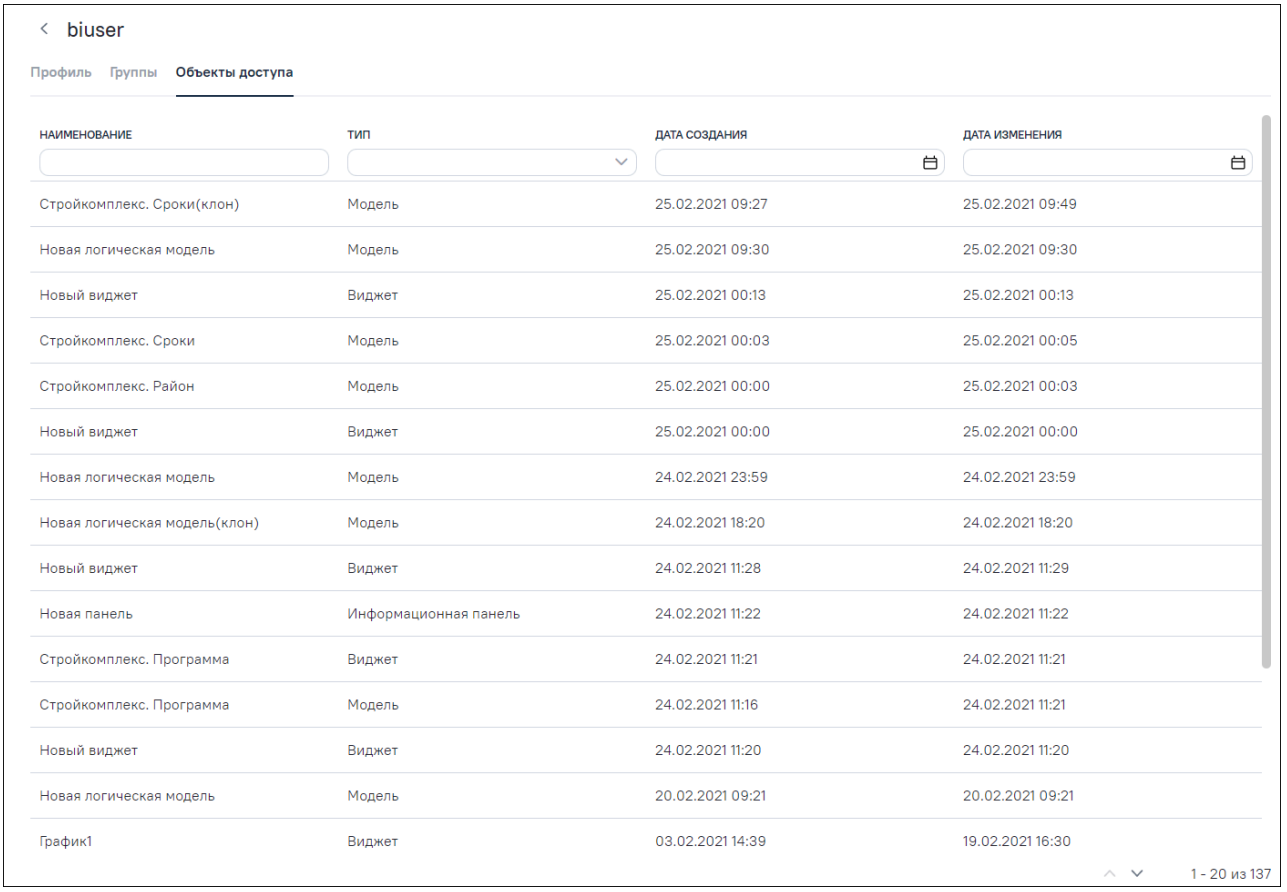


Рисунок 13 – Вкладка «Объекты доступа» – просмотр списка установленных пользователю прав доступа к объектам Системы

5.2.1.3 Блокировка пользователей Системы

Система не позволяет удалить пользователя. Пользователя можно только заблокировать (учетная запись пользователя станет неактивна).

Чтобы пользователь снова стал активен, в карточке пользователя установите «флажок» в поле «Активный».

Система позволяет блокировать ранее созданного (существующего) пользователя:

- в интерфейсе редактирования выбранной отдельной учетной записи пользователя (ссылка «Блокировать пользователя»);
- в интерфейсе просмотра списка пользователей, включая блокировку сразу нескольких – выберите пользователя (пользователей) и нажмите на кнопку «Блокировать».

Перед блокировкой откроется окно подтверждения действия (Рисунок 14).

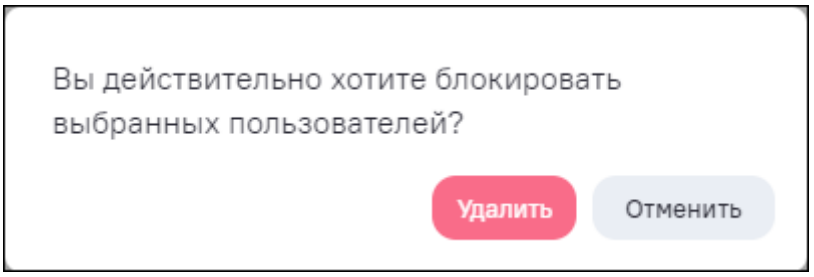


Рисунок 14 – Подтверждение операции блокировки пользователя

5.2.2 Управление группами пользователей

Группы пользователей предназначены для формирования, хранения и массового присвоения пользователям стандартных наборов разрешений. В Системе реализованы два вида групп пользователей: системные и пользовательские (Рисунок 15).

На обеих вкладках («Системные» и «Пользовательские») по всем столбцам реализована сортировка по возрастанию/убыванию. Нажмите на наименование необходимого столбца, список групп пользователей отсортируется по возрастанию. Повторно нажмите на наименование столбца, список групп пользователей отсортируется по убыванию. Нажмите на наименование столбца в третий раз, список групп пользователей отобразится без сортировки, и скроется кнопка сортировки.

Рисунок 15 – Интерфейс управления группами пользователей

5.2.2.1 Вкладка «Системные»

Системные группы – встроенные группы, которые невозможно удалить или добавить новую даже администратору. Системные обычно предназначены для выдачи пользователям комплекса разрешений, необходимых для работы в соответствующих функциональных блоках Системы. Встроенными группами являются (Рисунок 16):

- «Администратор» – предоставляет включенным в нее пользователям доступ к интерфейсу и функциям администрирования Системы;
- «Просмотр виджетов» – предоставляет включенным в нее пользователям доступ к интерфейсу и функциям работы с виджетами;
- «Просмотр источников» – предоставляет включенным в нее пользователям доступ к интерфейсу и функциям работы с источниками данных;
- «Просмотр личного кабинета» – предоставляет, включенным в нее пользователям, доступ к интерфейсу и функциям личного кабинета пользователя;
- «Просмотр моделей» – предоставляет включенным в нее пользователям доступ к интерфейсу и функциям работы с моделями;
- «Просмотр панелей» – предоставляет включенным в нее пользователям доступ к интерфейсу и функциям работы с информационными панелями;

– «Просмотр уведомлений» – предоставляет включенным в нее пользователям доступ к интерфейсу и функциям работы с центром уведомлений.

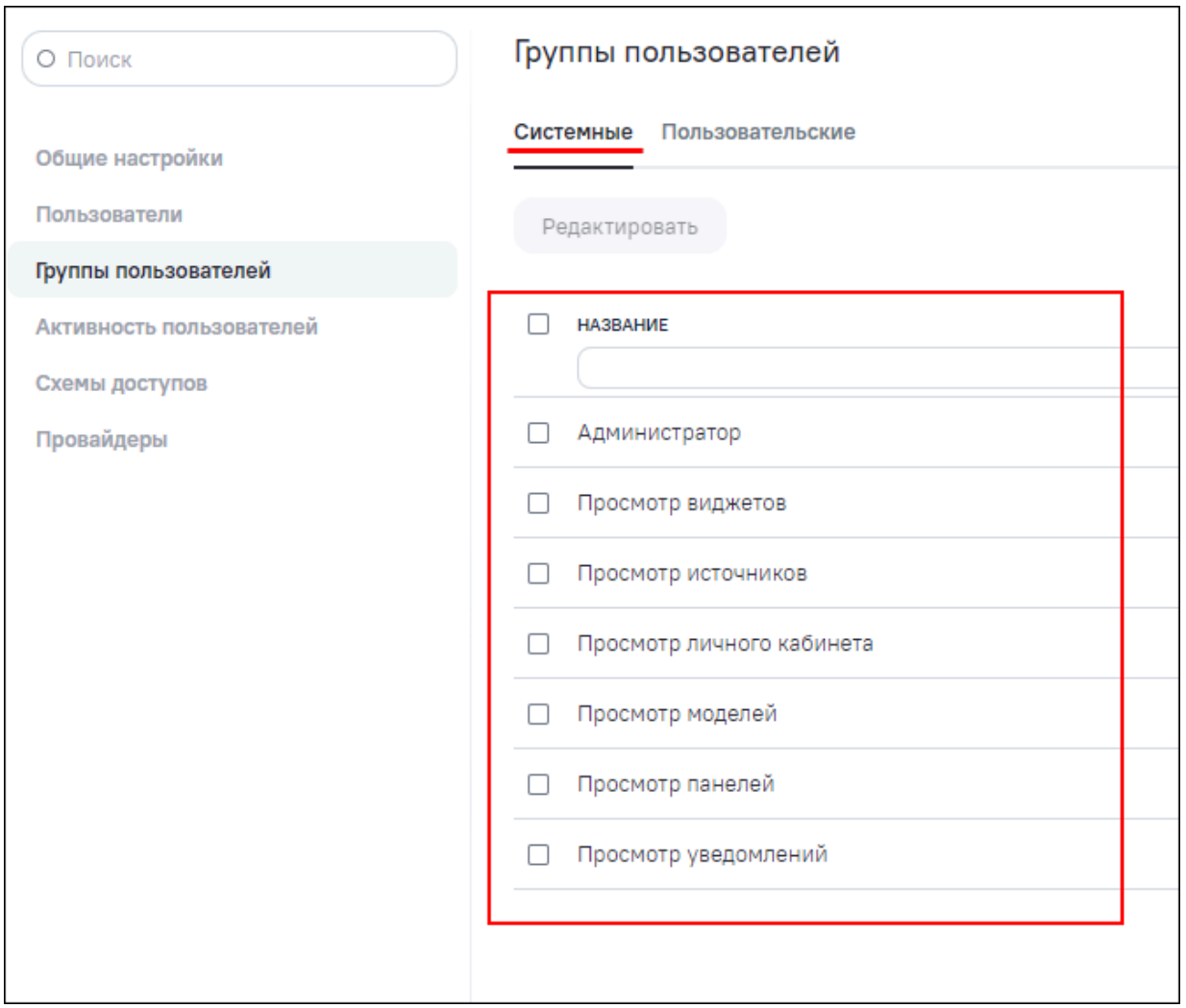


Рисунок 16 – Системные группы

Интерфейс управления системными группами пользователей позволяет выполнять редактирование системной группы в части изменения состава группы.

5.2.2.1.1 Редактирование системных групп пользователей

Для перехода к редактированию дважды нажмите левой кнопкой мыши на выбранной в списке группе или установите «флажок» напротив необходимой строки и нажмите на кнопку «Редактировать». Редактирование позволяет управлять составом группы.

Управление составом группы – добавление в группу пользователей либо их удаления из группы. Для включения пользователей в группу нажмите на кнопку «Добавить» и далее в окне поиска начните вводить логин пользователя, которого необходимо добавить. В выпадающем списке отобразятся подходящие логины (Рисунок 17). Необходимого пользователя выберите нажатием кнопки мыши или клавишами навигации и клавишей <Enter>.

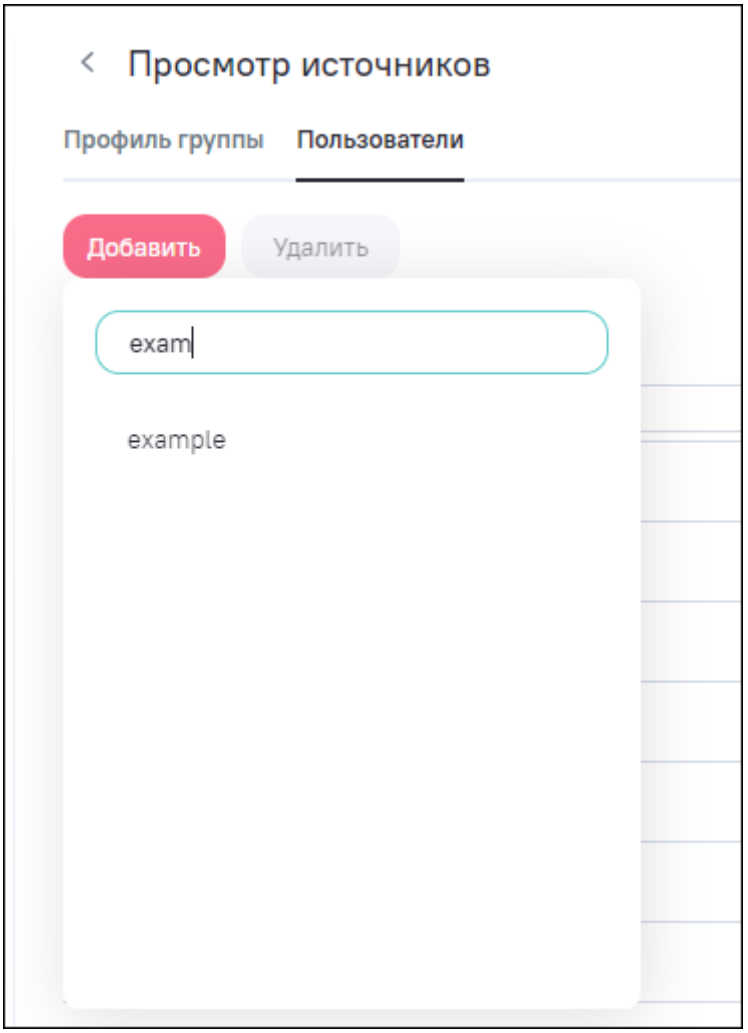


Рисунок 17 – Управление составом системных групп

5.2.2.2 Вкладка «Пользовательские»

Пользовательские группы – группы создаваемые, редактируемые и удаляемые администраторами, позволяющие создать и сохранить целевой набор разрешений на доступ к объектам Системы (конкретным источникам, моделям, виджетам и информационным панелям) и присвоить эти права нескольким пользователям (Рисунок 18).

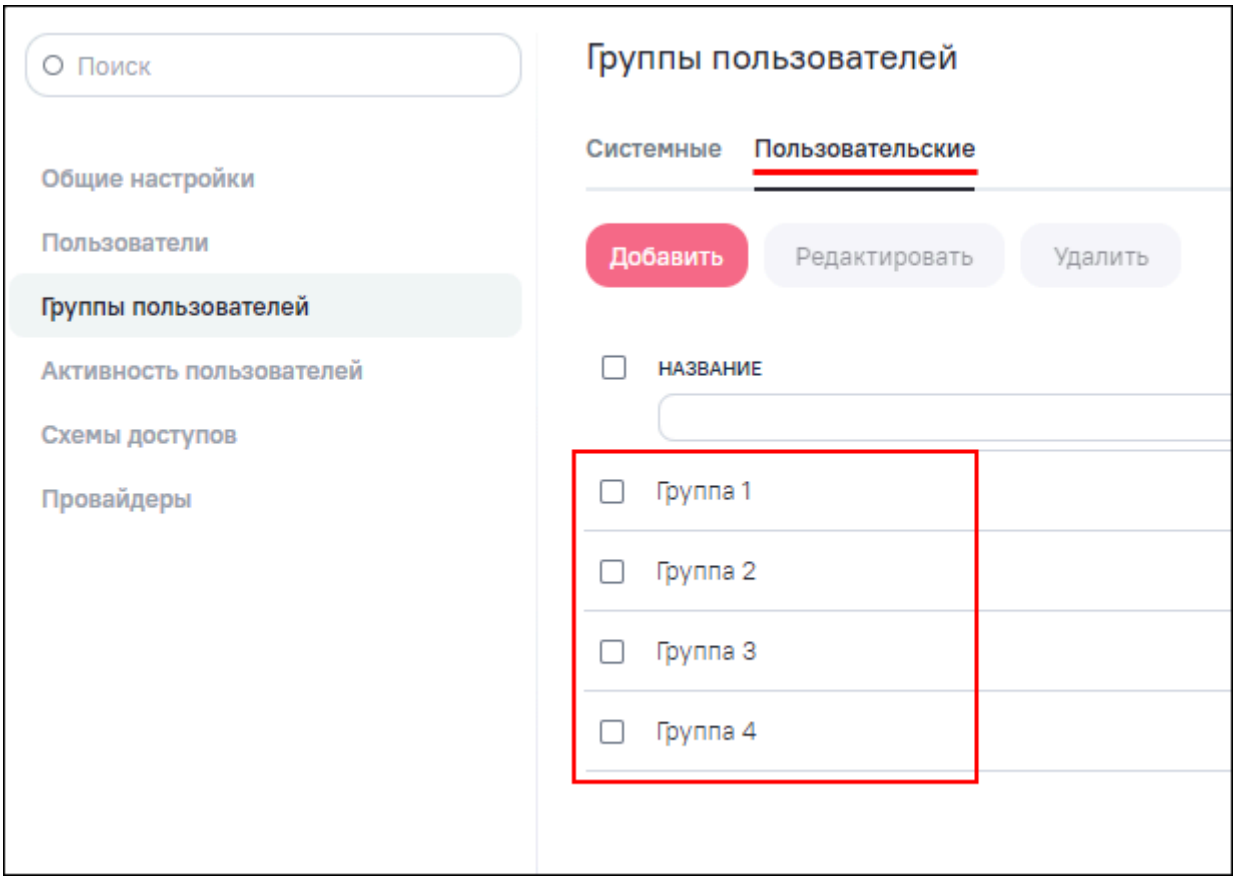


Рисунок 18 – Пользовательские группы

Интерфейс управления пользовательскими группами позволяет выполнять:

- создание групп пользователей Системы (кнопка «Добавить»);
- редактирование групп пользователей Системы;
- удаление групп пользователей Системы.

Ниже описаны операции создания, редактирования и удаления пользовательских групп (см. п. 5.2.2.2.1 – 5.2.2.2.3).

5.2.2.2.1 Создание пользовательских групп

Для добавления новой пользовательской группы заполните поля:

- «Код группы» – введите код группы (латинскими буквами, одним словом, без пробелов), который может быть использован при авторизации пользователя через внешний провайдер;

– «Наименование» – введите наименование группы.

Нажмите на кнопку «Сохранить» (Рисунок 19). Откроется интерфейс редактирования пользовательской группы (см. п. 5.2.2.2.2).

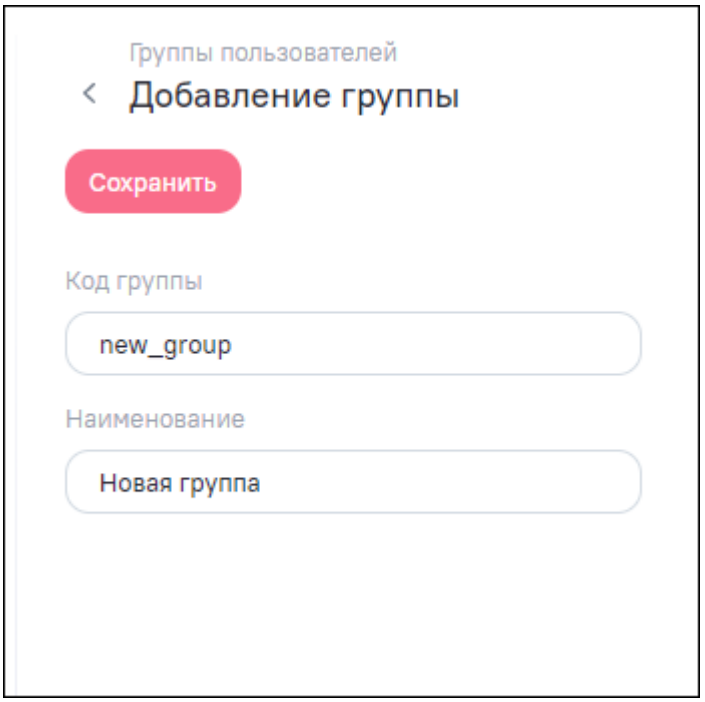


Рисунок 19 – Добавление новой пользовательской группы

5.2.2.2.2 Редактирование пользовательских групп

Чтобы отредактировать группу, дважды нажмите левой кнопкой мыши по группе в списке или установите «флажок» напротив необходимой строки. Нажмите на кнопку «Редактировать». Откроется окно редактирования пользовательской группы на вкладке «Профиль группы» (Рисунок 20).

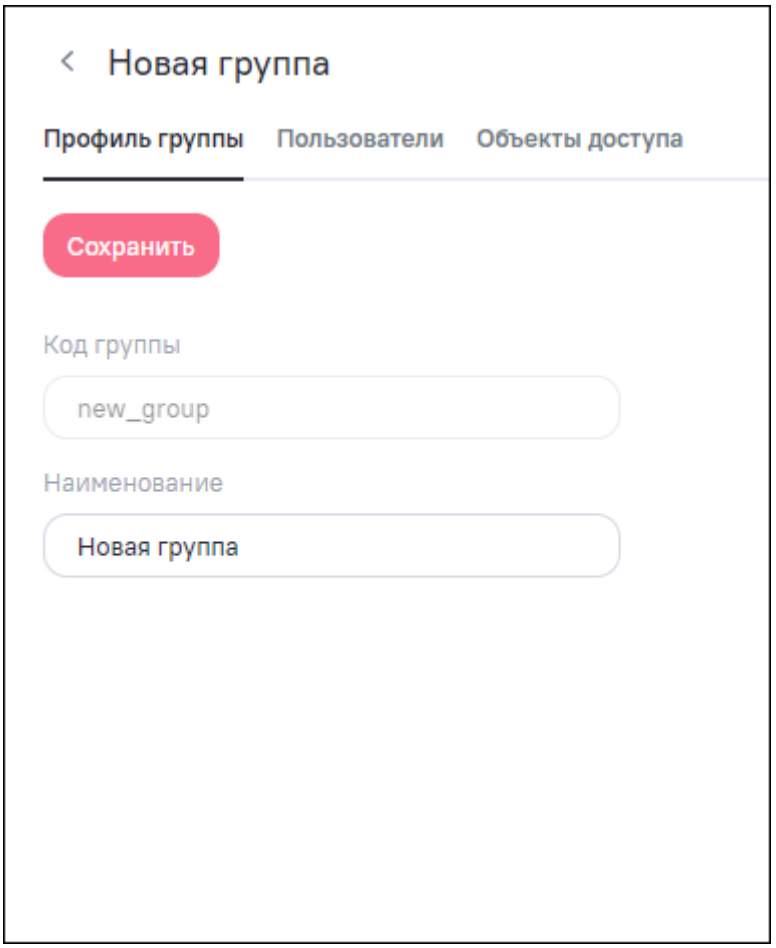


Рисунок 20 – Редактирование пользовательской группы

При редактировании группы можно изменить ее наименование (на вкладке «Профиль группы»), а также управлять составом группы (добавить или исключить пользователей на вкладке «Пользователи») или просматривать объекты доступа (на вкладке «Объекты доступа»).

5.2.2.2.2.1 Вкладка «Пользователи» в карточке редактирования пользовательской группы

Вкладка «Пользователи» предназначена для управления составом группы – добавления в группу пользователей либо их удаления из группы. Для включения пользователей в группу нажмите на кнопку «Добавить» и далее в окне поиска начните вводить логин пользователя, которого необходимо добавить (Рисунок 21). В выпадающем списке отобразятся логины согласно параметрам поиска. Выберите необходимого пользователя нажатием левой кнопки мыши или клавишами навигации и клавишей <Enter>.

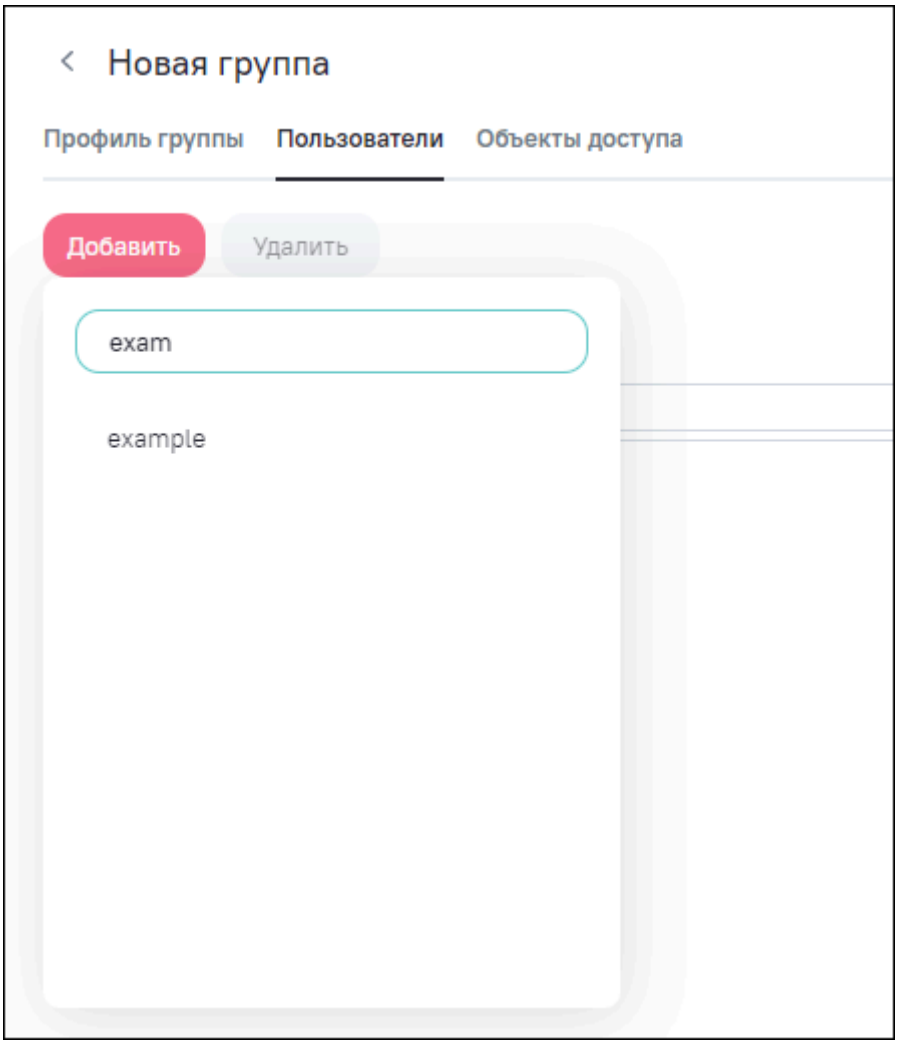


Рисунок 21 – Управление составом пользовательских групп

Предоставление данных прав доступа выполняется в контексте конкретного объекта и описано ниже.

5.2.2.2.2.2 Вкладка «Объекты доступа» в карточке редактирования пользовательской группы

Группа пользователей получает права доступа к объектам Системы, если:

- права ей предоставлены другими пользователями – владельцами (создателями) объектов или имеющими права на их «Администрирование»;
- права ей предоставлены администратором Системы.

Предоставление данных прав доступа выполняется в контексте конкретного объекта и описано ниже в п. 5.3.

Вкладка «Объекты доступа» содержит интерфейс только для просмотра списка фактически установленных данной группе прав доступа к объектам Системы (Рисунок 22). Данный список содержит поля:

- «Наименование» – наименование объекта, к которому предоставлен доступ;
- «Тип» – тип объекта Системы;
- «Дата создания» – дата и время создания объекта;
- «Дата изменения» – дата и время изменения объекта.

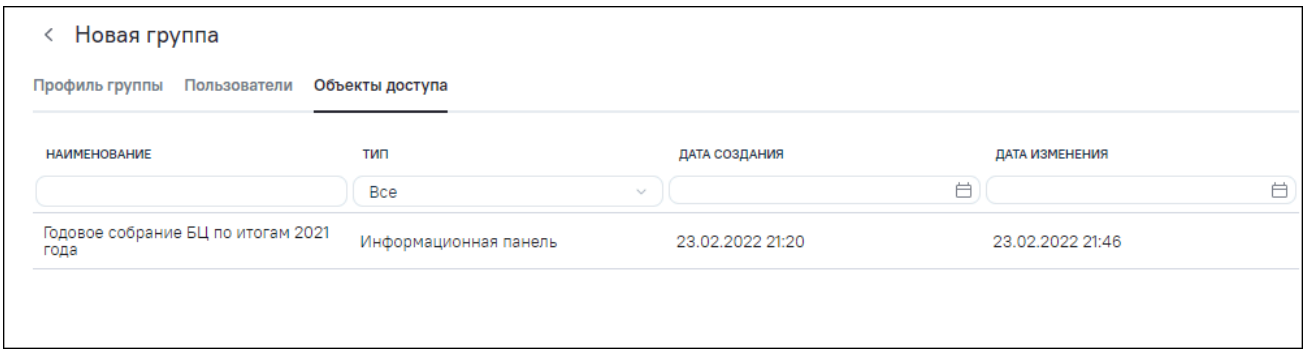


Рисунок 22 – Просмотр списка объектов доступа пользовательских групп

Для удобства поиска прав в списке есть возможность фильтрации выводимой информации по всем полям.

5.2.2.2.3 Удаление пользовательских групп

Система позволяет удалить ранее созданную (существующую) пользовательскую группу в интерфейсе просмотра списка групп пользователей. Для этого выберите нужную группу пользователей и нажмите на кнопку «Удалить». Аналогично можно выбрать и удалить сразу несколько пользовательских групп.

Перед удалением откроется окно подтверждения действия (Рисунок 23).

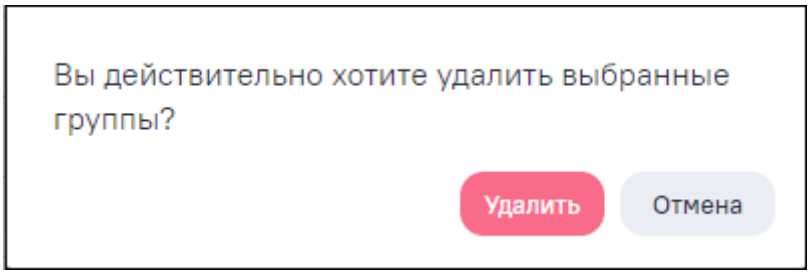


Рисунок 23 – Подтверждение операции удаления групп пользователей

5.2.3 Просмотр активности пользователей

Активность пользователей выводит информацию о пользовательских сессиях в виде таблицы со следующими полями (Рисунок 24):

- «Имя» – логин пользователя;
- «IP-адрес»;
- «Дата и время входа»;
- «Дата и время выхода»;
- «Время активности».

Рисунок 24 – Окно «Активность пользователей»

По столбцу «Имя» реализована сортировка по возрастанию/убыванию. Нажмите на наименование столбца, список записей отсортируется по возрастанию. Повторно нажмите на наименование столбца, список записей отсортируется по убыванию. Нажмите на наименование столбца в третий раз, список записей отобразится без сортировки, и скроется кнопка сортировки.

5.2.4 Управление схемами доступов

Схема доступов является дополнительным слоем между данными провайдеров и данными пользователей Системы. Упрощает настройку прав доступа к данным модели при добавлении нового провайдера.

Интерфейс управления схемой доступов (Рисунок 25) позволяет выполнять:

- создание атрибутов доступа;
- редактирование атрибутов доступа;
- удаление атрибутов доступа.

Схема доступов представляет собой список атрибутов доступа, которые передаются внешними провайдерами в Систему при авторизации пользователя или указываются в модели «user_permissions» при использовании внутреннего провайдера «Система» и которые используются для атрибутного доступа к данным модели (см. п. 5.4).

В Системе есть встроенные атрибуты доступа «login» (логин), «email» (E-mail) и «state» (статус), которые используются для внутреннего провайдера «Система». По ним сопоставляется учетная запись пользователя, и обновляются его данные. Встроенные атрибуты не подлежат редактированию и удалению.

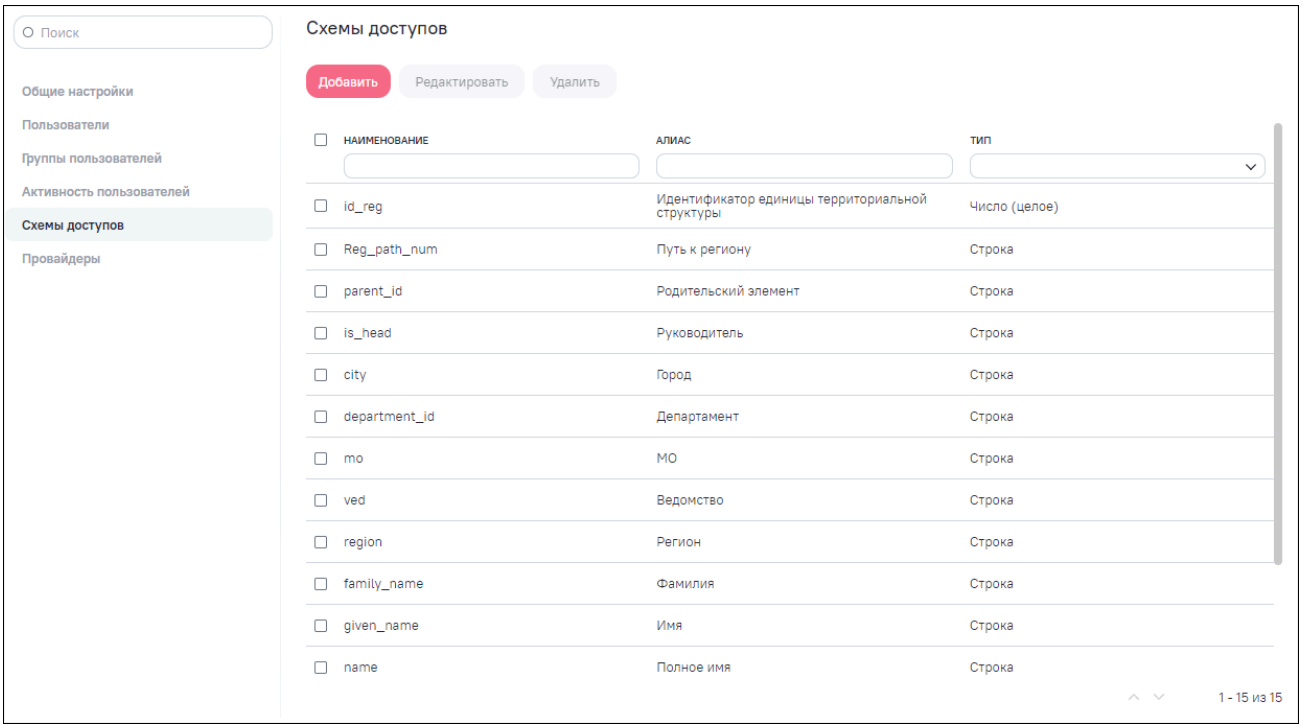


Рисунок 25 – Интерфейс управления схемами доступа

По всем столбцам реализована сортировка по возрастанию/убыванию. Нажмите на наименование необходимого столбца, список записей отсортируется по возрастанию. Повторно нажмите на наименование столбца, список записей отсортируется по убыванию. Нажмите на наименование столбца в третий раз, список записей отобразится без сортировки, и скроется кнопка сортировки.

5.2.4.1 Создание атрибутов доступа

Чтобы создать атрибут доступа, нажмите на кнопку «Добавить» в интерфейсе управления схемами доступа (см. Рисунок 25).

Откроется окно добавления нового атрибута доступа (Рисунок 26). Для добавления атрибута укажите следующие параметры:

- «Наименование» – целое слово без пробелов латинскими буквами, уникальное в рамках схемы;
- «Алиас»;
- «Тип».

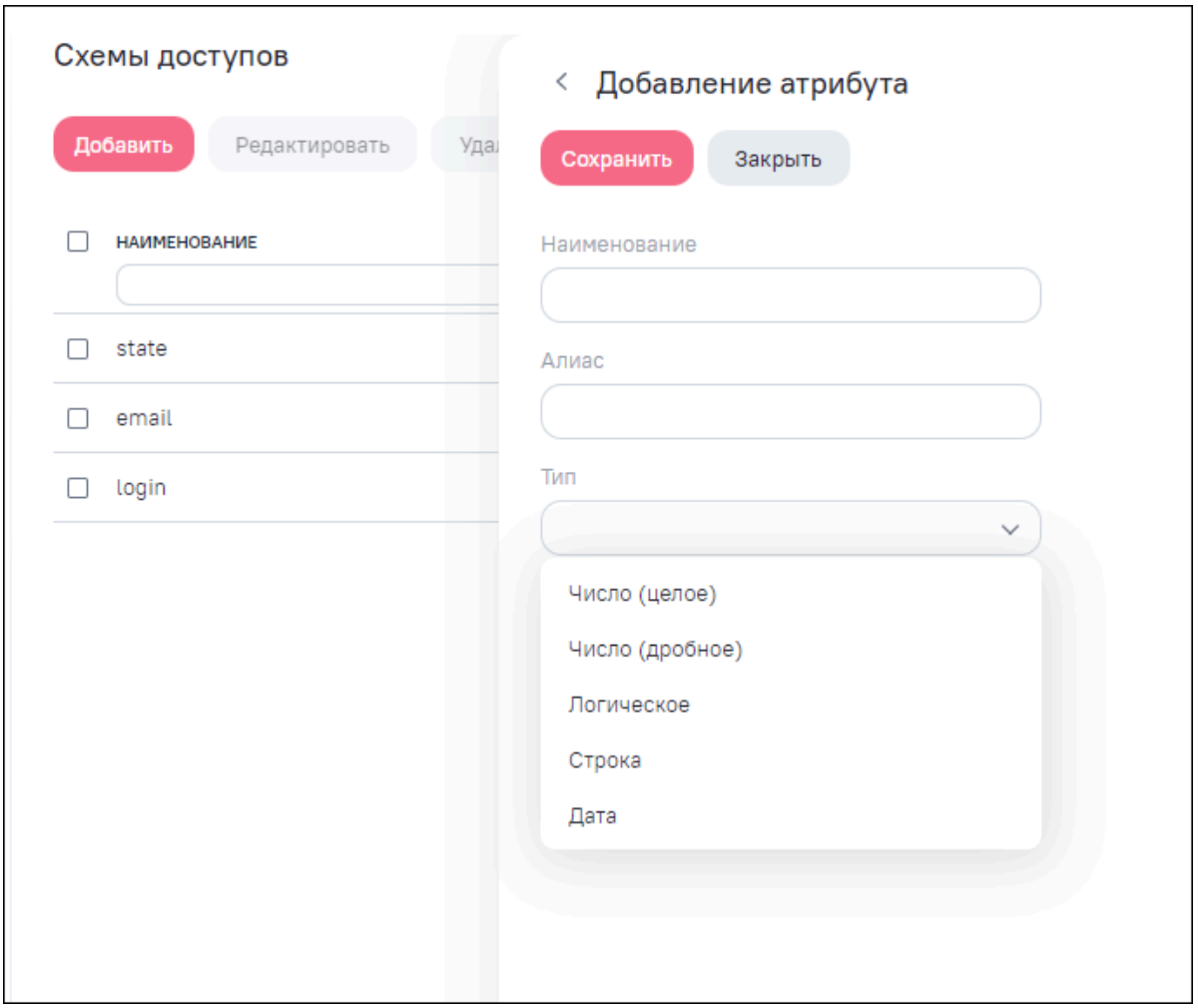


Рисунок 26 – Окно создания атрибута доступа

Нажмите на кнопку «Сохранить». В случае успешного сохранения отобразится уведомление о внесенных изменениях «Атрибут добавлен»

5.2.4.2 Редактирование атрибутов доступа

Чтобы отредактировать атрибут, дважды нажмите левой кнопкой мыши по записи в списке или установите «флажок» напротив необходимой строки и нажмите на кнопку «Редактировать» (Рисунок 27).

При редактировании атрибута можно изменить его наименование, алиас, а также тип данных.

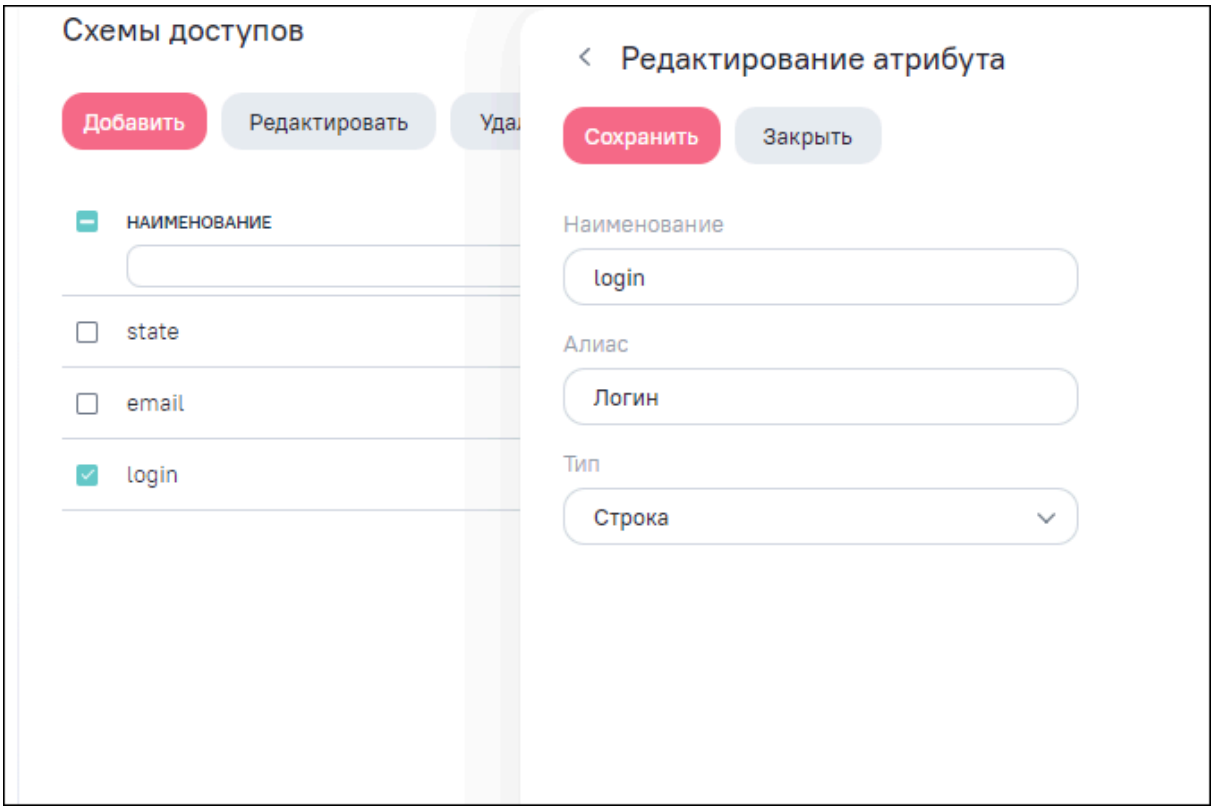


Рисунок 27 – Редактирование атрибута доступа

Примечание – Редактировать можно только те атрибуты, которые не задействованы ни в одном из провайдеров (см. п. 5.2.5.1.3).

5.2.4.3 Удаление атрибутов доступа

Ранее созданный атрибут можно удалить в интерфейсе просмотра списка атрибутов доступа. Для этого выберите нужный атрибут и нажмите на кнопку «Удалить». Чтобы удалить несколько атрибутов, установите напротив них «флажки» и нажмите на кнопку «Удалить».

Перед удалением атрибута (нескольких атрибутов) откроется окно подтверждения действия (Рисунок 28).

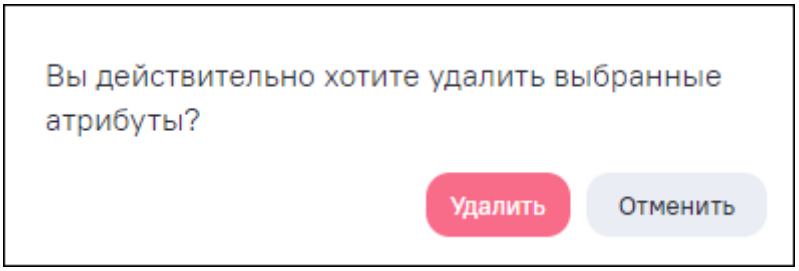


Рисунок 28 – Подтверждение операции удаления атрибутов доступа

Примечание – Удалить можно только те атрибуты, которые не задействованы ни в одном из провайдеров (см. п. 5.2.5.1.3).

5.2.5 Управление провайдерами

Раздел «Провайдеры» предназначен для настройки взаимодействия Системы с провайдерами пользователей. В Системе есть внутренний провайдер «Система» с типом «user_permissions», который используется по умолчанию. Также в Системе можно настроить авторизацию через внешний сервис аутентификации по протоколу Open ID Connect.

Примечание – Open ID Connect (OIDC) – это протокол аутентификации, который является расширением OAuth 2.0.

С помощью OpenID Connect пользователи могут проходить авторизацию и аутентификацию в нескольких облачных приложениях через единую точку с использованием одного логина и пароля.

Данный раздел представляет собой реестр всех настроенных провайдеров пользователей (Рисунок 29). В реестре отображается информация о провайдерах в полях:

- «Наименование»;
- «Тип»;
- «Активность».

По всем столбцам реализована сортировка по возрастанию/убыванию. Нажмите на наименование необходимого столбца, список провайдеров отсортируется по возрастанию. Повторно нажмите на наименование столбца, список провайдеров отсортируется по убыванию. Нажмите на наименование столбца в третий раз, список провайдеров отобразится без сортировки, и скроется кнопка сортировки.

Интерфейс управления провайдерами позволяет выполнять:

- создание провайдера;
- редактирование провайдера;
- удаление провайдера.

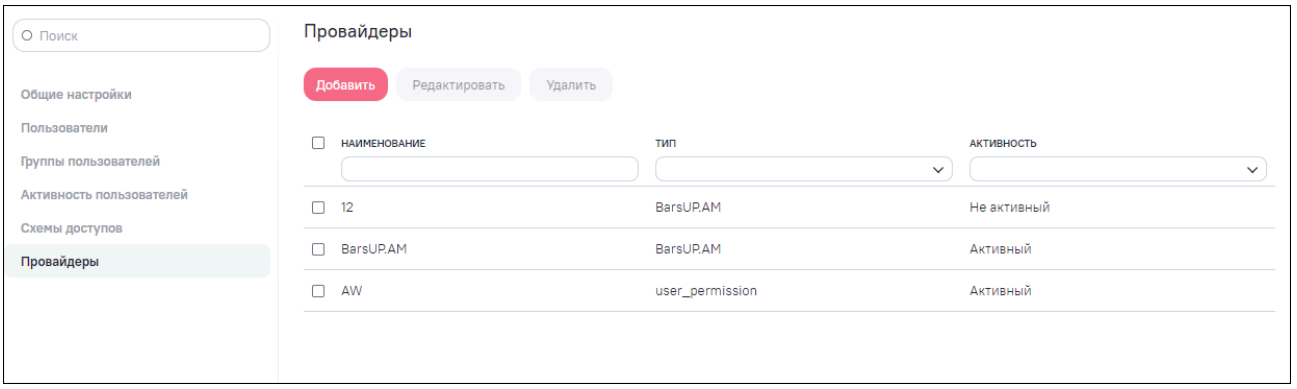


Рисунок 29 – Интерфейс управления провайдерами

Чтобы настроить взаимодействие, произведите настройку для обоих участников взаимодействия: провайдера (поставщика учетных записей) и Системы (поставщика сервиса). Для настройки взаимодействия Системы с провайдером выполните шаги, описанные в п. 5.2.5.1 – 5.2.5.2.

Примечание – Предполагается, что взаимодействие провайдера (поставщика учетных записей) с Системой настроено и учетные записи зарегистрированы.

5.2.5.1 Создание внешнего провайдера

Чтобы создать внешний провайдер, нажмите на кнопку «Добавить» в интерфейсе управления провайдерами.

Откроется окно создания и настроек провайдера (Рисунок 30), которое состоит из вкладок:

- «Основное»;
- «Параметры»;
- «Маппинг схемы».

Для ввода данных провайдера в Систему заполните обязательные поля на вкладках «Основное» и «Параметры» и нажмите на кнопку «Сохранить». В случае успешного сохранения отобразится уведомление о внесенных изменениях: «Провайдер сохранен».

5.2.5.1.1 Вкладка «Основное»

Вкладка «Основное» предназначена для ввода стартовой информации о провайдере (Рисунок 30). Заполните поля:

- «Активный» – установите «флажок» в поле, чтобы провайдер стал активным;
- «Наименование» – введите дружественное имя провайдера в Системе, поле обязательно для заполнения;
- «Тип» – выберите разновидность провайдера в зависимости от протокола взаимодействия из выпадающего списка. Поддерживается три типа: внутренний – «Система (user_permissions)» и внешние – «BarsUP.AM», «BarsUP.AM Token»;
- «Надпись кнопки сторонней аутентификации» – введите надпись кнопки, которая будет отображаться на странице авторизации Системы и выполнять переход на страницу авторизации провайдера;
- «Базовые группы» – выберите одно или несколько значений из выпадающего списка системных и пользовательских групп пользователей. Выбранные группы будут присваиваться пользователям автоматически при создании (для провайдеров типа «Система (user_permissions)» и «BarsUP.AM»/«BarsUP.AM Token») и при авторизации пользователя через SSO (для провайдера типа «BarsUP.AM»/«BarsUP.AM Token»);
- «Разрешить создание новых пользователей через внешнее управление» – установите «флажок» в параметр, при включении которого в Системе будет создаваться новый пользователь в случае его отсутствия. Если «флажок» не установлен, новый пользователь получит уведомление: «Для указанного в запросе пользователя не создана учетная запись. Необходимо обратиться к администратору Системы».

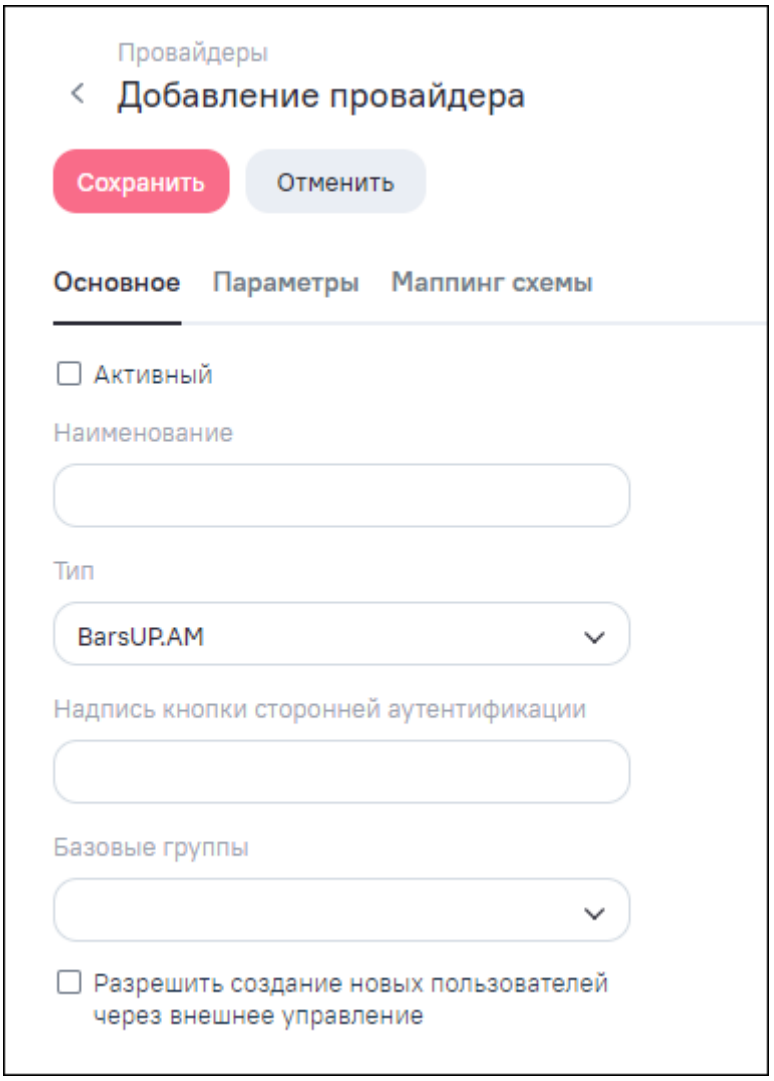


Рисунок 30 – Создание провайдера, в кладка «Основное»

Внешний провайдер с типом «BarsUP.AM Token» построен на базе провайдера с типом «BarsUP.AM». Отличительной чертой является то, что данный тип провайдера не отображается в окне авторизации Системы и для его настройки достаточно указать:

- на вкладке «Основное» – наименование и тип;
- на вкладке «Параметры» – идентификатор ИА и внешний URL.

Применяется данный тип провайдера для бесшовного перехода в Систему внутри стороннего приложения через единую точку входа и в случае работы с API Системы.

Примечание – В Систему невозможно добавить дополнительный провайдер с типом «Система (user_permissions)», так как внутренний провайдер должен быть Вкладка «Параметры»

Вкладка «Параметры» предназначена для ввода идентифицирующей информации о взаимодействии Системы и внешнего провайдера (Рисунок 31). Данную информацию передает администратор провайдера при регистрации заявки на подключение Системы к промышленному/тестовому контору ИА. Вкладка содержит поля, обязательные для заполнения:

- «Идентификатор ИА»;
- «Секретный ключ доступа»;
- «Внешний URL».

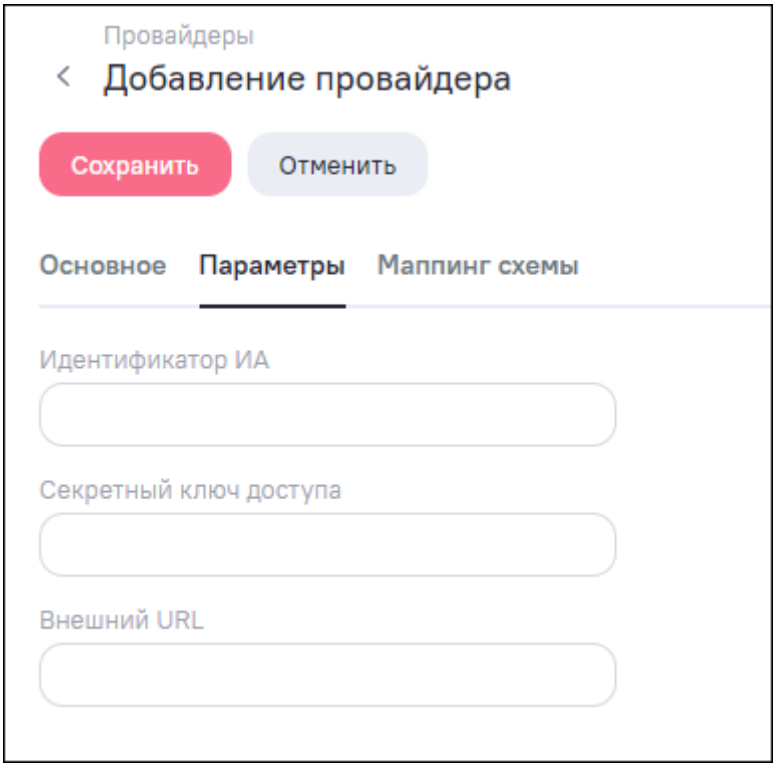


Рисунок 31 – Создание провайдера, вкладка «Параметры»

Примечание – Вкладка «Параметры» отсутствует в карточке провайдера с типом «Система (user_permissions)», так как это внутренний провайдер, который используется по умолчанию.

5.2.5.1.2 Вкладка «Маппинг схемы»

Вкладка «Маппинг схемы» содержит интерфейс для задания правил сопоставления атрибутов доступа схемы и атрибутов доступа провайдера пользователей (Рисунок 32). Вкладка содержит:

- параметр «Без соответствия» – при включении параметра отображаются атрибуты доступа схемы, которым не задано соответствие с атрибутами провайдера или атрибутами модели «user_permissions»;
- таблицу соответствия:
  - в первом столбце перечислены все атрибуты доступа схемы, объявленные в разделе Системы «Схемы доступов» (см. п. 5.2.4);
  - во втором столбце можно указать соответствующие атрибуты, передаваемые провайдером при взаимодействии или указанные в модели «user_permissions» при использовании внутреннего провайдера «Система ».

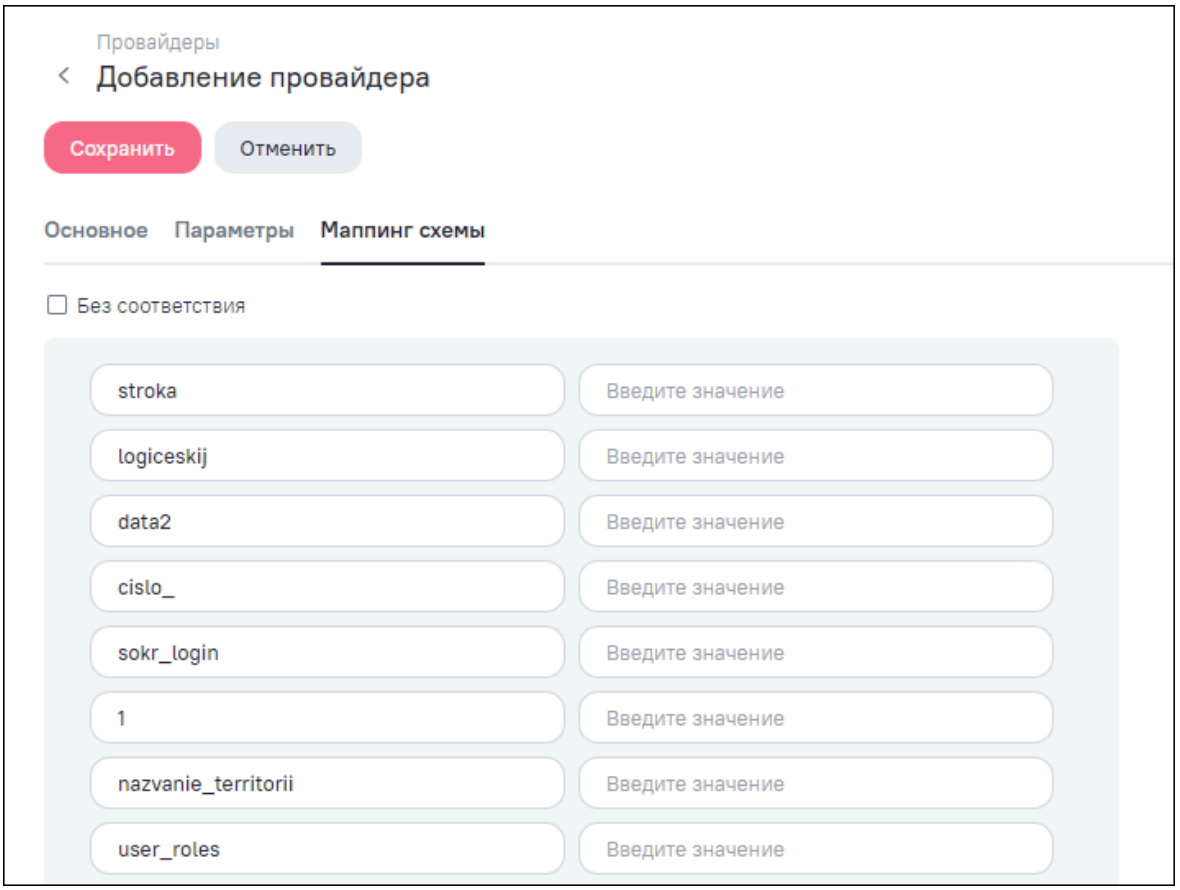


Рисунок 32 – Создание провайдера, вкладка «Маппинг схемы»

Примечание – Реализован «мягкий» маппинг данных внешних провайдеров. Если у пользователя есть атрибут, не указанный в схеме, значение сохраняется в списке дополнительных атрибутов. И наоборот, если при формировании критериев доступа на модель и у пользователя нет используемого атрибута, то его значение ищется в списке дополнительных атрибутов.

После заполнения правил соответствия атрибутов доступа схемы с атрибутами доступа провайдера и после сохранения данных провайдера, можно дополнительно задать соответствия к атрибутам пользователей в соответствующем атрибуте доступа.

Для этого на вкладке «Маппинг схемы» справа от атрибута доступа нажмите на кнопку [..]. Откроется окно «Маппинг атрибутов» для выбранного атрибута доступа.

Окно «Маппинг атрибутов» содержит интерфейс для задания правил сопоставления атрибутов пользователей внешнего провайдера и атрибутов пользователей, используемых в Системе (Рисунок 33).

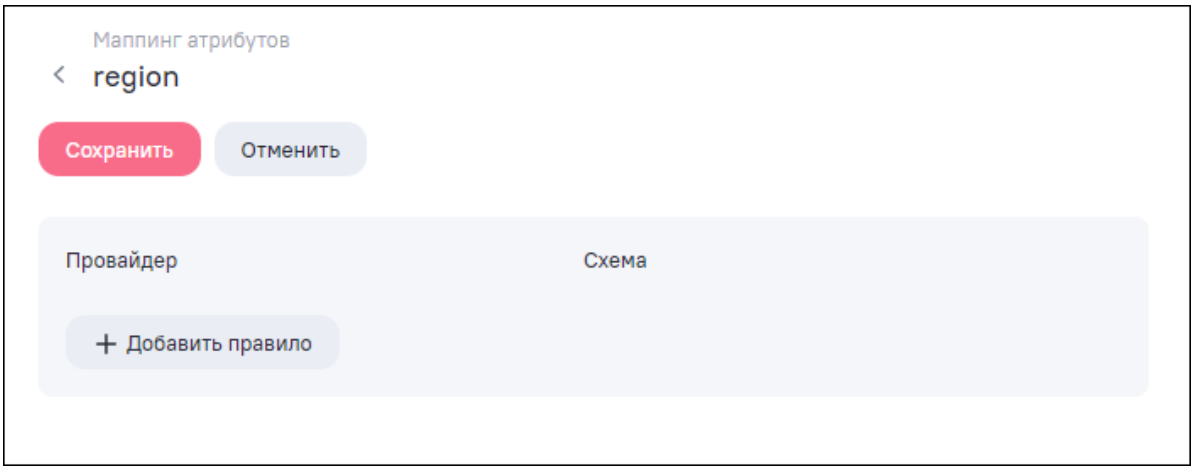


Рисунок 33 – Окно «Маппинг атрибутов»

На вкладке можно задать дополнительные правила сопоставления и группировки атрибутов. Правила сопоставления атрибутов пользователей применяются при входе пользователя в Систему через провайдер.

Для создания правила нажмите на кнопку «Добавить правило». Отобразятся поля для ввода параметров. В поле «Провайдер» введите название атрибута, передаваемого провайдером, а в поле «Схема» укажите значение, которое будет использоваться при настройке правил доступа в моделях (Рисунок 34). Создайте необходимое количество правил. Чтобы удалить правило, нажмите на кнопку  напротив необходимого правила.

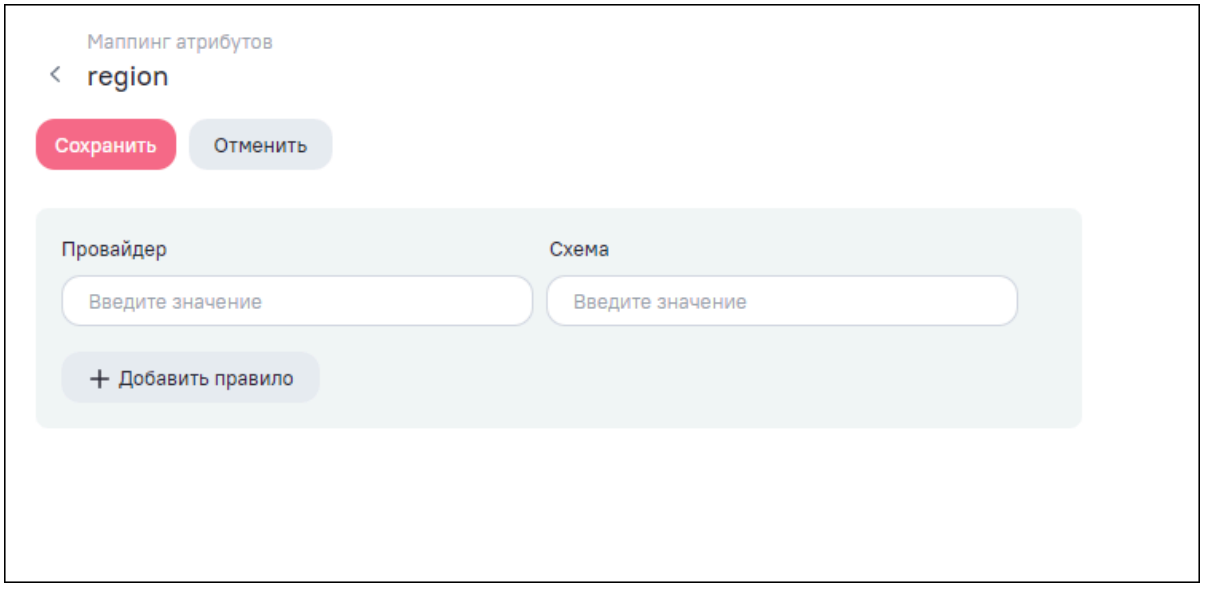


Рисунок 34 – Создание провайдера, добавление правила сопоставления

Атрибуты доступа, которые содержат маппинг атрибутов пользователей, отмечены пиктограммой  (Рисунок 35).

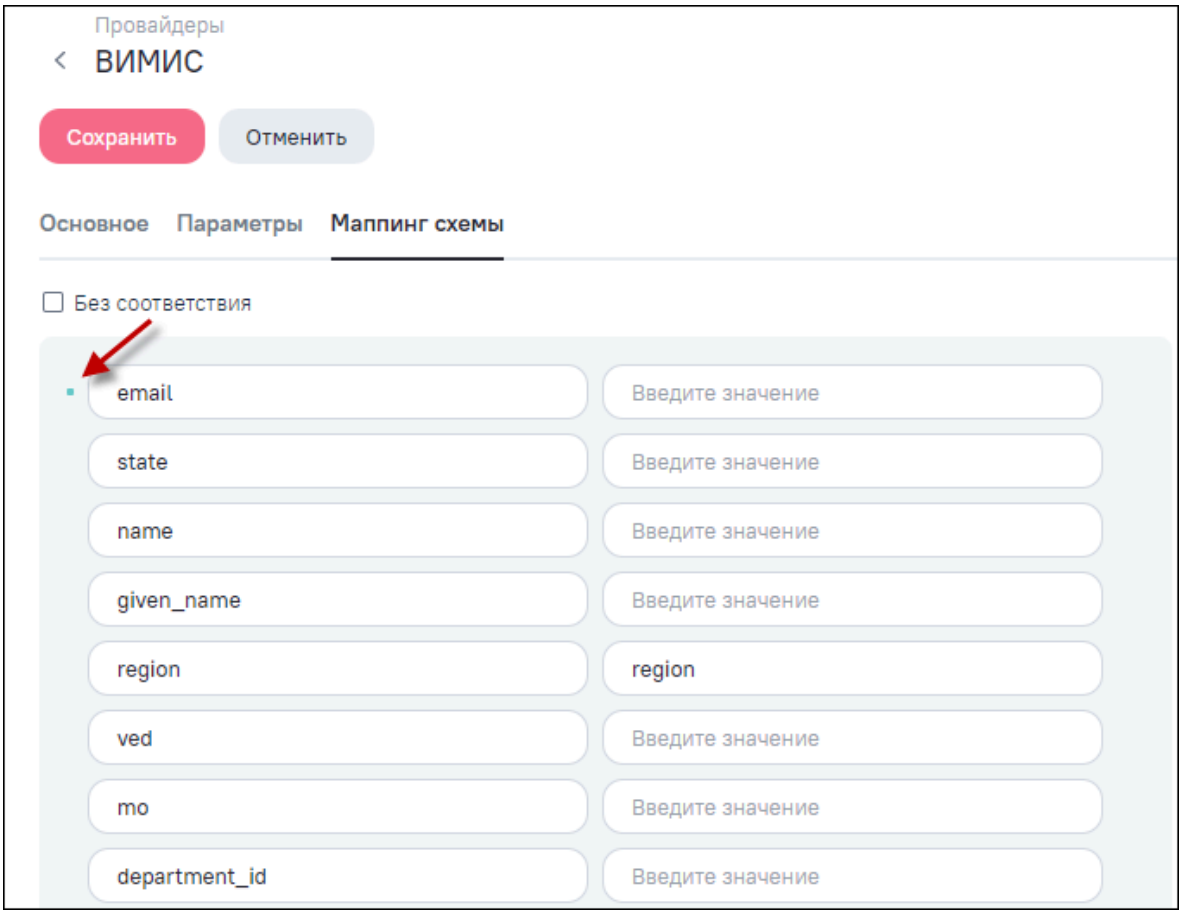


Рисунок 35 – Отображение атрибута, который содержит маппинг атрибутов пользователей

Примечание – Окно «Маппинг атрибутов» присутствует в карточке редактирования внутреннего провайдера «Система (user_permissions)», но, как правило, не используется при настройке атрибутного доступа.

5.2.5.2 Редактирование провайдера

Чтобы отредактировать провайдер, дважды нажмите левой кнопкой мыши по провайдеру в списке или установите «флажок» напротив строки провайдера и нажмите на кнопку «Редактировать».

Доступно изменение следующих параметров и настроек провайдера:

- на вкладке «Основное»:
  - активация и деактивация провайдера – для этого установите или снимите «флажок» в поле «Активный»;
  - изменение наименования в поле «Наименование»;

- изменение типа провайдера в поле «Тип»;
- изменение надписи кнопки сторонней аутентификации в поле «Надпись кнопки сторонней аутентификации»;
- выбор списка базовых групп в поле «Базовые группы»;
- установка или снятие разрешения на создание новых пользователей через внешнее управление – для этого установите или снимите «флажок» в поле «Разрешить создание новых пользователей через внешнее управление».

- настройка параметров подключения на вкладке «Параметры»;
- добавление соответствий атрибутов доступа схемы и атрибутов доступа провайдера на вкладке «Маппинг схемы»;
- управление соответствиями атрибутов пользователей провайдера с атрибутами пользователей, используемых в Системе, на вкладке «Маппинг схемы».

Окно редактирования внешнего провайдера аналогично окну добавления провайдера (см. п. 5.2.5.1).

Окно редактирования внутреннего провайдера – содержит вкладки «Основное», «Маппинг схемы».

Примеры настроек внутреннего и внешних провайдеров представлены в п. 5.4.4.

Для сохранения внесенных изменений убедитесь, что заполнены обязательные поля на вкладках «Основное» (для внешнего и внутреннего провайдера) и «Параметры» (для внешнего провайдера). Нажмите на кнопку «Сохранить». В случае успешного сохранения отобразится уведомление о внесенных изменениях – «Провайдер сохранен».

Примечание – Если внутренний провайдер «Система » будет деактивирован, то вход через страницу авторизации Системы (локальная аутентификация) будет доступен только под учетной записью «admin» (главный администратор Системы). Все остальные пользователи должны будут проходить авторизацию через внешний сервис аутентификации, с помощью ссылки «Войти через X», где «X» – наименование провайдера.

5.2.5.3 Удаление провайдера

Ранее созданный провайдер можно удалить:

- в интерфейсе редактирования выбранного провайдера – ссылка «Удалить» на вкладке «Основное»;
- в интерфейсе просмотра списка провайдеров – выберите нужный провайдер и нажмите на кнопку «Удалить». Аналогично можно выбрать и удалить сразу несколько провайдеров.

Перед удалением откроется окно подтверждения действия (Рисунок 36).

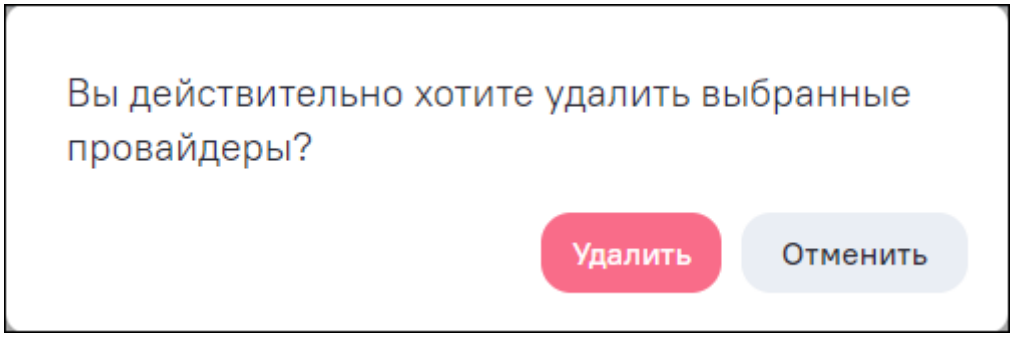


Рисунок 36 – Подтверждение операции удаления провайдеров

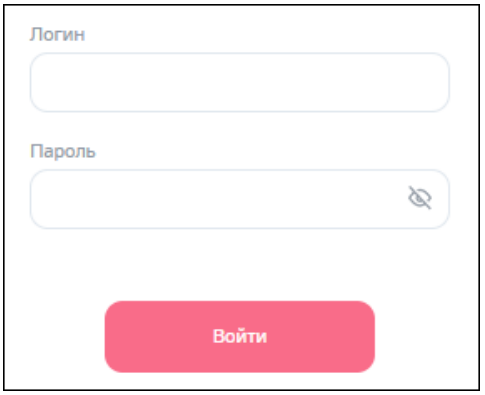
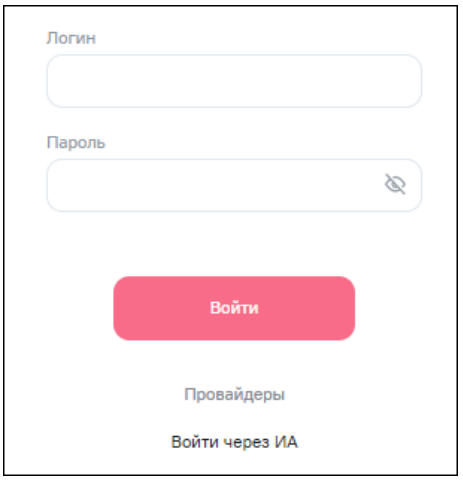
В Системе невозможно удалить активные провайдеры, а так же внутренний провайдер «Система» с типом «Система (user_permissions)», который используется по умолчанию, провайдер «Система» можно только деактивировать.

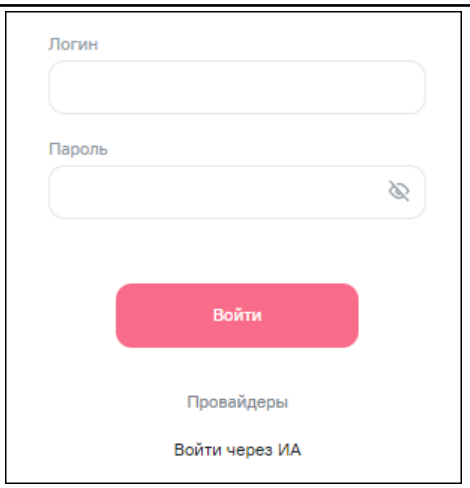
5.2.5.4 Сценарии работы Системы при настроенных провайдерах

5.2.5.4.1 Поведение страницы аутентификации при различных настройках Системы

Отображение страницы аутентификации Системы и сценарии аутентификации при различных настройках описаны ниже (Таблица 3).

Таблица 3 – Страница аутентификации при различных настройках Системы

Состояние внешнего провайдера с типом «BarsUP.AM»	**Состояние внешнего провайдера с типом «BarsUP.AM Token»**	**Состояние внутреннего провайдера «Система»**	**Отображение**
Не активный (или отсутствует)	Не активный (или отсутствует)/Активный	Активный	Пользователю на странице входа в приложение доступна кнопка локальной аутентификации. 
Активный	Не активный (или отсутствует)/Активный	Активный (локальная аутентификация разрешена)	Пользователю на странице входа в приложение доступны кнопки локальной аутентификации и входа через провайдер с типом «BarsUP.AM». При нажатии на кнопку провайдера происходит переадресация на его страницу аутентификации. 
Активный	Не активный (или отсутствует)/Активный	Не активный (локальная аутентификация запрещена)	Пользователю на странице входа в приложение доступны кнопки локальной аутентификации и входа через провайдер с типом «BarsUP.AM». При этом вход через кнопку локальной аутентификация доступен только под учетной записью «admin» (главный администратор Системы). При нажатии на кнопку провайдера происходит переадресация на его страницу аутентификации.

Состояние внешнего провайдера с типом «BarsUP.AM»	Состояние внешнего провайдера с типом «BarsUP.AM Token»	Состояние внутреннего провайдера «Система»	Отображение
			

5.2.5.4.2 Пользовательский сценарий авторизации через внешний провайдер BarsUP.AM по протоколу OpenID Connect

При авторизации через внешний провайдер BarsUP.AM по протоколу OpenID Connect:

1) администратор Системы подает заявку администратору провайдера на подключение Системы к тестовому/промышленному контуру провайдера, в которой указывает:

- протокол взаимодействия;
- необходимость запрашивать согласие у пользователя на передачу данных в Систему в процессе аутентификации;
- список атрибутов для передачи из провайдера;
- роли пользователя.

2) администратор провайдера создает роли для Системы;
3) необходимые учетные записи заводятся по соответствующим заявкам администраторами Системы и провайдера;

4) взаимодействие пользователей через провайдер может происходить по следующим сценариям:
   1) в сторонней системе пользователь нажимает на кнопку для открытия виджета или информационной панели Системы (Система получает REST-запрос от сторонней системы);
   2) пользователь сторонней системы переходит в соответствующий раздел для перехода и дальнейшей работы в Системе (Система получает REST-запрос от сторонней системы);
   3) пользователю сторонней системы предоставляется ссылка на открытие ресурса Системы (Система отправляет запрос на делегирование задачи аутентификации провайдеру);
   4) пользователь сторонней системы в web-браузере вводит адрес Системы и выполняет вход через провайдер (Система отправляет запрос на делегирование задачи аутентификации провайдеру);
5) сервисы для взаимодействия Системы с BarsUP.AM по протоколу OpenID Connect:

- сервис по делегированию задачи аутентификации провайдеру:
  - делегирование задачи аутентификации провайдеру;
  - получение identity token и access token от провайдера;
  - проверка наличия учетной записи пользователя в базе:
    - учетная запись есть – выполняется обновление ролей (групп) пользователя из полученного access token, предоставление доступа к ресурсам;
    - учетная запись отсутствует – выполняется проверка наличия разрешения на создание новых пользователей через внешнее управление:
      - если разрешения нет – выводится сообщение об отсутствии пользователя: «Для указанного в запросе пользователя не создана учетная запись. Необходимо обратиться к Администратору Системы»;

- если разрешение есть – создается новый пользователь с ролью (группами) из токена, добавляется информация по пользователю в атрибут auth_provider_data, предоставляется доступ к ресурсам с атрибутного ограничениями по модели.

- REST сервис по получению запроса на предоставление ресурсов другим сторонним системам:
  - Система получает REST-запрос от стороннего приложения;
  - из запроса извлекается access token;
  - выполняется проверка наличия учетной записи пользователя в базе:
    - учетная запись есть – выполняется проверка подписи, обновляется информация из токена по ролям (группам) пользователя, открывается запрашиваемый фрейм с ограничениями по модели user_permissions или по системным ролям (группам) пользователя;
    - если учетная запись отсутствует – выполняется проверка наличия разрешения на создание новых пользователей через внешнее управление:
      - если разрешения нет – выводится сообщение об отсутствии пользователя: «Для указанного в запросе пользователя не создана учетная запись. Необходимо обратиться к Администратору Системы»;
      - если разрешение есть – создается новый пользователь с ролью (группами) из токена, добавляется информация по пользователю в атрибут auth_provider_data, предоставляется доступ к ресурсам с атрибутными ограничениями по модели.

6) отработка сценариев взаимодействия при кросс-авторизации:

- для сценариев 1 и 2:

- сторонняя система отправляет в провайдер BarsUP.AM запрос на предоставление access token, который может быть использован для доступа к ресурсам Системы от имени пользователя;
- провайдер BarsUP.AM проводит аутентификацию пользователя, затем при необходимости высылает пользователю запрос на согласие в предоставлении доступа, после чего отправляет в стороннюю систему access token;
- провайдер BarsUP.AM перенаправляет пользователя на Систему с code, полученный код верифицируется с помощью REST-запроса на стороне провайдера, и в ответ Система получает access token;
- REST сервис в Системе обрабатывает запрос, извлекает access token. Выполняется проверка подписи и доступов:
  - при прохождении проверки – открывается запрашиваемый фрейм, исходя из роли (группы) пользователя и настройках доступа;
  - при возникновении ошибок – отображается сообщение об ошибке.

- для сценариев 3 и 4:
  - при обращении к адресу ресурса Системы выполняется перенаправление в провайдер BarsUP.AM для аутентификации и авторизации пользователя, если ранее пользователь не был авторизован;
  - Система извлекает identity token и access token. Выполняется проверка наличия пользователя, подписи и доступов:
    - при выполнении проверки – открывается запрашиваемый фрейм, исходя из роли (группы) пользователя и настройках доступа;
    - при возникновении ошибок – отображается сообщение об ошибке.

Примечание – В Системе для протокола OpenID Connect реализован режим работы (поток) – Authorization Code. Поток работает через редирект запроса аутентификации на BarsUP.AM (Authorization Endpoint). После успешной аутентификации пользователя с помощью BarsUP.AM создается код авторизации, и происходит редирект обратно в приложение. Затем приложение использует код авторизации вместе со своими учетными данными, чтобы получить токен доступа (Access Token), токен обновления (Refresh Token) и токен идентификатора (ID Token) из BarsUP.AM (Token Endpoint).Поток ориентирован на веб-приложения, включая мобильные приложения, где возможно использовать web-браузер. Подробнее описано в спецификации Authorization Code Flow по адресу **https://openid.net/specs/openid-connect-core-1_0.html#CodeFlowAuth**.

5.2.5.4.3 Пользовательский сценарий авторизации через внешний провайдер BarsUP.AM Token по протоколу OpenID Connect

Внешний провайдер с типом «BarsUP.AM Token» построен на базе провайдера с типом «BarsUP.AM». Отличительной чертой является то, что данный тип провайдера не отображается на форме авторизации Системы, и для его настройки достаточно указать на вкладке «Основное» – наименование и тип, на вкладке «Параметры» – идентификатор ИА и внешний URL. Применяется данный тип провайдера для бесшовного перехода в Систему внутри стороннего приложения через единую точку входа и в случае работы с API Системы.

При авторизации через внешний провайдер BarsUP.AM Token по протоколу OpenID Connect:

1) администратор Системы подает заявку администратору провайдера на подключение Системы к тестовому/промышленному контуру провайдера, в которой указывает:

- протокол взаимодействия;
- необходимость запрашивать согласие у пользователя на передачу данных в Систему в процессе аутентификации;
- список атрибутов для передачи из провайдера;
- коды ролей (коды групп) пользователей.

2) администратор провайдера создает роли для Системы;
3) необходимые учетные записи заводятся по соответствующим заявкам администраторами Системы и провайдера;
4) взаимодействие пользователей через провайдер может происходить по следующим сценариям:

- основной принцип взаимодействия пользователей:
  - пользователь авторизуется в стороннем приложении с помощью единой точки входа BarsUP.AM;
  - работает с разделами стороннего приложения;
  - нажимает на кнопки для перехода к Системе, после чего переходит в Систему, минуя форму авторизации (Система получает access_token от сторонней системы).
- сценарии, по которым осуществляется бесшовный переход из стороннего приложения в Систему:
  1) пользователь сторонней системы переходит в соответствующий раздел для дальнейшей работы с объектами Системы – при нажатии на кнопку открывается окно стороннего приложения (реестр/таблица) со списком доступных пользователю объектов из Системы и доступными операциями. При открытии объекта, например, на просмотр, открывается окно Системы на просмотр объекта, и все дальнейшие операции с объектом происходят в интерфейсе Системы;
  2) пользователь сторонней системы переходит в соответствующий раздел для перехода и дальнейшей работы в Системе – при нажатии на кнопку раздела открывается раздел Системы с доступными пользователю объектами и доступными операциями. Все дальнейшие операции происходят в интерфейсе Системы;
  3) пользователю сторонней системы предоставляется кнопка с ссылкой ресурса Системы – при нажатии на кнопку открывается окно Системы на

просмотр виджета или информационной панели по ссылке. Все дальнейшие операции с виджетом или панелью происходят в интерфейсе Системы;

4) в сторонней системе пользователь нажимает на кнопку для открытия объекта Системы – при нажатии на кнопку открывается окно Системы на просмотр или редактирование объекта. Все дальнейшие операции с объектом происходят в интерфейсе Системы.

5) отработка сценариев взаимодействия при кросс-авторизации:

- для сценария 1: 1 вариант – взаимодействие с API Системы:
  - сторонняя система отправляет в провайдер BarsUP.AM запрос на предоставление access tokena, который она может использовать для доступа к ресурсам Системы от имени пользователя;
  - провайдер BarsUP.AM проводит аутентификацию пользователя. Затем при необходимости отправляет пользователю запрос на согласие в предоставлении доступа. После чего отправляет в стороннюю систему access token;
  - сторонняя система делает POST запрос к api/auth-provider/verify-code (верификация кода авторизации) с обязательными параметрами: id – идентификатор провайдера в Системе, code – access_token, полученный от провайдера;
  - если все проверки на стороне Системы пройдены успешно, то в ответ сторонняя система получает token Системы. Дальше его используют для последующих запросов к API Системы.
- для сценариев 2, 3, 4: 2 вариант – фронтовое взаимодействие пользователей с Системой (через web-браузер):
  - сторонняя система отправляет в провайдер BarsUP.AM запрос на предоставление access tokena, который она может использовать для доступа к ресурсам Системы от имени пользователя;

- провайдер BarsUP.AM проводит аутентификацию пользователя. Затем при необходимости отправляет пользователю запрос на согласие в предоставлении доступа. После чего отправляет в стороннюю систему access token;
- сторонняя система отправляет запрос на frontend Системы /auth/verify-code/ с обязательными параметрами: id – идентификатор провайдера в Системе, code – access_token, полученный от провайдера, и дополнительными параметрами: sessionId – идентификатор сессии пользователя и redirectUrl – URL Системы, запрашиваемый пользователем;
- frontend Системы перехватывает запрос и обращается к backend Системы, backend обращается к провайдеру;
- если все проверки на стороне Системы пройдены успешно, то генерируется внутренний token Системы. Дальше frontend использует его для открытия запрашиваемого ресурса в redirectUrl (например, /app/widgets, при отсутствии адреса в redirectUrl пользователю откроется первый доступный раздел Системы).

5.2.5.4.4 Принципы создания новых пользователей и обновления их доступов к разделам Системы

Для внутреннего провайдера с типом «Система (user_permissions)»:

- при создании нового пользователя по умолчанию добавляются в карточку его учетной записи базовые группы, которые указаны в настройке провайдера с типом «Система (user_permission)»;
- все дополнительные доступы добавляются администратором Системы в карточке пользователя на вкладке «Группы» (см. п. 5.2.1.2.1.1).

Для внешних провайдеров с типами «BarsUP.AM», «BarsUP.AM Token»:

1) когда в Систему через кросс-авторизацию переходит пользователь без учетной записи, Система проверяет настройку провайдера:

- если нет «флажка» в поле «Разрешить создание новых пользователей через внешнее управление», то открывается сообщение об ошибке «Для указанного в запросе пользователя не создана учетная запись. Необходимо обратиться к Администратору Системы»;
- если установлен «флажок» в поле «Разрешить создание новых пользователей через внешнее управление», то в Системе создается новая учетная запись пользователя с определенными параметрами: логин, электронная почта, группы.

2) если установлен «флажок» в поле «Разрешить создание новых пользователей через внешнее управление», Система проверяет, какие коды ролей (групп) передал провайдер для Системы (блок endpoint с идентификатором Системы в ИА):

- если в блоке ролей имеются коды ролей, которые соответствуют кодам групп пользователей Системы (системным или пользовательским группам), то в карточку пользователя добавляются эти группы;
- далее проверяется настройка базовых групп: если в настройках провайдера указаны базовые группы пользователя, то в учетную запись пользователя добавляются базовые группы из настройки.

3) когда в Систему через кросс-авторизацию переходит пользователь с учетной записью в Системе, то:

- в учетной записи пользователя удаляются все настройки по доступным группам (даже те, которые были добавлены администратором Системы вручную);
- далее группы записываются снова по тому же принципу, что и при создании учетной записи.

5.3 Управление доступом к объектам

Пользователь Системы при наличии у него права на администрирование конкретного объекта может самостоятельно предоставить разрешения к нему другим

пользователям и группам. Такое право он по умолчанию получает на созданные им объекты.

5.3.1 Управление доступом к источникам данных

Предварительным условием получения пользователем доступа к конкретному источнику данных является наличие у него прав работы в блоке (интерфейсе) «Источники данных». Для получения этих прав пользователь должен быть включен администратором Системы во встроенную группу пользователей «Просмотр источников».

Доступ к источникам данных включает установку разрешений для пользователей и групп по следующим категориям:

- «Просмотр» – разрешение только на просмотр информации, получаемой из источника данных;
- «Редактирование» – разрешение на просмотр и изменение характеристик (настроек) соединения с источником данных;
- «Клонирование» – разрешение на создание нового источника данных копированием всех настроек текущего;
- «Удаление» – разрешение на удаление выбранного источника данных (удаление данного соединения в Системе – физически сам внешний источник данной настройкой не затрагивается);
- «Администрирование» – разрешение на управление доступом к источнику данных (операции, описываемые в данном разделе).

Настройка доступа выполняется в контексте каждого источника данных через интерфейс «Настройки». Чтобы открыть интерфейс настройки, нажмите на кнопку  в режиме редактирования выбранного источника данных. Права могут предоставляться как отдельным пользователям, так и группам пользователей.

5.3.1.1 Управление доступом отдельных пользователей

Для предоставления прав отдельным пользователям выберите пункт «Пользователи» и далее в окне поиска начните вводить логин пользователя, которому

предоставляются права. В выпадающем списке отобразятся подходящие логины. Необходимый логин выберите нажатием левой кнопки мыши или клавишами навигации и клавишей <Enter> (Рисунок 37).

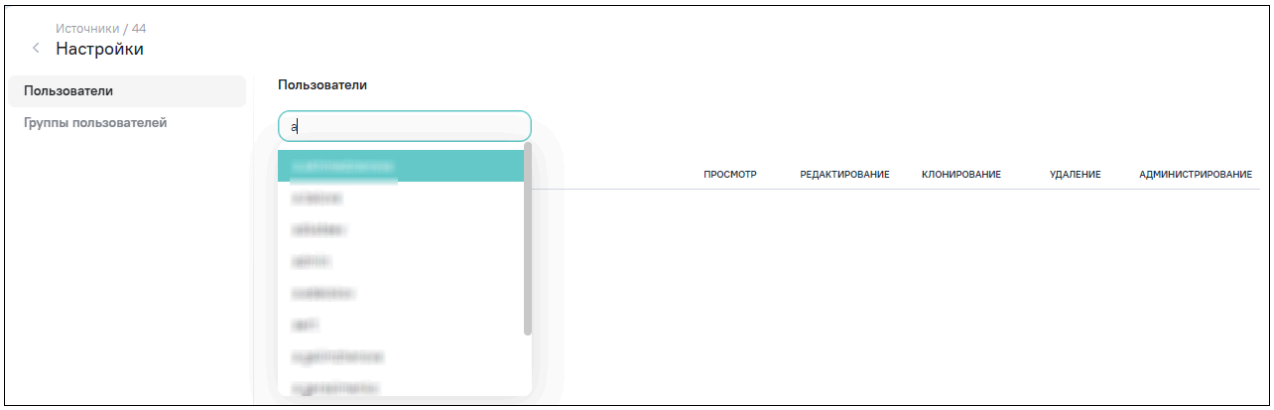


Рисунок 37 – Добавление доступа пользователю к источнику данных

Добавленному пользователю сразу предоставляется право «Просмотр» (Рисунок 38). Чтобы добавить дополнительные права, установите «флажки» в поля необходимых прав. Для установки пользователю всех прав установите «флажок» в поле «Выбрать все».

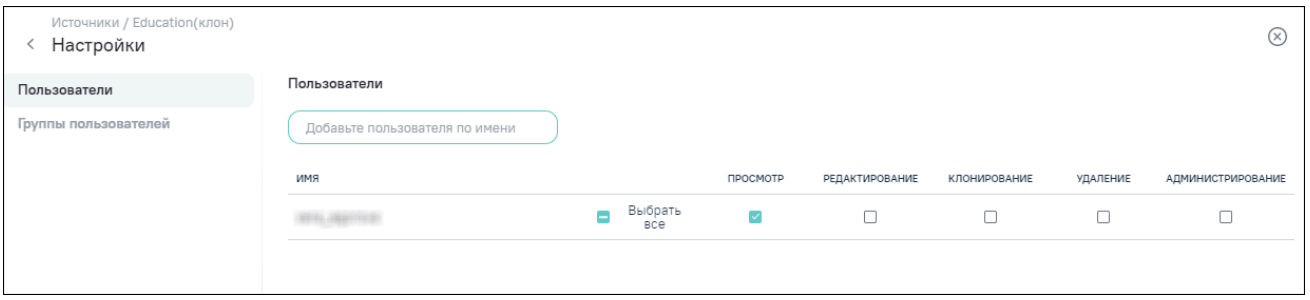


Рисунок 38 – Доступ пользователя к источнику данных на просмотр

Чтобы удалить пользователя из данного списка (отменить доступ), уберите все разрешения (включая просмотр). При следующем входе в данный интерфейс такого пользователя в списке разрешений не будет.

Если в Системе для пользователей с триальным доступом установлено ограничение «Запрет на предоставление прав к объекту отдельным пользователям», то для таких пользователей при попытке предоставить доступ к источникам данных вместо списка пользователей отобразится предупреждение «Недоступно в демо-версии», а при нажатии на текст предупреждения откроется уведомление: «В демо-версии нельзя делиться объектами».

5.3.1.2 Управление доступом групп пользователей

Для предоставления прав группам пользователей выберите пункт «Группы пользователей» и далее в окне поиска начните вводить название группы, которой предоставляются права. В выпадающем списке отобразятся подходящие группы пользователей. Необходимую группу выберите нажатием левой кнопки мыши или клавишами навигации и клавишей <Enter> (Рисунок 39).

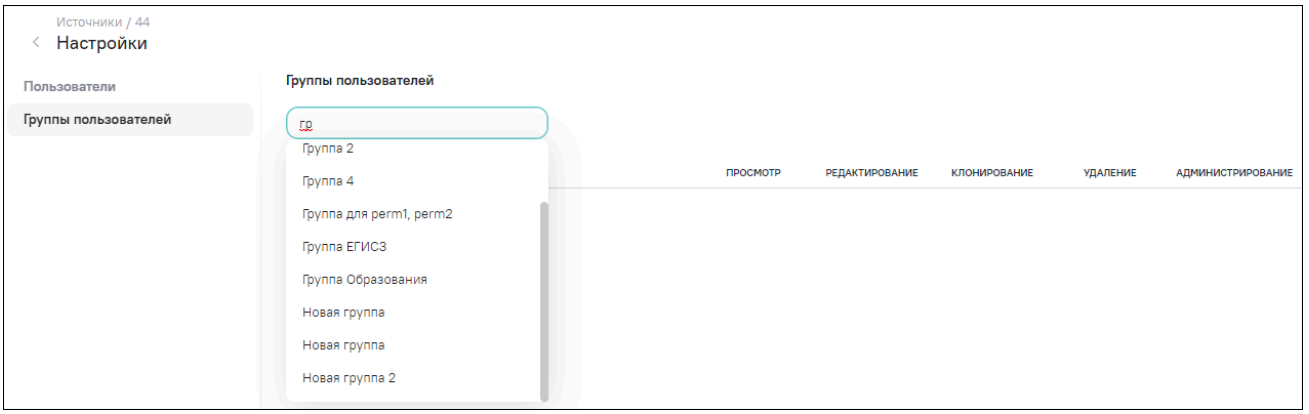


Рисунок 39 – Добавление доступа группе пользователей к источнику данных

Добавленной группе пользователей сразу предоставляется право «Просмотр» (Рисунок 40). Чтобы добавить дополнительные права, установите «флажки» в поля необходимых прав. Для установки группе пользователей всех прав установите «флажок» в поле «Выбрать все».

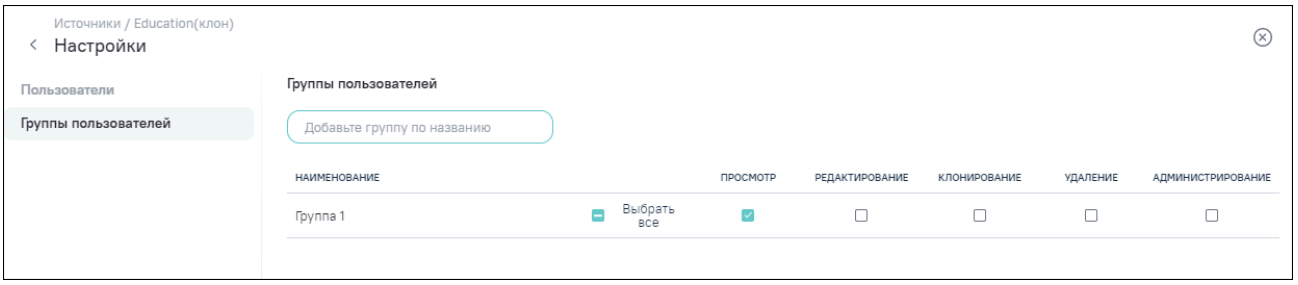


Рисунок 40 – Доступ группы пользователей к источнику данных на просмотр

Чтобы удалить группу пользователей из данного списка (отменить доступ), уберите все разрешения (включая просмотр). При следующем входе в данный интерфейс такой группы пользователей в списке разрешений не будет.

5.3.2 Управление доступом к моделям и настройки планировщика

Предварительным условием получения пользователем доступа к конкретной модели является наличие у него прав работы в блоке (интерфейсе) «Модели». Для получения этих прав пользователь должен быть включен администратором Системы во встроенную группу пользователей «Просмотр моделей».

Доступ к моделям включает установку разрешений для пользователей и групп по следующим категориям:

- «Просмотр» – разрешение только на просмотр модели и итоговых данных;
- «Редактирование» – разрешение на доступ к форме и операциям редактирования модели;
- «Клонирование» – разрешение на создание новой модели копированием всех настроек текущей;
- «Удаление» – разрешение на удаление данной модели из Системы;
- «Изменение источника» – разрешение на изменение источников данных;
- «Изменение схемы» – разрешение на изменение топологии соединений данных источников и работу в интерфейсе редактирования схемы;
- «Изменение инкрементальных настроек» – разрешение на изменение настроек инкрементальной загрузки;
- «Загрузка данных» – разрешение на запуск процесса обновления включенных в модель данных из используемых источников;
- «Изменение настроек синхронизации» – разрешение на доступ и изменение расписания планировщика обновления данных (операция, описываемая в данном разделе);
- «Управление полями модели» – разрешение на создание и изменение в составе итоговых данных модели полей, вычисляемых полей и иерархий;

– «Администрирование» – разрешение на управление доступом к модели (операции, описываемые в данном разделе).

Настройка доступа выполняется в контексте каждой конкретной модели данных через интерфейс «Настройки». Чтобы перейти к интерфейсу «Настройки», нажмите на кнопку  в режиме редактирования выбранной модели. Права доступа могут предоставляться как отдельным пользователям, так и группам пользователей. В этом же интерфейсе выполняется настройка «Правил доступа» (атрибутного доступа к данным модели) и настройка «Планировщика» (установка и изменение расписания обновления данных модели из источников данных).

5.3.2.1 Управление доступом отдельных пользователей

Для предоставления прав отдельным пользователям выберите пункт «Пользователи» и далее в окне поиска начните вводить логин пользователя, которому предоставляются права. В выпадающем списке отобразятся подходящие логины. Необходимый логин выберите нажатием левой кнопки мыши или клавишами на клавиатуре и клавишей <Enter> (Рисунок 41).

Рисунок 41 – Добавление доступа пользователю к модели

Добавленному пользователю сразу предоставляется право «Просмотр» (Рисунок 42). Чтобы добавить дополнительные права, установите «флажки» в поля необходимых прав. Для установки всех прав пользователю установите «флажок» в поле «Выбрать все».

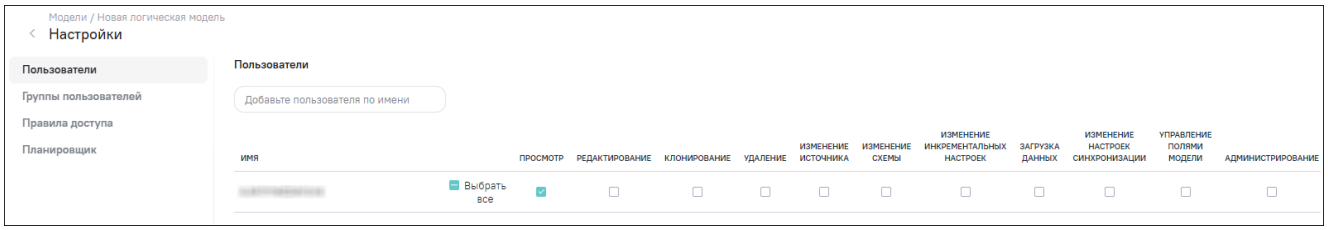


Рисунок 42 – Доступ пользователя к модели на просмотр

Чтобы удалить пользователя из данного списка (отменить доступ), уберите все разрешения (включая просмотр). При следующем входе в данный интерфейс такого пользователя в списке разрешений не будет.

Если у пользователя есть доступы «Изменение источника» и «Изменение схемы», то в карточке редактирования модели (Рисунок 43) можно изменить/добавить источники данных с помощью кнопки + напротив блоков «Источники данных» и «Модели».

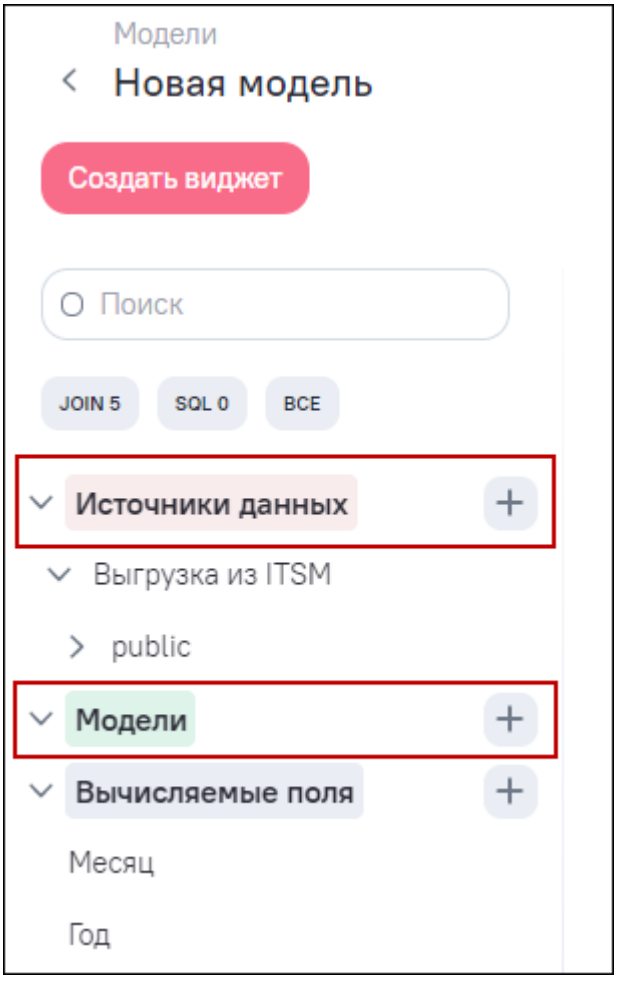


Рисунок 43 – Карточка редактирования модели с правами на «Изменение источника» и «Изменение схемы»

Если у пользователя есть доступ «Изменение источника», но нет доступа «Изменение схемы», то в карточке редактирования модели кнопки + у блоков «Источники данных» и «Модели» не будет, так как доминирующий ключ на изменение схемы отсутствует. Если у пользователя есть доступ «Изменение схемы» и нет доступа «Изменение источника», то в карточке редактирования модели кнопка + у блоков «Источники данных» и «Модели» также не отобразится (Рисунок 44).

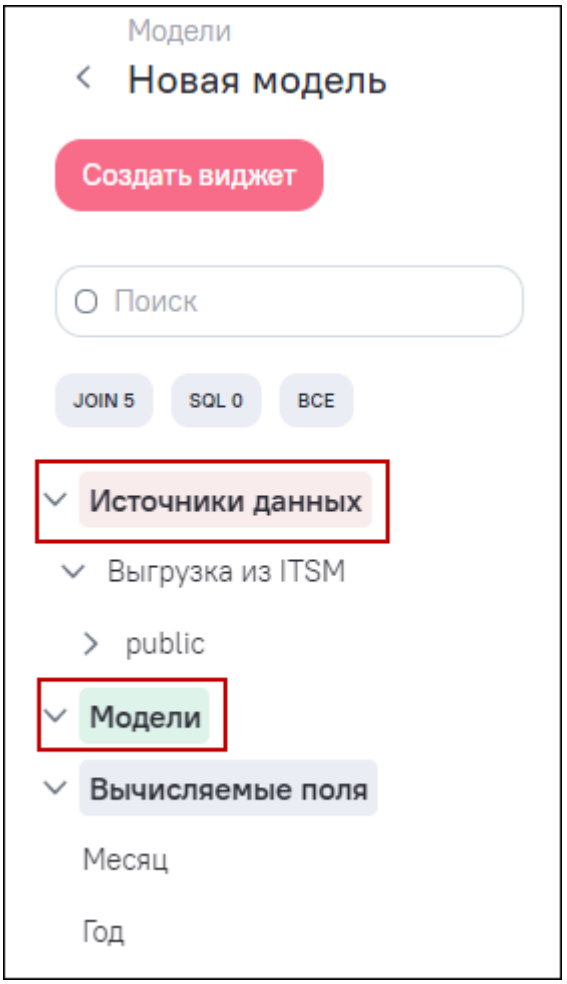


Рисунок 44 – Карточка редактирования модели с отсутствием права «Изменение источника»

Если у пользователя есть доступ «Управление полями модели», то в карточке редактирования модели будет доступна кнопка + напротив наименования блока «Вычисляемые поля», также будет доступно дополнительное меню каждого вычисляемого поля, которое открывается при нажатии на кнопку ... напротив вычисляемого поля (Рисунок 45). Над таблицей данных будут доступны кнопки «Обновить», «Вычисляемое

поле», «Иерархия», поле «Показать скрытые колонки» для установки «флажка» (1, Рисунок 46). В столбцах будет доступно дополнительное меню для редактирования полей модели, которое открывается при нажатии на кнопку [··] (2, Рисунок 46).

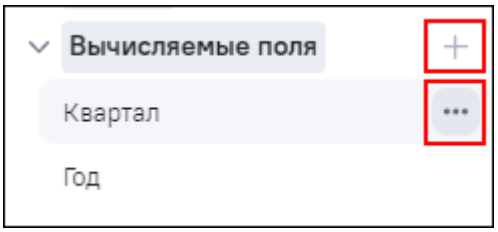


Рисунок 45 – Карточка редактирования модели с наличием доступа «Управление полями модели», кнопки для настройки вычисляемых полей

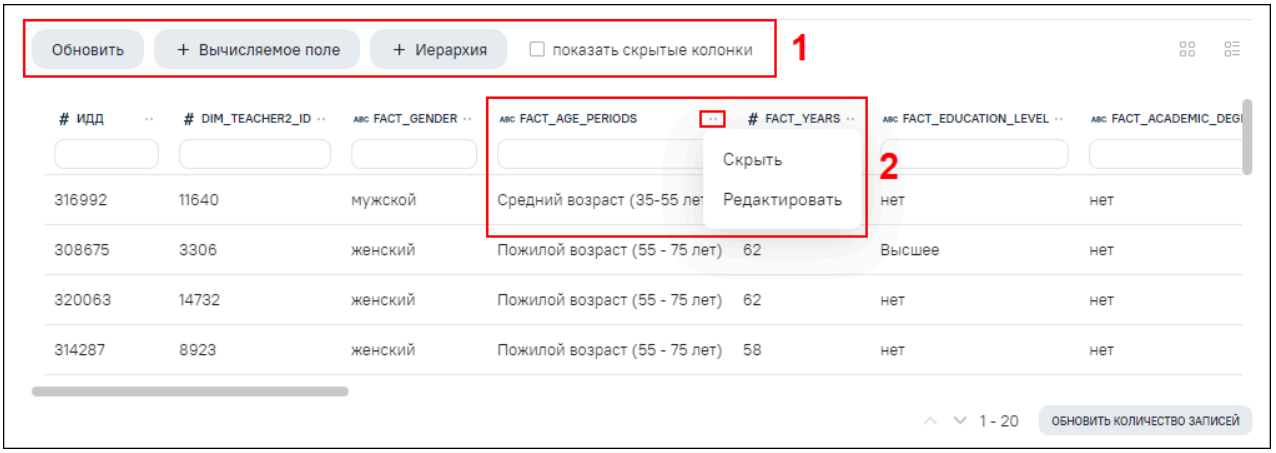


Рисунок 46 – Карточка редактирования модели с наличием доступа «Управление полями модели», кнопки для настройки полей

Если у пользователя нет доступа «Управление полями модели», то в карточке редактирования модели не будут доступны кнопки, описанные выше (Рисунок 47).

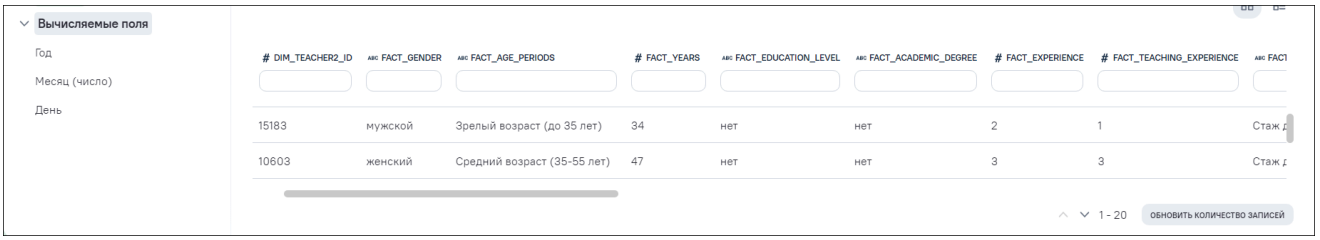


Рисунок 47 – Карточка редактирования модели с отсутствием доступа «Управление полями модели»

Если у пользователя есть доступ «Изменение инкрементальных настроек», то в карточке редактирования модели на вкладке «Инкрементальная загрузка» для фрагмента

будет доступно дополнительное меню «Настройка», которое открывается при нажатии на кнопку  (Рисунок 48).

Рисунок 48 – Карточка редактирования модели с наличием доступа «Изменение инкрементальных настроек»

Если у пользователя нет доступа «Изменение инкрементальных настроек», то в карточке редактирования модели на вкладке «Инкрементальная загрузка» для фрагмента не будет доступно дополнительное меню «Настройка» (Рисунок 49).

Рисунок 49 – Карточка редактирования модели с отсутствием доступа «Изменение инкрементальных настроек»

Если в Системе для пользователей с триальным доступом установлено ограничение «Запрет на предоставление прав к объекту отдельным пользователям», то для таких пользователей при попытке предоставить доступ к моделям вместо списка пользователей отобразится предупреждение «Недоступно в демо-версии», а при нажатии на текст предупреждения откроется уведомление: «В демо-версии нельзя делиться объектами».

5.3.2.2 Управление доступом групп пользователей

Для предоставления прав группам пользователей выберите пункт «Группы пользователей» и далее в окне поиска начните вводить название группы, которой предоставляются права. В выпадающем списке отобразятся подходящие группы пользователей. Необходимую группу выберите нажатием левой кнопки мыши или клавишами навигации и клавишей <Enter> (Рисунок 50).

Рисунок 50 – Добавление доступа группе пользователей к модели

Добавленной группе пользователей сразу предоставляется право «Просмотр» (Рисунок 51). Чтобы добавить дополнительные права, установите «флажки» в поля необходимых прав. Для установки всех прав группе пользователей установите «флажок» в поле «Выбрать все».

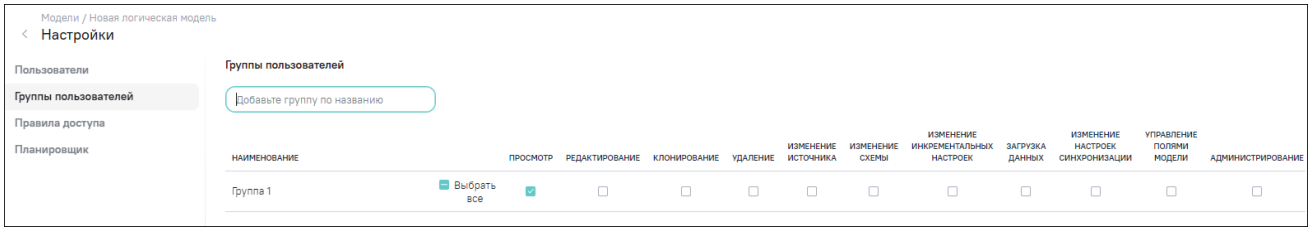


Рисунок 51 – Доступ группы пользователей к модели на просмотр

Чтобы удалить группу пользователей из данного списка (отменить доступ), уберите все разрешения (включая просмотр). При следующем входе в данный интерфейс такой группы пользователей в списке разрешений не будет.

Если у группы пользователей есть доступы «Изменение источника» и «Изменение схемы», то в карточке редактирования модели (Рисунок 52) можно изменить/добавить источники данных с помощью кнопки  напротив блоков «Источники данных» и «Модели».

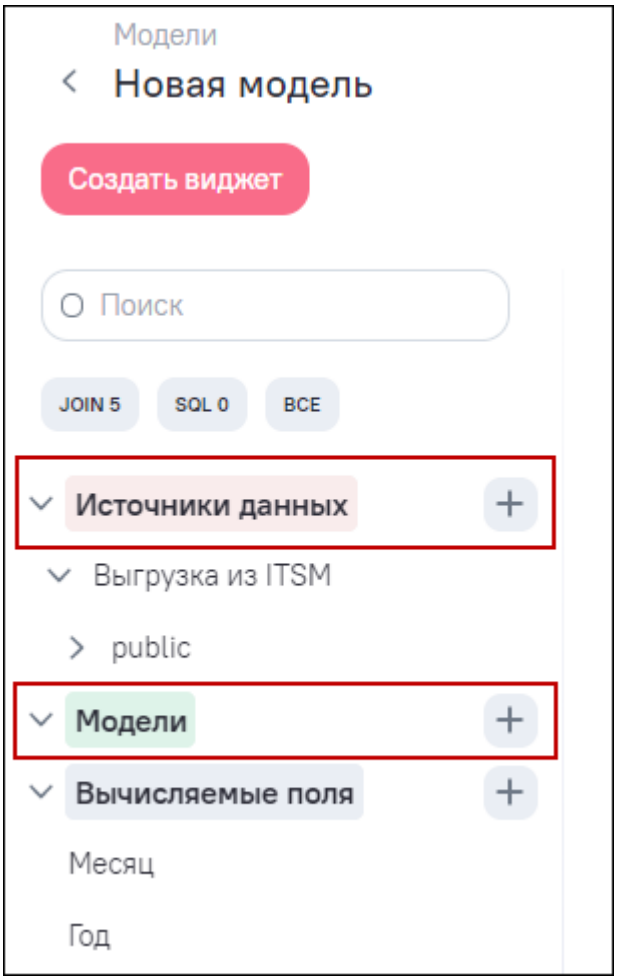


Рисунок 52 – Карточка редактирования модели с правами на «Изменение источника» и «Изменение схемы»

Если у группы пользователей есть доступ «Изменение источника», но нет доступа «Изменение схемы», то в карточке редактирования модели кнопки + у блоков «Источники данных» и «Модели» не будет, так как доминирующий ключ на изменение схемы отсутствует. Если у пользователя есть доступ «Изменение схемы» и нет доступа «Изменение источника», то в карточке редактирования модели кнопка + у блоков «Источники данных» и «Модели» также не отобразится (Рисунок 53).

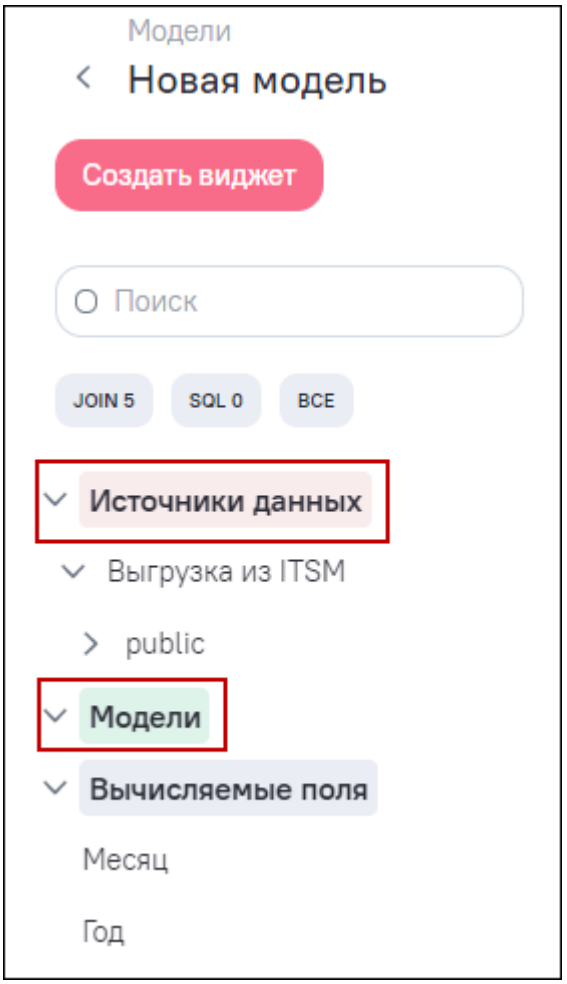


Рисунок 53 – Карточка редактирования модели с отсутствием права на «Изменение источника»

Если у группы пользователей есть доступ «Управление полями модели», то в карточке редактирования модели будет доступна кнопка [+] напротив наименования блока «Вычисляемые поля», также будет доступно дополнительное меню каждого вычисляемого поля, которое открывается при нажатии на кнопку [...] напротив вычисляемого поля (см. Рисунок 45). Над таблицей данных будут доступны кнопки «Обновить», «Вычисляемое поле», «Иерархия», поле «Показать скрытые колонки» для установки «флажка» (см. 1, Рисунок 46). В столбцах будет доступно дополнительное меню для редактирования полей модели, которое открывается при нажатии на кнопку [..] (см. 2, Рисунок 46).

Если у группы пользователей нет доступа «Управление полями модели», то в карточке редактирования модели не будут доступны кнопки, описанные выше (см. Рисунок 47).

Если у группы пользователей есть доступ «Изменение инкрементальных настроек», то в карточке редактирования модели на вкладке «Инкрементальная загрузка» для фрагмента будет доступно дополнительное меню «Настройка», которое открывается при нажатии на кнопку  (см. Рисунок 48).

Если у группы пользователей нет доступа «Изменение инкрементальных настроек», то в карточке редактирования модели на вкладке «Инкрементальная загрузка» для фрагмента не будет доступно дополнительное меню «Настройка» (см. Рисунок 49).

5.3.2.3 Управление правилами доступа

Описание настройки правил доступа к пользовательской модели описано в п. 5.4.5.

5.3.2.4 Управление планировщиком

Настройки планировщика позволяют для каждой модели отдельно установить оптимальный режим обновления данных.

Для настройки планировщика выберите пункт «Планировщик». Настройки планировщика через интерфейс (режим «Неделя») позволяют создать обновление с периодичностью не чаще 1 раза в день и не реже 1 раза в неделю. При этом можно выбрать конкретный день (или дни) недели и указать с точностью до минуты (по времени сервера) время старта процесса обновления (Рисунок 54).

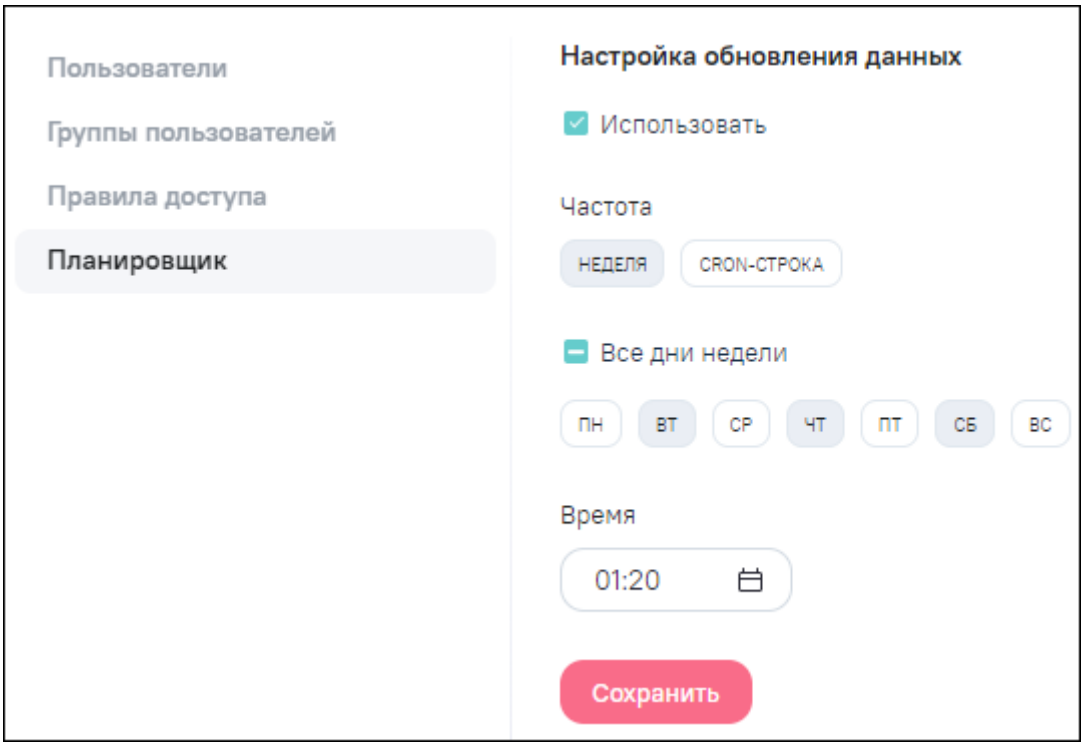


Рисунок 54 – Настройки планировщика обновления данных модели

Для настройки расписания через интерфейс (режим «Неделя») выберите день (дни) недели или установите «флажок» в поле «Все дни недели», чтобы выбрать все дни недели, и укажите время. Поля для выбора дней недели и времени являются обязательными для заполнения. Если данные поля не заполнены, то при сохранении откроется уведомление об ошибке.

Для использования более сложных конфигураций планировщика можно использовать режим «CRON-строка». Введите необходимую строку файла linux CRONTAB в соответствии с принятыми правилами ее написания. На рисунке (Рисунок 55) настроен запуск каждые 5 минут.

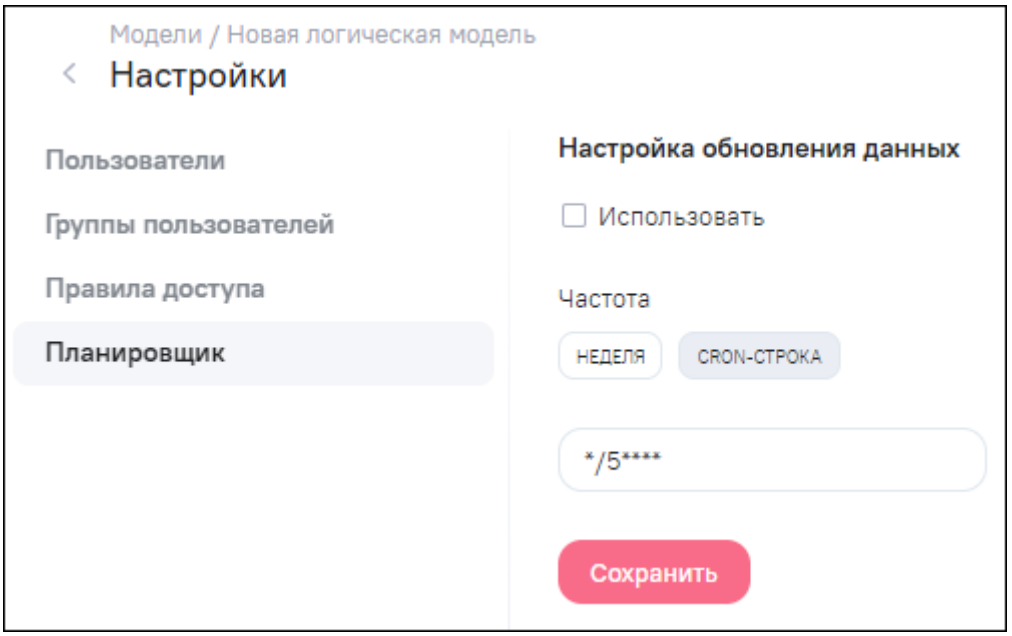


Рисунок 55 – Настройки планировщика обновления данных модели с использованием «CRON-строки»

Примечание – При сохранении некорректного выражения «cron-строки» отобразится уведомление об ошибке (Рисунок 56).

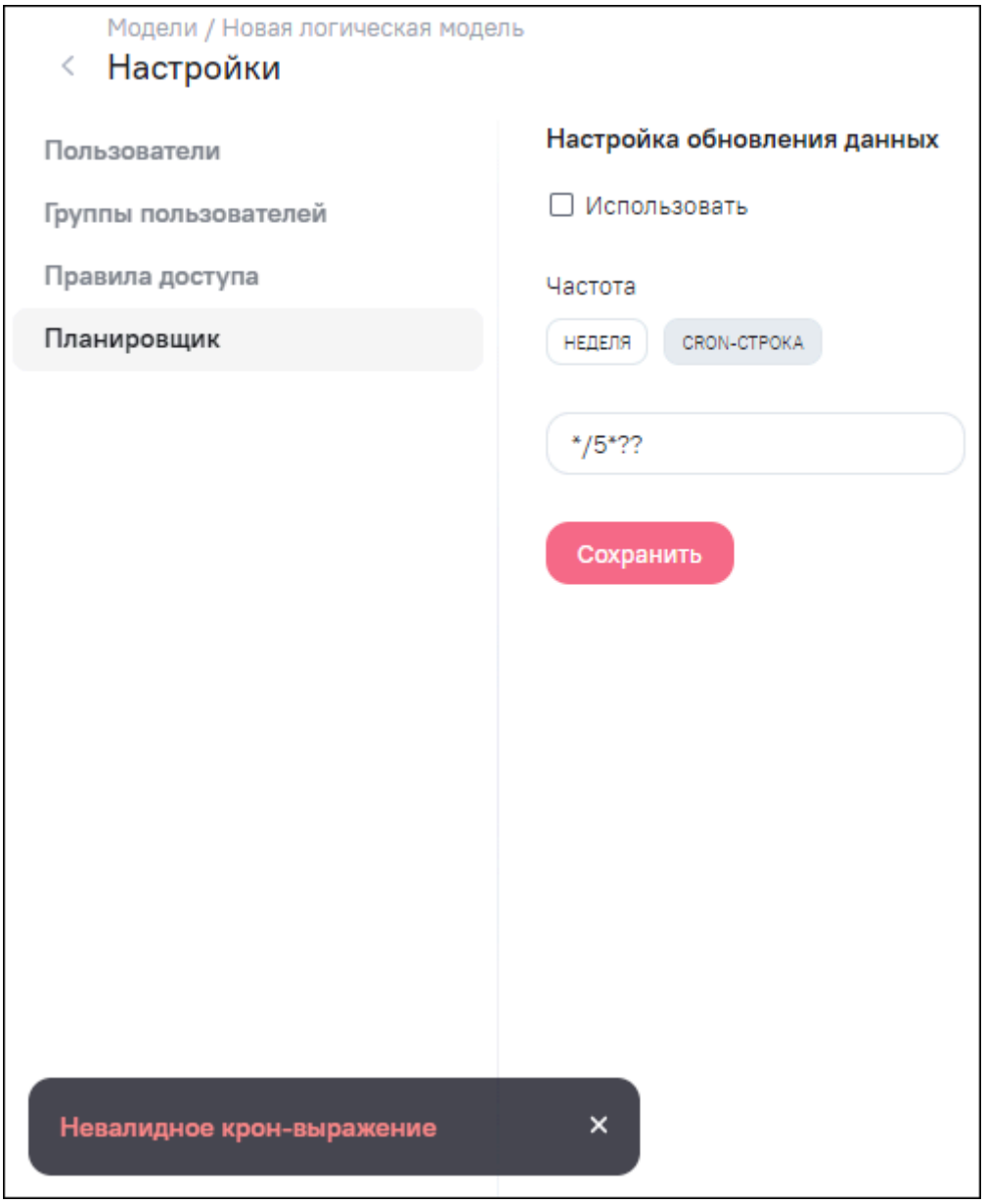


Рисунок 56 – Уведомление об ошибке при сохранении некорректного выражения «cron-строки»

Установкой/снятием «флажка» в поле «Использовать» можно включить/отключить обновление, например, если необходимо отключить временно, не удаляя созданное расписание.

После настройки планировщика нажмите на кнопку «Сохранить».

5.3.3 Управление доступом к виджетам

Предварительным условием получения пользователем доступа к конкретному виджету является наличие у него прав работы в блоке (интерфейсе) «Виджеты». Для

получения этих прав пользователь должен быть включен администратором Системы во встроенную группу пользователей «Просмотр виджетов».

Доступ к виджетам включает установку разрешений для пользователей и групп по следующим категориям:

- «Просмотр» – разрешение только на просмотр виджета;
- «Редактирование» – разрешение на просмотр и изменение характеристик (настроек) виджета;
- «Клонирование» – разрешение на создание нового виджета с копированием всех настроек текущего;
- «Удаление» – разрешение на удаление данного виджета из Системы;
- «Изменение модели» – разрешение на изменение модели данных;
- «Выгрузка в csv» – разрешение на экспорт данного виджета в файл векторного рисунка формата .csv;
- «Создание ссылки» – разрешение на публикацию данного виджета по прямой ссылке;
- «Администрирование» – разрешение на управление доступом к виджету (операции, описываемые в данном разделе).

Настройка доступа выполняется в контексте каждого конкретного виджета через интерфейс «Настройки». Чтобы перейти к интерфейсу «Настройки», нажмите на кнопку  в режиме редактирования выбранного виджета. Права доступа могут предоставляться как отдельным пользователям, так и группам пользователей.

5.3.3.1 Управление доступом отдельных пользователей

Для предоставления прав отдельным пользователям выберите пункт «Пользователи» и далее в окне поиска начните вводить логин пользователя, которому предоставляются права. В выпадающем списке отобразятся подходящие логины.

Необходимый логин выберите нажатием левой кнопки мыши или клавишами навигации и клавишей <Enter> (Рисунок 57).

Рисунок 57 – Добавление доступа пользователю к виджету

Добавленному пользователю сразу предоставляется право «Просмотр» (Рисунок 58). Чтобы добавить дополнительные права, установите «флажки» в поля необходимых прав. Для установки всех прав пользователю установите «флажок» в поле «Выбрать все».

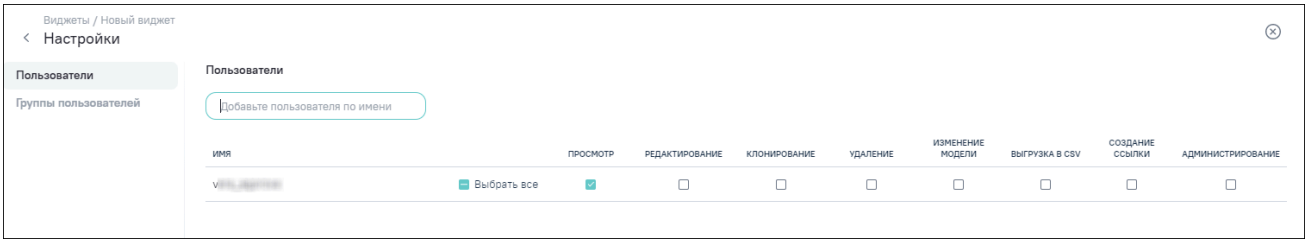


Рисунок 58 – Доступ пользователя к виджету на просмотр

Чтобы удалить пользователя из данного списка (отменить доступ), уберите все разрешения (включая просмотр). При следующем входе в данный интерфейс такого пользователя в списке разрешений не будет.

Если в Системе для пользователей с триальным доступом установлено ограничение «Запрет на предоставление прав к объекту отдельным пользователям», то для таких пользователей при попытке предоставить доступ к виджетам вместо списка пользователей отобразится предупреждение «Недоступно в демо-версии», а при нажатии на текст предупреждения откроется уведомление: «В демо-версии нельзя делиться объектами».

5.3.3.2 Управление доступом групп пользователей

Для предоставления прав группам пользователям выберите пункт «Группы пользователей» и далее в окне поиска начните вводить название группы, которой предоставляются права. В выпадающем списке отобразятся подходящие группы

пользователей. Необходимую группу выберите нажатием левой кнопки мыши или клавишами навигации и клавишей <Enter> (Рисунок 59).

Рисунок 59 – Добавление доступа группе пользователей к виджету

Добавленной группе пользователей сразу предоставляется право «Просмотр» (Рисунок 60). Чтобы добавить дополнительные права, установите «флажки» в поля необходимых прав. Для установки всех прав группе пользователей установите «флажок» в поле «Выбрать все».

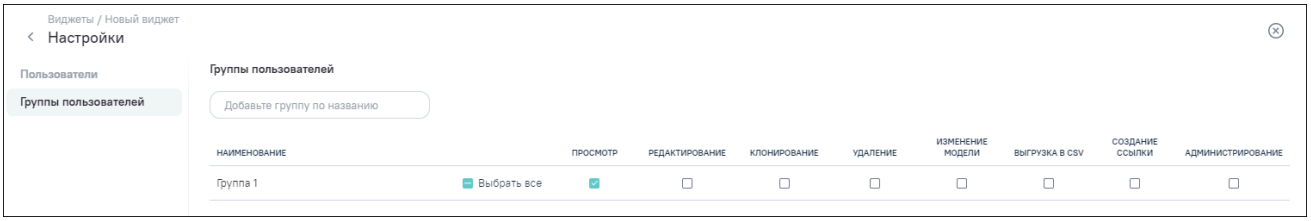


Рисунок 60 – Доступ группы пользователей к виджету на просмотр

Чтобы удалить группу пользователей из данного списка (отменить доступ), уберите все разрешения (включая просмотр). При следующем входе в данный интерфейс такой группы пользователей в списке разрешений не будет.

5.3.4 Управление доступом к информационным панелям

Предварительным условием получения пользователем доступа к конкретной информационной панели является наличие у него прав работы в блоке (интерфейсе) «Информационные панели». Для получения этих прав пользователь должен быть включен администратором Системы во встроенную группу пользователей «Просмотр панелей».

Доступ к информационным панелям включает установку разрешений для пользователей и групп по следующим категориям:

- «Просмотр» – разрешение только на просмотр информационной панели;

- «Редактирование» – разрешение на просмотр и изменение информационной панели;
- «Клонирование» – разрешение на создание новой информационной панели с копированием всех настроек текущей;
- «Удаление» – разрешение на удаление данной информационной панели из Системы;
- «Создание ссылки» – разрешение на публикацию данной информационной панели по прямой ссылке;
- «Экспорт» – разрешение на экспорт данной информационной панели в файл графического формата;
- «Администрирование» – разрешение на управление доступом к информационной панели (операции, описываемые в данном разделе).

Настройка доступа выполняется в контексте каждой конкретной информационной панели через интерфейс «Настройки». Чтобы перейти к интерфейсу «Настройки», нажмите на кнопку  в режиме редактирования выбранной информационной панели. Права доступа могут предоставляться как отдельным пользователям, так и группам пользователей.

5.3.4.1 Управление доступом отдельных пользователей

Для предоставления прав отдельным пользователям выберите пункт «Пользователи» и далее в окне поиска начните вводить логин пользователя, которому предоставляются права. В выпадающем списке отобразятся подходящие логины. Необходимый логин выберите нажатием левой кнопки мыши или клавишами навигации и клавишей <Enter> (Рисунок 61).

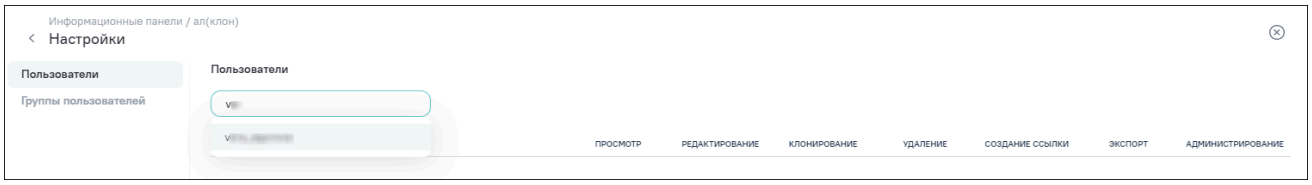


Рисунок 61 – Добавление доступа пользователю к информационной панели

Добавленному пользователю сразу предоставляется право «Просмотр» (Рисунок 62). Чтобы добавить дополнительные права, установите «флажки» в поля необходимых прав. Для установки всех прав пользователю установите «флажок» в поле «Выбрать все».

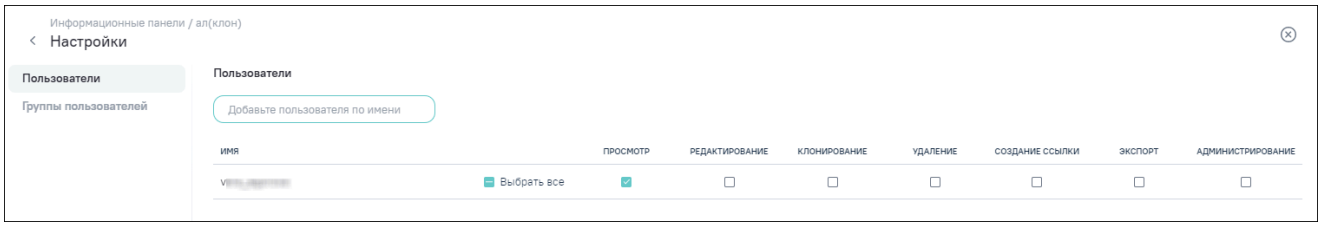


Рисунок 62 – Доступ пользователя к информационной панели на просмотр

Чтобы удалить пользователя из данного списка (отменить доступ), уберите все разрешения (включая просмотр). При следующем входе в данный интерфейс такого пользователя в списке разрешений не будет.

Если у пользователя есть доступ «Экспорт», то в карточке просмотра и редактирования информационной панели доступна кнопка «Экспорт».

Если в Системе для пользователей с триальным доступом установлено ограничение «Запрет на предоставление прав к объекту отдельным пользователям», то для таких пользователей при попытке предоставить доступ к информационным панелям вместо списка пользователей отобразится предупреждение «Недоступно в демо-версии», а при нажатии на текст предупреждения откроется уведомление: «В демо-версии нельзя делиться объектами».

5.3.4.2 Управление доступом групп пользователей

Для предоставления прав группам пользователей выберите пункт «Группы пользователей» и далее в окне поиска начните вводить название группы, которой предоставляются права. В выпадающем списке отобразятся подходящие группы пользователей. Необходимую группу выберите нажатием левой кнопки мыши или клавишами навигации и клавишей <Enter> (Рисунок 63).

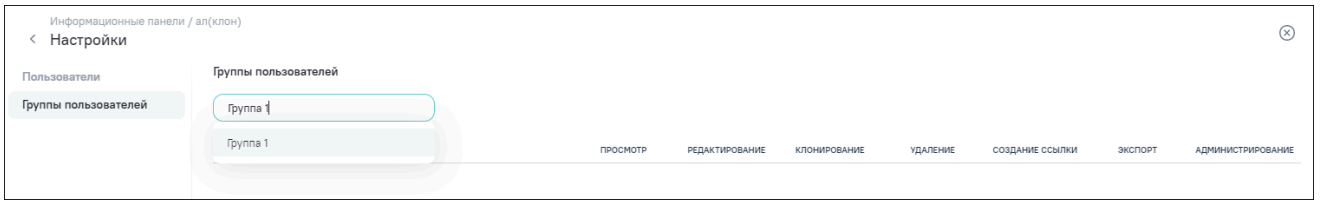


Рисунок 63 – Добавление доступа группе пользователей к информационной панели

Добавленной группе пользователей сразу предоставляется право «Просмотр» (Рисунок 64). Чтобы добавить дополнительные права, установите «флажки» в поля необходимых прав. Для установки всех прав группе пользователей установите «флажок» в поле «Выбрать все».

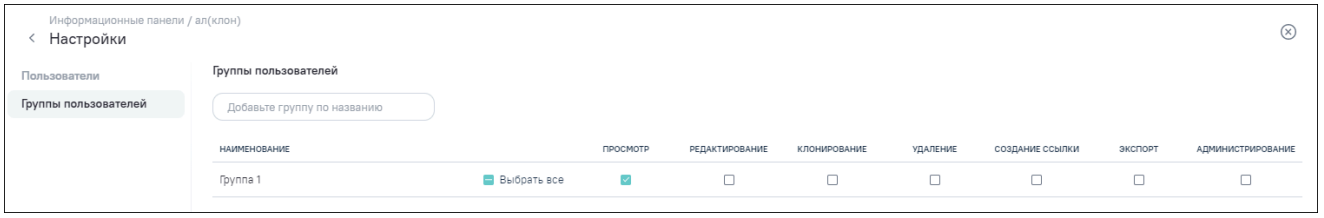


Рисунок 64 – Доступ группы пользователей к информационной панели на просмотр

Чтобы удалить группу пользователей из данного списка (отменить доступ), уберите все разрешения (включая просмотр). При следующем входе в данный интерфейс такой группы пользователей в списке разрешений не будет.

5.4 Атрибутный доступ к данным

5.4.1 Общие принципы

Атрибутный доступ к данным включает получение пользователем доступа к отдельным строкам данных модели на основании значений параметров (атрибутов) его учетной записи, полученных от провайдера. Данный универсальный принцип позволяет реализовать множество различных сценариев управления доступом, таких как:

- доступ только к области ответственности специалиста, например:
  - данным по деятельности собственной и нижестоящих организационных структур;
  - данным по собственному региону и его субъектам.

- разделение доступа к данным по времени (периоду) к которому они относятся:
  - доступ только к данным созданным соответствующим периоду работы сотрудника;
  - доступ определенных категорий сотрудников только к историческим данным (данным за прошедшие периоды).

Для реализации атрибутного доступа через внутренний провайдер «Система» с типом «user_permissions» в Системе встроена модель данных «user_permissions», в которой администратор может создать и поддерживать любую необходимую для стыковки с данными структуру атрибутов пользователя. Для реализации атрибутного доступа через внешний провайдер модель данных «user_permissions» не используется, все необходимые атрибуты пользователя Система получает от провайдера.

В настройках целевой модели (доступ к которой ограничивается атрибутными правилами) задаются условия, использующие сравнение значений атрибутов пользователя и выбранных полей данных модели. Если такие условия заданы для модели – доступ к каждой строке данных предоставляется дифференциально каждому конкретному пользователю. Если для модели не заданы условия атрибутного доступа – доступ к строкам не ограничивается.

Ограничения атрибутного доступа применяются в интерфейсе просмотра виджетов и информационных панелей и не применяются в интерфейсе просмотра данных моделей или источников. Пользователи, на которых должны распространяться ограничения, во избежание несанкционированного доступа не должны иметь доступ к исходным моделям и источникам для данных виджетов и информационных панелей.

Атрибутный доступ только накладывает дополнительные ограничения, независимо от его применения, у пользователя должны быть обеспечены права для работы с соответствующим разделом Системы и даны, как минимум, на права просмотр для соответствующего объекта Системы (виджета или информационной панели).

5.4.2 Настройка схемы доступов

Раздел «Схемы доступов» находится в блоке «Администрирование». Раздел доступен пользователям, наделенным административными правами через встроенную системную группу «Администратор».

Схема доступов представляет собой список атрибутов доступа, которые передаются внешними провайдерами в Систему при авторизации пользователя или указываются в модели «user_permissions» при использовании внутреннего провайдера «Система» и которые используются для атрибутного доступа к данным модели.

В Системе есть встроенные атрибуты доступа «login» (логин), «email» (E-mail) и «state» (статус). По ним сопоставляется учетная запись пользователя и обновляются его данные. Встроенные атрибуты не подлежат редактированию и удалению. Настройте схему доступов так, чтобы она содержала все необходимые атрибуты пользователей, которые необходимы для атрибутного доступа к данным моделей, например:

- оргструктурную принадлежность (департамент, подразделение, ведомство и т.д.);
- территориальную привязку (регион, город и т.д.);
- принадлежность к определенным ролям (руководитель, бухгалтер, ответственный за, и т.д.);
- дополнительные атрибуты, делающие информацию более понятной и наглядной (ФИО пользователя, название организационной единицы, название территории).

Настройка атрибутов доступа в схеме доступов описана в п. 5.2.4. На рисунке (Рисунок 65) представлен пример настроенной схемы доступов.

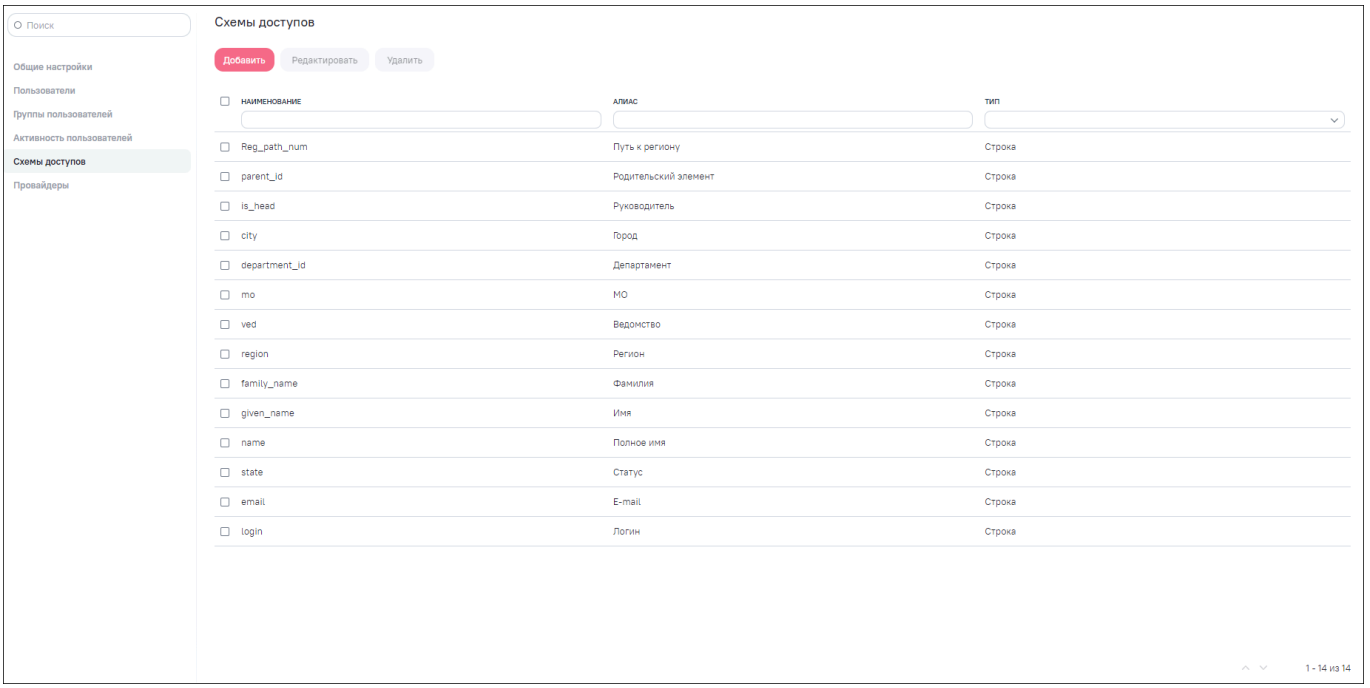


Рисунок 65 – Пример настройки схемы доступов

5.4.3 Настройка встроенной модели «user_permissions»

В Системе изначально встроена модель данных «user_permissions», доступная только пользователю «admin».

Чтобы войти в режим редактирования модели «user_permissions», дважды нажмите левой кнопкой мыши на модель, в открывшейся форме просмотра модели нажмите на кнопку «Редактировать». Установка «флажка» на модель «user_permissions» из списка моделей недоступна.

Модель «user_permissions» по умолчанию «пустая» (не содержит источников, данных и связей), настройте ее структуру данных так, чтобы она содержала:

- поле «login», содержащее логины пользователей, совпадающие с логинами, созданными в Системе;
- атрибуты пользователей, на основе значений которых должен быть настроен доступ к данным (таблицы данных должны тоже содержать эти значения), например:
  - оргструктурную принадлежность;

- территориальную привязку;
- принадлежность к определенным ролям, например:
  - руководитель;
  - бухгалтер;
  - ответственный за.
- дополнительные атрибуты, делающие информацию более понятной и наглядной, например:
  - ФИО пользователя;
  - название организационной единицы;
  - название региона, территории.

Так же как и все остальные модели, данная модель извлекает и соединяет данные из поддерживаемых видов источников данных (описание работы с моделями представлено в Руководстве пользователя). Администратор Системы самостоятельно принимает решение, откуда загружать и обновлять необходимую информацию. Источником может выступать как внешняя база данных, так и подготовленный в соответствии с требованиями к модели Excel-файл. Также возможна комбинация данных из нескольких источников, например, когда основная информация извлекается из внешней базы данных, а Excel-файл дополняет недостающие сведения. Все возможности работы с моделями описаны в Руководстве пользователя.

После настройки структуры данных модели «user_permissions» значения ее полей становятся дополнительными атрибутами учетных записей пользователей.

Чтобы атрибутные разрешения и политики доступа на их основе работали после завершения настройки модели «user_permissions», ее данные должны быть загружены. Как минимум, должна быть выполнена разовая загрузка данных вручную (описание представлено в Руководстве пользователя). При необходимости регулярной поддержки

актуальности данных должно быть настроено расписание обновления модели в «Планировщике» (описание представлено в Руководстве пользователя и в п. 5.3.2.4).

5.4.4 Настройка провайдера пользователя

Раздел «Провайдеры» находится в блоке «Администрирование». Раздел доступен пользователям, наделенным административными правами через встроенную системную группу «Администратор». Раздел предназначен для настройки взаимодействия Системы с провайдерами пользователей. В Системе есть внутренний провайдер «Система» с типом «user_permissions», который используется по умолчанию. Так же в Системе есть возможность настроить авторизацию через внешний сервис аутентификации по протоколу Open ID Connect.

5.4.4.1 Настройка внутреннего провайдера «Система»

Система не позволяет добавить дополнительный провайдер с типом «Система (user_permissions)», так как внутренний провайдер должен быть уникальным. Поэтому настройка провайдера «Система» доступна только с помощью редактирования встроенной записи внутреннего провайдера (см. п. 5.2.5.2).

При настройке заполните данные на вкладке «Маппинг схемы» (см. п. 5.2.5.1.3). Таблица соответствия в первом столбце будет содержать все атрибуты схемы доступов (см. п. 5.4.2). Во втором столбце укажите соответствующие атрибуты, используемые в модели «user_permissions» (см. п. 5.4.3). Нажмите на кнопку «Сохранить». В случае успешного сохранения отобразится уведомление о внесенных изменениях – «Провайдер сохранен».

На рисунке (Рисунок 66) представлен пример настроенного внутреннего провайдера «Система».

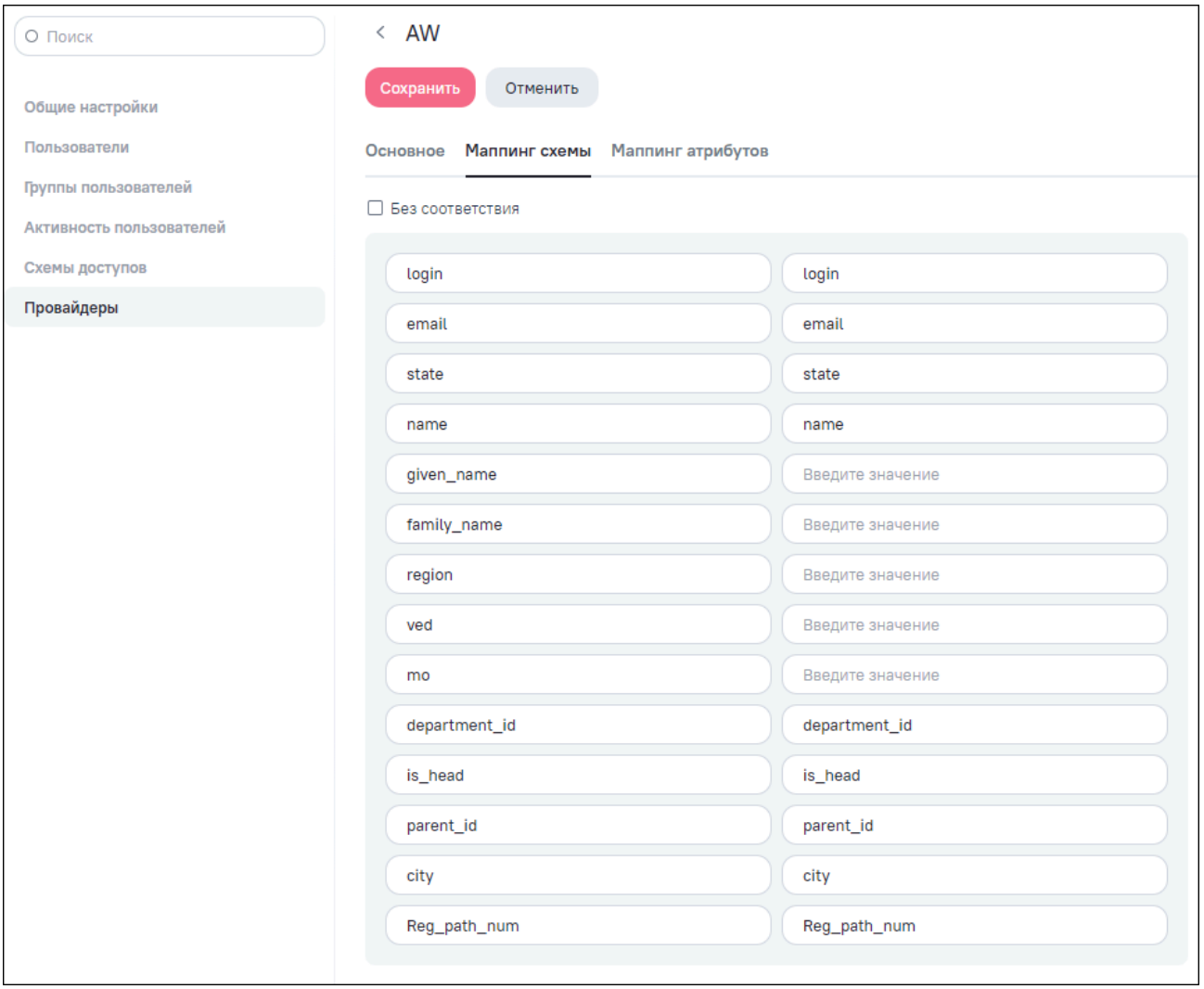


Рисунок 66 – Пример настройки внутреннего провайдера «Система»

5.4.4.2 Настройка внешнего провайдера

Чтобы настроить взаимодействие, произведите настройки для обоих участников взаимодействия: провайдера (поставщика учетных записей) и Системы (поставщика сервиса). Для настройки взаимодействия Системы с провайдером выполните шаги, описанные в п. 5.2.5.1.

Примечание – Предполагается, что взаимодействие провайдера (поставщика учетных записей) с Системой настроено, и учетные записи зарегистрированы.

На рисунках (Рисунок 67 – Рисунок 70) представлен пример настроенного внешнего провайдера «BarsUP.AM».

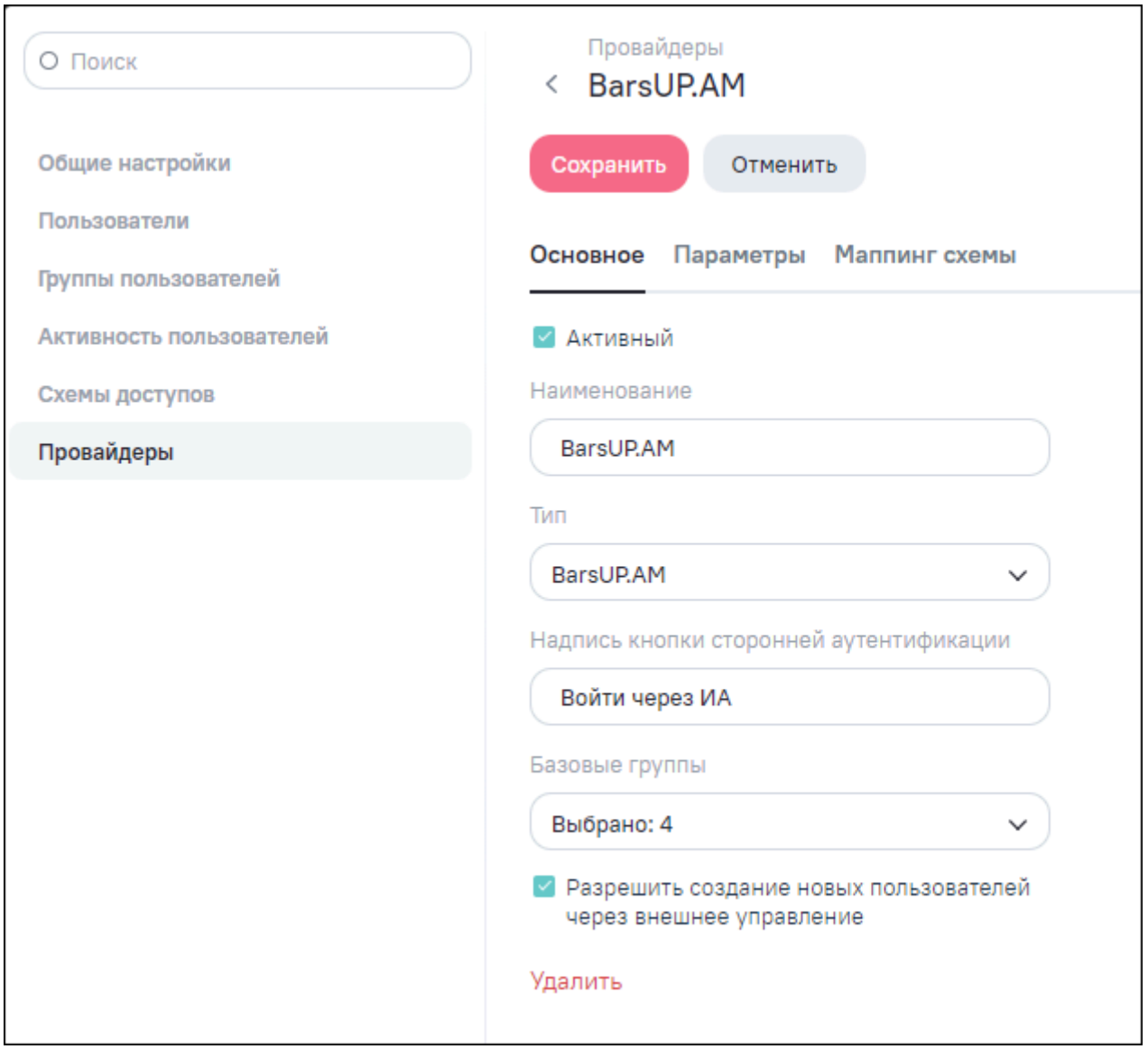


Рисунок 67 – Пример настройки внешнего провайдера, вкладка «Основное»

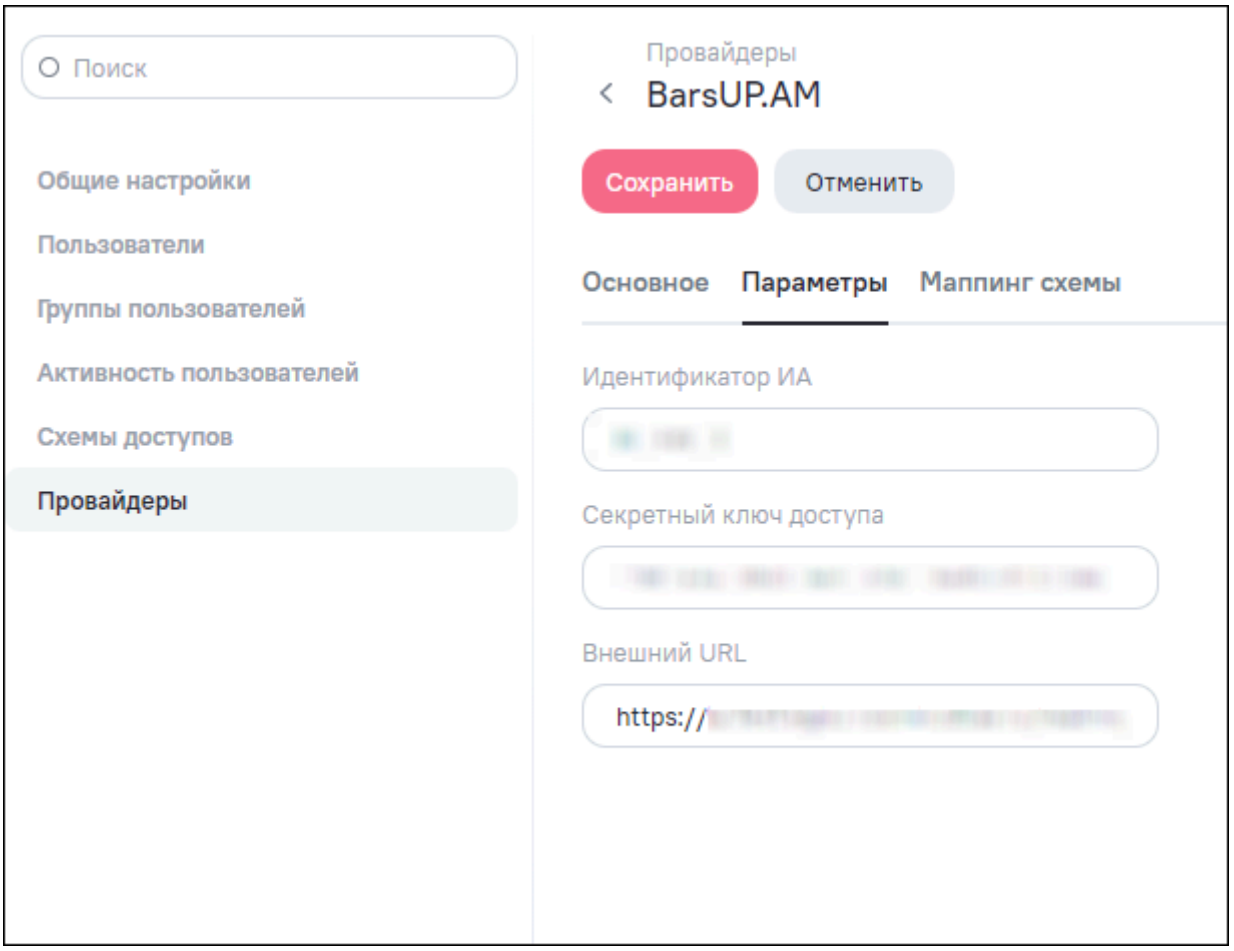


Рисунок 68 – Пример настройки внешнего провайдера, вкладка «Параметры»

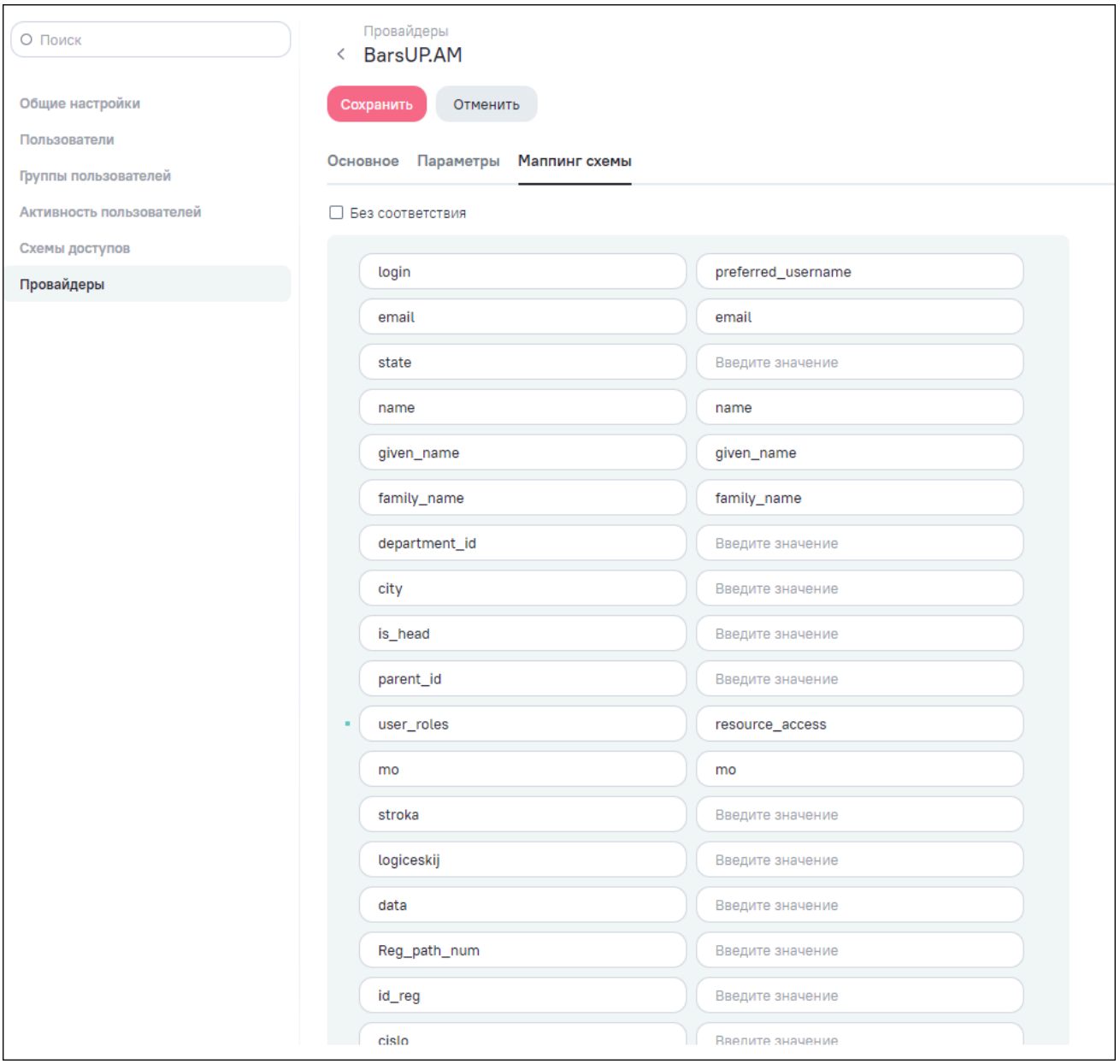


Рисунок 69 – Пример настройки внешнего провайдера, вкладка «Маппинг схемы»

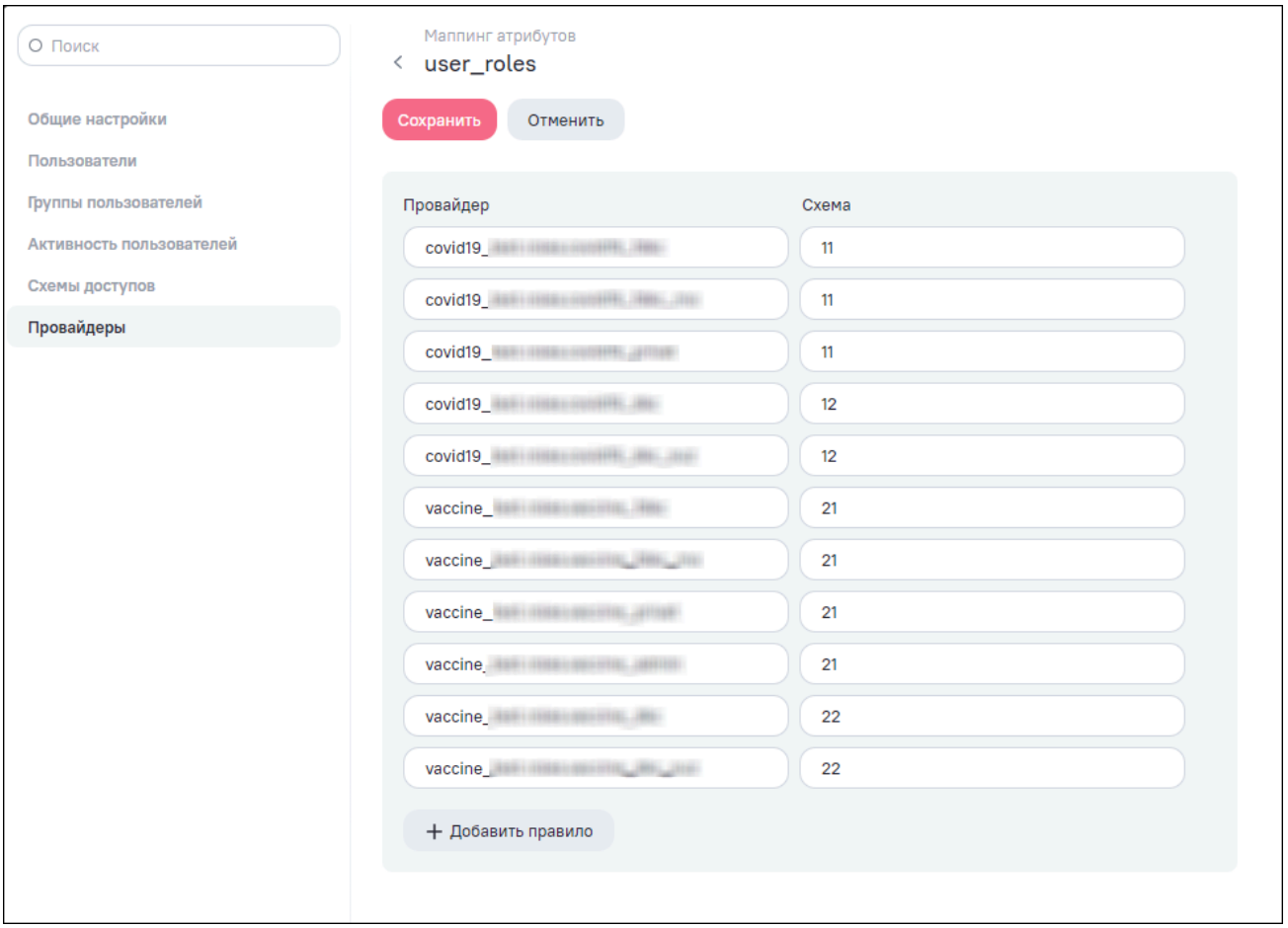


Рисунок 70 – Пример настройки внешнего провайдера, вкладка «Маппинг схемы». Окно «Маппинг атрибутов»

5.4.5 Настройка правил доступа к пользовательской модели

Настройка правил доступа может выполняться пользователем, создавшим модель или имеющим права на администрирование данной модели. Объектом доступа являются строки данных. Настройка правил определяет условия, которым должны отвечать доступные пользователю строки (например, территориальная привязка пользователей соответствует территориальной привязке данных модели).

Настройка правил атрибутного доступа выполняется в интерфейсе настройки доступа к конкретной модели (см. п. 5.3.2) на вкладке «Правила доступа» (Рисунок 71).

Рисунок 71 – Вкладка «Правила доступа» интерфейса настройки моделей

Интерфейс настройки правил доступа содержит список созданных правил, а также предоставляет возможности:

- создания нового правила;
- изменения существующего правила;
- удаления одного или нескольких существующих правил.

Подробно данные операции описаны в п. 5.4.5.1 – 5.4.5.5.

5.4.5.1 Создание нового правила

Чтобы добавить новое правило, нажмите на кнопку «Добавить» (см. Рисунок 71).

Отобразится интерфейс добавления правила доступа (Рисунок 72), содержащий:

1) редактируемое поле названия правила (1);
2) кнопку «Сохранить» для сохранения нового правила или внесенных изменений (2);
3) поле выбора типа субъекта доступа «Тип объекта доступа» (3);
4) интерфейс ввода условий (4).

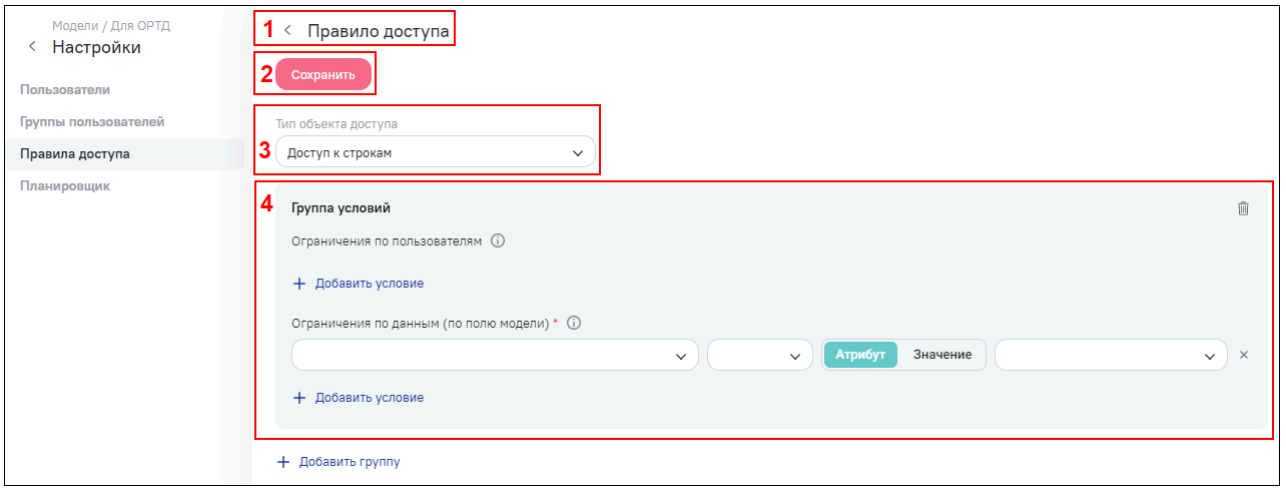


Рисунок 72 – Интерфейс добавления правила доступа

5.4.5.1.1 Создание правила доступа по строкам

Для настройки правил доступа по строкам в поле «Тип объекта доступа» выберите значение «Доступ к строкам» (см. Рисунок 72).

Группа условий может включать в себя два вида ограничений:

- ограничения по пользователям (необязательно) – дает ограничения на пользователей, т.е. определяет группу пользователей (кого ограничиваем), к которым будут применены условия по полю модели (как ограничиваем);
- ограничения по данным (обязательно) – дает ограничения на данные, т.е. определяет поля модели, которые ограничивают видимость данных.

Для добавления условия нажмите на кнопку «Добавить условие» в необходимом блоке.

Условия в блоке «Ограничения по пользователям» строятся из следующих компонентов:

- атрибут пользователя, входящий в состав схемы доступов. Выберите значение из выпадающего списка (Рисунок 73);

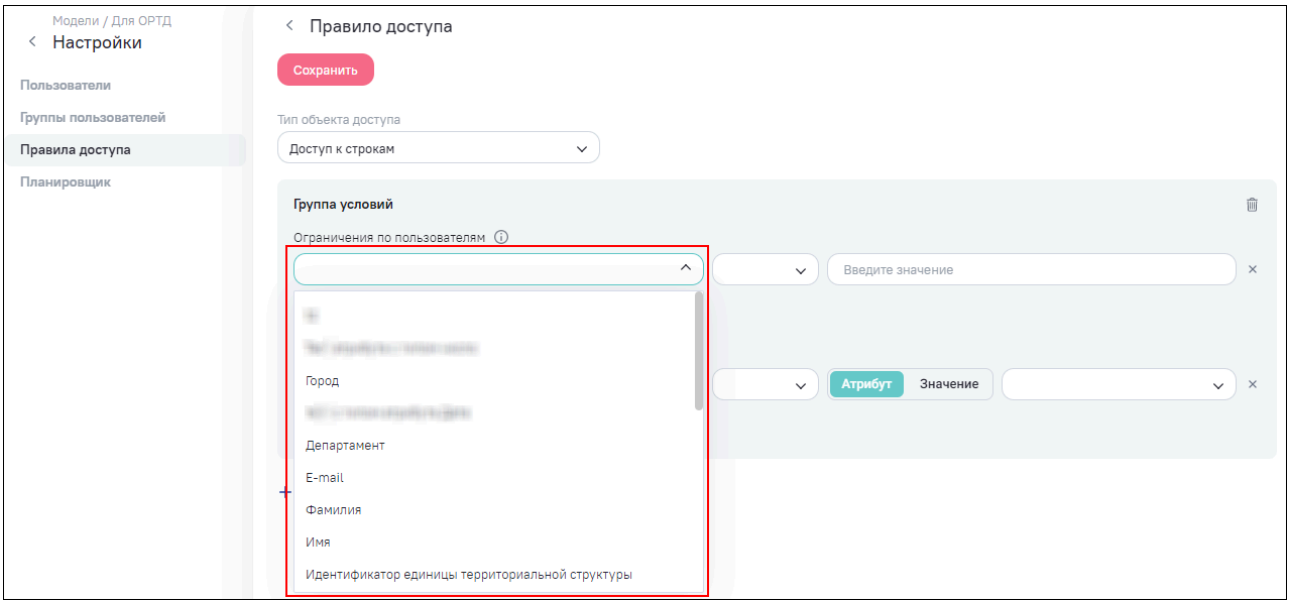


Рисунок 73 – Выбор атрибута доступа в блоке «Ограничения по пользователям»

Примечание – Специальный атрибут «Роль» применяется в настройке атрибутного доступа к пользовательской модели для ограничения пользователей внешнего провайдера с помощью задания условий по значениям, указанным в маппинге атрибутов внешнего провайдера.

- оператор сравнения. Выберите значение из выпадающего списка (Рисунок 74);

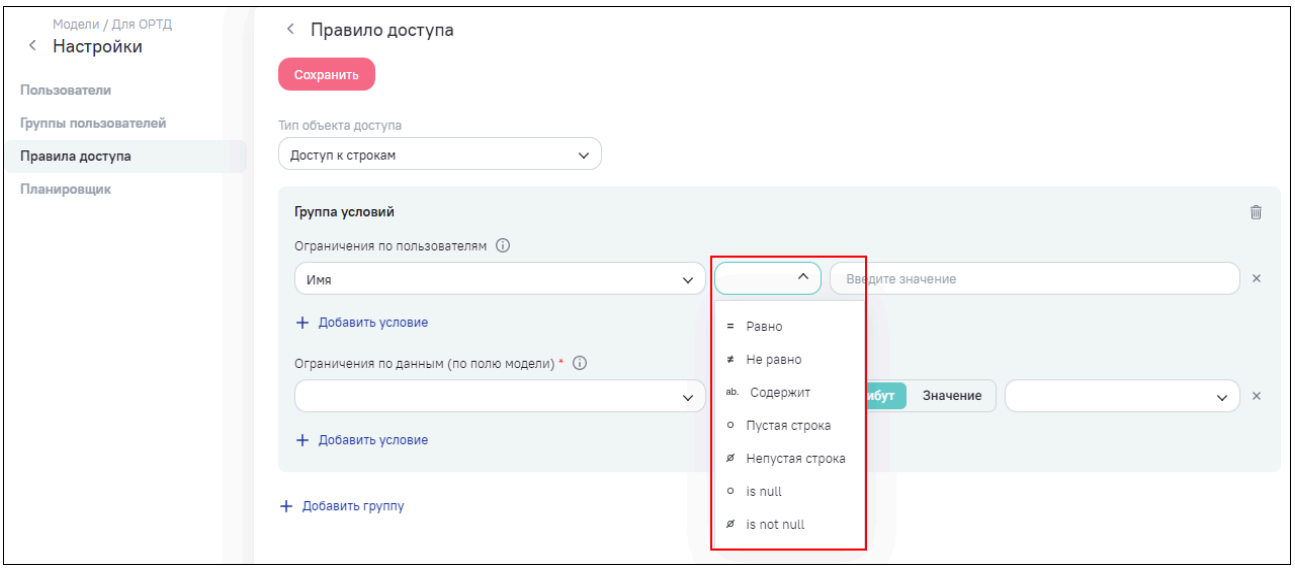


Рисунок 74 – Выбор оператора сравнения в блоке «Ограничения по пользователям»

- постоянное значение для сравнения, с которым будет сравниваться значение атрибута. Введите значение с клавиатуры (Рисунок 75).

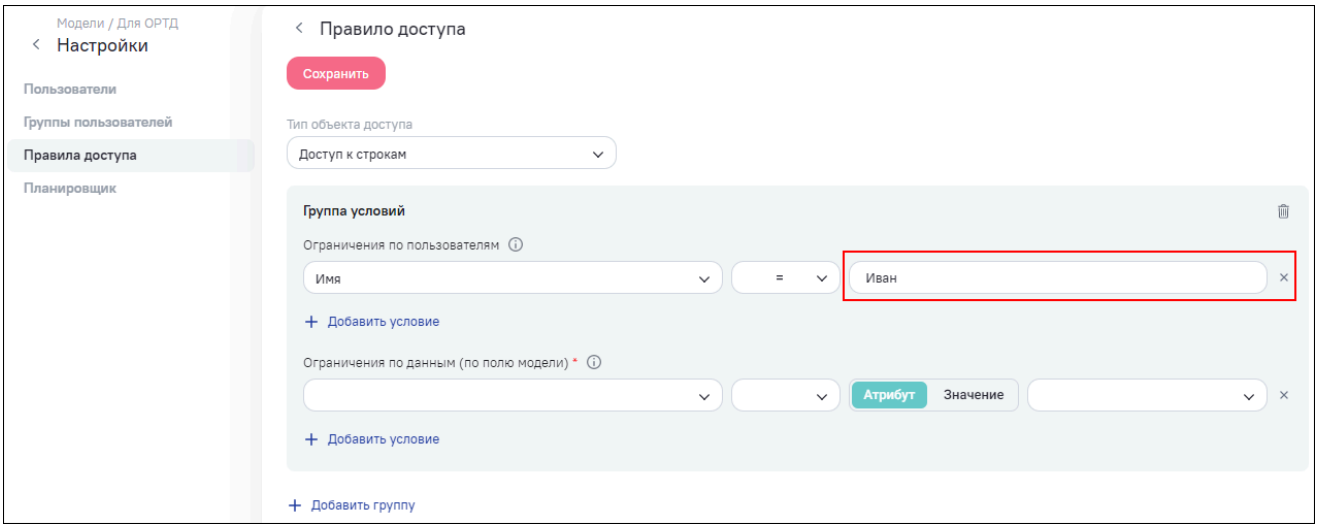


Рисунок 75 – Ввод постоянного значения для сравнения в блоке «Ограничения по пользователям»

Условия в блоке «Ограничения по данным (по полю модели)» строятся из следующих компонентов:

- поле модели. Выберите значение из выпадающего списка (Рисунок 76);

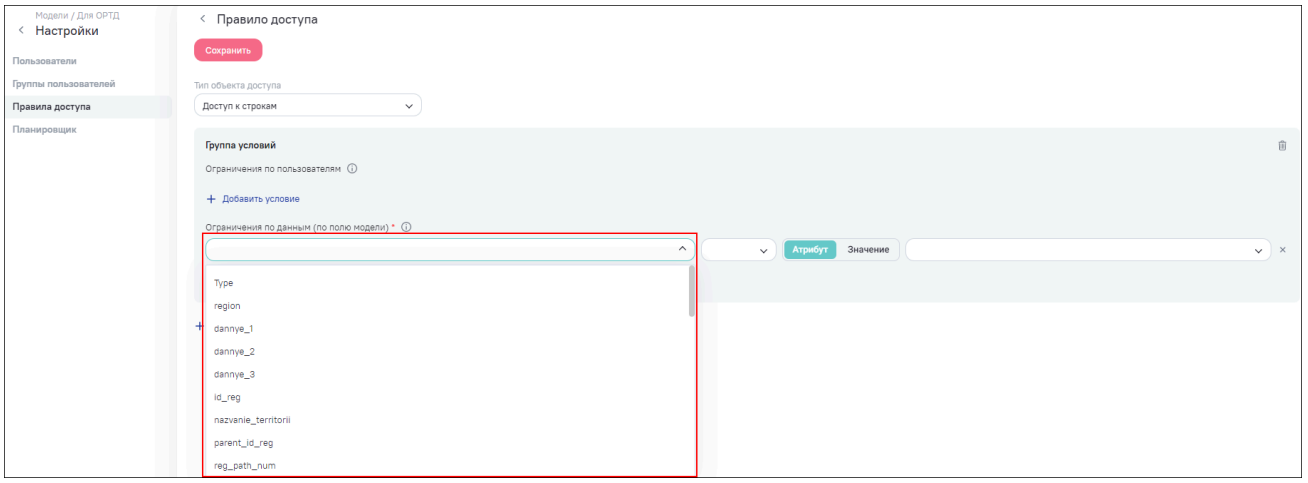


Рисунок 76 – Выбор вида сравнения в блоке «Ограничения по данным (по полю модели)»

- оператор сравнения. Выберите значение из выпадающего списка (Рисунок 77);

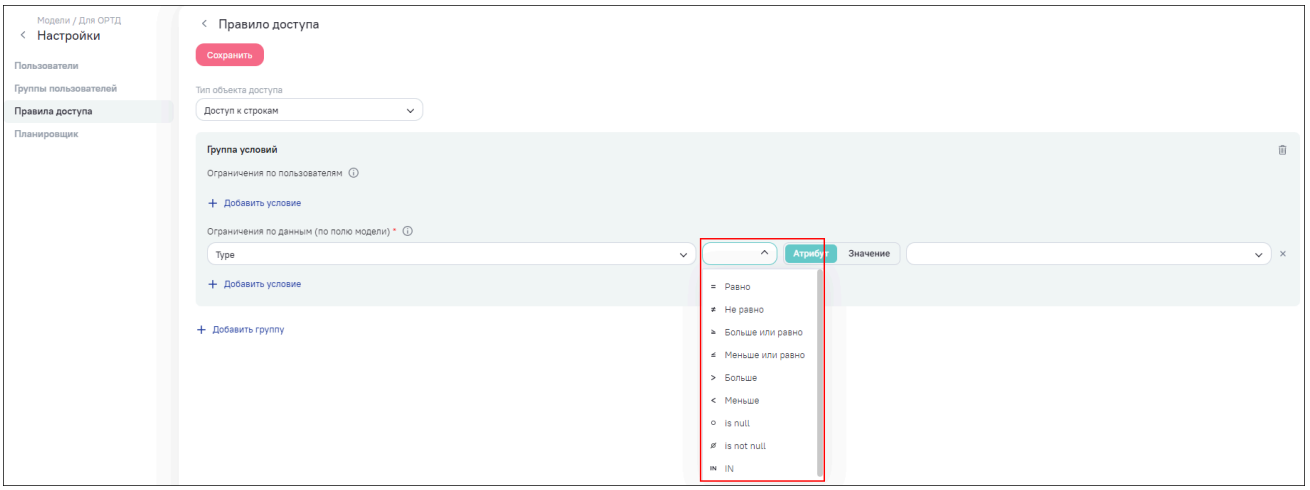


Рисунок 77 – Выбор оператора сравнения в блоке «Ограничения по данным (по полю модели)»

- вид сравнения (Рисунок 78):
  - «Значение» – для ввода в следующем поле константы, с которой будет сравниваться атрибут пользователя;
  - «Атрибут» – для выбора поля из модели (к которой ограничивается доступ), с которым будет сравниваться атрибут пользователя.

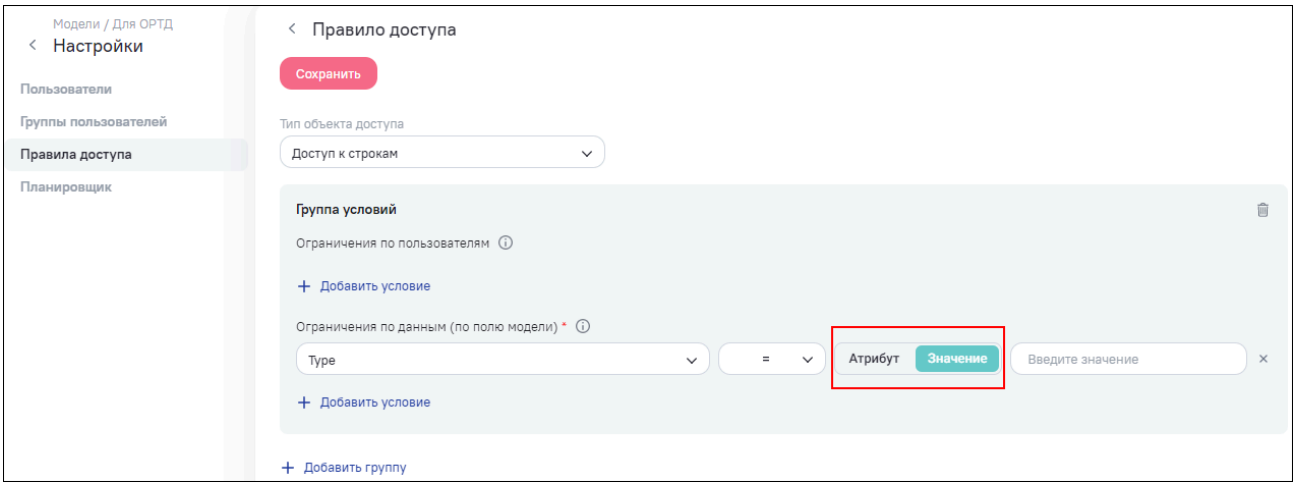


Рисунок 78 – Выбор вида сравнения в блоке «Ограничения по данным (по полю модели)»

- атрибут пользователя или постоянное значение, с которым будет сравниваться значение в поле модели. Введите значение с клавиатуры (если вид сравнения

«Значение») или выберите из выпадающего списка (если вид сравнения «Атрибут») (Рисунок 79).

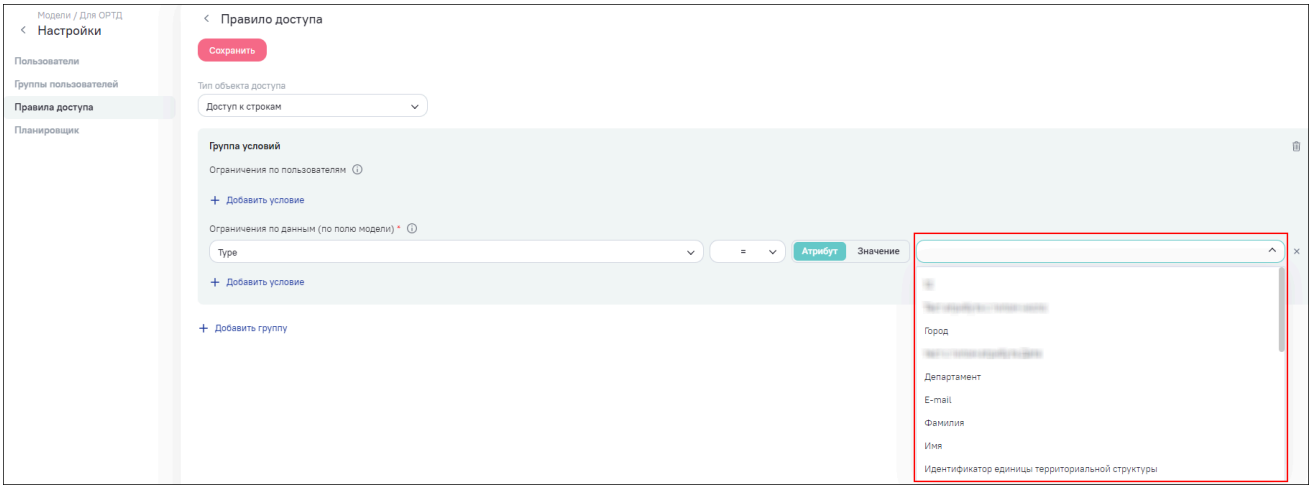


Рисунок 79 – Выбор атрибута пользователя в блоке «Ограничения по данным (по полю модели)»

В составе одного правила может быть введено одно или несколько условий в одной группе либо несколько условий в разных группах, при этом:

- условия, введенные в каждой группе, объединяются по принципу логического «И» – доступ к строке данных будет предоставлен только при выполнении всех условий, или логического «ИЛИ» – доступ к строке данных будет предоставлен при выполнении одного из условий;
- группы условий объединяются между собой по принципу логического «ИЛИ» – доступ к строке данных будет предоставлен при выполнении любой из заданных групп условий.

На рисунке (Рисунок 80) настроено правило, при котором пользователям будет предоставлен доступ к данным их региона и дочерних структур, кроме пользователей из региона 12, для которых будет предоставлен доступ к данным только их собственного региона.

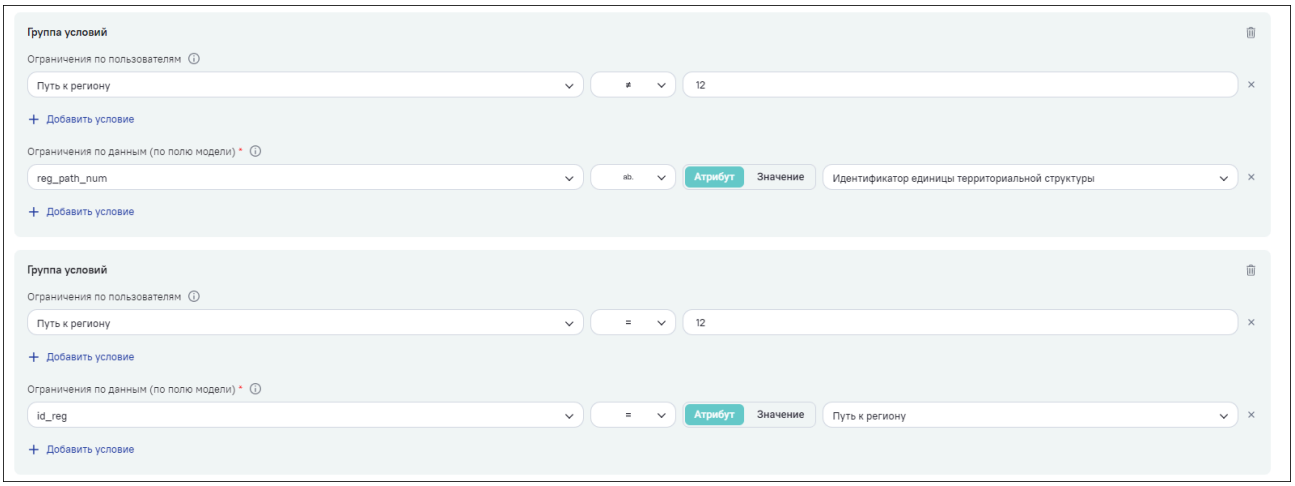


Рисунок 80 – Настроенное правило доступа с использованием групп условий

5.4.5.2 Изменение существующего правила доступа

Чтобы перейти в окно редактирования и изменить существующее правило, дважды нажмите левой кнопкой мыши по строке данного правила в списке правил (см. Рисунок 71). Операции и интерфейс изменения существующего правила ограничения доступа аналогичны описанным действиям по созданию нового правила (см. п. 5.4.5.1).

5.4.5.3 Применение нескольких правил

Если для доступа к модели создано несколько отдельных правил (см. п. Рисунок 71), то при формировании итоговых доступов пользователя все заданные отдельными правилами ограничения будут соединяться операцией логического умножения (логическое «И»), то есть к доступу будут применяться все ограничения из отдельных правил.

5.4.5.4 Удаление правил

Чтобы удалить одно или несколько из существующих правил, выполните следующие действия:

1) выберите в списке удаляемые правила установкой «флажка»;
2) нажмите на кнопку «Удалить»;
3) подтвердите действие в открывшемся окне (Рисунок 81).

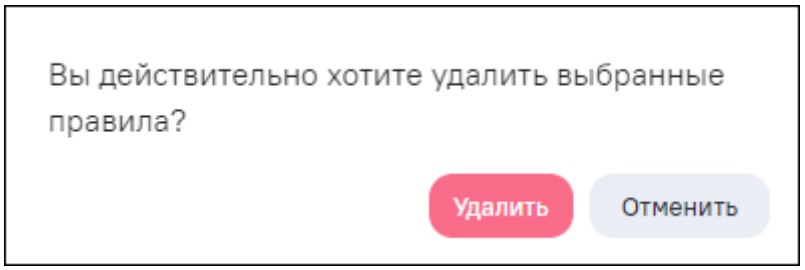


Рисунок 81 – Подтверждение операции удаления правил доступа

5.4.5.5 Применение изменений правил

Применение изменений правил по отношению к пользователям происходит сразу после их сохранения. Вход и выход пользователей в Систему (перелогинивание) для этого не требуются.

При выполнении операции замены одного правила на другое необходимо помнить, что после удаления правила все связанные с ним ограничения также удаляются и пользователи получат полный доступ к данным. Аналогичная ситуация может возникнуть при некорректном изменении правила. Поэтому рекомендуется вначале создать новое (заменяющее) правило, а после удалять существующее.

5.4.6 Сценарии настройки атрибутного доступа

Сценарии настройки атрибутного доступа представлены в таблице ниже (Таблица 4).

Таблица 4 – Сценарии настройки атрибутного доступа

Состояние внешнего провайдера	**Состояние внутреннего провайдера «Система»**	**Этапы настройки атрибутного доступа**
Не активный (или отсутствует)	Активный	– настройка модели данных «user_permissions»; – настройка схемы доступов; – настройка внутреннего провайдера «Система» на вкладке «Маппинг схемы»; – настройка правил доступа к данным пользовательской модели

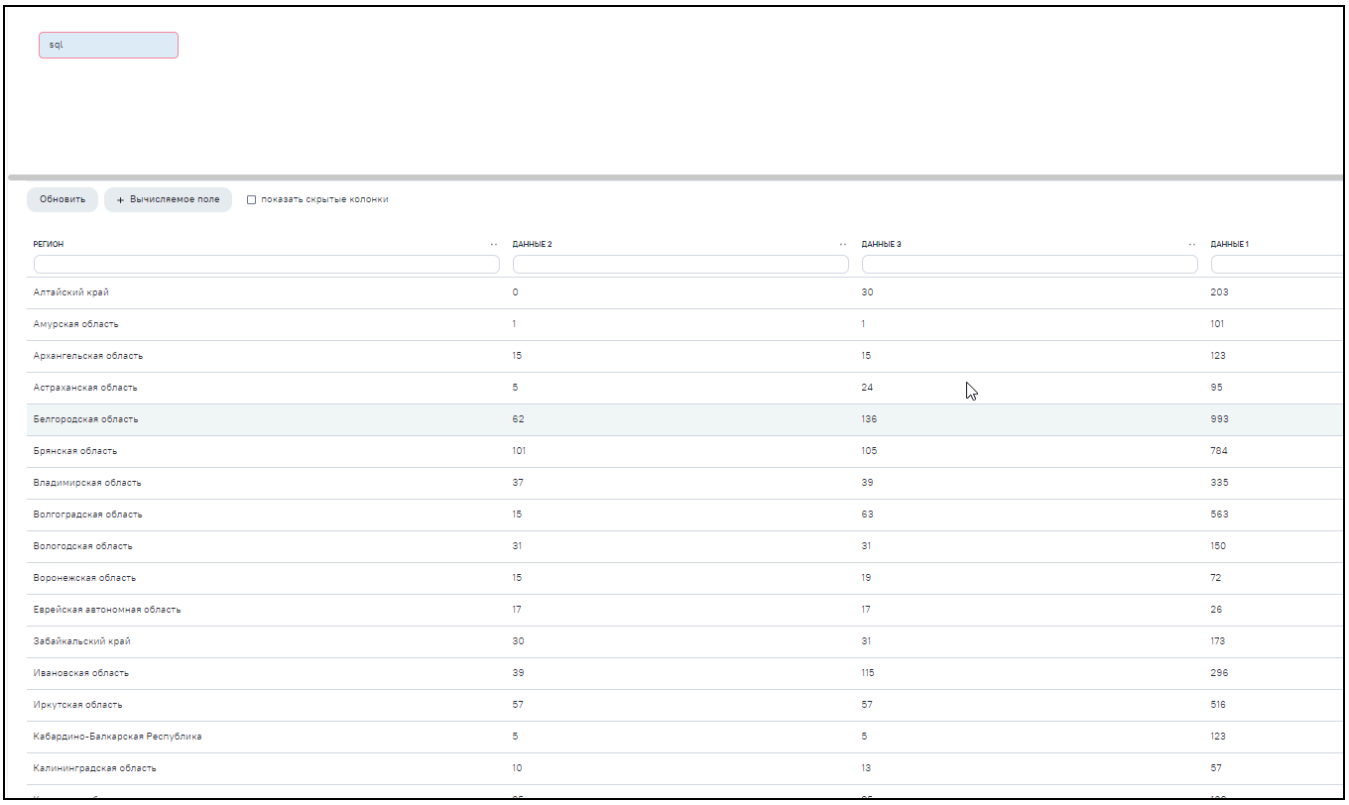
Состояние внешнего провайдера	Состояние внутреннего провайдера «Система»	Этапы настройки атрибутного доступа
Активный	Активный (локальная аутентификация разрешена)	– настройка схемы доступов; – настройка модели данных «user_permissions»; – настройка внутреннего провайдера «Система» на вкладке «Маппинг схемы»; – настройка внешнего провайдера на вкладках «Маппинг схемы» и «Маппинг атрибутов»; – настройка правил доступа к данным пользовательской модели
Активный	Не активный (локальная аутентификация запрещена)	– настройка схемы доступов; – настройка внешнего провайдера на вкладках «Маппинг схемы» и «Маппинг атрибутов»; – настройка правил доступа к данным пользовательской модели

5.4.7 Пример применения правил атрибутного доступа

В п. 5.4.7.1 – 5.4.7.7 приведен пример настройки правил атрибутного доступа для пользователей внутреннего провайдера «Система» с типом «user_permissions», иллюстрирующий изложенные выше принципы.

5.4.7.1 Исходная задача

Необходимо ограничить доступ к данным по территориальной принадлежности. Есть источник и модель «Модель А», содержащая данные из источника, извлекаемые SQL-запросом. В самих данных есть столбец, содержащий названия региона России, к которому относятся значения в строке (Рисунок 82).



РЕГИОН	ДАННЫЕ 2	ДАННЫЕ 3	ДАННЫЕ 1
Алтайский край	0	30	203
Амурская область	1	1	101
Архангельская область	15	15	123
Астраханская область	5	24	95
Белгородская область	62	136	993
Брянская область	101	105	784
Владимирская область	37	39	335
Волгоградская область	15	63	563
Вологодская область	31	31	150
Воронежская область	15	19	72
Еврейская автономная область	17	17	26
Забайкальский край	30	31	173
Ивановская область	39	115	296
Иркутская область	57	57	516
Кабардино-Балкарская Республика	5	5	123
Калининградская область	10	13	57

Рисунок 82 – Данные, к которым будет предоставляться (ограничиваться) доступ и их привязка к регионам

Необходимо обеспечить доступ:

- пользователям центрального аппарата – к данным по всем регионам;
- пользователям регионов – к данным только своего собственного региона.

Чтобы выстроить такие разрешения, необходимо:

1) расширить данные исходной таблицы недостающей информацией об иерархии регионов;
2) обеспечить в информации о пользователях (в данных модели «user_permissions») сведения о принадлежности пользователя региону и ветке иерархии, содержащей данный регион.

5.4.7.2 Настройка модели данных «user_permissions»

Источником данных о пользователях и их территориальной привязке является Excel-файл. Данные сохранены в источнике в виде следующей структуры таблиц (листов) (Таблица 5).

Таблица 5 – Структура источника данных

Таблица (Лист)	Поле	Тип данных	Пример наполнения	Описание поля
Территориальная структура	ID_reg	Целое число	2	Идентификатор единицы территориальной структуры
Территориальная структура	Название	Строка	Нижегородская область	Название единицы территориальной структуры
Территориальная структура	Parent_ID_reg	Целое число	1	Идентификатор «родительской» единицы территориальной структуры
Территориальная структура	Reg_path_num	Строка	1;2;	«Путь» – последовательность идентификаторов единиц территориальной структуры, составляющих ветку от корневого до данного элемента
Пользователи	login	Строка	Maslow	Логин (обеспечивает связку с системным справочником пользователей)
Пользователи	ФИО	Строка	Маслов	ФИО (или иная дополнительная информация о пользователе)
Пользователи	ID_reg	Целое число	4	

Таблица «Территориальная структура» содержит информацию об иерархической структуре регионов (Таблица 6).

Таблица 6 – Информация таблицы «Территориальная структура»

ID_reg	Название территории	Parent_ID_reg	Reg_path_num
1	Российская Федерация		1;
2	Нижегородская область	1	1;2;
3	Республика Татарстан	1	1;3;

ID_reg	Название территории	Parent_ID_reg	Reg_path_num
4	Удмуртская Республика	1	1;4;
5	Ярославская область	1	1;5;

Иерархия регионов сохранена в поле REG_PATH_NUM, содержащем последовательность ID_REG для всей ветки территориальной структуры от корневого ID_REG = 1 (Российская Федерация) до ID_REG данного региона. В качестве разделителя в данной строке используется символ «;». Данный разделитель также обязательно должен присутствовать в конце значения в REG_PATH_NUM (даже если это значение содержит только 1 элемент, например: «1;» для позиции «Российская Федерация»).

Таблица «Пользователи» содержит логины пользователей и привязки к регионам (Таблица 7).

Таблица 7 – Данные таблицы «Пользователи»

login	ФИО	ID_reg
Ivanov	Иванов	1
Petrov	Петров	2
Stepanova	Степанова	3
Maslow	Маслов	4
Znamenskii	Знаменский	5

На основании этих данных администратором Системы создается следующая структура модели «user_permissions» (Рисунок 83).

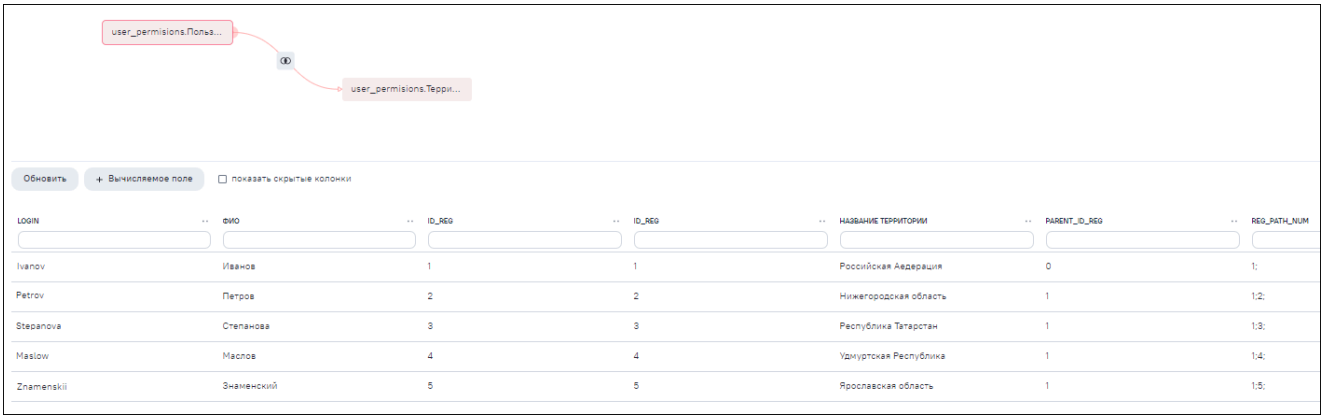


Рисунок 83 – Структура модели «user_permissions» для примера

В основе – данные таблицы «Пользователи». Они дополнены данными таблицы «Территориальная структура» на основе связи по равенству поля ID_REG. В результате для каждого пользователя добавлено название его региона и значение REG_PATH_NUM.

5.4.7.3 Дополнение «Модели А» информацией об иерархии регионов

Таблица «Территориальная структура» используется также для дополнения данных «Модели А» информацией об иерархии регионов (Рисунок 84). Эту операцию может выполнить пользователь, создавший данную модель или имеющий права на ее редактирование. В примере добавлен тип связи таблиц «inner join». Это ограничивает состав строк в модели данных только теми регионами, к которым привязаны пользователи.

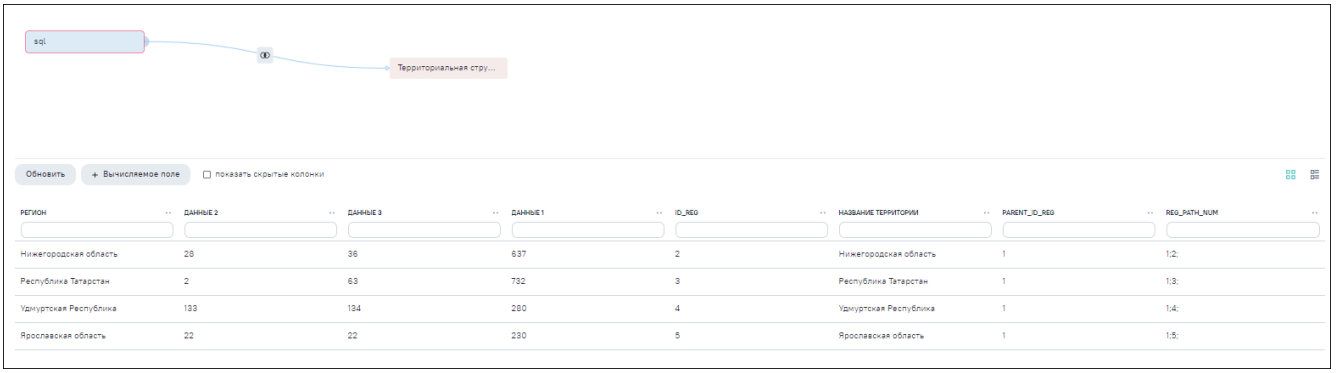


Рисунок 84 – Структура «Модели А» с привязанной таблицей «Территориальная структура» и ограничением только регионами к которым привязаны пользователи

5.4.7.4 Настройка схемы доступа

Администратор Системы или пользователь, наделенный административными правами через встроенную системную группу «Администратор», производит настройку схемы доступов. В примере добавлен атрибут доступа REG_PATH_NUM (Рисунок 85).

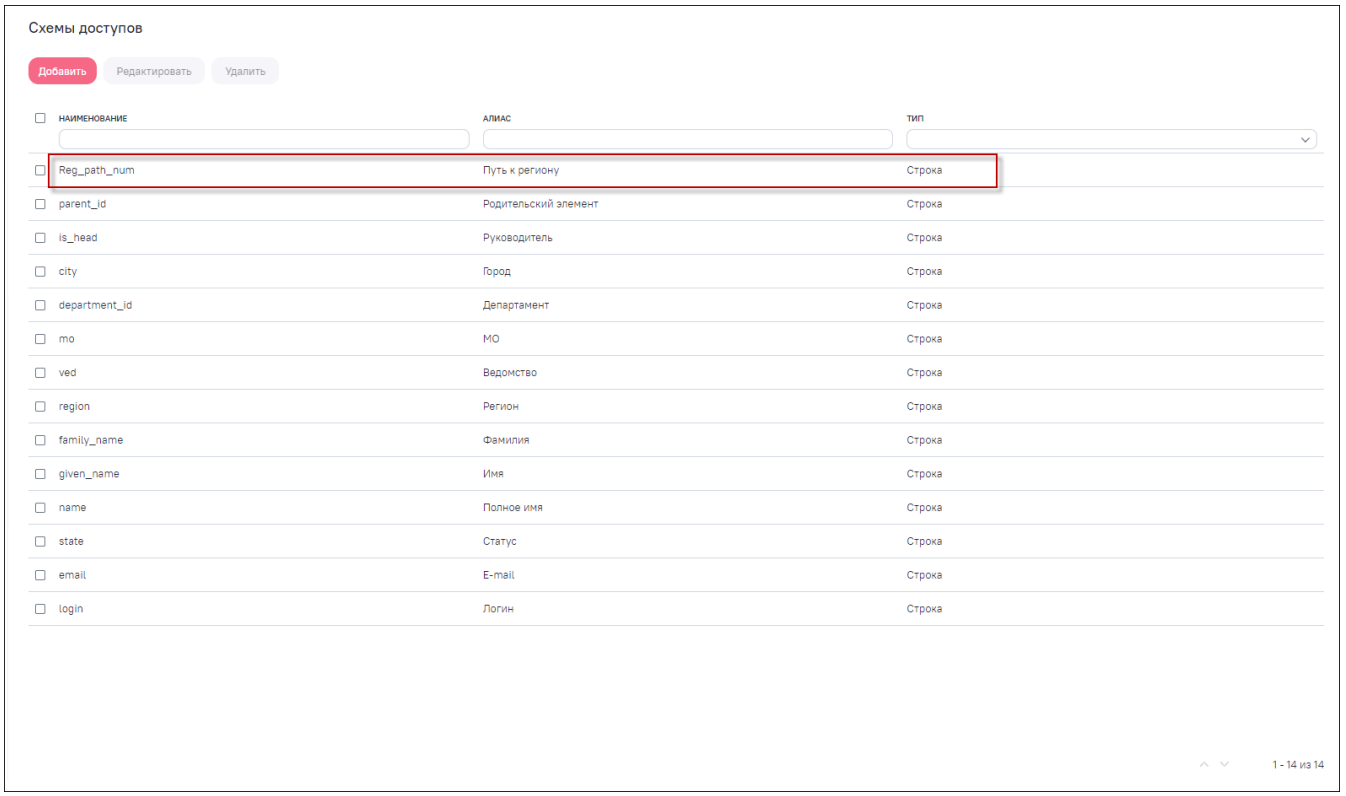


Рисунок 85 – Настройка схемы доступа – добавление атрибута по иерархии регионов

5.4.7.5 Настройка маппинга атрибутов доступа схемы и провайдера

Администратор Системы или пользователь, наделенный административными правами через встроенную системную группу «Администратор», производит настройку внутреннего провайдера. В примере в карточке редактирования внутреннего провайдера на вкладке «Маппинг схемы» добавлено соответствие атрибуту доступа по иерархии регионов REG_PATH_NUM к полю модели «user_permissions» REG_PATH_NUM (Рисунок 86).

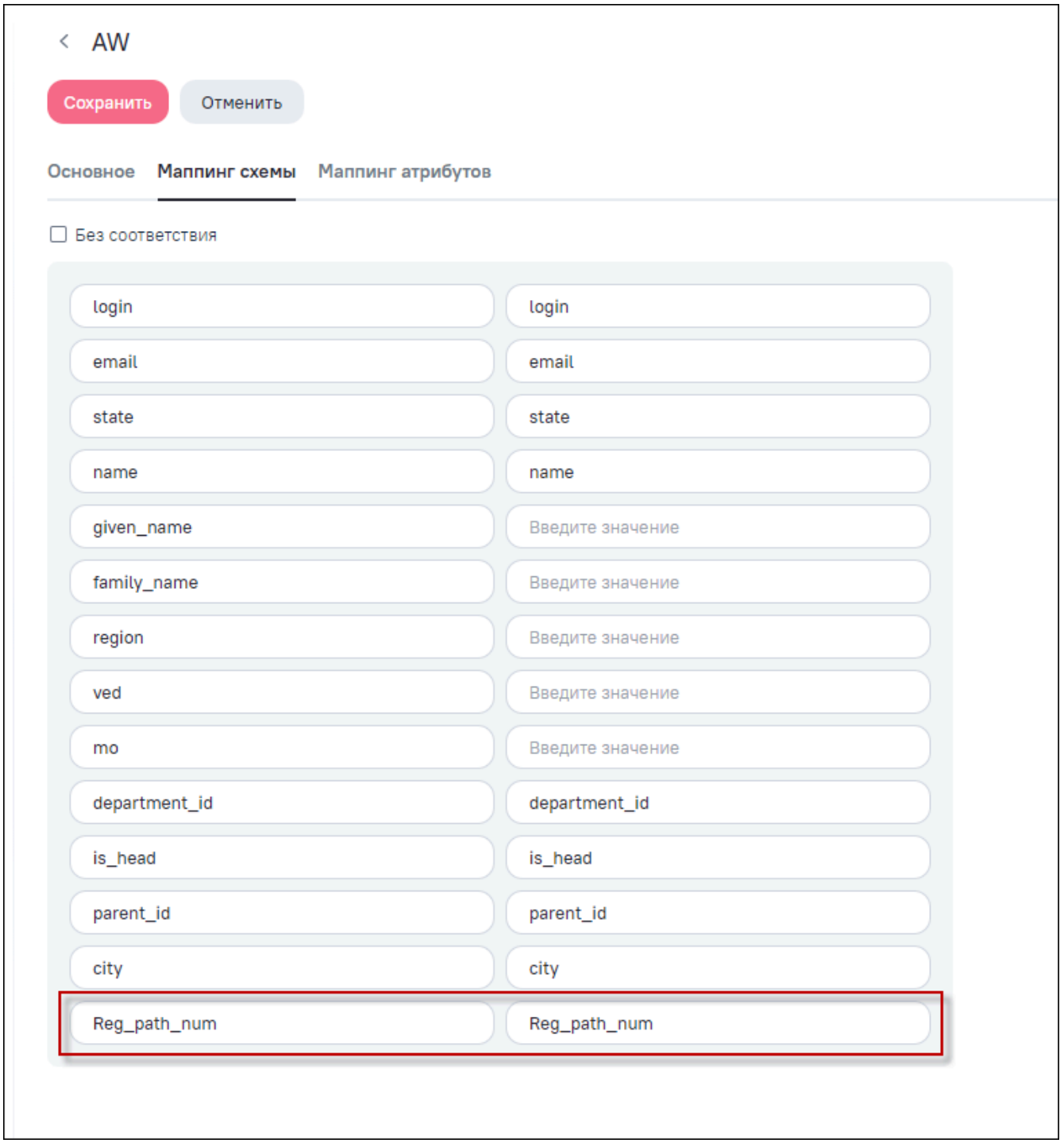


Рисунок 86 – Настройка внутреннего провайдера – добавление соответствия атрибуту доступа по иерархии регионов к полю модели «user_permissions»

5.4.7.6 Настройка правил доступа к данным «Модели А»

В интерфейсе настройки правил доступа к данным модели (см. п. 5.4.5) для реализации поставленных целей создайте единственное правило «Данные по своему

региону» (Рисунок 87), содержащее условие: значение поля модели REG_PATH_NUM включает значение атрибута пользователя «Путь к региону» (REG_PATH_NUM).

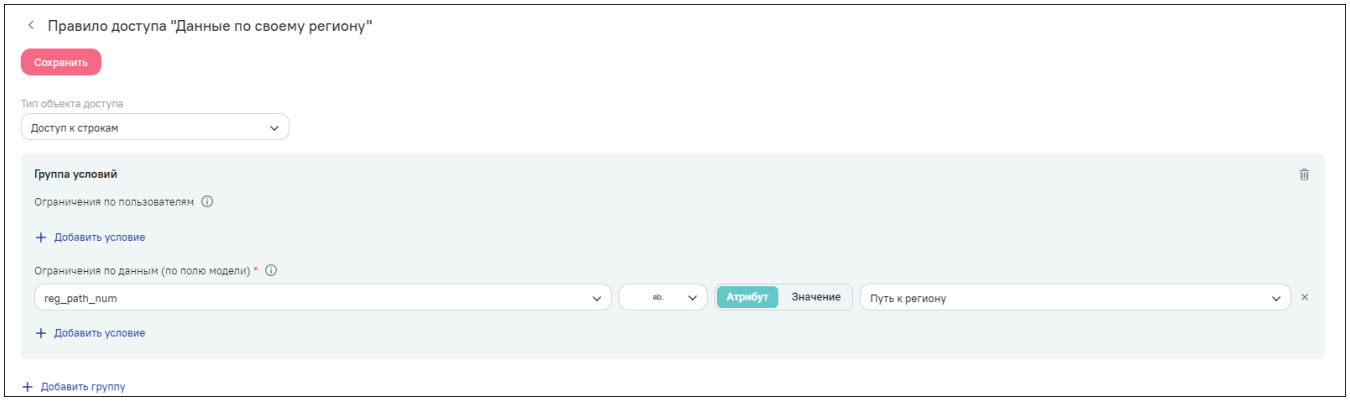


Рисунок 87 – Правило «Данные по своему региону»

5.4.7.7 Результат применения настроенного правила доступа к данным «Модели А»

Пользователь Ivanov отнесен к региону 1 («Российская Федерация»). Значение его атрибута REG_PATH_NUM = '1;'. Данный текст присутствует в значениях свойства REG_PATH_NUM всех регионов (всех строк данных «Модели А»). Поэтому пользователь получает доступ ко всем данным в виджетах (Рисунок 88).

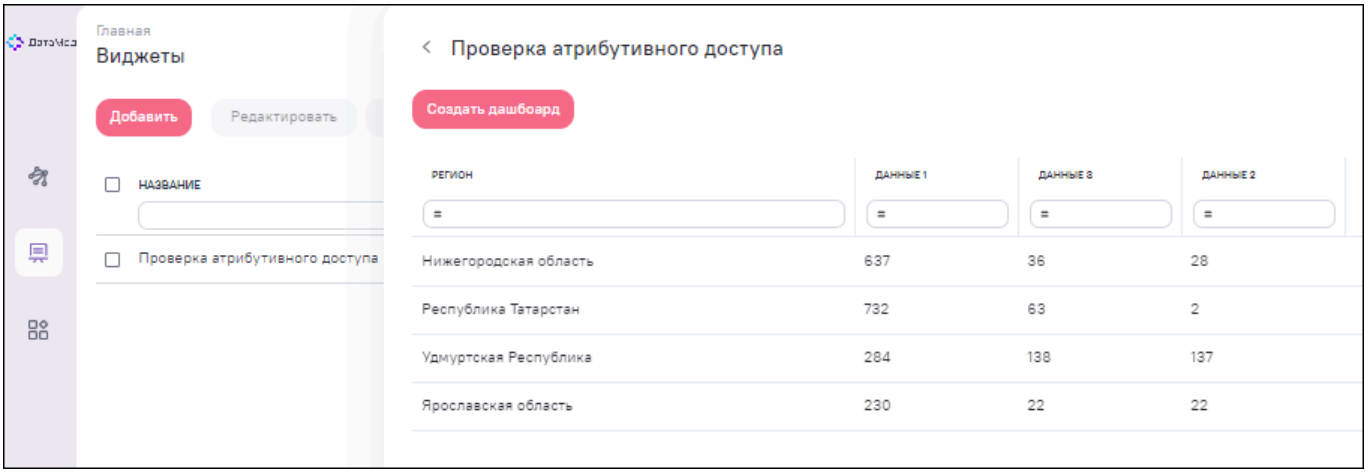


Рисунок 88 – Данные доступные пользователю Ivanov («Российская Федерация»)

Пользователь Petrov отнесен к региону 2 («Нижегородская область»). Значение его атрибута REG_PATH_NUM = '1;2;'. Данный текст присутствует в значениях свойства REG_PATH_NUM только для записи региона 2 («Нижегородская область»). Поэтому пользователь получает только доступ к данным региона (Рисунок 89).

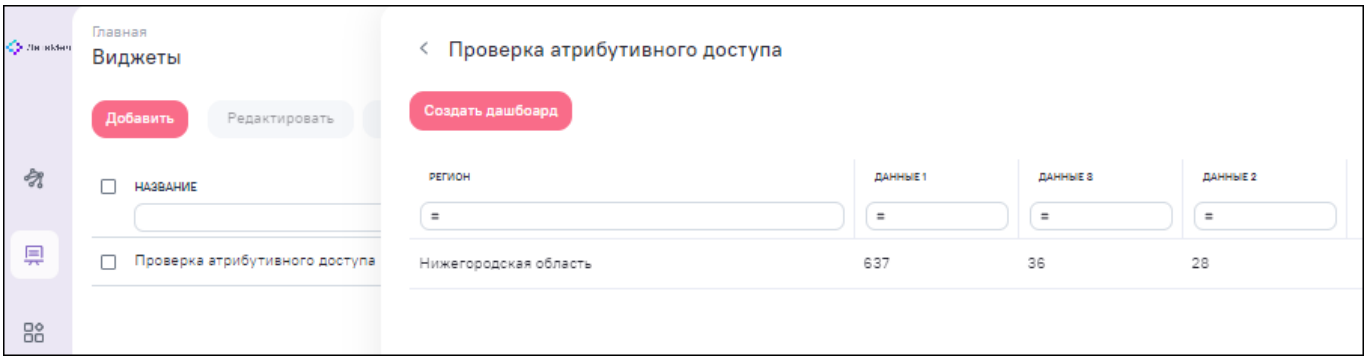


Рисунок 89 – Данные доступные пользователю Petrov («Нижегородская область»)

Остальные введенные в примере пользователи аналогично пользователю Petrov получают доступ только к данным «своих» регионов.

При наличии в «Модели А» информации по дочерним по отношению к регионам уровням (например, городам или районам) пользователи регионов также получили бы доступ и к этим данным в соответствии с тем же принципом, по которому пользователь Ivanov получил доступ ко всем входящим в «Российскую Федерацию» регионам.

Заданные ограничения действуют для виджетов, построенных на данных «Модели А»:

- для виджетов:
  - в интерфейсе их просмотра;
  - в интерфейсе их редактирования;
  - в интерфейсе их просмотра по прямой ссылке.
- для информационных панелей:
  - в интерфейсе их просмотра;
  - в интерфейсе их редактирования;
  - в интерфейсе их просмотра по прямой ссылке.

5.5 Центр управления приложением

В функции администратора Системы входят задачи управления:

- информацией о Системе (см. п. 5.5.1);
- лицензиями (см. п. 5.5.2);
- конфигурациями приложения (подробное описание по конфигурированию Системы приведено в Инструкции по развертыванию и обновлению Программы для ЭВМ «ДатаМед»);
- обслуживанием Системы (подробное описание по обновлению Системы приведено в Инструкции по развертыванию и обновлению Программы для ЭВМ «ДатаМед»);
- экспортом/импортом данных (см. п. 5.5.3);
- переменными окружения (см. п. 5.5.4).

Для перехода в центр управления Системой в адресной строке web-браузера добавьте в конце ссылки на Систему латинские буквы «cc».

Например, для приложения **https://datamed-demo/** раздел «Центр управления приложением» открывается по ссылке **https://datamed-demo/cc**.

После ввода нужного адреса в строке web-браузера откроется окно входа в центр управления (Рисунок 90). Раздел доступен пользователю, наделенному правами администратора.

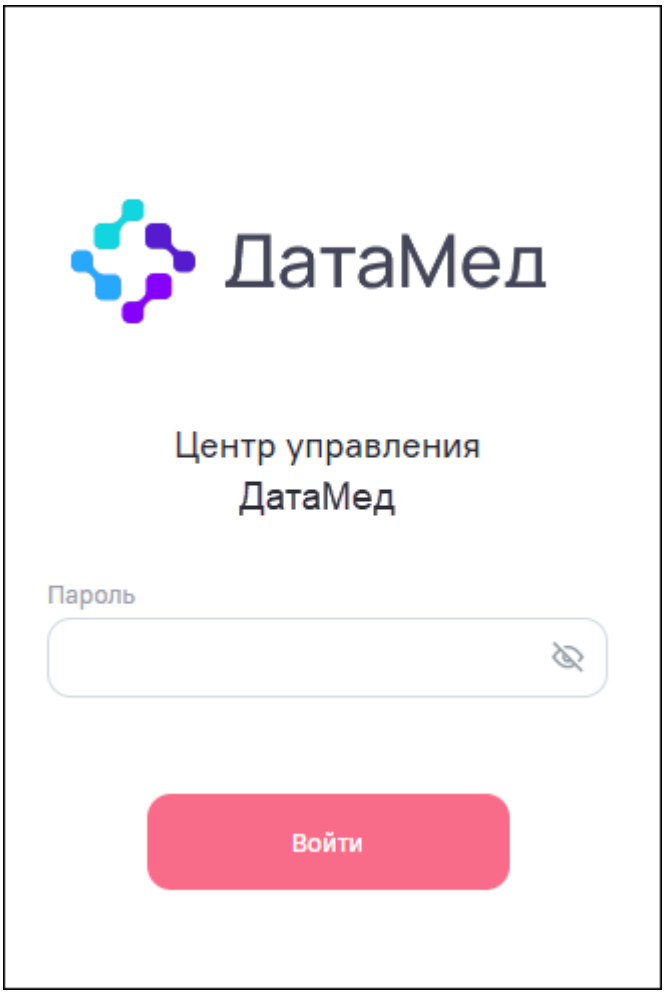


Рисунок 90 – Окно входа в центр управления

Введите пароль и нажмите на кнопку «Войти».

Откроется окно «Центр управления» на вкладке «Система» (Рисунок 91).

Примечание – Пароль для входа в центр управления приложением задается в .env файле.

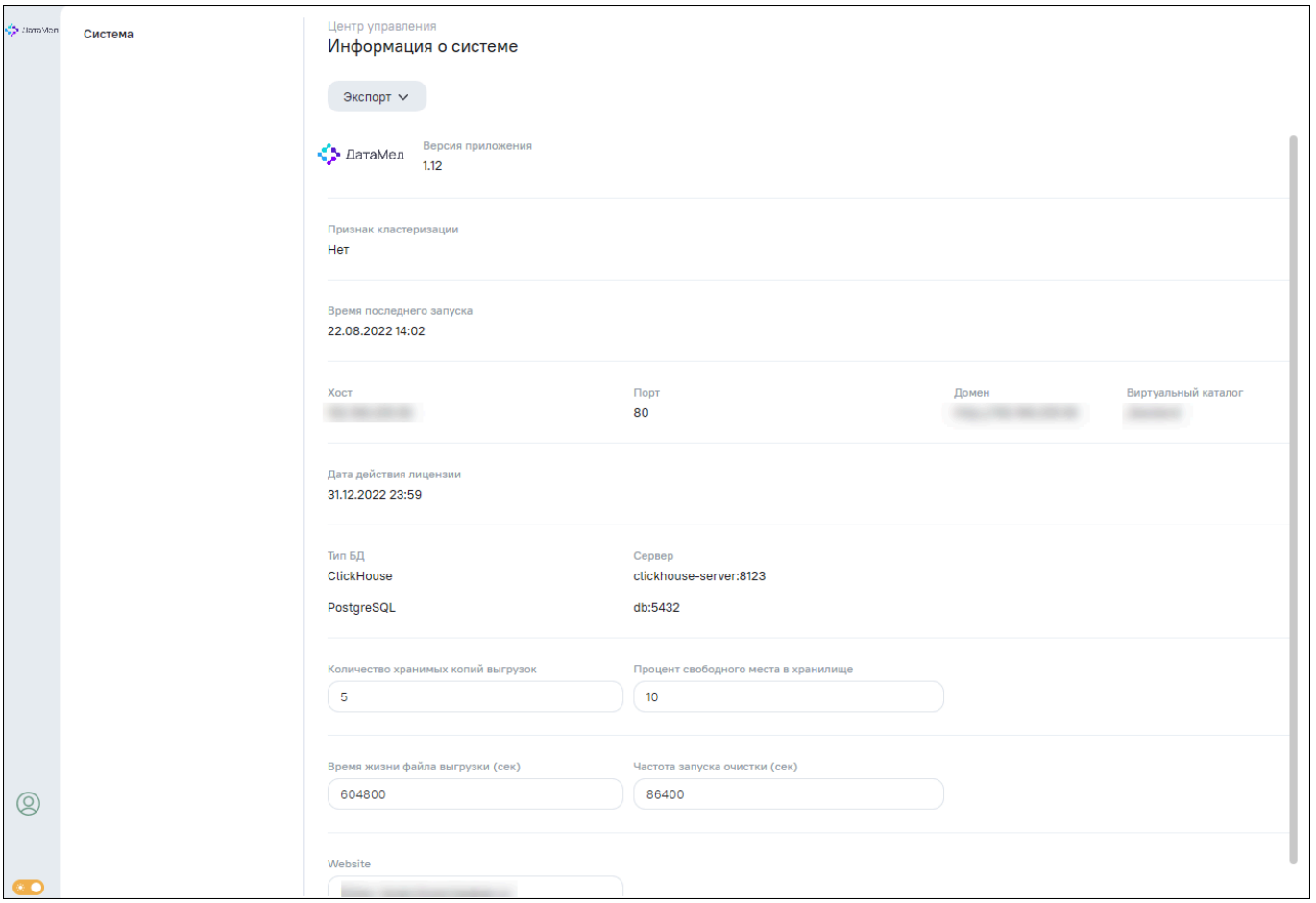


Рисунок 91 – Окно «Центр управления», вкладка «Система»

5.5.1 Система

На вкладке «Система» (см. Рисунок 91) отображается информация о Системе в следующих полях:

- «Версия приложения» – данные доступны только для просмотра;
- «Признак кластеризации» – данные доступны только для просмотра;
- «Время последнего запуска» – данные доступны только для просмотра;
- «Хост» – данные доступны только для просмотра;
- «Порт» – данные доступны только для просмотра;
- «Домен» – данные доступны только для просмотра;

- «Виртуальный каталог» – данные доступны только для просмотра;
- «Дата действия лицензии» – данные доступны только для просмотра;
- «Тип БД» – данные доступны только для просмотра;
- «Сервер» – данные доступны только для просмотра;
- «Количество хранимых копий выгрузок» (параметр «count_of_stored_files») – измените значение при необходимости, по умолчанию установлено значение «5». При превышении лимита реализуется метод по удалению старого неактуального набора данных по текущему объекту Системы данного пользователя;
- «Процент свободного места в хранилище» (параметр «free_storage_space») – измените значение при необходимости, по умолчанию установлено значение «10». Позволяет резервировать свободное место в хранилище для работы Системы;
- «Время жизни файла выгрузки (сек)» (параметр «file_lifetime») – измените значение при необходимости, по умолчанию установлено значение «604800» (7 дней). Проверяется по cron, по истечении срока реализуется механизм удаления старых данных из хранилища. Время указывается в секундах, если параметр равен «0» или значение не указано, то считается, что установлено значение «Неограниченное время жизни выгрузки», т.е. разрешено хранение всех версий выгрузок неограниченное количество времени;
- «Частота запуска очистки (сек)» (параметр «storage_cleared_start_interval») – измените значение при необходимости, по умолчанию установлено значение «86400» (1 день). Запускается принудительный механизм очистки хранилища:
  - сначала очищается хранилище от копий, остаются только последние выгрузки пользователя по объектам Системы (на один объект Системы по одной выгрузке);

- если необходимое место не освобождено, то удаляются самые старые файлы до тех пор, пока не будет освобождено необходимое пространство, регулируемое параметром «free_storage_space».

- «Website» – измените значение при необходимости.

Для выгрузки информации о Системе нажмите на кнопку «Экспорт» и в выпадающем списке выберите пункт «Экспорт информации» (Рисунок 92). На ПК выгрузится файл формата .csv.

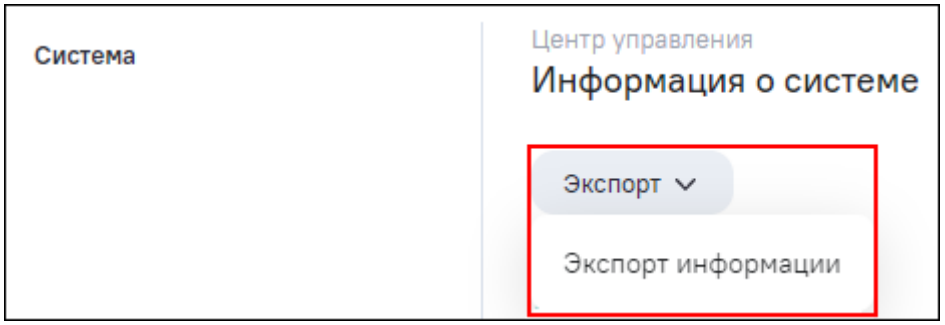


Рисунок 92 – Кнопка «Экспорт» на вкладке «Система»

При необходимости измените адрес сайта Системы в поле «Website». При нажатии на ссылку «Официальный сайт» в окне авторизации (см. Рисунок 2) откроется сайт с адресом, указанным в поле «Website».

5.5.2 Лицензия

5.5.2.1 Установка и обновление файла лицензии

Примечание – Доступ к функциональности осуществляется через сервер.

Скопируйте выданный файл лицензии в каталог «/opt/aw/file_storage/licence» (лицензия должна быть выдана на URL, указанный в строке FRONTEND_URL, и совпадать с URL, через который будет осуществляться вход в Систему в web-браузере):

```
cp /path/to/licence.lic /opt/aw/file_storage/licence
#Необходимо, чтобы у файла licence.lic был владелец 1000:1000
chown 1000:1000 /opt/aw/file_storage/licence/licence.lic
chmod 660 /opt/aw/file_storage/licence/licence.lic
```

5.5.2.2 Ограничения триального доступа к Системе

Триальный доступ к Системе – это ограниченный доступ к Системе в рамках демонстрационной версии программного обеспечения Системы.

Для задания необходимых ограничений в конфигурационный файл .env добавьте переменные, перечисленные в таблице ниже (Таблица 8).

Таблица 8 – Переменные для ограничений работы пользователей с триальным доступом к Системе

Код	Наименование	Значение по умолчанию	Примечание
TRIAL_USER_ACTIVE_DAY_COUNT	Количество дней активности пользователя	14	Если задана переменная, то при создании нового пользователя демонстрационной версии программного обеспечения и после его первого входа в Систему отсчитывается количество дней и проверяется, чтобы оно не превысило допустимого лимитного значения. Когда время активности истекло, происходит автоматическая блокировка пользователя
TRIAL_CLEAR_DATA_DAY_COUNT	Количество дней до запуска очистки хранилища от объектов заблокированного пользователя	14	После автоматической блокировки пользователя демонстрационной версии программного обеспечения устанавливается отсчет дней до запуска процесса очистки хранилища от всех объектов пользователя демонстрационной версии программного обеспечения
TRIAL_USER_MODEL_COUNT	Количество моделей на одного пользователя	5	Указывается количество моделей, допустимое к созданию одним пользователем демонстрационной версии программного обеспечения
TRIAL_USER_FILE_DATA_SOURCE_COUNT	Количество файловых источников на одного пользователя	5	Указывается количество файловых источников, допустимое к созданию одним пользователем демонстрационной версии программного обеспечения
TRIAL_FILE_DATA_SOURCE_SIZE	Предельный объем каждого файлового источника	100 МБ	Указывается ограничение на размер импортируемого файла с данными для пользователей демонстрационной версии программного обеспечения
TRIAL_MODEL_SIZE	Предельный объем каждой модели	524 МБ	Указывается ограничение на размер импортируемой модели в хранилище Системы. **Примечание** – Распространяется на всех пользователей Системы
TRIAL_USER_SHARE	Запрет на предоставление прав к объекту	true	Указывается одно из значений:

Код	Наименование	Значение по умолчанию	Примечание
	отдельным пользователям		– true – для применения ограничений к учетным записям пользователей, для которых определен триальный доступ; – false – для снятия ограничений на предоставление прав к объекту отдельным пользователям

Для создания пользователей с триальным доступом выполните следующие действия:

1) авторизуйтесь с помощью метода API – POST /user/login:

```
{
"username": "string",
"password": "string"
}
```

где:

- username – логин пользователя, учетная запись которого наделена правами администратора;
- password – пароль пользователя.

2) добавьте новую учетную запись пользователя с триальным доступом через метод API – POST /user/create:

```
{
"login": "string",
"email": "string",
"password": "string",
"ldap": 0,
"state": 1,
"is_trial": true
}
```

где:

- login – логин пользователя с триальным доступом;
- password – пароль пользователя;

- email – электронная почта нового пользователя;
- ldap – необходимость проверки через LDAP сервер, принимает значения «0» или «1» (значение «1» – аутентификация происходит через LDAP сервер, значение «0» – аутентификация проходит через внутренний локальный провайдер с типом «user_permissions»);
- state – признак активной учетной записи, принимает значения «0» или «1» (значение «1» – активный, значение «0» – заблокированный);
- is_trial – метка триального доступа.

Для получения информации по дате завершения пробного периода выполните следующие действия:

3) авторизуйтесь с помощью метода API – POST /user/login:

```
{
"username": "string",
"password": "string"
}
```

где:

- username – логин пользователя, учетная запись которого наделена правами администратора;
- password – пароль пользователя.

4) получите дату завершения пробного периода через метод API – GET /user/trial-info, указав логин пользователя с триальным доступом.

5.5.3 Экспорт и импорт данных

5.5.3.1 Экспорт и импорт данных объектов с помощью консольных команд

Примечание – Доступ к функциональности осуществляется через сервер.

Для сотрудников службы DevOps и администраторов Системы доступна функциональность по экспорту данных с одного приложения и импорт выгруженных данных на стенд другого приложения.

Для запуска экспорта перейдите в запущенный контейнер backend и выполните команду:

1) для экспорта всех объектов:

```
./yii export {zip}
```

2) для экспорта объектов, связанных с определенными моделями:

```
./yiiexport/by-models {zip} {models}
```

3) для экспорта объектов пользователя:

```
./yii export/by-user {zip} {login}
```

где:

- {zip} – принимает значения 0 или 1 (если указано значение 1, то в архив добавляются и файлы файловых источников);
- {models} – идентификаторы моделей перечисленные через запятую, не обязательный параметр. Если параметр указан – будет выполнена выгрузка только по источникам, виджетам и дашбордам указанных моделей, в ином случае – выгрузка всего содержимого стенда (вариант экспорта 1);
- {login} – login пользователя (выгружаются объекты, автором которых является указанный пользователь).

Файл с дампом будет находиться внутри контейнера backend (**/file_storage/api/import/aw_dump.zip**).

Для запуска импорта поместите экспортированный файл в папку контейнера backend (например, **/file_storage/api/import/aw_dump.zip**) и выполните команду с указанием адреса файла:

```
./yii import {path} {key} {type}
```

где:

- {path} – путь до файла, например **/file_storage/api/import/aw_dump.zip**;
- {key} – необязательный параметр, содержит логин пользователя или код группы. Если параметр указан, пользователю или группе будут предоставлены права на все импортируемые объекты;
- {type} – необязательный параметр, принимает значения:
  - u: параметр key – это логин пользователя;
  - g: то параметр key – это код группы.

После завершения импорта можно найти сформированный файл лога по пути /**file_storage/api/import/import.log**.

На все объекты, добавленные с помощью импорта, можно дать права доступа к объектам необходимым пользователям, выполнив соответствующую команду:

4) доступ пользователю:

```
./yii import/join-user {model_id} {login}
```

5) доступ пользовательской группе:

```
./yii import/join-group {model_id} {group}
```

где:

- {model_id} – идентификатор новой модели;
- {login} – логин пользователя;
- {group} – код пользовательской группы.

5.5.3.2 Экспорт и импорт данных объектов через API

Примечание – Доступ к функциональности осуществляется через Swagger.

Для администраторов Системы доступна функциональность по экспорту данных с одного приложения и импорт выгруженных данных на стенд другого приложения.

Для запуска экспорта выполните следующие действия:

1) авторизуйтесь с помощью метода API в центре управления приложением – POST /app-control-center/login:

```
{
"password": "string"
}
```

где password – пароль администратора Системы в Центре управления.

2) выполните один из следующих методов (Рисунок 93):

- для экспорта всех данных экземпляра Системы – GET /export;
- для экспорта данных по моделям – GET /export/by-models – укажите идентификаторы моделей через запятую;
- для экспорта всех данных пользователя – GET /export/by-user – укажите логин пользователя.

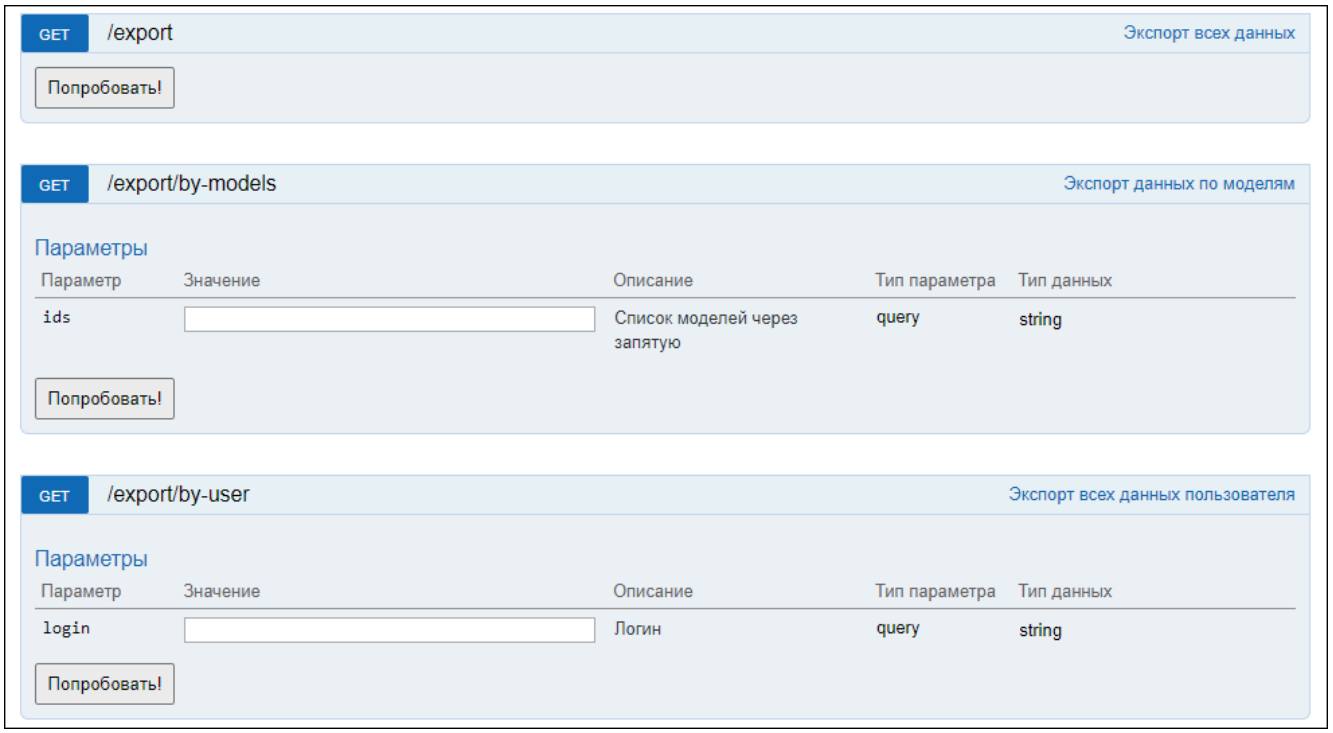


Рисунок 93 – Методы в API по экспорту данных объектов

Для запуска импорта выполните следующие действия:

1) авторизуйтесь с помощью метода API в центре управления приложением – POST /app-control-center/login:

```
{
"password": "string"
}
```

где password – пароль администратора Системы в Центре управления.

2) выполните метод POST /import/by-file – выберите файл и укажите необходимые параметры (Рисунок 94):

- {key} – необязательный параметр, содержит логин пользователя или код группы. Если параметр указан, пользователю или группе будут предоставлены права на все импортируемые объекты;
- {type} – необязательный параметр, принимает значения:
  - u: параметр key – это логин пользователя;
  - g: то параметр key – это код группы.

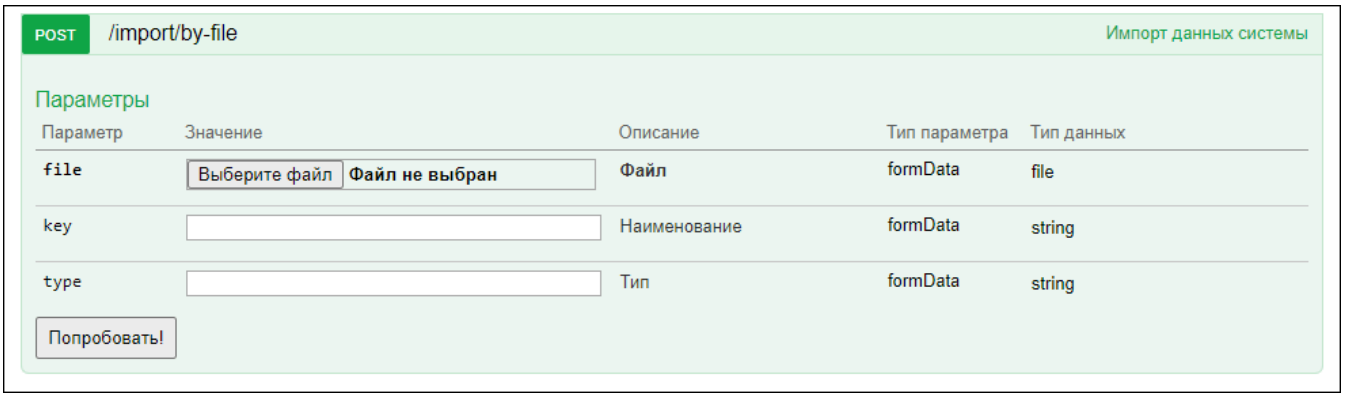


Рисунок 94 – Методы в API по импорту данных объектов

3) дайте права доступа на импортированные объекты. На все объекты, добавленные с помощью импорта, можно дать права доступа необходимым пользователям с помощью методов (Рисунок 95):

- доступ пользователю – GET /import/join-user – укажите идентификатор новой модели и логин пользователя;
- доступ группе пользователей – GET /import/join-group – укажите идентификатор новой модели и код пользовательской группы.

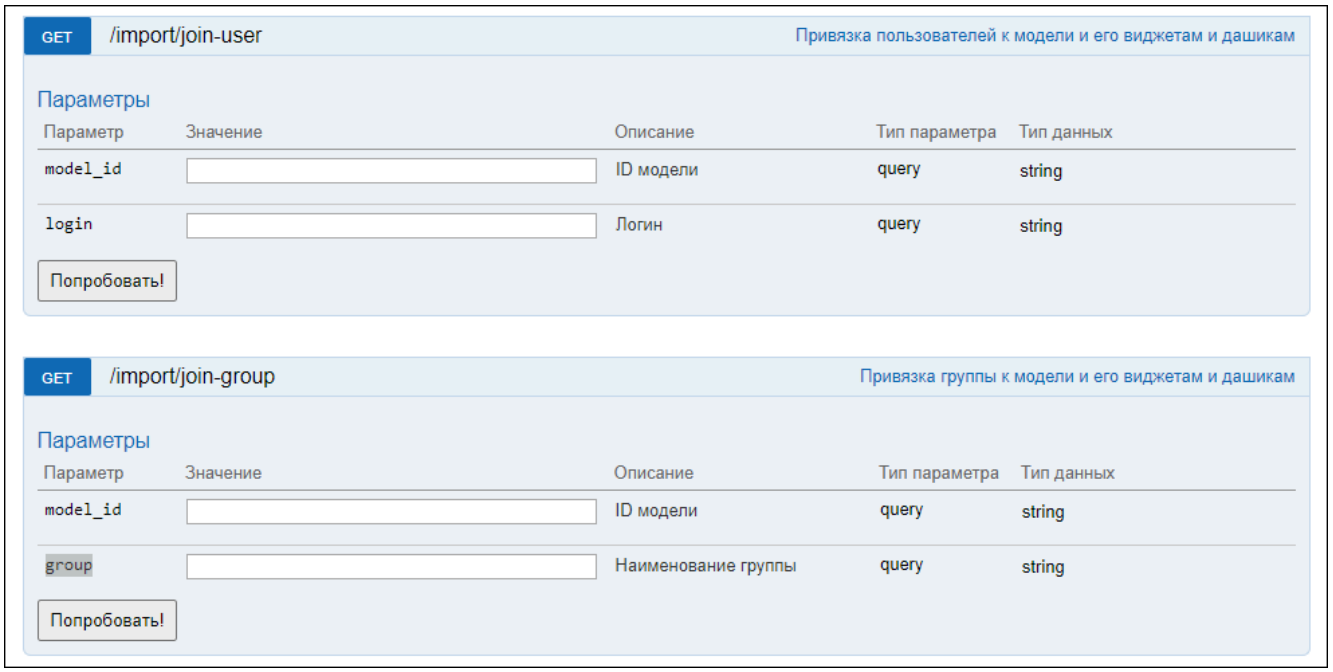


Рисунок 95 – Методы в API по предоставлению доступа к импортируемым объектам

5.5.4 Переменные

Примечание – Доступ к функциональности осуществляется через сервер.

Для задания необходимых ограничений в конфигурационный файл .env добавьте переменные, перечисленные в таблице (Таблица 9).

Таблица 9 – Переменные

Код	Наименование	Значение по умолчанию	Примечание
etl-stats			
ETL_KEEP_FILES_DAYS	Время жизни файлов в ETL	7	Указывается количество дней, после истечения которых файлы в ETL подлежат удалению
ETL_KEEP_DAGS_DAYS	Время жизни DAG в Airflow	7	Указывается количество дней, в течение которых DAG в Apache Airflow считается активным. Отсчет количества дней начинается от ближайшей из двух дат: дата создания/обновления модели; дата создания/обновления модели; дата последнего запуска синхронизации. Неактивные DAG без установленного расписания удаляются из Apache Airflow до следующего запуска синхронизации или редактирования модели
Модели			

Код	Наименование	Значение по умолчанию	Примечание
MODEL_SYNC_COUNT	Количество хранимых версий	2	Указывается количество хранимых версий таблицы модели
TRIAL_MODEL_SIZE	Предельный объем каждой модели	524 МБ	Указывается ограничение на размер импортируемых моделей в хранилище Системы
Виджеты			
AW_WIDGET_EXPORT_MAX_FILE_SIZE	Максимальный размер формируемого файла	8 ГБ	8 ГБ. Задается ограничение на размер экспортируемого файла с данными виджета. При превышении лимита в сообщение и в конец файла дописывается строка с сообщением: «Достигнут предельный размер файла, данные экспортированы не полностью»
file_lifetime	Время жизни файла выгрузки (сек)	604800	7 дней. Проверяется по cron, по истечении вызывается механизм удаления старых данных из хранилища. Время указывается в секундах. Если значение равно «0» или не указано, то считается что установлено значение «Неограниченное время жизни выгрузки», т.е. разрешено хранение всех версий выгрузок неограниченное количество времени
count_of_stored_files	Количество хранимых копий выгрузок	5	5 экземпляров. При превышении лимита вызывается механизм по удалению старого неактуального набора данных по текущему виджету данного пользователя
free_storage_space	Процент свободного места в хранилище	10	10 %. Резервируется свободное место в хранилище для работы Системы
storage_cleared_start_interval	Частота запуска очистки (сек)	86400	1 день. Запускается принудительный механизм очистки хранилища: сначала очищается хранилище от копий, остаются только последние выгрузки пользователя по виджетам (на виджет по одной выгрузке); если необходимое место не освобождено, то удаляются самые старые файлы до тех пор, пока не будет освобождено необходимое пространство, регулируемое параметром free_storage_space

6 Аварийные ситуации

6.1 Нештатные ситуации

Возникающие при работе с Системой нештатные ситуации и способы их решения описаны в таблице ниже (Таблица 10).

Таблица 10 – Описание нештатных ситуаций

Сообщение/ название ошибки	**Причина появления**	**Вывод ошибки на экране/ консоли**	**Действия пользователя/ способы устранения**
404 – not found	В адресную строку введен неверный адрес	404 – not found	Проверьте правильность ввода ссылки в адресной строке web-браузера
Ошибка валидации данных	Неверно введен логин/пароль	При авторизации в Системе отображается уведомление об ошибке: «Ошибка валидации данных». В консоли: "success":false,"error":{"code":422,"message":"Ошибка валидации данных"},"data":{"username":"Не удалось авторизоваться в системе"}}	В окне идентификации пользователя заново заполните поля «Логин» и «Пароль», предварительно проверив, не включена ли клавиша <Caps Lock> и правильность выбора раскладки языка
Файл не найден	Файл лицензии не вмонтирован	"success":false,"error":{"code":401,"message":" Лицензия: Файл не найден"}}	Обратитесь к администратору Системы
Ошибка чтения/записи	Нет прав чтения записи в файл лицензии	"success":false,"error":{"code":401,"message":"Лицензия:Ошибка чтения/записи"}}	Обратитесь к администратору Системы
Ошибка формата	Нарушение целостности данных файла лицензии и теперь его невозможно расшифровать	"success":false,"error":{"code":401,"message":"Лицензия: Ошибка формата"}	Обратитесь к администратору Системы
Срок действия лицензии еще не наступил		{"success":false,"error":{"code":401,"message":"Лицензия: Срок действия лицензии еще не наступил "}}	Обратитесь к администратору Системы
Срок действия лицензии истек		{"success":false,"error":{"code":401,"message":"Лицензия: Срок действия лицензии истек"}}	Обратитесь к администратору Системы

Сообщение/ название ошибки	Причина появления	Вывод ошибки на экране/ консоли	Действия пользователя/ способы устранения
Неверная дата	Была попытка изменения даты и времени на сервере		Обратитесь к администратору Системы
Ошибка домена	Файл лицензии не привязан к домену	{"success":false,"error":{"code":401,"message":"Лицензия: Ошибка домена"}}	Обратитесь к администратору Системы

7 Рекомендации по освоению

7.1 Вызов и загрузка Системы

Вызов и загрузка Системы осуществляется согласно алгоритму запуска Системы, описанному в п. 4.1.

7.2 Последовательность действий при работе с Системой

Последовательность действий пользователя при работе с Системой соответствует следующему алгоритму:

1) запустите web-браузер, в случае возникновения ошибки проверьте интернет-соединение;
2) осуществите вход в Систему, введя логин и пароль в соответствующие поля (подробнее см. п. 4.1);
3) выполните действия по администрированию Системы (подробнее см. п. 5);
4) выйдите из Системы, нажав кнопку «Выйти» в главном меню Системы (подробнее см. п. 4.2).

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докумменте	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	Измененных	замененных	новых	аннулированных					
