Программное обеспечение
«CrossTech Database Security»

Версия 0.2.0 © ООО «Кросстех Солюшнс Групп», 2025.06

СОДЕРЖАНИЕ

1. Общие сведения ... 3
2. Элементы интерфейса Системы ... 4
   2.1. Экраны ... 4
   2.2. Кнопки ... 6
   2.3. Поля ... 9
   2.4. Списки ... 11
   2.5. Фильтры и поиск ... 13
3. Использование Системы ... 14
   3.1. Вход в Систему ... 14
   3.2. Панель навигации ... 15
   3.3. Агенты ... 16
   3.4. Трафик ... 19
   3.5. Политики ... 22
      3.5.1. Общая информация ... 22
      3.5.2. Создание политики ... 24
      3.5.3. Управление политиками ... 30
   3.6. Базы данных ... 32
      3.6.1. Общая информация ... 32
      3.6.2. Добавление базы данных ... 34
   3.7. Регулярные выражения ... 35
      3.7.1. Общая информация ... 35
      3.7.2. Создание регулярного выражения ... 37
   3.8. Справочник ... 38
      3.8.1. Общая информация ... 38
      3.8.2. Создание списка ... 41
4. Администрирование ... 42
   4.1. Пользователи ... 42
      4.1.1. LDAP-пользователи ... 42
      4.1.2. Локальные пользователи ... 43
   4.2. Ролевая модель управления доступом ... 46
      4.2.1. Матрица ролей и полномочий ... 46
      4.2.2. Роли ... 47
   4.3. LDAP ... 57
   4.4. Логирование ... 58
      4.4.1. Расположение и назначение журналов с логами ... 58
      4.4.2. Просмотр логов (аудит действий пользователя) ... 58
5. Глоссарий ... 59

1. ОБЩИЕ СВЕДЕНИЯ

«CrossTech Database Security» – система для отслеживания и анализа активности в базах данных (далее – БД), обеспечения защиты БД от несанкционированного доступа, атак и утечек данных.

Система обнаруживает в отслеживаемых БД необычные или потенциально вредоносные запросы, такие как: изменение данных, попытки вторжения.

Система способствует защите конфиденциальной информации, хранимой в таблицах БД, протоколирует действия пользователей в БД, а также действия пользователей в соответствии с заданными параметрами (политиками) и информирует о выполнении подозрительных операций.

Система решает следующие задачи:

- выявление подозрительных запросов пользователей БД в реальном времени;
- выявление и предотвращение нарушений политик безопасности или превышения прав пользователей;
- управление правами доступа пользователей.

2. ЭЛЕМЕНТЫ ИНТЕРФЕЙСА СИСТЕМЫ

Во всех разделах Системы для работы с пользовательским интерфейсом используются одинаковые концепции и элементы управления.

2.1. Экраны

Экран – основной элемент интерфейса для взаимодействия пользователя с объектами Системы. Экраны могут быть разных типов и включать в себя разные наборы компонентов, но имеют общее назначение: отображение и изменение информации о различных объектах Системы.

Экраны в Системе бывают двух типов:

– список;
– карточка.

1) Список

   Представляет собой таблицу с записями об объектах без возможности редактирования их атрибутов. При наличии в списке количества объектов, превышающего отображаемое на странице количество строк, доступно переключение страниц с помощью кнопок пагинации.

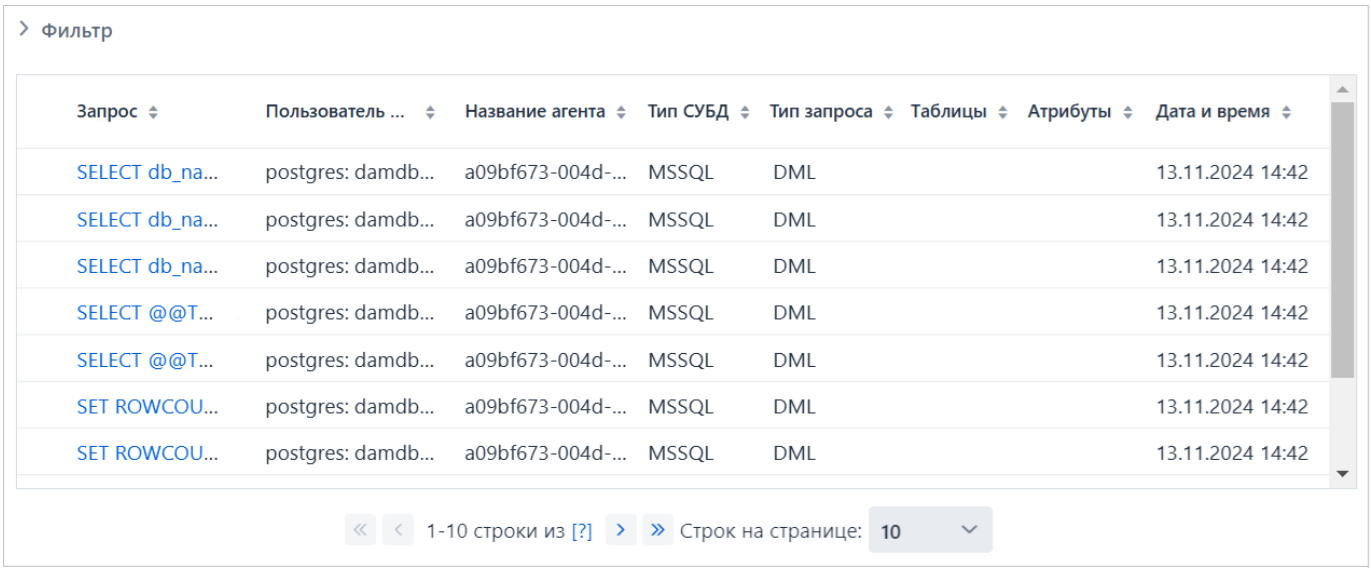

Рисунок 1 – Тип экрана: список

2) Карточка

Карточка содержит детальную информацию об атрибутах объекта. При наличии соответствующих прав у пользователя он может изменять и сохранять атрибуты объекта.

Переход к карточке объекта может выполняться двумя способами:

– нажатие на название объекта в списке, если название объекта является гиперссылкой;
– выбор объекта из списка и нажатие на кнопку «Просмотр» или «Изменить» над списком.

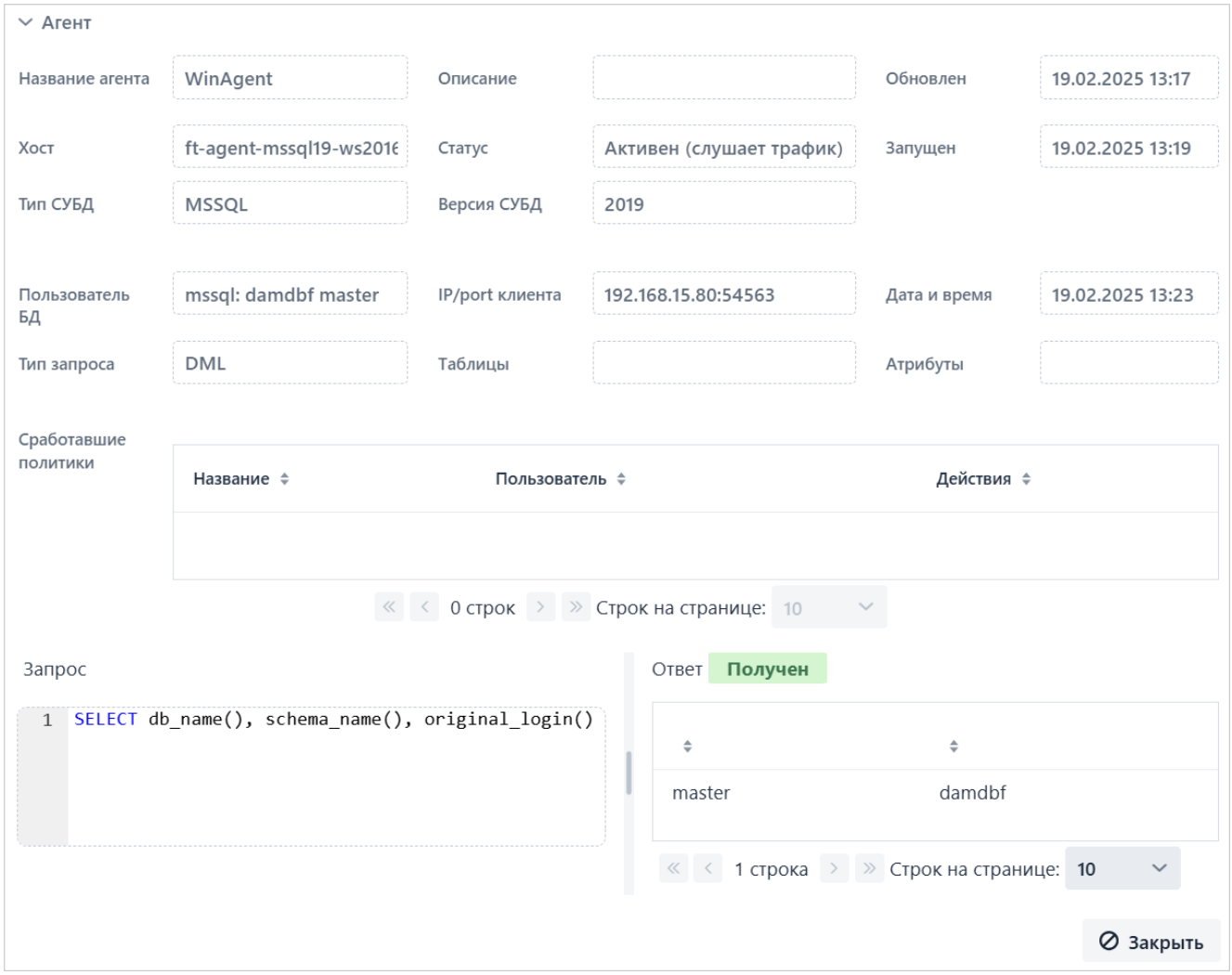

Рисунок 2 – Тип экрана: карточка

2.2. Кнопки

Экраны могут содержать в себе кнопки, выполняющие какие-либо действия. На различных типах экранов кнопки могут располагаться в разных местах и иметь разный тип. Ниже представлены примеры использования кнопок в различных областях экранов Системы.

1) Область фильтра

   Кнопки в области фильтра предназначены для поиска объектов в выбранном разделе.

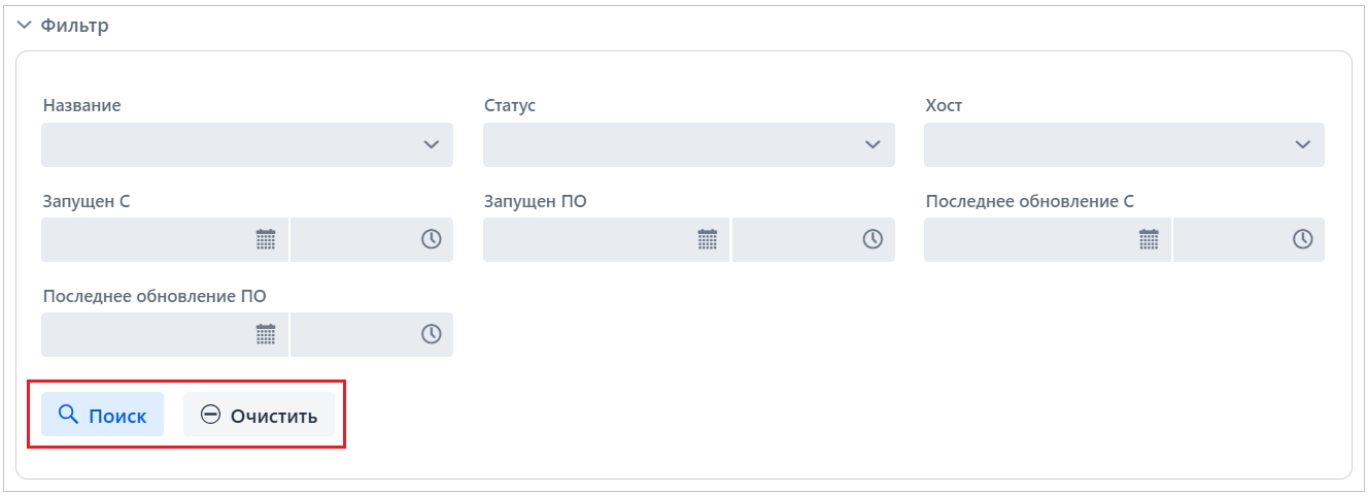

Рисунок 3 – Кнопки в области фильтра

2) Область пагинации

   Кнопки в области пагинации предназначены для постраничной навигации в экранах со списками объектов.

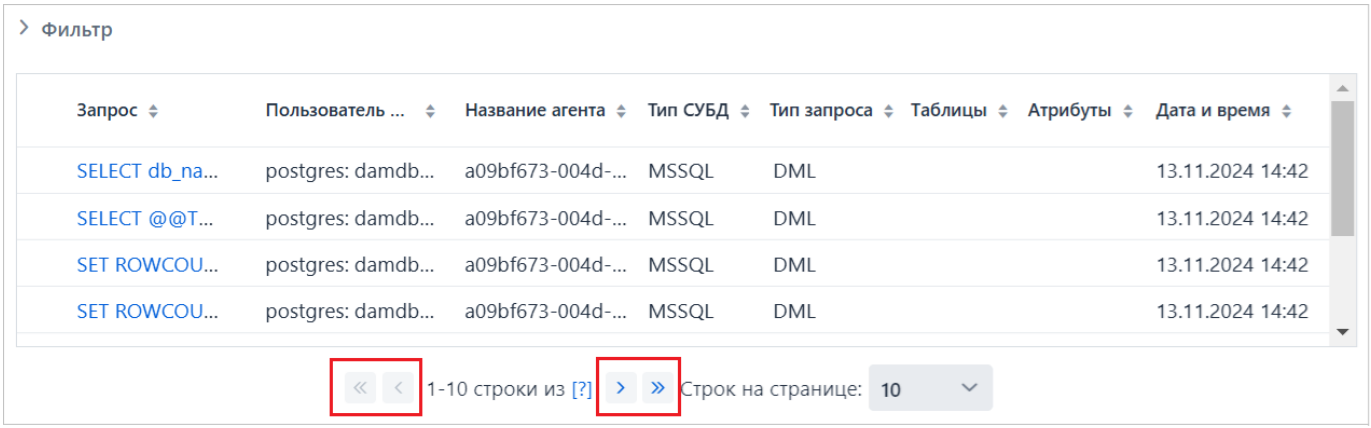

Рисунок 4 – Кнопки в области пагинации

3) Карточка объекта

Кнопки в карточках объектов предназначены для управления информацией об атрибутах этих объектов. Данные кнопки могут быть использованы для сохранения карточки, закрытия карточки, отмены изменений в карточке, добавления информации или других объектов в карточку и т.п.

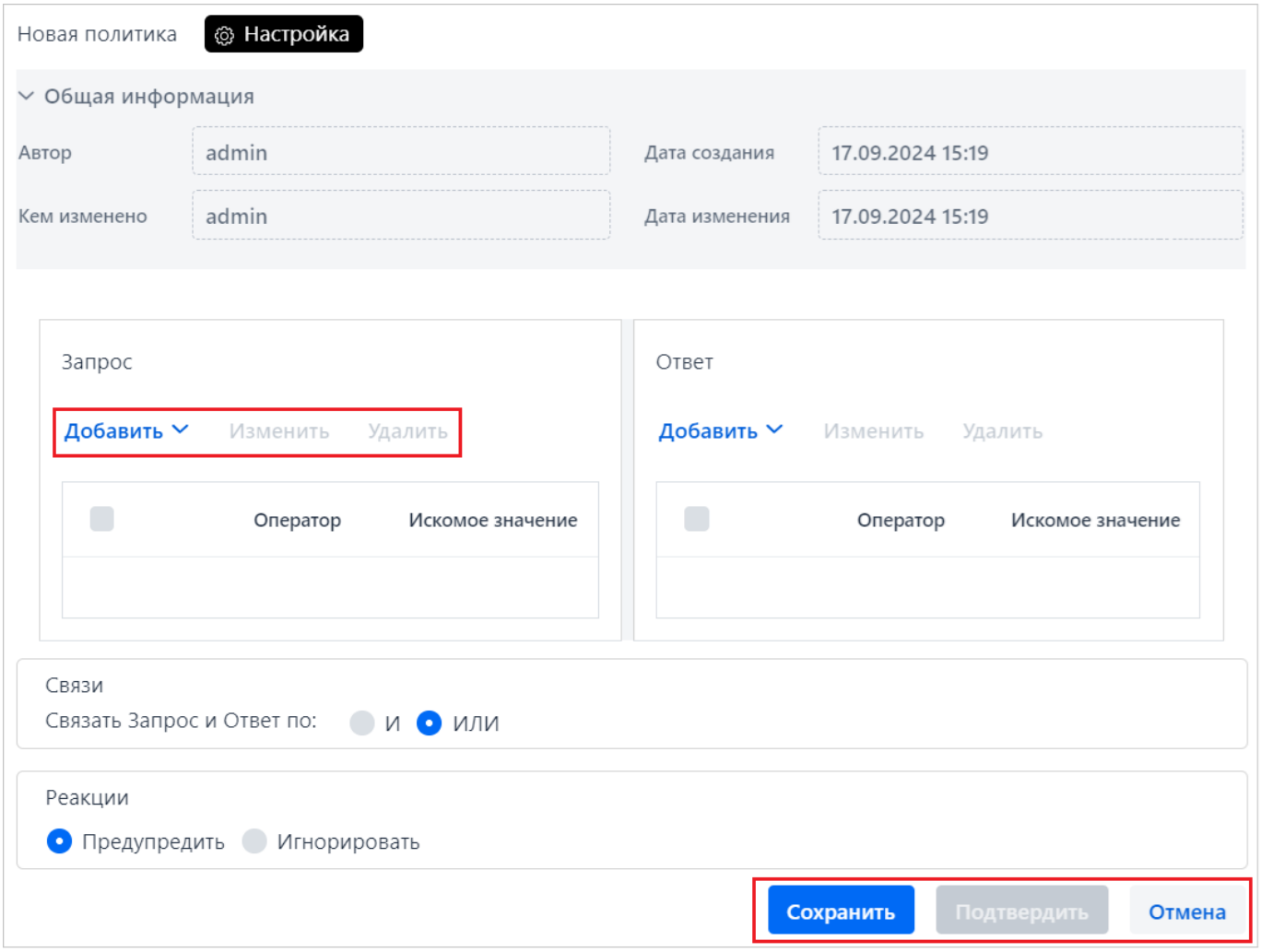

Рисунок 5 – Кнопки в карточке объекта

4) Панель над списком объектов

Кнопки над списком объектов предназначены для управления объектами из списка. В зависимости от выбранного раздела и типа находящихся в нем объектов, набор кнопок может отличаться.

Для большинства экранов со списками доступны кнопки управления объектами: «Создать», «Изменить», «Удалить».

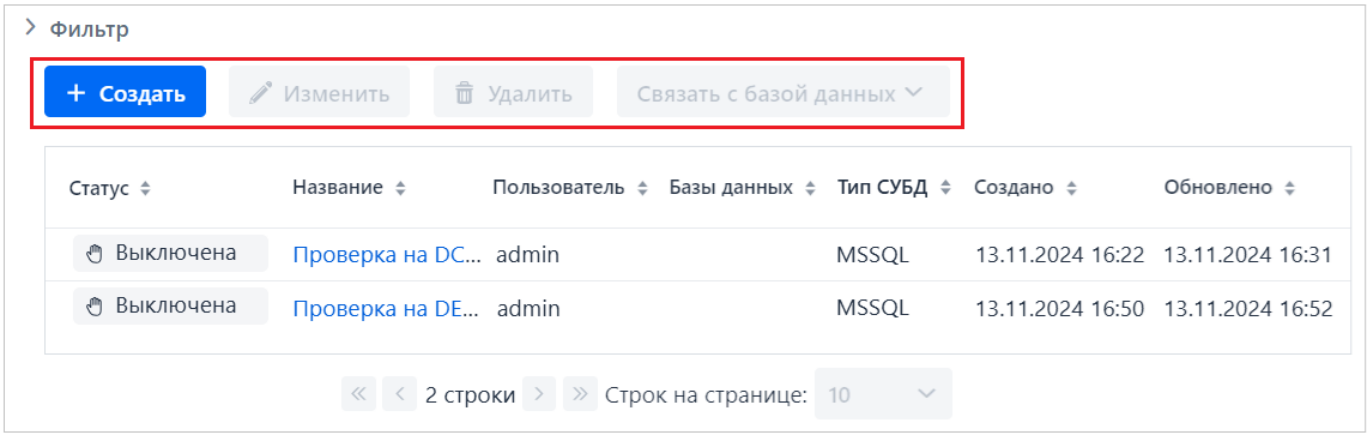

Рисунок 6 – Кнопки над списком объектов

2.3. Поля

Поля на экранах могут быть разных типов.

Поля, отмеченные значком ▪ или ▪, обязательны для заполнения.

1) Простое текстовое поле

   К данному типу полей относятся однострочные или многострочные поля для ввода текста.

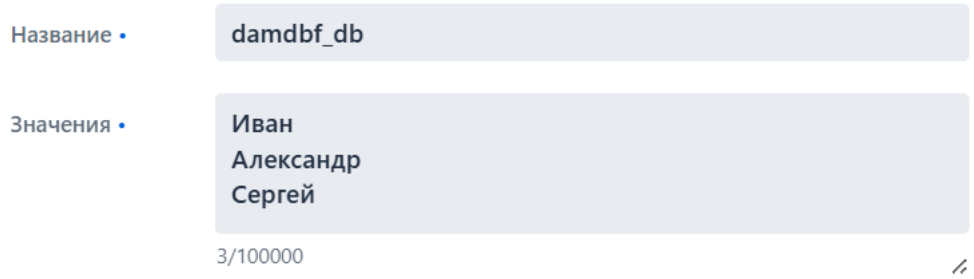

Рисунок 7 – Поля для ввода текста

   Обязательное незаполненное поле окрашивается в красный цвет.

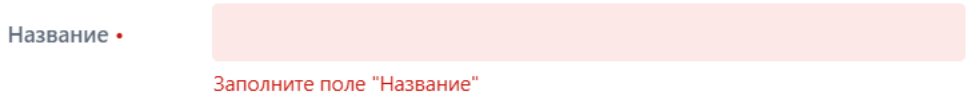

Рисунок 8 – Незаполненное обязательное поле

   Поле, недоступное для редактирования, светло-серого цвета.

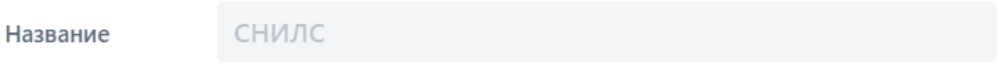

Рисунок 9 – Поле, недоступное для редактирования

   Поле, всегда доступное только для чтения, имеет пунктирную границу.

Рисунок 10 – Поле, доступное только для чтения

2) Поле с SQL-запросом

   К данному типу полей относятся поля с SQL-запросами к БД.

Рисунок 11 – Текстовое поле с с SQL-запросом

3) Поля для ввода даты и времени

К данному типу полей относятся поля для ввода времени или даты. Время и дата могут быть введены вручную, а также выбраны из списка и календаря соответственно.

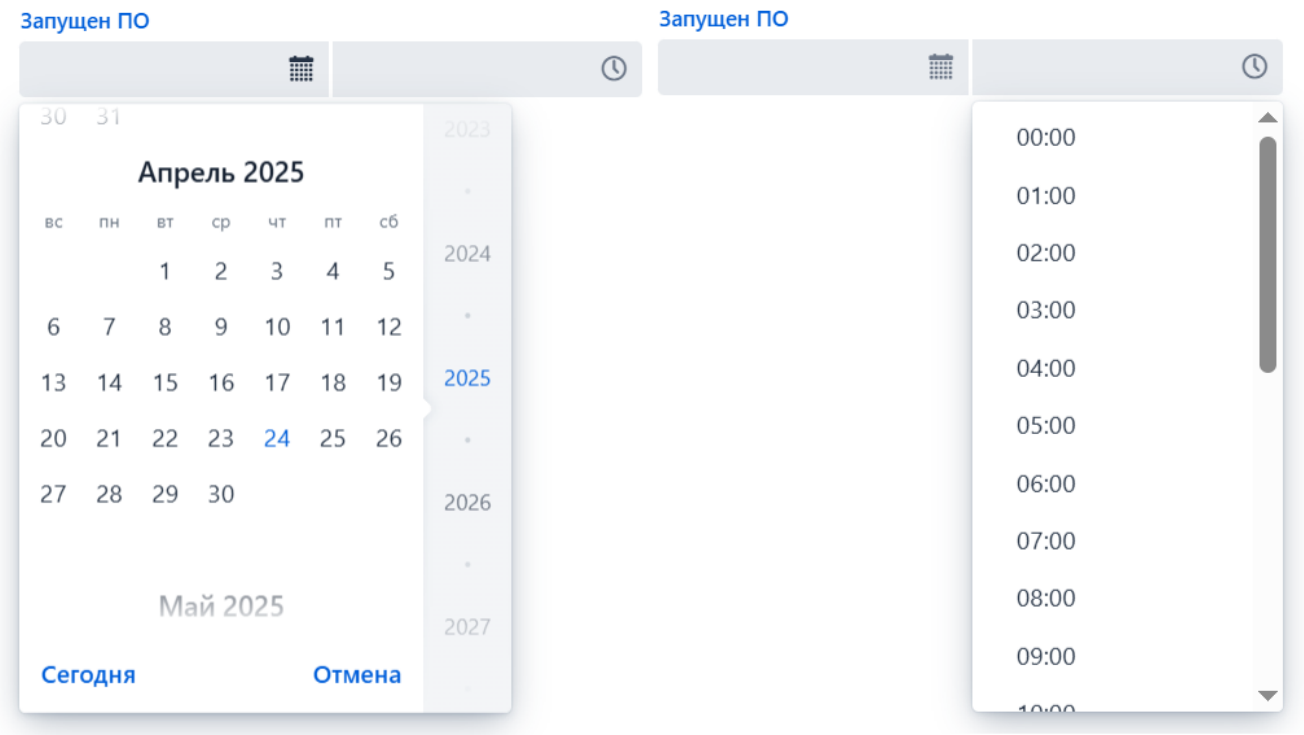

Рисунок 12 – Поля для ввода даты и времени

4) Поля выбора

К данному типу полей относятся чекбоксы и радиокнопки.

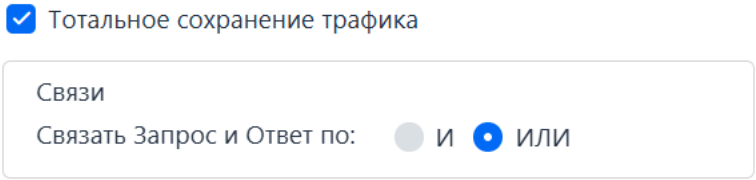

Рисунок 13 – Поля выбора

5) Выпадающий список

К данному типу полей относятся выпадающие и комбинированные списки.

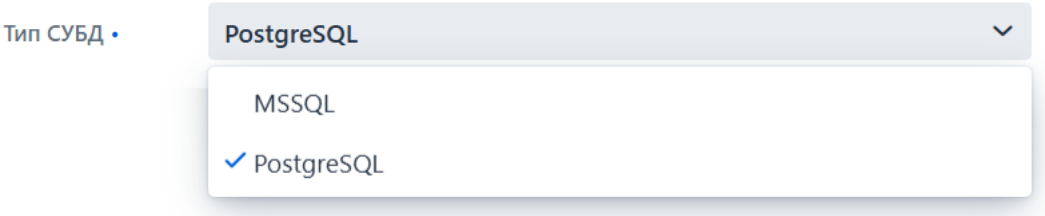

Рисунок 14 – Выпадающий список

2.4. Списки

Список – это таблица с набором записей об объектах Системы. Список позволяет искать записи и открывать карточки этих записей для просмотра детальной информации об объектах. Списки в Системе являются плоскими и не поддерживают множественный выбор для редактирования записей об объектах.

При открытии списка в нем отображается количество записей, настроенное в Системе по умолчанию. Для выбора количества записей, отображаемых в списке на одной странице, используется выпадающий список «Строк на странице».

Если в списке находится больше записей, чем может быть отображено на одной странице, общее количество записей будет отображаться в виде значка [?]. Для отображения общего числа записей необходимо нажать на значок [?].

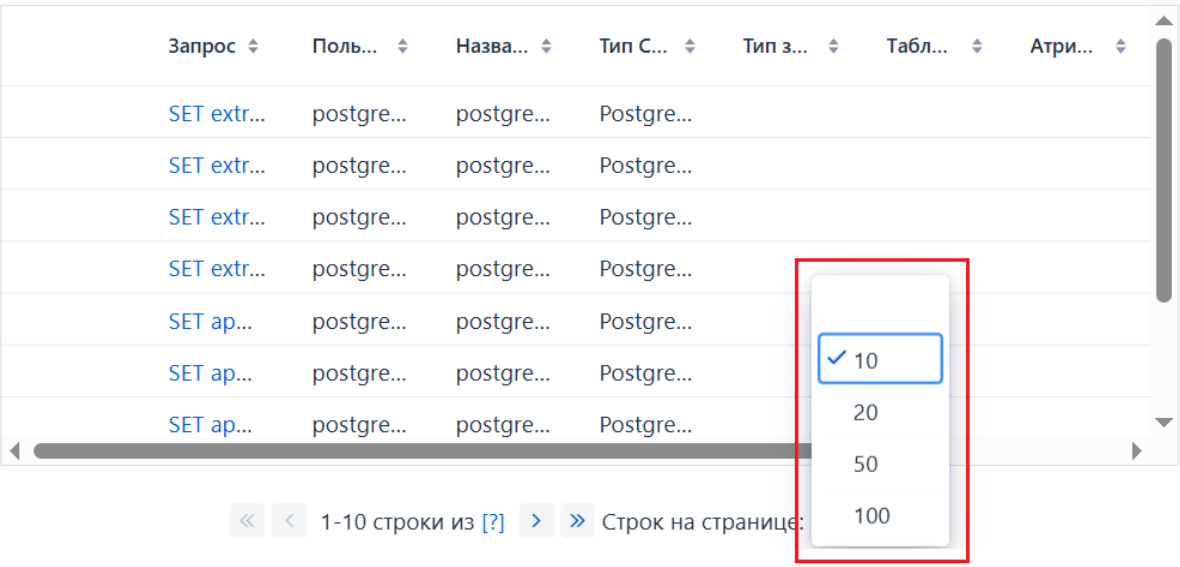

Рисунок 15 – Выбор количества записей на одной странице

Для переключения между страницами списка используются кнопки в области пагинации.

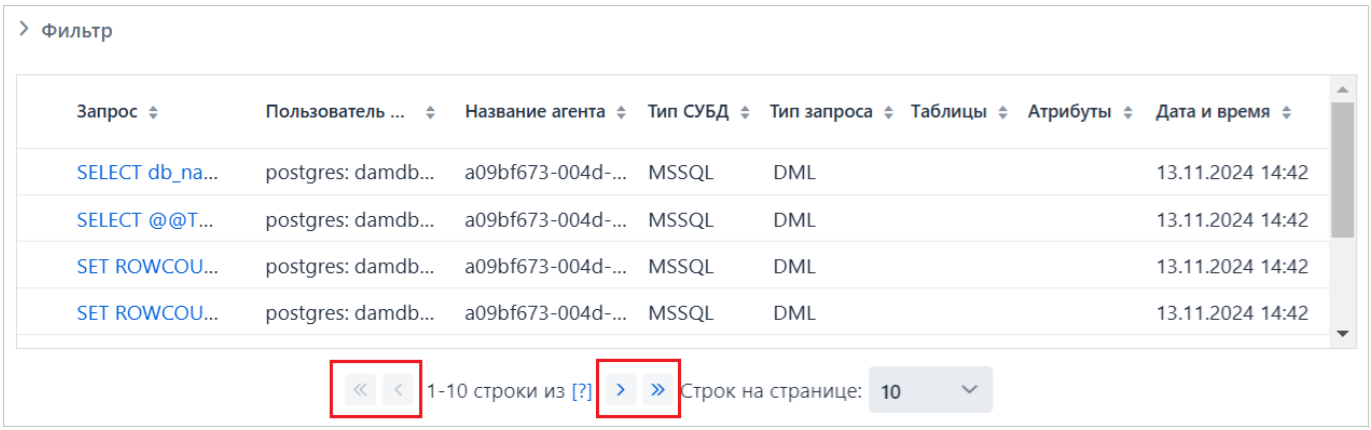

Рисунок 16 – Кнопки для переключения между страницами

Для сортировки записей об объектах по одному из их атрибутов нажмите на заголовок соответствующего столбца списка. При первом нажатии производится сортировка в порядке возрастания, при втором – в порядке убывания, при третьем – сортировка сбрасывается.

Название	Пользователь	Создано	Обновлено
IP-адрес	system	29.01.2025 00:00	
Адрес электронной ...	system	29.01.2025 00:00	
ИНН	system	29.01.2025 00:00	
Кредитные карты	system	29.01.2025 00:00	

Рисунок 17 – Отсортированный список

Для изменения ширины столбца в списке наведите курсор на его правую границу – он изменит свой вид на разделитель, нажмите и удерживайте, перемещая курсор влево или вправо.

Для изменения очередности расположения столбцов в списке нажмите на заголовок столбца и, удерживая его, перемещайте в нужное место.

Название	Пользователь		Создано	Обновлено
СНИЛС	system		29.01.2025 00:00	
Адрес электронной ...	system		29.01.2025 00:00	
IP-адрес	system		29.01.2025 00:00	
MAC-адрес	system		29.01.2025 00:00	

Рисунок 18 – Изменение ширины столбца

2.5. Фильтры и поиск

Область фильтра располагается в верхней части страницы со списком и предназначена для поиска объектов из списка в соответствии с заданными условиями. Состав полей фильтра отличается для разных разделов Системы.

Для поиска объектов по одному или нескольким атрибутам необходимо ввести нужные значения в поля фильтра и нажать кнопку «Поиск». В списке отобразятся записи, соответствующие поисковому запросу.

Для очистки фильтра используется кнопка «Очистить».

Для сворачивания и разворачивания области фильтра необходимо нажать на его название.

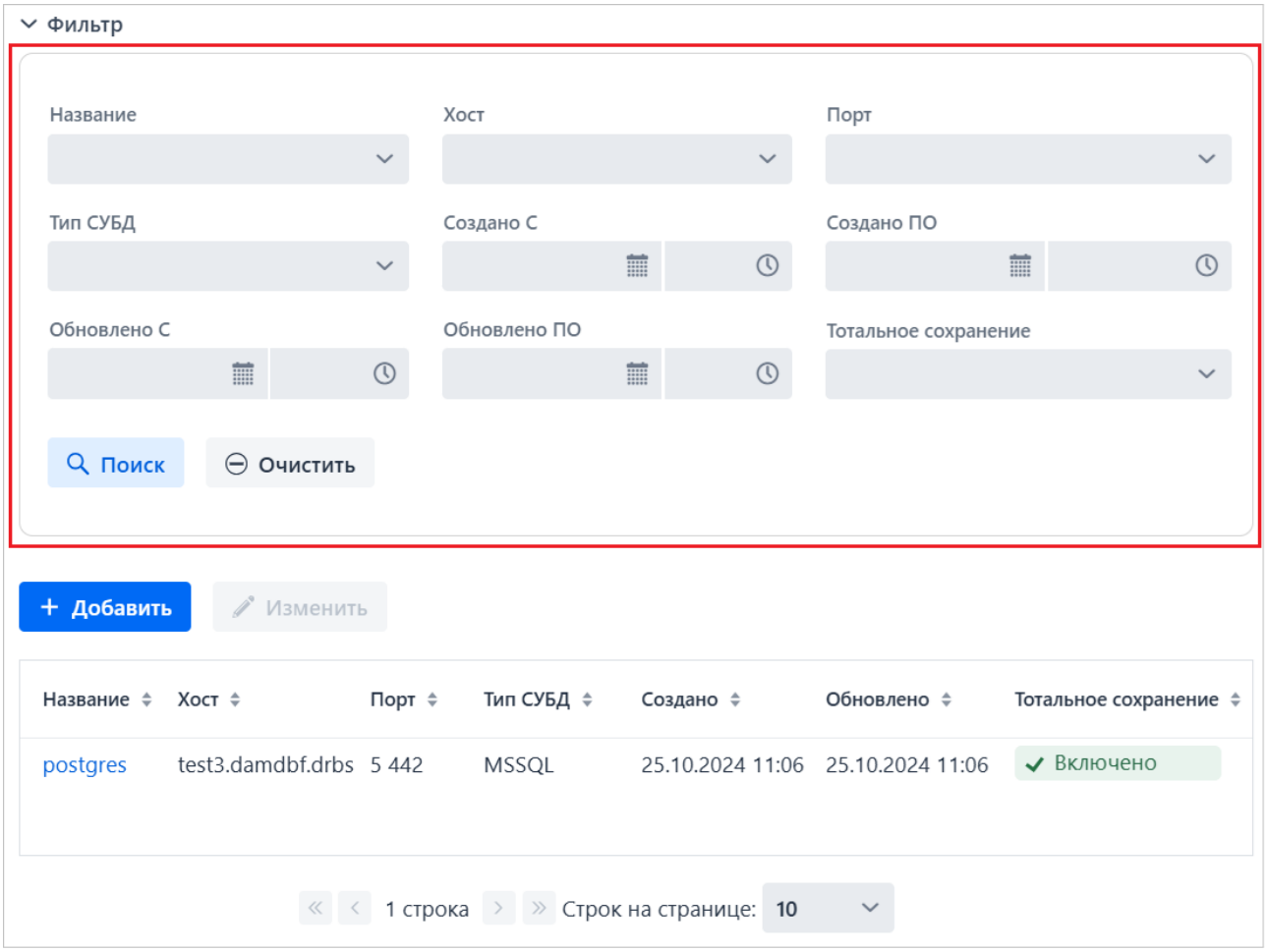

Рисунок 19 – Область фильтра

3. ИСПОЛЬЗОВАНИЕ СИСТЕМЫ

3.1. Вход в Систему

Работа с пользовательским интерфейсом Системы осуществляется с помощью браузера. Для входа в Систему необходимо ввести в адресную строку браузера URL-адрес, по которому развернута Система.

Ввод данных для входа выполняется в форме авторизации. Пользователь может войти в Систему с помощью доменного логина и пароля или с помощью стандартной учетной записи. При входе в Систему производится синхронизация данных учетной записи с Active Directory. После входа пользователя в Систему по умолчанию отображается стартовый экран и панель навигации.

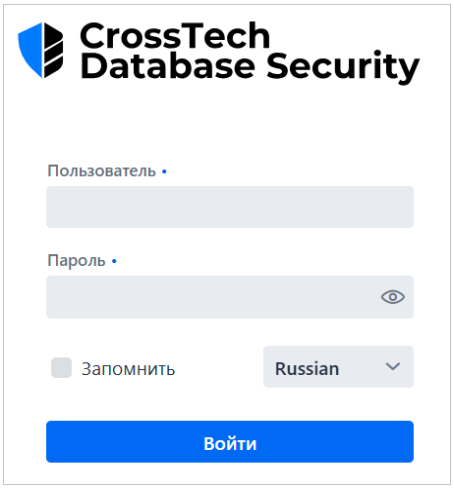

Рисунок 20 – Форма авторизации в Системе

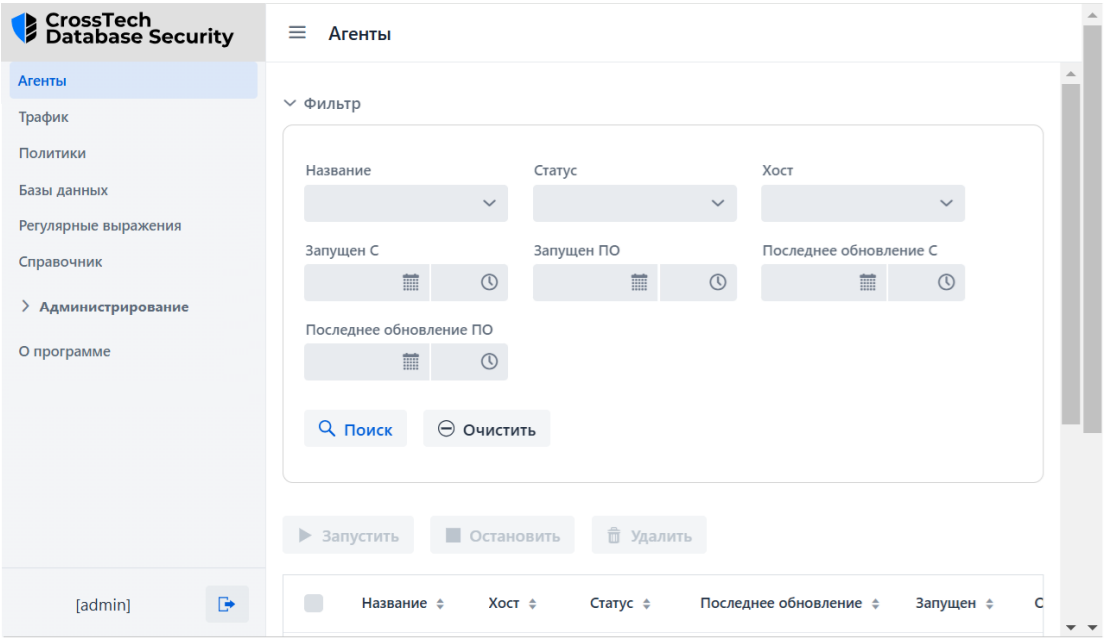

Рисунок 21 – Стартовый экран Системы

3.2. Панель навигации

Панель навигации расположена в левой части окна Системы. С помощью панели навигации осуществляется доступ к разделам Системы. Для перехода к содержимому раздела необходимо нажать на его название. Для сворачивания и разворачивания панели навигации используется кнопка ≡ справа от нее.

В верхней части панели навигации располагается наименование Системы, в нижней – логин текущего пользователя и кнопка выхода из Системы.

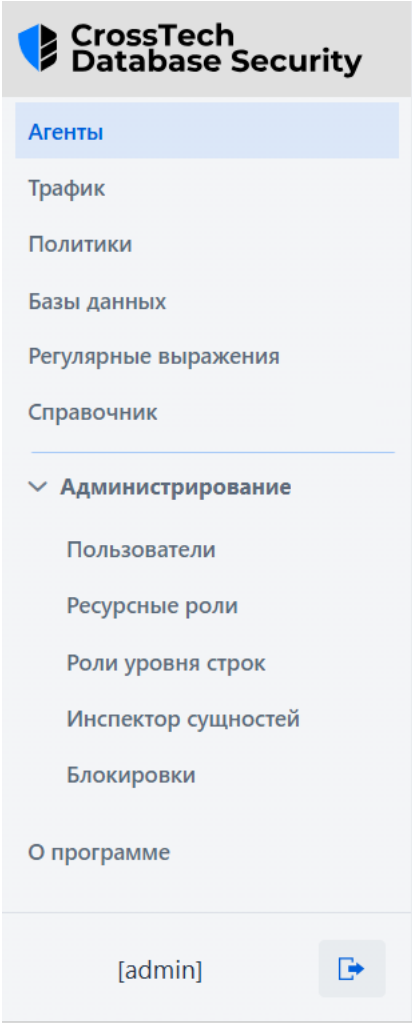

Рисунок 22 – Панель навигации Системы

3.3. Агенты

Агент – приложение, которое устанавливается администратором Системы на хост с отслеживаемой БД. После окончания установки агента запускается его автообнаружение в Системе. Обнаруженный агент отображается в Системе со статусом «Новый» и начинает работать только после запуска. Запущенный агент перехватывает поток трафика, идущий к отслеживаемой БД, и передает его в коллектор для проведения анализа в соответствии с настроенными политиками.

Список агентов содержится в разделе Системы «Агенты». Над таблицей со списком присутствует фильтр для поиска агентов по различным атрибутам.

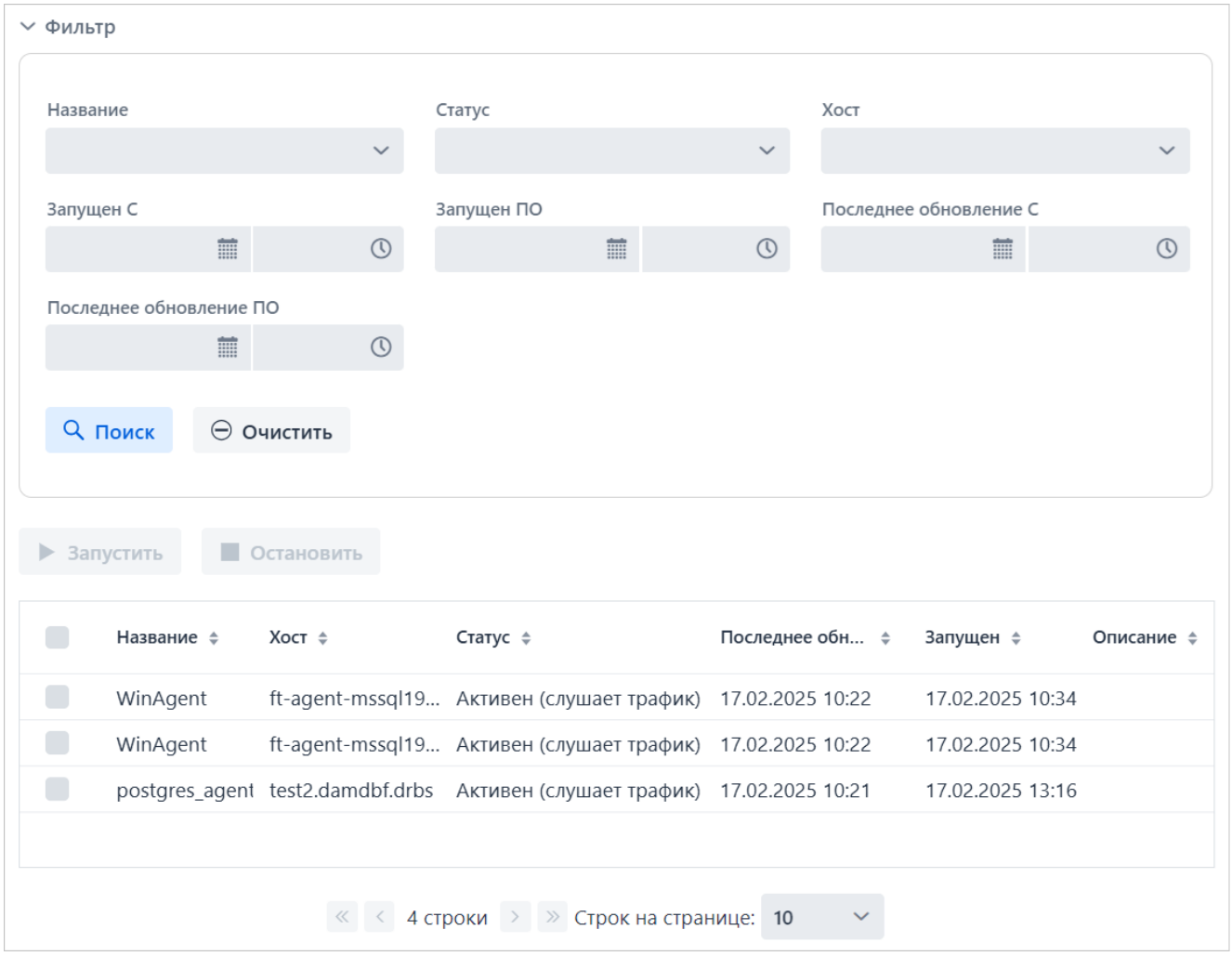

Рисунок 23 – Раздел «Агенты»

Установленный на хост агент по умолчанию не собирает трафик. Для запуска перехвата трафика агент должен быть запущен вручную из интерфейса Системы, для прекращения перехвата агент должен быть остановлен вручную. Правами на запуск и остановку агентов обладает только администратор Системы.

Агент может быть запущен, если он находится в статусе «Новый» или «Не активен (не слушает трафик)». Необходимо выбрать агент и нажать кнопку «Запустить» – его статус изменится на «Запускается», затем – на «Активен (слушает трафик)». Если для запуска выбрано несколько агентов одновременно и среди них есть уже запущенные агенты, такие агенты будут пропущены, а остальные незапущенные агенты будут запущены.

Агент может быть остановлен, если он находится в статусе «Активен (слушает трафик)». Необходимо выбрать агент и нажать кнопку «Остановить» – его статус изменится на «Останавливается», затем – на «Не активен (не слушает трафик)». Если для остановки выбрано несколько агентов одновременно и среди них есть уже остановленные агенты или агенты со статусом «Новый», такие агенты будут пропущены, а остальные запущенные агенты будут остановлены.

Для просмотра детальной информации об агенте необходимо установить флажок напротив его названия в списке, правой кнопкой мыши вызвать контекстное меню и выбрать пункт «Изменить» – откроется окно с подробными сведениями об агенте. Для редактирования доступно только поле «Описание». Для сохранения измененного описания агента используется кнопка «Сохранить».

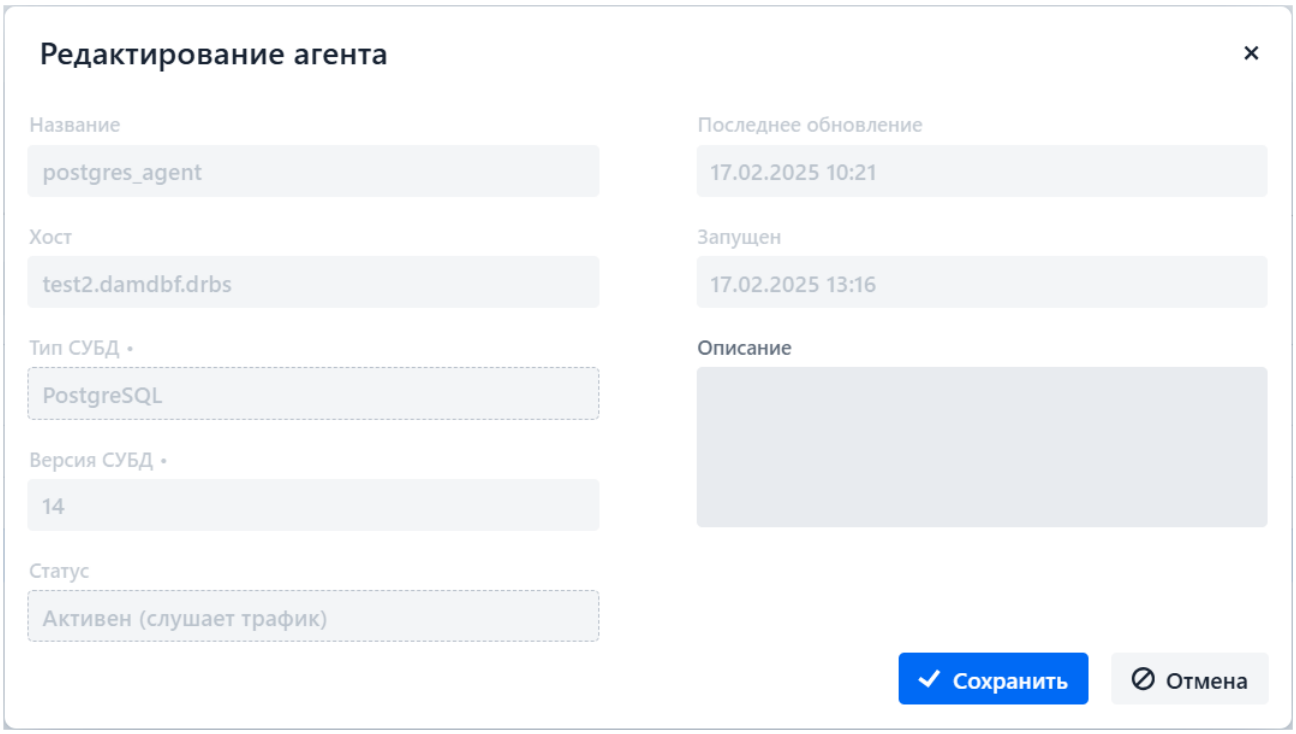

Рисунок 24 – Карточка агента при редактировании

Карточка агента содержит в себе следующие поля:

- «Название» – имя агента;
- «Хост» – адрес хоста, на котором установлен агент;
- «Тип СУБД» – тип отслеживаемой СУБД;
- «Версия СУБД» – версия отслеживаемой СУБД;
- «Статус» – текущий статус агента;
- «Последнее обновление» – время и дата последнего обновления агента;
- «Запущен» – дата и время перехода агента в текущий статус;
- «Описание» – краткое описание функций агента.

3.4. Трафик

Информация о трафике (запросах и ответах на запросы), идущем к отслеживаемым БД, перехватывается агентами и отображается в интерфейсе Системы. По умолчанию трафик отображается в Системе, если для него сработала хотя бы одна политика. Абсолютно весь трафик, идущий к отслеживаемой БД, будет отображаться и сохраняться в Системе, только если для этой БД включен режим тотального сохранения.

Список трафика содержится в разделе Системы «Трафик». Над таблицей со списком присутствует фильтр для поиска трафика по различным атрибутам.

Каждая строка таблицы содержит отдельный SQL-запрос (технический или пользовательский) к таблице БД, отображает содержание запроса и детальную информацию о нем. В случае, если для перехваченного запроса сработала хотя бы одна политика, в левой части строки с запросом будет отображен значок ⚠.

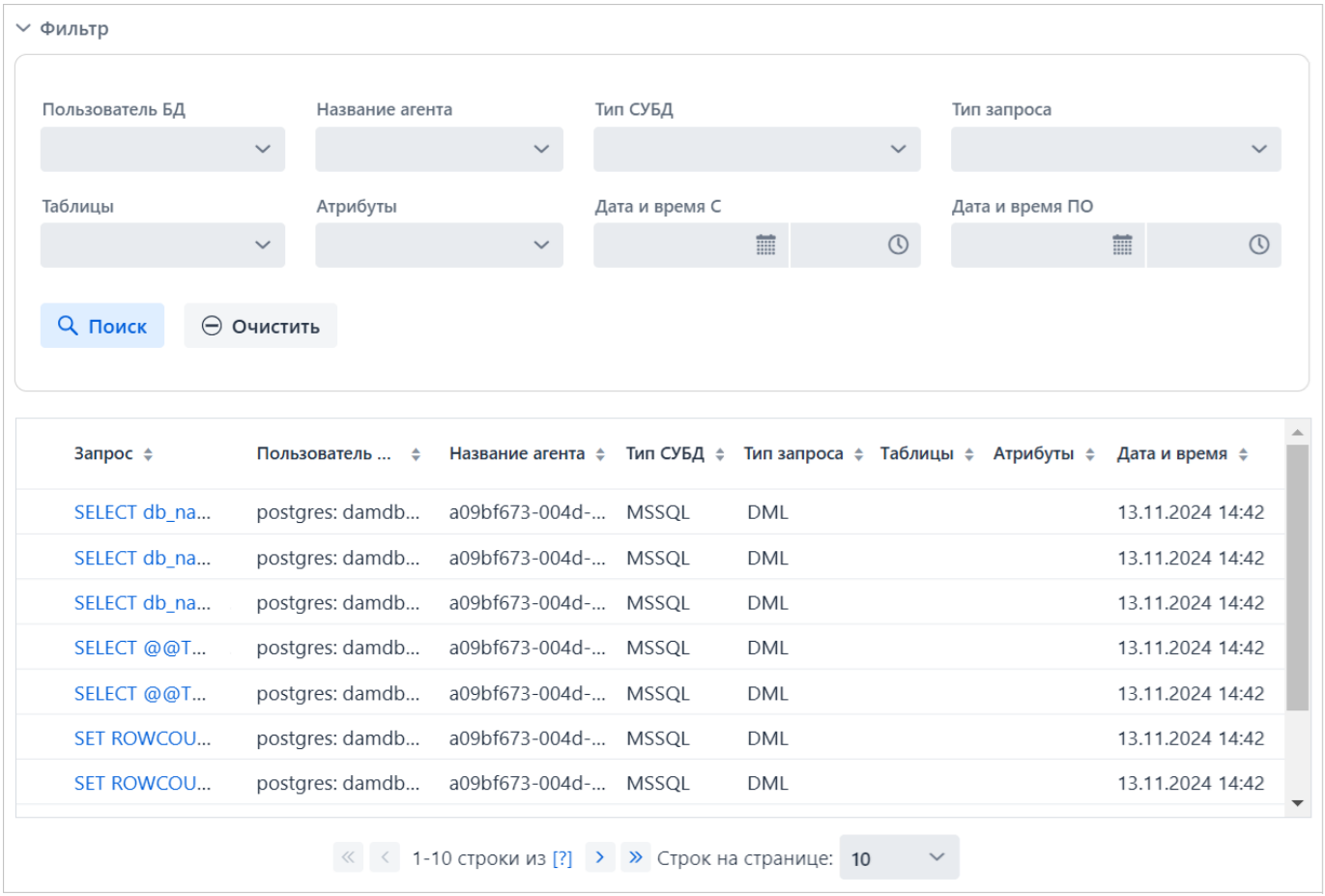

Рисунок 25 – Раздел «Трафик»

Для просмотра информации о трафике необходимо нажать на гиперссылку с SQL-запросом в строке с записью. В карточке трафика содержится информация об агенте, перехватившем этот трафик (по умолчанию данный блок свернут):

- «Название агента» – название агента;
- «Описание» – краткое описание назначения агента;
- «Обновлен» – дата и время последнего обновления агента;
- «Хост» – адрес хоста с БД, на котором установлен агент;
- «Статус» – текущий статус агента;
- «Запущен» – дата и время запуска агента;
- «Тип СУБД» – тип отслеживаемой СУБД;
- «Версия СУБД» – версия отслеживаемой СУБД.

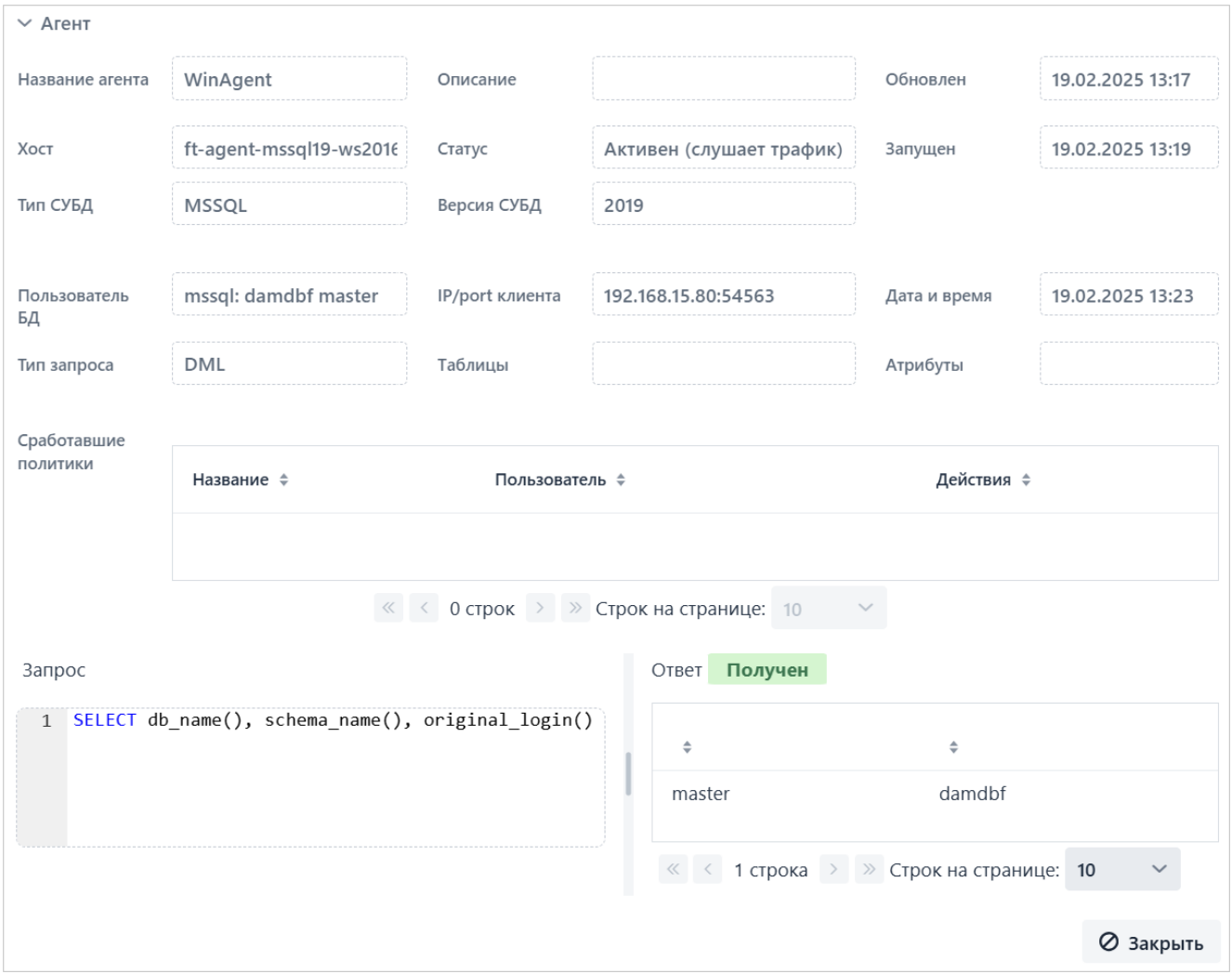

Рисунок 26 – Карточка трафика

В карточке трафика содержится детальная информация о нем:

- «Пользователь БД» – данные пользователя, создавшего запрос к БД;
- «IP/port клиента» – прослушиваемый агентом IP/port компьютера, от которого исходит запрос;
- «Дата и время» – дата и время выполнения запроса;
- «Тип запроса» – принадлежность запроса к одному из типов: DML, DDL, DCL, TCL;
- «Таблицы» – одна или несколько таблиц БД, к которым осуществлялся запрос;
- «Атрибуты» – атрибуты, использованные в запросе;
- «Сработавшие политики» – список политик, сработавших при выполнении запроса;
- «Запрос» – непосредственное содержание запроса;
- «Ответ» – ответ, полученный в результате выполнения запроса.

Для закрытия карточки трафика используется кнопка «Отмена».

3.5. Политики

3.5.1. Общая информация

Политики в Системе используются для автоматического определения нетипичного или вредоносного поведения при работе пользователей с внешними БД. Весь трафик, идущий к отслеживаемым БД, проверяется на соответствие политикам. К вредоносному поведению могут быть отнесены: запросы к БД с определенными командами, запросы к определенным таблицам БД, выполнение «Sysdba» команд по изменению данных в БД, выполнение «delete» и «drop table» запросов к БД.

Также с помощью политик, содержащих регулярные выражения в качестве условия для проверки, Система способна распознавать в запросах и ответах на запросы конфиденциальную информацию.

Список политик содержится в разделе Системы «Политики». Над таблицей со списком присутствует фильтр для поиска политик по различным атрибутам.

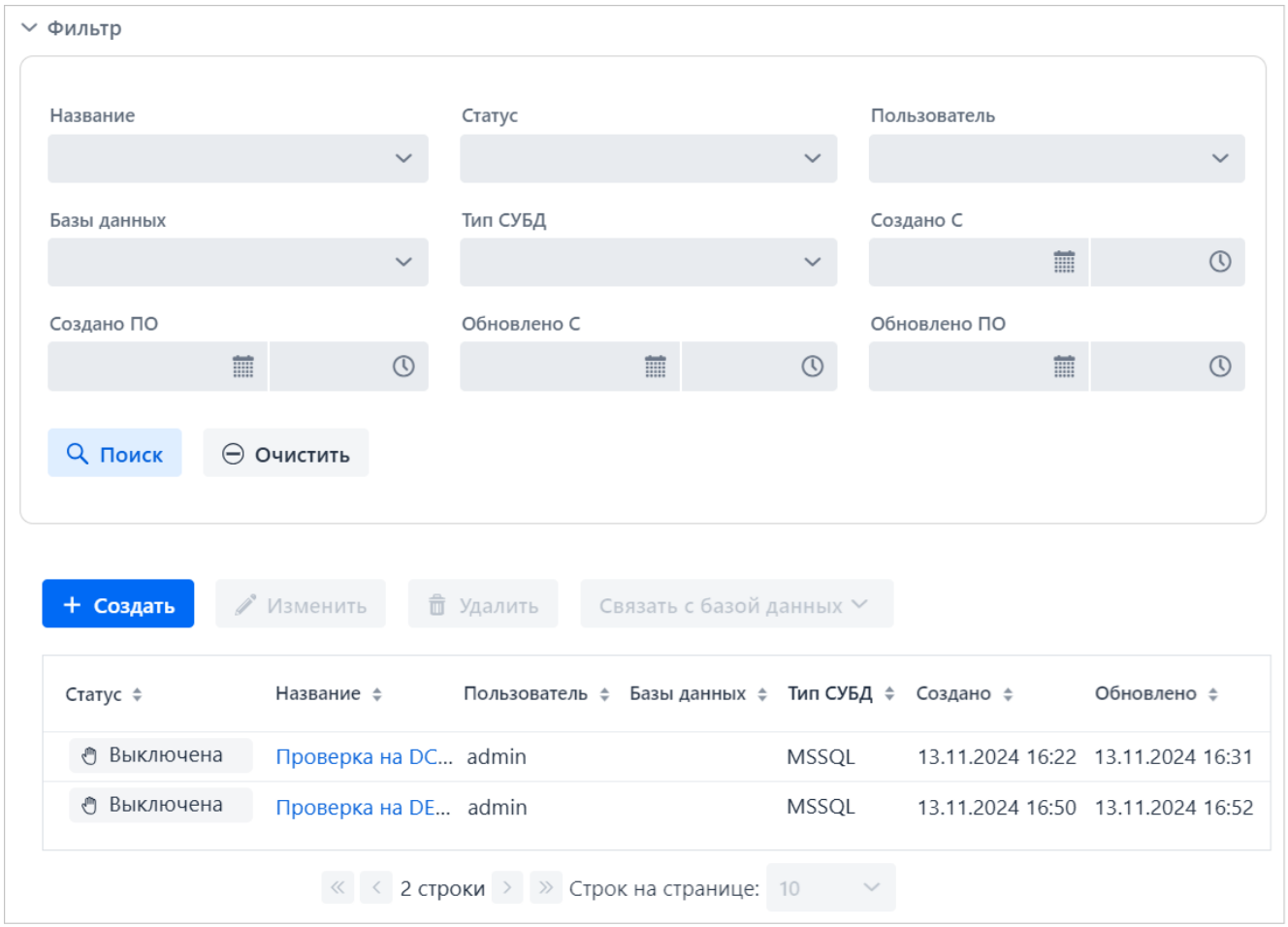

Рисунок 27 – Раздел «Политики»

При выборе политики из списка в правой части экрана отображается информация об условиях ее срабатывания и выполняющихся при этом действиях.

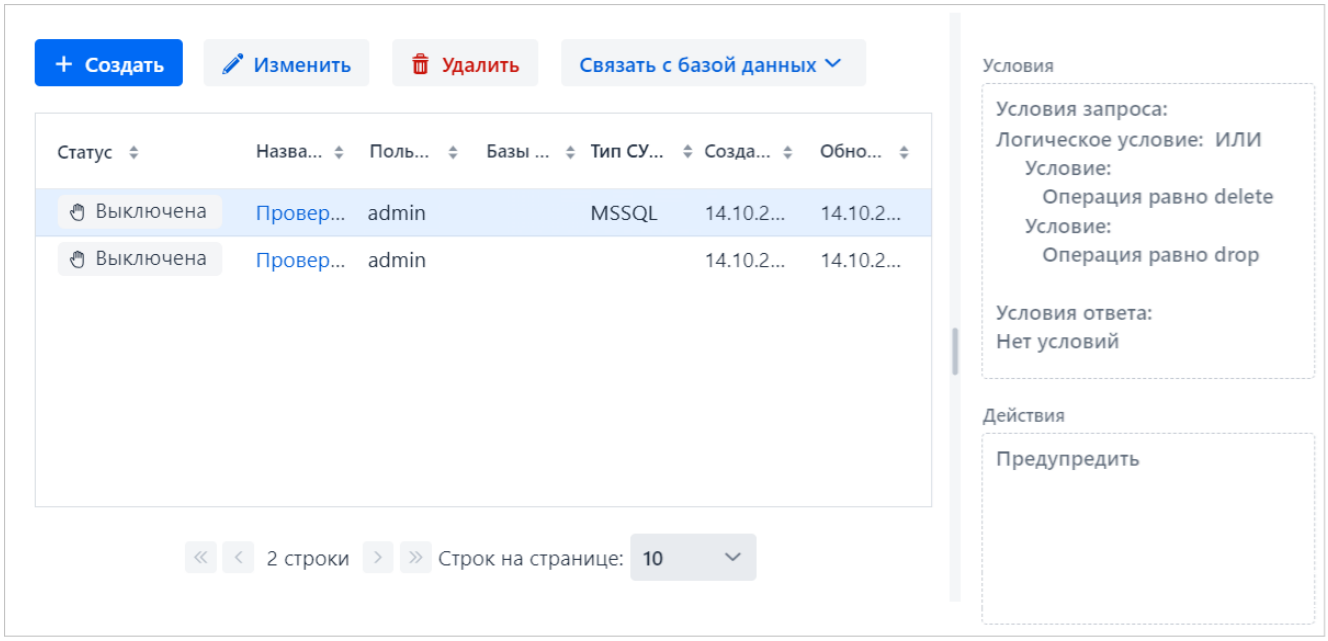

Рисунок 28 – Информация о выбранной политике

В случае срабатывания политики информация о ней отобразится в карточке соответствующего трафика в таблице «Сработавшие политики».

Для редактирования политики необходимо выбрать из списка политику со статусом «Выключена» или «Настройка» и нажать кнопку «Изменить» или нажать на гиперссылку с названием политики – откроется карточка политики. При переходе к редактированию политики со статусом «Выключена» ее статус изменяется на «Настройка». Для сохранения внесенных изменений используется кнопка «Сохранить» в карточке политики.

Для удаления политики необходимо выбрать из списка политику со статусом «Настройка» или «Выключена», нажать кнопку «Удалить» и подтвердить действие в появившемся окне – статус политики изменится на «Удалена».

Правами на создание, изменение, удаление и управление (включение и отключение) политиками обладает только администратор Системы.

3.5.2. Создание политики

Для создания политики используется кнопка «Создать» в разделе Системы «Политики». В окне создания политики необходимо ввести ее название и нажать кнопку «Сохранить» – политика появится в списке всех политик, откроется ее карточка. До подтверждения созданная политика будет находится в статусе «Настройка», она не будет применяться и ее нельзя будет включить.

При попытке сохранения политики с названием (чувствительно к регистру), уже существующим в Системе, возникнет соответствующая ошибка.

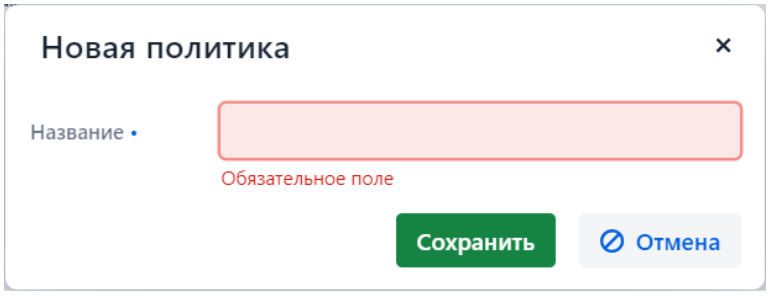

Рисунок 29 – Окно создания политики

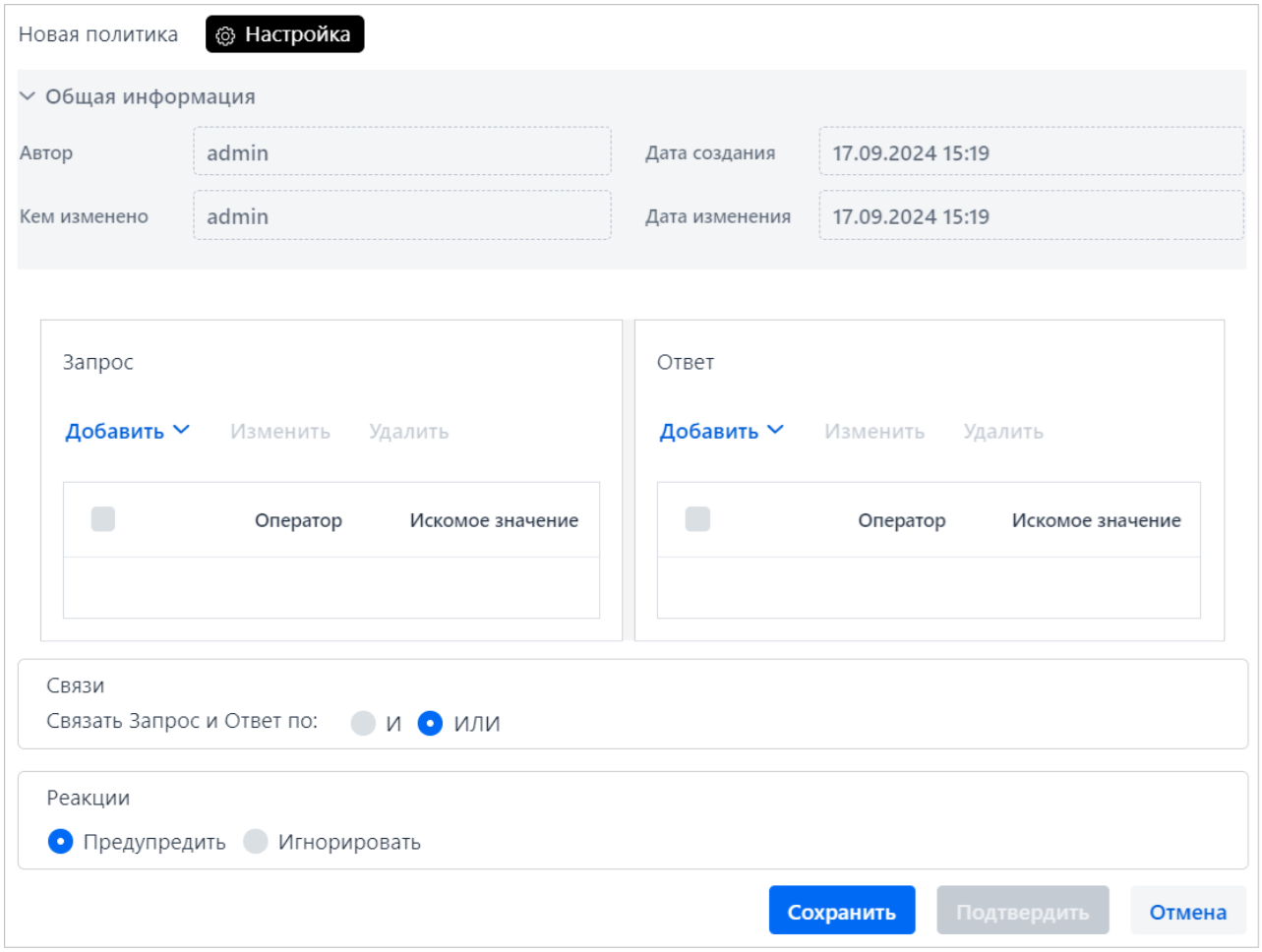

Рисунок 30 – Карточка политики при создании

Карточка политики состоит из следующих блоков с данными.

1) «Общая информация»

   Блок по умолчанию свернут. Содержит сведения о: пользователе, создавшем политику, дате и времени создания политики, пользователе, изменившем политику последним, дате и времени последнего изменения политики.

2) «Запрос»

   Содержит одно или несколько условий для проверки запроса.

   Для добавления условия необходимо вызвать выпадающее меню «Добавить» в блоке «Запрос» и выбрать пункт «Условие».

   В появившемся окне добавления условия из комбинированного списка «Тип» необходимо выбрать проверяемый параметр для запроса.

   Из комбинированного списка «Оператор» необходимо выбрать значение для связывания атрибута «Тип» с атрибутом «Значение» или «Список». Набор доступных операторов зависит от выбранного типа.

   В карточке политики доступны способы ввода: «Вручную» (установлен по умолчанию), «Регулярные выражения» или «Из списка». Способ «Регулярные выражения» может быть выбран, только если в поле «Оператор» установлено значение «удовлетворяет». Способ «Из списка» может быть выбран, только если в поле «Оператор» установлено значение «входит в» или «не входит в».

   При выборе типа в окне добавления условия появляется поле «Значение». Поле «Значение» недоступно при использовании оператора «задан». Поле «Значение» заменяется на «Список» при выборе способа ввода «Из списка».

   При использовании поля «Значение» необходимо ввести данные для проверки выбранного параметра. При использовании поля «Список» необходимо выбрать одно из доступных значений в списке.

   Для сохранения данных, введенных в окне добавления условия, и возврата в карточку создания политики используется кнопка «Сохранить». Для сохранения текущего условия и добавления еще одного условия используется кнопка «Сохранить и добавить еще».

   Если при создании условия для способа «Вручную» был выбран оператор «удовлетворяет», сохранить такое условие не получится – Система отобразит соответствующую ошибку.

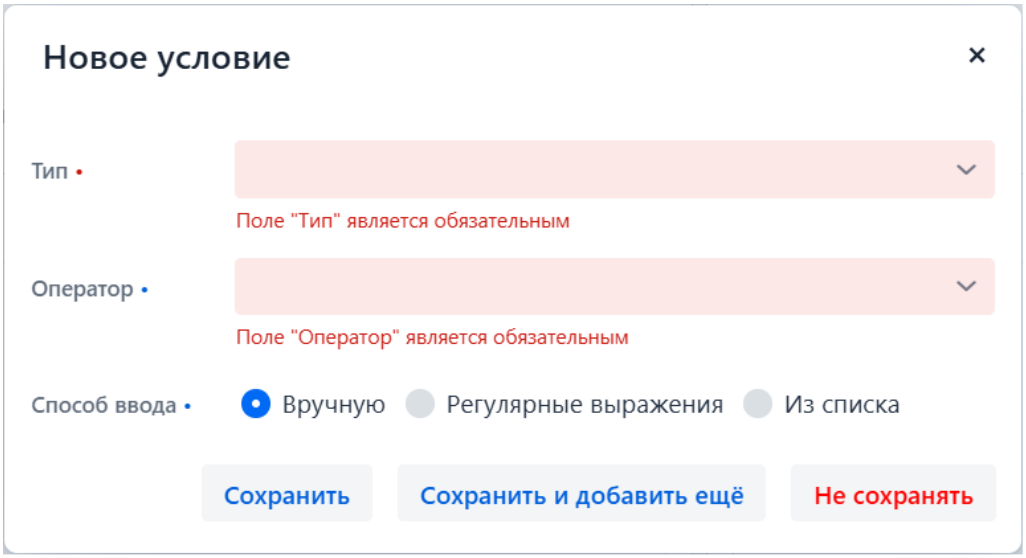

Рисунок 31 – Окно добавления условия

Для редактирования условия необходимо выбрать его из списка в блоке «Запрос» и нажать кнопку «Изменить», в появившемся окне внести изменения и нажать кнопку «Сохранить».

Для удаления условия необходимо выбрать его из списка в блоке «Запрос», нажать кнопку «Удалить» и подтвердить действие в появившемся окне.

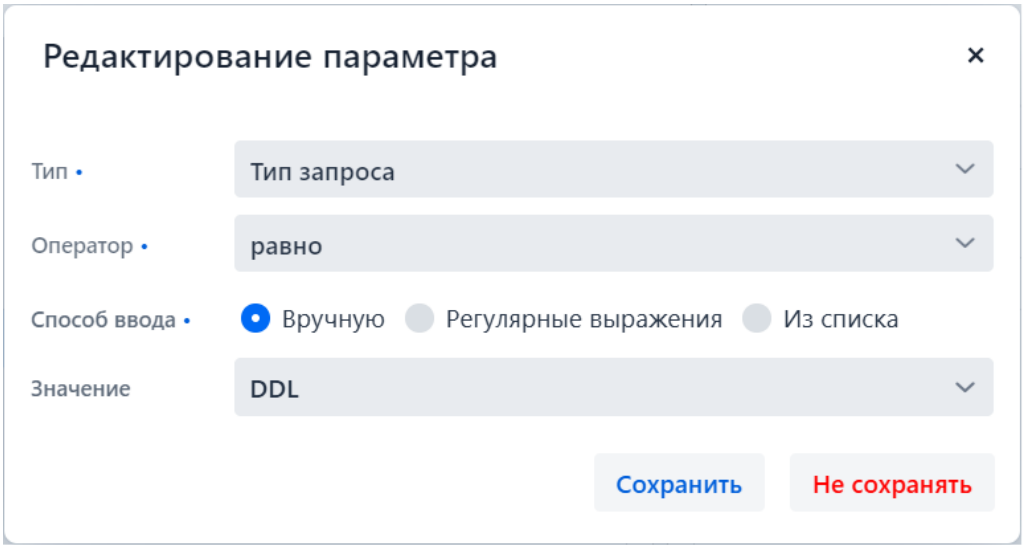

Рисунок 32 – Окно редактирования условия

Условия могут быть связаны между собой с помощью логического условия. Для добавления логического условия необходимо вызвать выпадающее меню «Добавить» в блоке «Запрос» и выбрать пункт «Логическое условие».

В появившемся окне необходимо выбрать одно из значений: «И» (выполнены одновременно все условия, объединенные в группу), «ИЛИ» (выполнено одно или более условий, входящих в группу), «НЕ» (условия из группы не выполняются), «ИСКЛ. ИЛИ» (выполнено только одно условие из группы) и нажать кнопку «Сохранить».

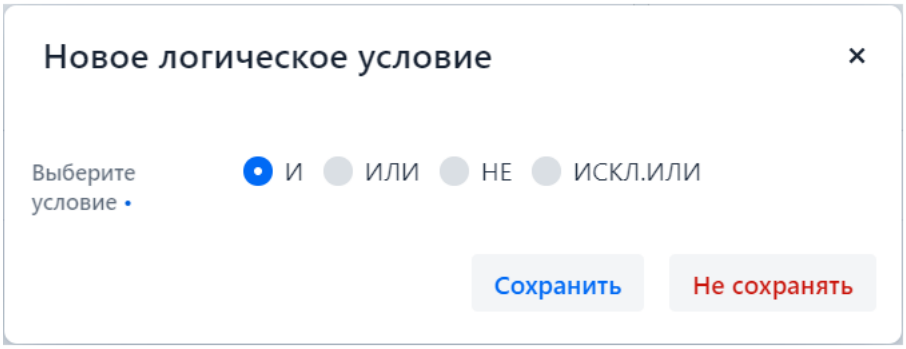

Рисунок 33 – Окно добавления логического условия

Для редактирования логического условия необходимо выбрать его из списка в блоке «Запрос» и нажать кнопку «Изменить», внести изменения в появившемся окне и нажать кнопку «Сохранить».

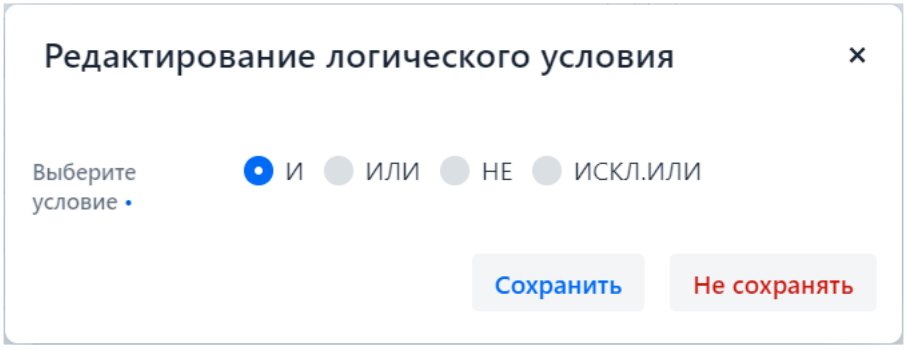

Рисунок 34 – Окно редактирования логического условия

Для удаления логического условия необходимо выбрать его из списка в блоке «Запрос», нажать кнопку «Удалить» и подтвердить действие в появившемся окне. При удалении логического условия все дочерние записи, входящие в него, также будут удалены.

При добавлении условий и логических условий существуют правила, от выполнения которых зависит иерархическое размещение созданных объектов:

- список пустой и добавляется условие или логическое условие – новое условие или логическое условие будет добавлено на верхний уровень иерархии;
- в списке содержится одно условие и добавляется условие – новое условие будет объединено с уже существующим с помощью логического условия «И»;
- из существующего иерархического списка ничего не выбрано и добавляется условие – новое условие будет добавлено в корень логического условия на верхнем уровень иерархии;
- из существующего иерархического списка на одном уровне выбрано одно или несколько условий и добавляется условие – новое условие будет добавлено на тот же уровень, что и выбранные условия;
- из списка выбрано логическое условие и добавляется условие – новое условие будет добавлено внутрь выбранного логического условия;
- из существующего иерархического списка ничего не выбрано и добавляется логическое условие – новое логическое условие будет добавлено на верхний уровень иерархии, существовавшая ранее иерархия объектов будет перемещена внутрь него;
- из существующего иерархического списка на одном уровне выбрано одно или несколько условий и добавляется логическое условие – выбранные условия будут перемещены внутрь нового логического условия, которое будет добавлено на текущий уровень иерархии;
- из списка выбрано логическое условие и добавляется логическое условие – новое логического условие будет добавлено внутрь выбранного логического условия.

Если при добавлении условия или логического условия были выбраны строки из разных родительских элементов, или выбраны строки только с логическими условиями, или выбраны строки с условиями разного типа, Система выдаст ошибку.

3) «Ответ»

   Содержит одно или несколько условий для проверки ответа на запрос.

   Блок «Ответ» идентичен блоку «Запрос», управляющие элементы и правила добавления условий и логических условий аналогичные.

   В качестве проверяемых параметров могут выступать: «Значение» (полученное в ответе на запрос), «Название колонки», «Время перехвата ответа».

4) «Связи»

   Определяет необходимость выполнения условий для проверки запроса и ответа на запрос в соответствии с логическим условием «И»/«ИЛИ».

5) «Реакции»

   Определяет действие («Предупредить» или «Игнорировать»), которое будет применено к запросу в результате срабатывания политики.

Для сохранения изменений, внесенных в карточку политики, используется кнопка «Сохранить».

До подтверждения политика будет находиться в статусе «Настройка».

3.5.3. Управление политиками

После создания политики она появляется в списке политик в статусе «Настройка».

Для начала использования политики необходимо нажать кнопку «Подтвердить» в ее карточке. Кнопка подтверждения доступна при наличии хотя бы одного добавленного условия для проверки запроса в карточке политики. Для успешного подтверждения политики все логические условия в блоках «Запрос» и «Ответ» должны содержать дочерние элементы.

Для включения или выключения политики на отдельных БД необходимо выбрать ее из списка, вызвать выпадающее меню «Связать с базой данных» и выбрать пункт «Вкл/Выкл выборочно».

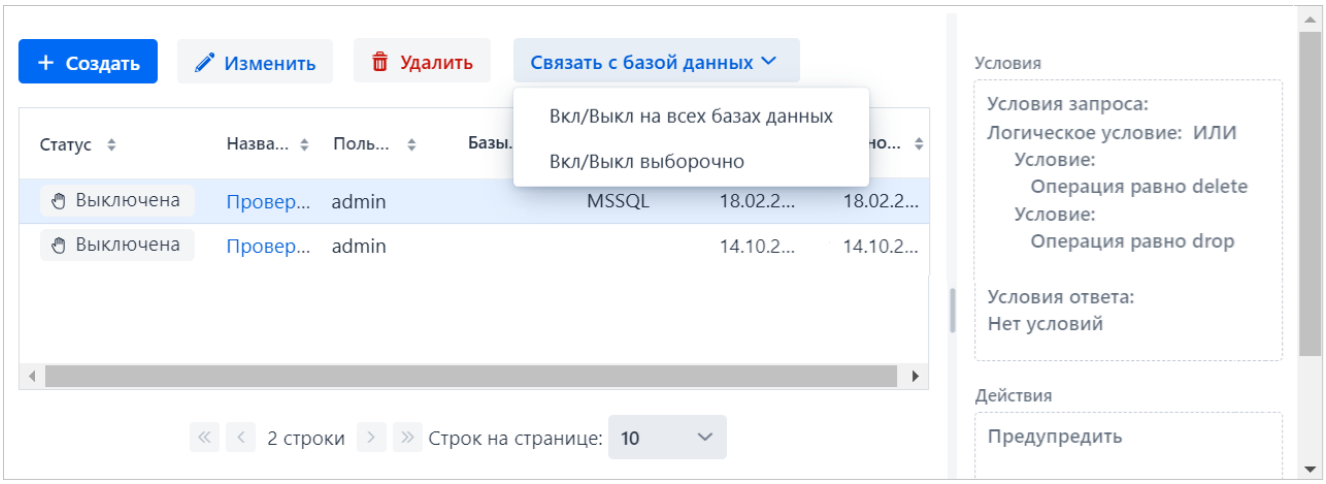

Рисунок 35 – Включение/выключение политики

В появившемся окне необходимо выбрать из списка БД, для которых должна применяться политика, и нажать кнопку «Сохранить». Для БД, не выбранных из списка, политика применяться не будет.

Если из списка выбрана хотя бы одна БД, политика будет находиться в статусе «Включена». Если из списка не выбрана ни одна БД, политика будет находиться в статусе «Выключена».

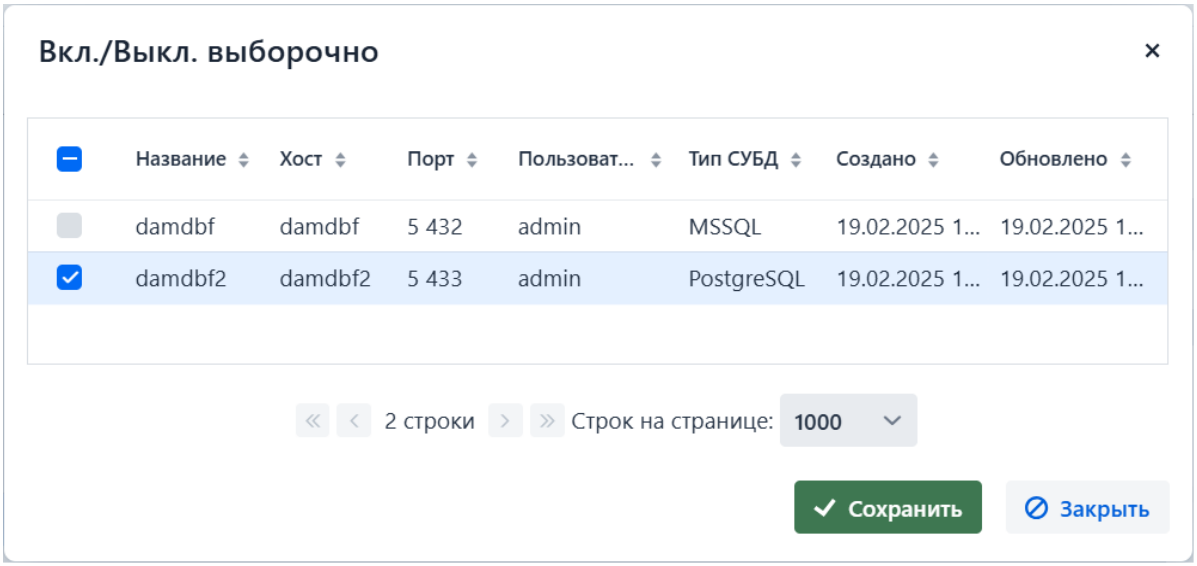

Рисунок 36 – Выборочное включение/выключение политики

Для включения политики на всех БД, добавленных в Систему, необходимо выбрать из списка политику со статусом «Выключена», вызвать выпадающее меню «Связать с базой данных» и выбрать пункт «Вкл/Выкл на всех базах данных» – статус политики изменится на «Включение», затем – на «Включена». Если при попытке включения политики возникнет ошибка в коллекторе или сообщение о включении политики не поступит в коллектор, политика останется в статусе «Включение».

Для выключения политики на всех БД, добавленных в Систему, необходимо выбрать из списка политику со статусом «Включена», вызвать выпадающее меню «Связать с базой данных» и выбрать пункт «Вкл/Выкл на всех базах данных» – статус политики изменится на «Выключение», затем – на «Выключена». Если при попытке выключения политики возникнет ошибка в коллекторе или сообщение о выключении политики не поступит в коллектор, политика останется в статусе «Выключение». Если политика была включена выборочно на отдельных БД, при попытке ее выключения она не будет выключена, и произойдет включение этой политики на всех БД.

3.6. Базы данных

3.6.1. Общая информация

Трафик, идущий к отслеживаемой БД, проверяется на соответствие политикам, созданным в Системе. Сначала БД должна быть добавлена в Систему. После этого в отношении данной БД могут быть включены политики.

Список БД содержится в разделе Системы «Базы данных». Над таблицей со списком присутствует фильтр для поиска БД по различным атрибутам.

Для БД может применяться тотальное сохранение трафика, при котором в Системе будет отображаться и сохраняться весь трафик (запросы и ответы на запросы), идущий к данной БД. При включении или выключении режима тотального сохранения в строке с БД будет отображен статус «В процессе», при завершении включения – «Включено», при завершении выключения – «Выключено», при ошибке включения или выключения – «Ошибка».

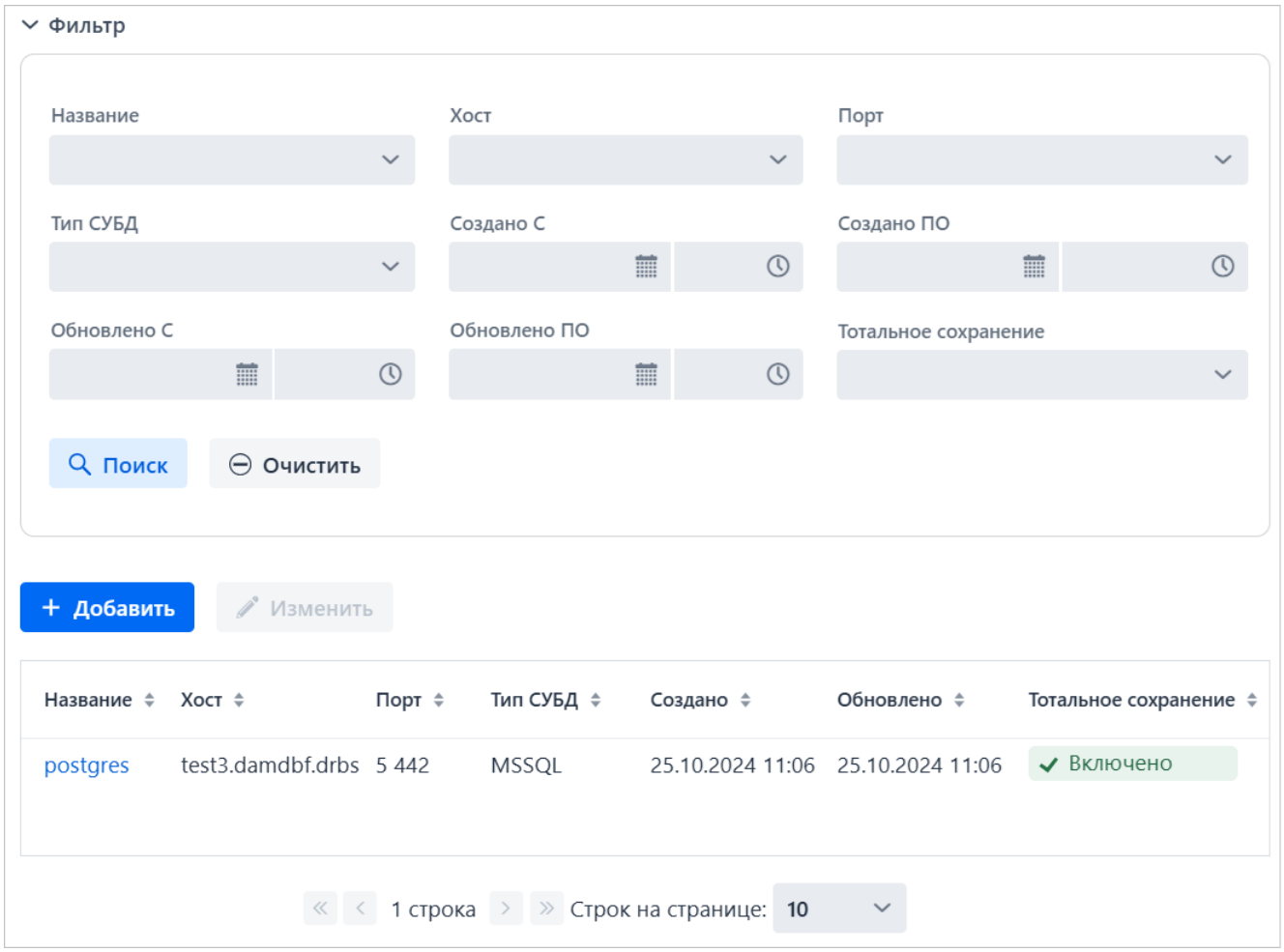

Рисунок 37 – Раздел «Базы данных»

Для редактирования существующей БД необходимо выбрать ее из списка, нажать кнопку «Изменить».

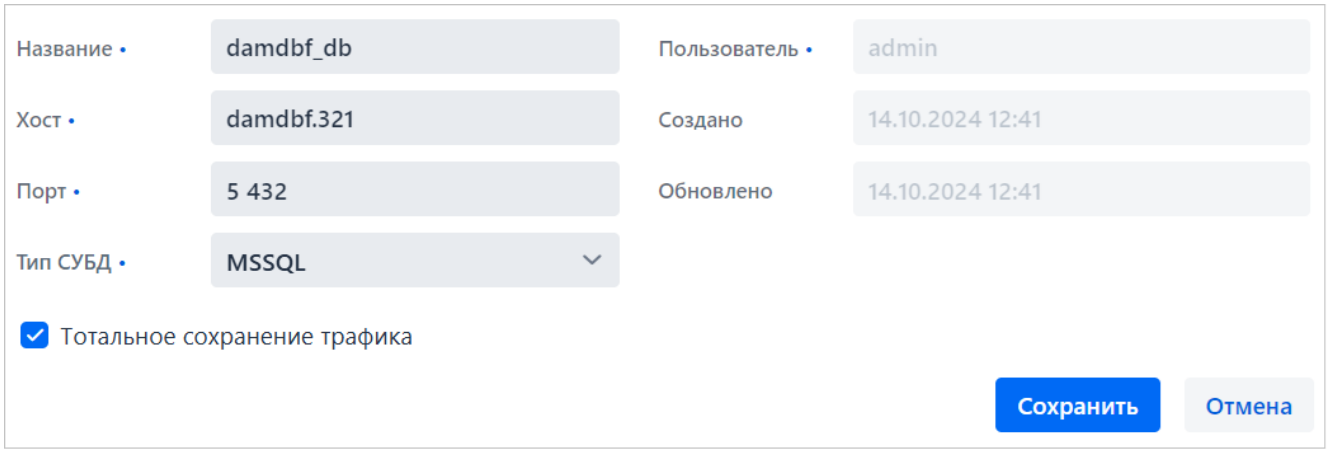

Рисунок 38 – Карточка БД при редактировании

Карточка БД содержит в себе следующие поля:

- «Название» – название БД;
- «Хост» – хост БД (максимальное количество вводимых символов – 255);
- «Порт» – порт БД (может быть заполнено только целым неотрицательным числом от 0 до 65535);
- «Тип СУБД» – тип СУБД, поддерживаемый Системой;
- «Тотальное сохранение трафика» – флажок для включения режима тотального сохранения трафика, идущего к данной БД;
- «Пользователь» – пользователь, добавивший БД в Систему;
- «Создано» – дата и время добавления БД;
- «Обновлено» – «Создано» – дата и время обновления сведений о БД.

Сведения о пользователе и времени создания/обновления БД изменению не подлежат.

Для сохранения изменений, внесенных в карточку БД, используется кнопка «Сохранить».

3.6.2. Добавление базы данных

Для добавления БД используется кнопка «Добавить» в разделе Системы «Базы данных». На странице добавления БД необходимо заполнить все обязательные поля и нажать кнопку «Сохранить» – БД появится в списке всех БД.

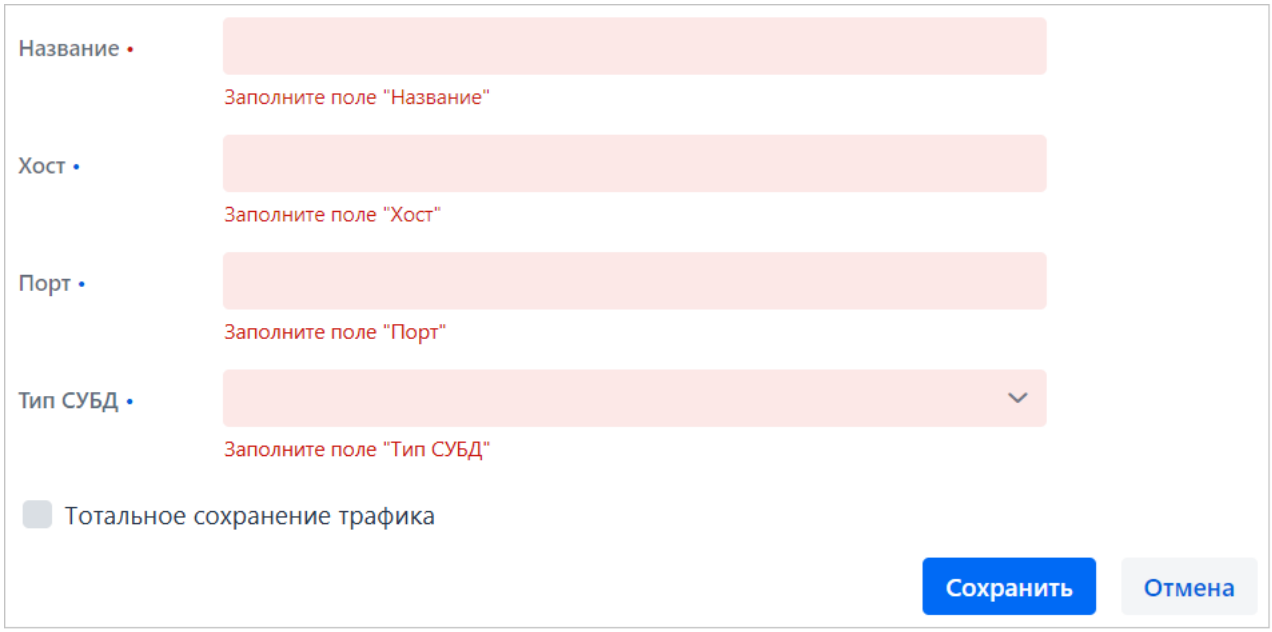

Рисунок 39 – Карточка БД при создании

3.7. Регулярные выражения

3.7.1. Общая информация

Регулярные выражения (далее – РВ) используются в политиках для анализа и фильтрации трафика. Они позволяют распознавать в запросах и ответах на запросы наличие конфиденциальной информации (такой как номера кредитных карт, паспортные данные, ИНН, адреса электронной почты и другие типы личной информации). Для начала использования РВ оно должно быть добавлено в политику в качестве условия для проверки.

Список РВ содержится в разделе Системы «Регулярные выражения». Над таблицей со списком присутствует фильтр для поиска РВ по различным атрибутам.

В разделе содержится набор предустановленных РВ, которые не могут быть изменены или удалены. Пользователь может создавать собственные РВ.

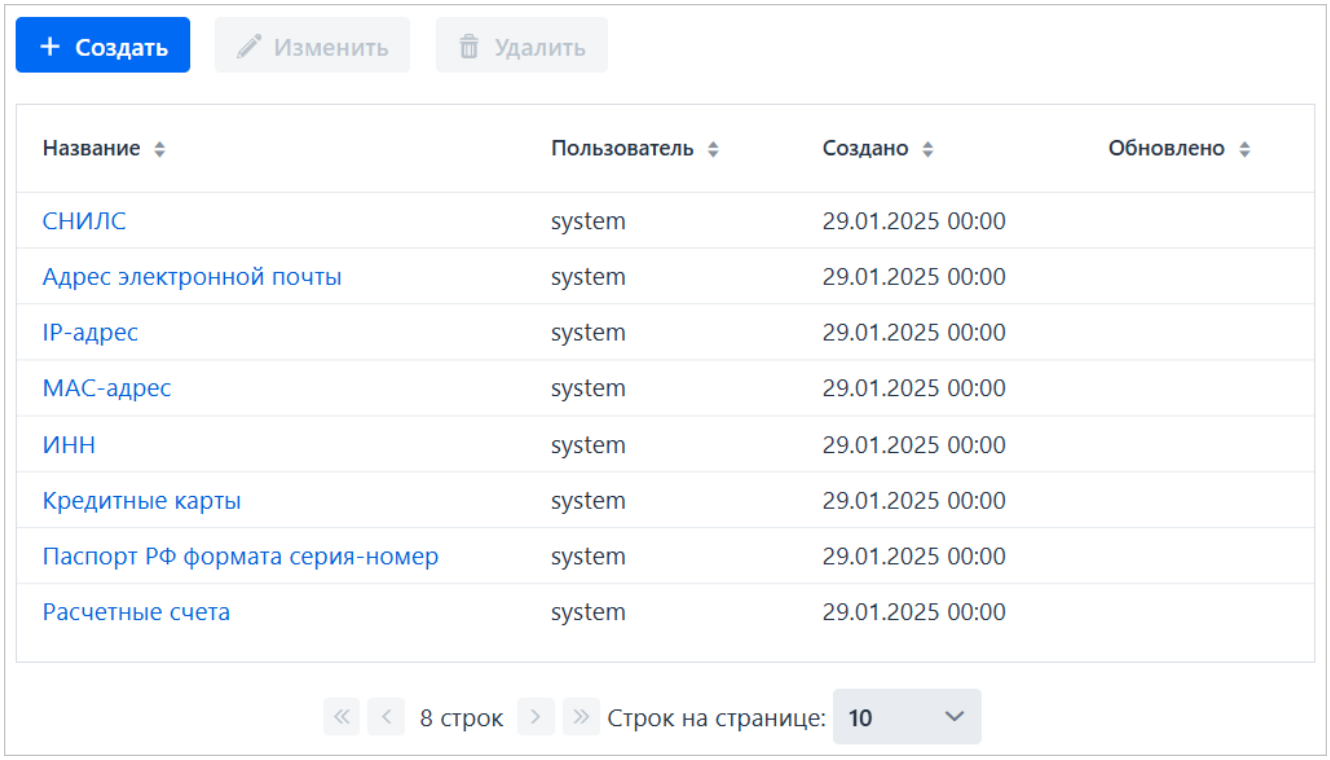

Рисунок 40 – Раздел «Регулярные выражения»

Переход к просмотру любого РВ выполняется нажатием на его название, являющееся гиперссылкой.

Карточка РВ содержит в себе следующие поля:

– «Название» – название РВ, отображаемое в Системе;
– «Значение» – значение РВ.

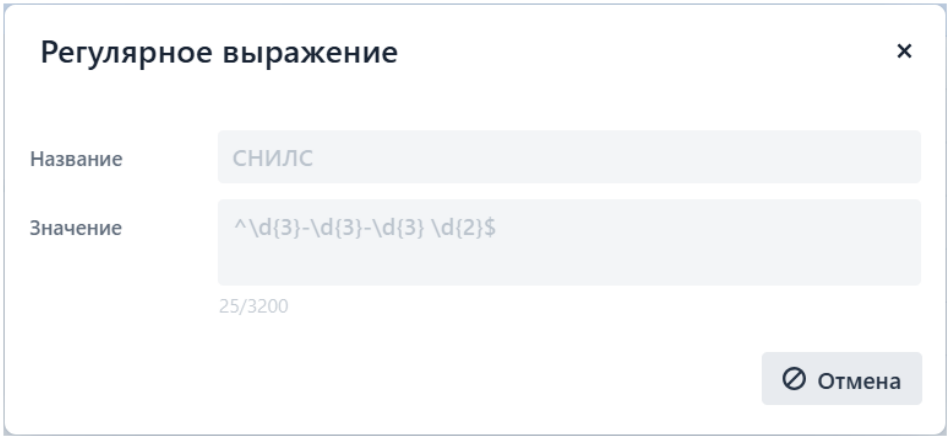

Рисунок 41 – Окно просмотра регулярного выражения

Для редактирования пользовательского РВ необходимо выбрать его из списка, нажать кнопку «Изменить», внести изменения в появившемся окне и нажать кнопку «Сохранить».

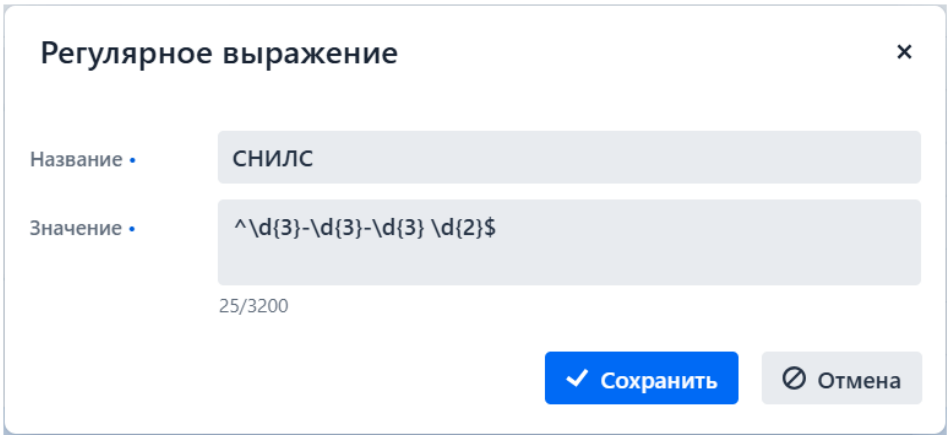

Рисунок 42 – Окно редактирования пользовательского регулярного выражения

Для удаления пользовательского РВ необходимо выбрать его из списка, нажать кнопку «Удалить» и подтвердить действие в появившемся окне.

Если выбранное РВ используется хотя бы в одной политике, его изменение и удаление будут невозможны, а Система отобразит соответствующее сообщение об ошибке со списком связанных политик. Название каждой политики является гиперссылкой, при нажатии на которую открывается новая вкладка браузера с карточкой политики.

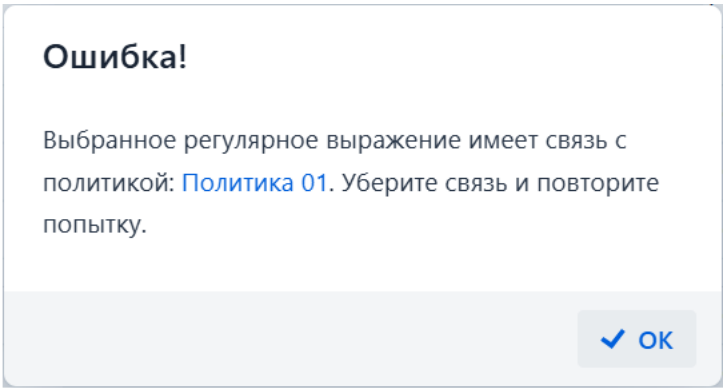

Рисунок 43 – Ошибка при удалении/редактировании регулярного выражения

3.7.2. Создание регулярного выражения

Для создания РВ используется кнопка «Создать» в разделе Системы «Регулярные выражения». В окне создания РВ необходимо заполнить все обязательные поля и нажать кнопку «Сохранить» – РВ появится в списке. Для сохранения текущего РВ и добавления еще одного РВ используется кнопка «Сохранить и добавить еще».

При наличии ошибок в синтаксисе значения РВ Система отобразит соответствующее сообщение. При попытке сохранения РВ с названием (чувствительно к регистру), уже существующим в Системе, также возникнет ошибка.

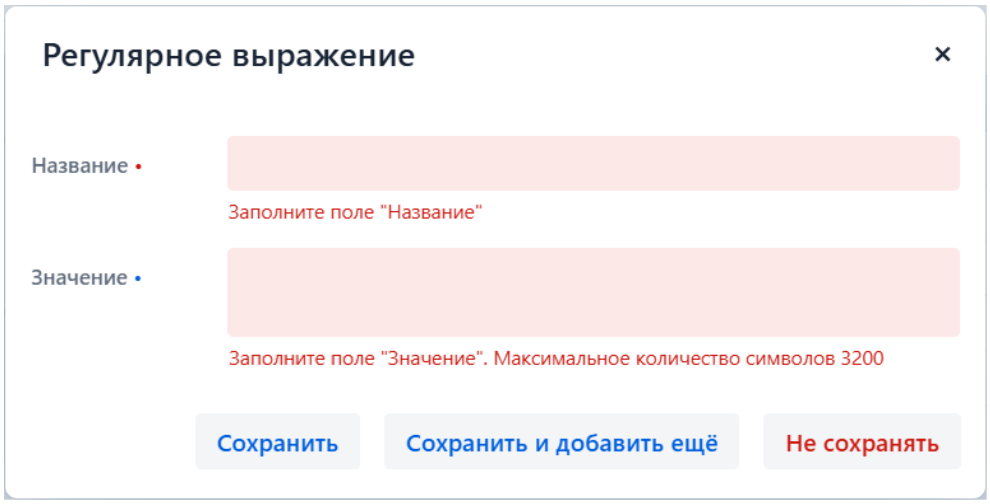

Рисунок 44 – Карточка регулярного выражения при создании

3.8. Справочник

3.8.1. Общая информация

Справочник содержит списки значений, которые могут быть загружены в качестве условий при настройке политик. Данная форма удобна для использования и позволяет создавать одно условие для проверки набора значений вместо создания множества условий. Список может содержать в себе не более 10000 значений.

Списки из справочника содержатся в разделе Системы «Справочник». Над таблицей присутствует фильтр для поиска списков по различным атрибутам. Доступ к данному разделу есть только у администратора Системы.

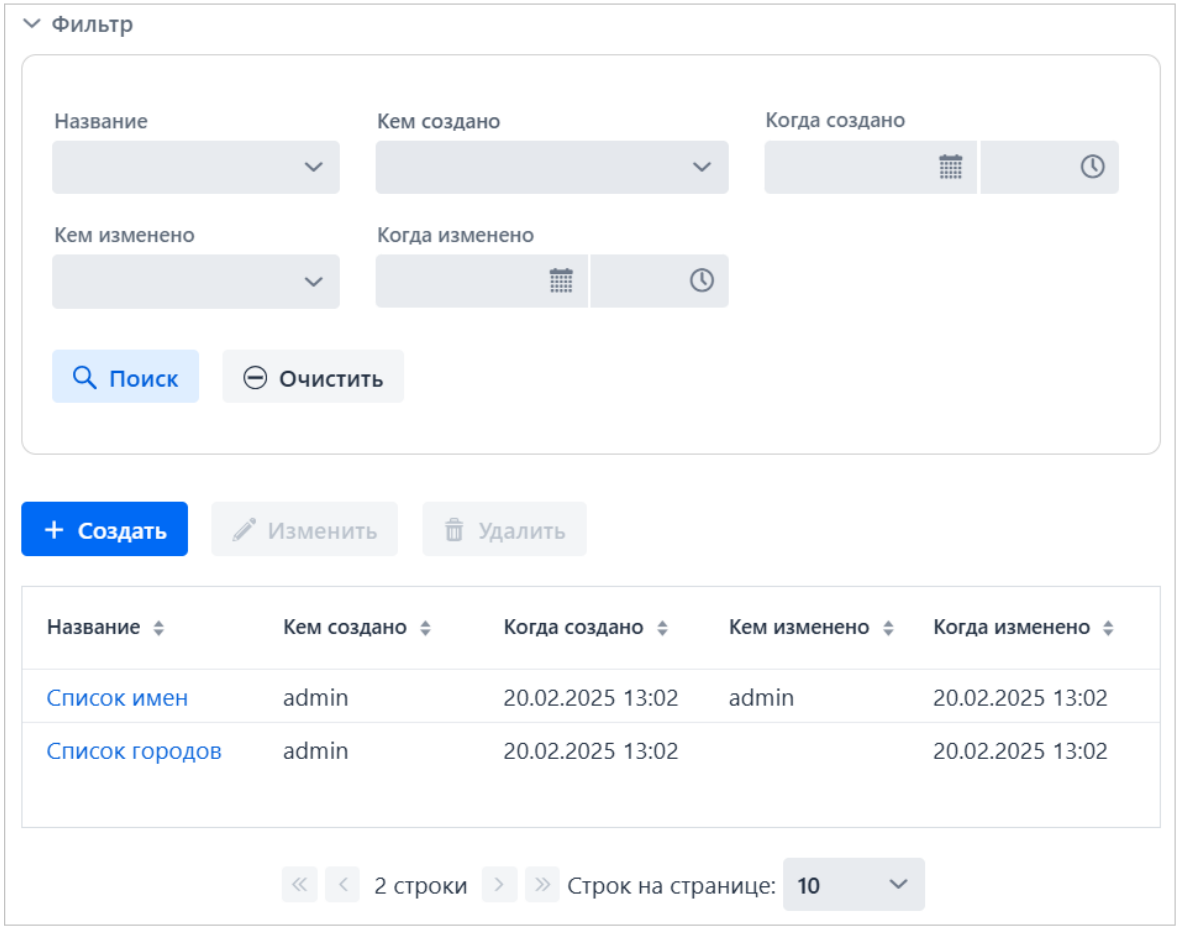

Рисунок 45 – Раздел «Справочник»

Для редактирования списка необходимо нажать на его название, являющееся гиперссылкой, или выбрать список и нажать кнопку «Изменить» – откроется карточка со значениями списка. С помощью фильтра вверху карточки осуществляется поиск по значениям списка.

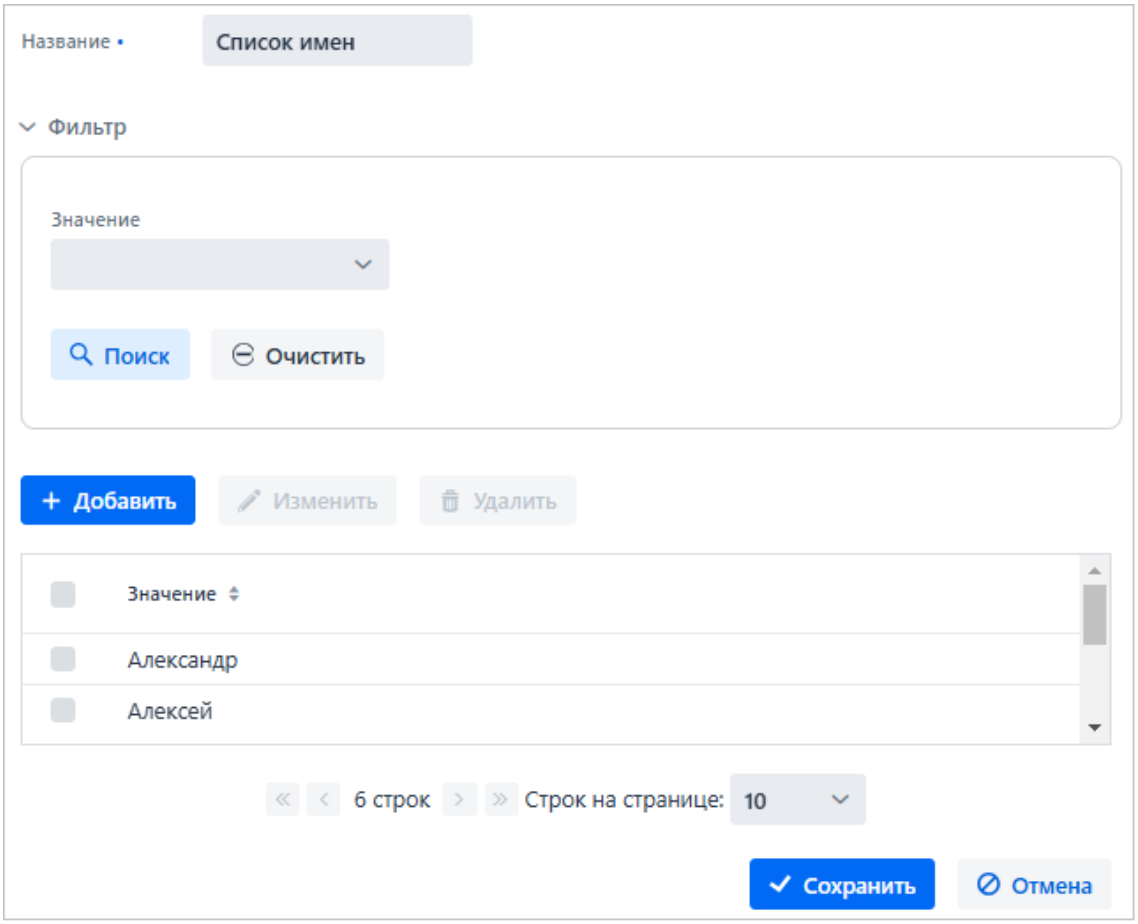

Рисунок 46 – Карточка списка при редактировании

Для редактирования значения списка необходимо установить флажок напротив него, нажать кнопку «Изменить», внести изменения и нажать кнопку «Сохранить» в окне изменения значения.

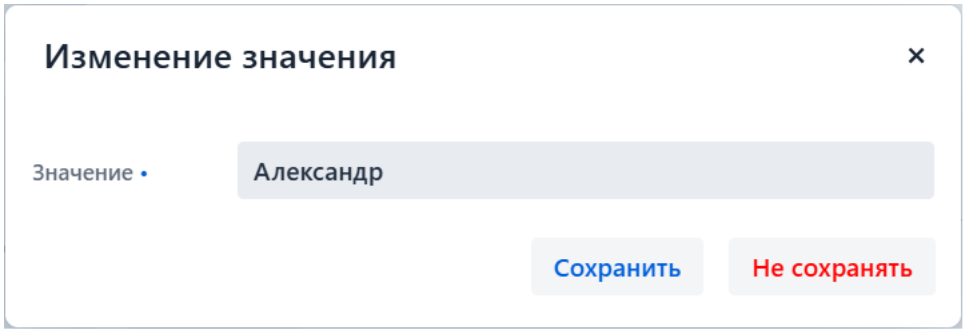

Рисунок 47 – Окно редактирования значения списка

Для удаления одного или нескольких значений списка необходимо установить флажки напротив них и нажать кнопку «Удалить» в карточке списка.

Для сохранения изменений, внесенных в карточку списка, используется кнопка «Сохранить».

Для удаления списка необходимо выбрать его в разделе «Справочник», нажать кнопку «Удалить» и подтвердить действие в появившемся окне.

Если выбранный список используется хотя бы в одной политике, его изменение и удаление будут невозможны, а Система отобразит соответствующее сообщение об ошибке со списком связанных политик. Название каждой политики является гиперссылкой, при нажатии на которую открывается новая вкладка браузера с карточкой политики.

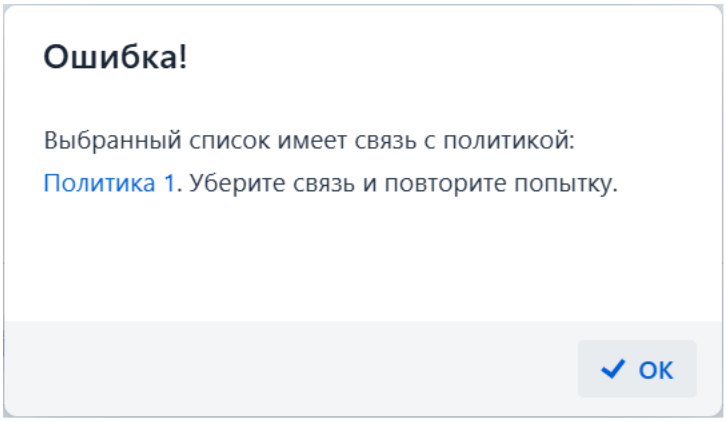

Рисунок 48 – Ошибка при удалении/редактировании списка

3.8.2. Создание списка

Для создания списка используется кнопка «Создать» в разделе Системы «Справочник». На странице создания списка необходимо заполнить поля:

- «Название» – название списка, отображаемое в Системе;
- «Значение» – перечень значений списка (в список может быть добавлено не более 10000 значений, каждое значение вводится с новой строки).

Для сохранения внесенных данных используется кнопка «Сохранить». При попытке сохранения списка с названием (чувствительно к регистру), уже существующим в Системе, возникнет соответствующая ошибка.

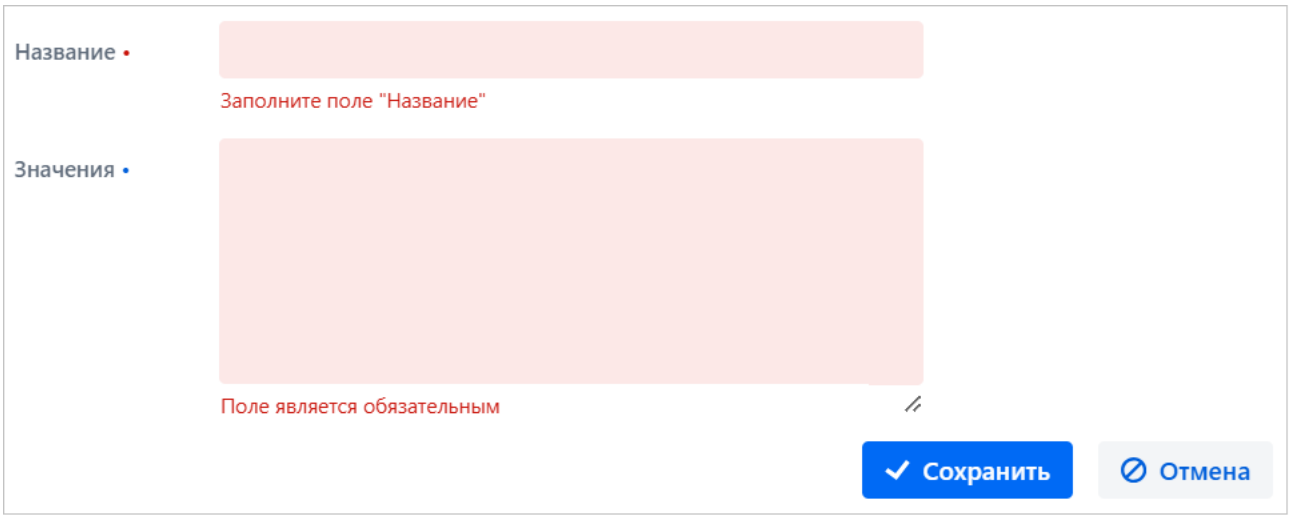

Рисунок 49 – Карточка списка при создании

После создания списка в него могут быть добавлены дополнительные значения. Для этого необходимо перейти в карточку списка, нажать кнопку «Добавить» и в появившемся окне ввести новое значение. Для сохранения и возврата в карточку списка используется кнопка «Сохранить» в окне добавления значения. Для сохранения текущего значения и добавления еще одного значения используется кнопка «Сохранить и добавить еще».

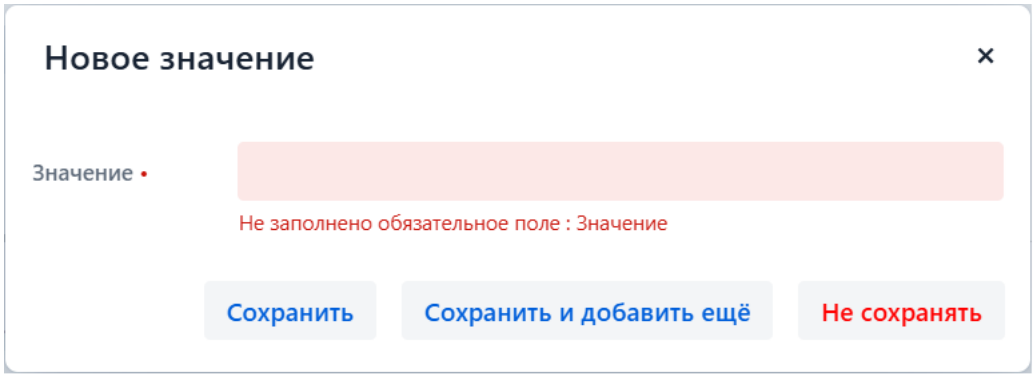

Рисунок 50 – Окно добавления значения списка

4. АДМИНИСТРИРОВАНИЕ

4.1. Пользователи

4.1.1. LDAP-пользователи

4.1.1.1. Общая информация

LDAP-пользователи могут быть загружены в Систему из Active Directory. При попытке входа через LDAP учетную запись аутентификация в Системе будет происходить с помощью средств Active Directory.

Для LDAP учетной записи нельзя сбросить или изменить пароль, дополнительно для такой учетной записи автоматически проставляется признак «Ldap» – так можно отличать Ldap-учетные записи от локальных учетных записей. При деактивации учетной записи в Active Directory она также будет деактивирована в Системе.

Таким образом, интеграция с LDAP позволяет автоматически синхронизировать параметры пользователя (таких, как фамилия, имя, email и др.) со службой каталогов Active Directory.

4.1.1.2. Создание LDAP-пользователя

При первом входе пользователя в Систему с использованием доменных учетных данных в базе данных Системы автоматически создается соответствующий пользователь (если он еще не был создан ранее), и производится его синхронизация с LDAP (все атрибуты пользователя приводятся в соответствие с Active Directory).

4.1.1.3. Редактирование LDAP-пользователя

При настроенной интеграции с LDAP изменение атрибутов пользователя происходит в Active Directory, т.к. при следующем входе пользователя в Систему атрибуты будут обновлены в карточке пользователя в самой Системе. Изменения, внесенные в карточку пользователя через интерфейс Системы, при следующем входе пользователя из Active Directory будут перезаписаны на данные из Active Directory.

4.1.2. Локальные пользователи

4.1.2.1. Общая информация

При входе пользователя в Систему с локальной учетной записью корректность введенных логина и пароля проверяется самой Системой. Список учетных записей пользователей, зарегистрированных в Системе, содержится в разделе «Администрирование» → «Пользователи».

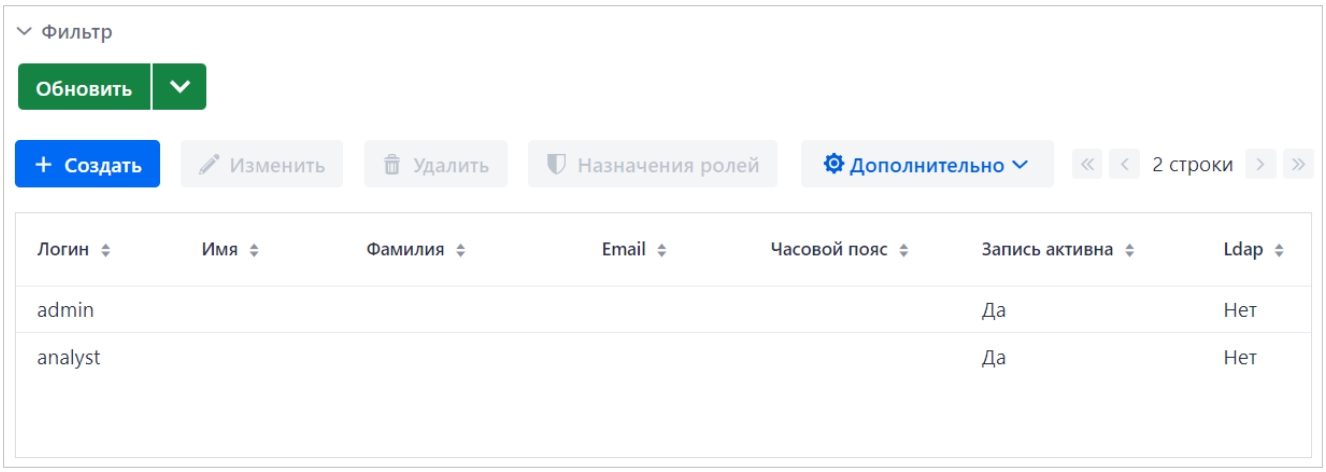

Рисунок 51 – Подраздел «Пользователи»

Для просмотра или изменения учетной записи пользователя необходимо выбрать ее из списка и нажать кнопку «Изменить».

Карточка учетной записи пользователя содержит в себе следующие поля:

- «Логин» – логин пользователя, используемый для входа в Систему;
- «Имя» – имя пользователя;
- «Фамилия» – фамилия пользователя;
- «Email» – адрес электронной почты пользователя;
- «Часовой пояс» – часовой пояс пользователя;
- «Запись активна» – признак активности учетной записи, позволяющий ее использование в Системе;
- «Ldap» – признак, указывающий на то, что учетная запись была синхронизирована через LDAP (всегда недоступен для редактирования).

Для сохранения внесенных изменений используется кнопка «ОК» в карточке.

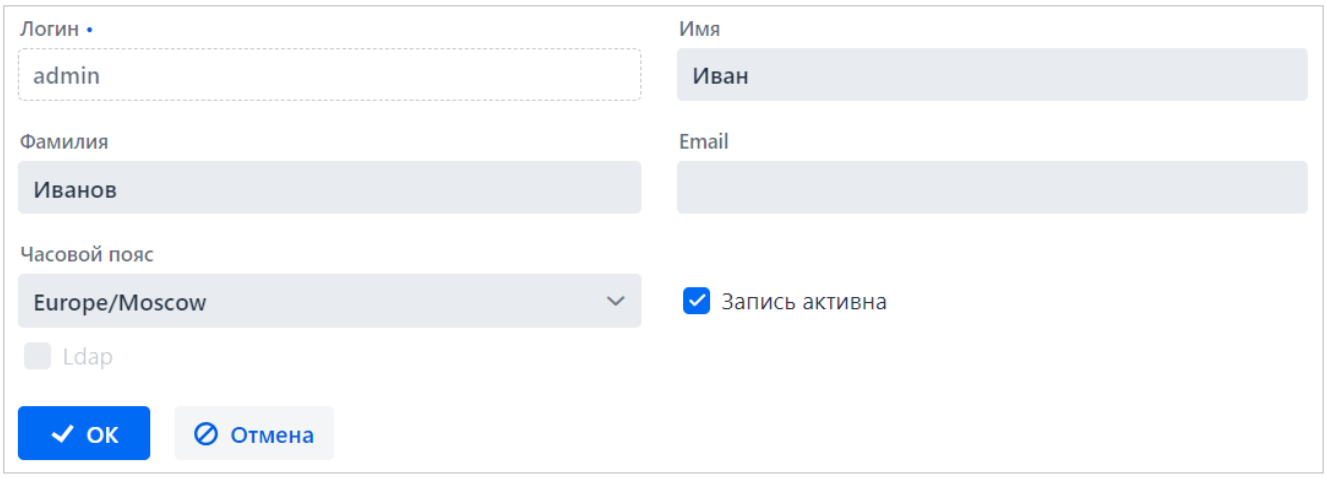

Рисунок 52 – Карточка учетной записи пользователя

Для изменения пароля учетной записи пользователя необходимо выбрать запись из списка, раскрыть выпадающее меню «Дополнительно» и выбрать пункт «Сменить пароль». В открывшемся окне необходимо ввести текущий пароль, новый пароль и нажать кнопку «ОК». При следующем входе в Систему выбранному пользователю необходимо будет ввести заданный новый пароль.

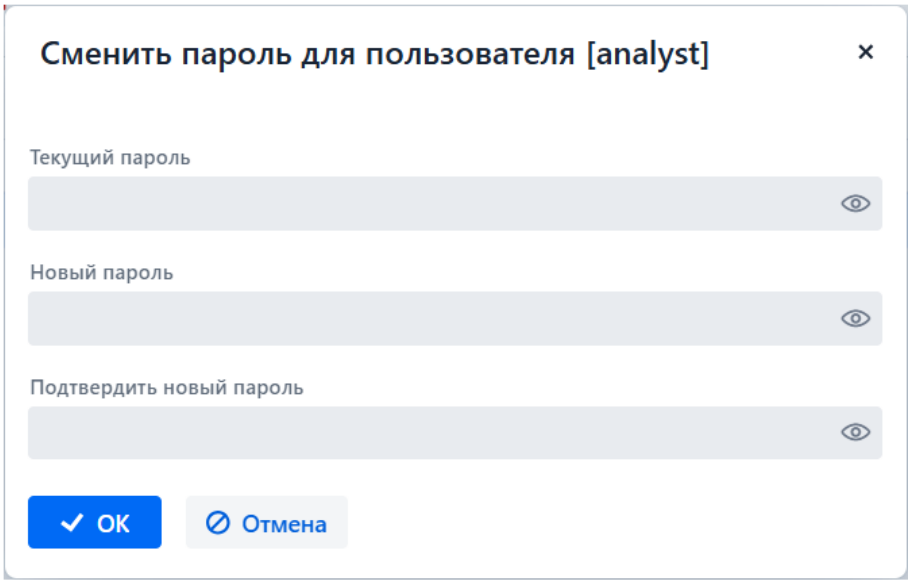

Рисунок 53 – Окно изменения пароля учетной записи пользователя

Для сброса и генерации нового пароля учетной записи пользователя необходимо выбрать запись из списка, раскрыть выпадающее меню «Дополнительно» и выбрать пункт «Сброс паролей». В появившемся окне необходимо нажать кнопку «Сгенерировать и сохранить» – появится поле с логином и новым паролем, который необходимо передать пользователю для использования при следующем входе в Систему.

Рисунок 54 – Генерация нового пароля учетной записи пользователя

Для удаления учетной записи пользователя необходимо выбрать ее из списка, нажать кнопку «Удалить» и подтвердить удаление в появившемся окне.

4.1.2.2. Создание локального пользователя

Для создания учетной записи пользователя используется кнопка «Создать» в разделе Системы «Администрирование» → «Пользователи».

На странице создания учетной записи пользователя необходимо заполнить все обязательные поля и нажать кнопку «ОК» – учетная запись появится в списке. Для того, чтобы учетную запись можно было использовать в Системе, в ее карточке должен быть установлен флажок «Запись активна».

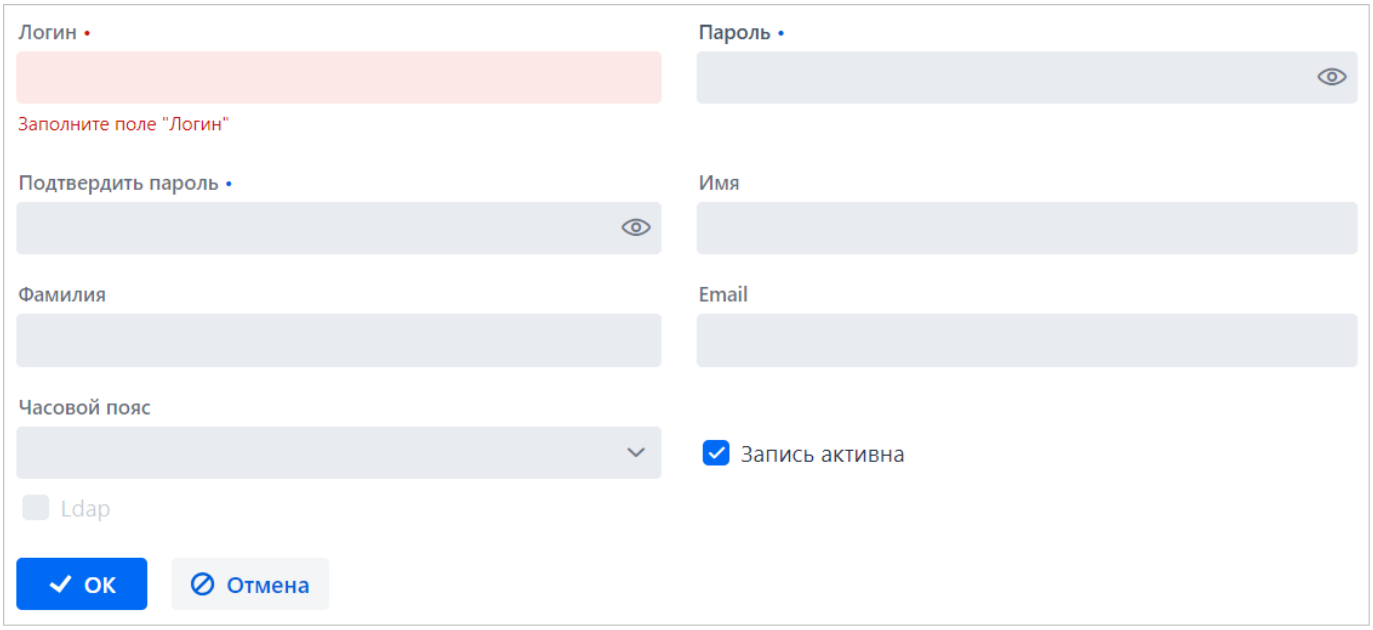

Рисунок 55 – Карточка учетной записи пользователя при создании

4.2. Ролевая модель управления доступом

4.2.1. Матрица ролей и полномочий

В таблице 1 представлена матрица ролей и полномочий пользователей Системы («C» – создание (CREATE), «R» – чтение (READ), «U» – изменение (UPDATE), «D» – удаление (DELETE), прочерк – отсутствие доступа).

Таблица 1 – Матрица ролей и полномочий пользователей Системы

Разделы Системы	Роли пользователей	
	Аналитик	Администратор
Агенты	R	RU
Трафик	R	R
Политики	R	CRUD
Базы данных	R	CRU
Регулярные выражения	R	CRUD*
Справочник	–	CRUD
Пользователи	–	CRUD
Ресурсные роли	–	CRUD
Роли уровня строк	–	CRUD

* – удаление доступно только для объектов, созданных пользователем

4.2.2. Роли

4.2.2.1. Общая информация

В Системе используется преднастроенная ролевая модель управления доступом. Существуют ресурсные роли и роли уровня строк.

Каждому пользователю может быть назначено несколько ролей. В таком случае он получит объединенные права от всех имеющихся у него ролей.

В Системе настроены ресурсные роли:

- аналитик – обладает минимальными правами на просмотр разделов Системы и их содержимого;
- администратор – обладает полными правами на выполнение любых действий в Системе.

Если для роли не предусмотрен доступ к какому-то разделу в Системе, этот раздел не отображается в панели навигации у пользователей с этой ролью.

Если у пользователя есть доступ к разделу Системы, но нет прав на действия в нем, соответствующие этим действиям кнопки будут недоступны.

Запрещается пользователям без роли администратора Системы создавать, редактировать, удалять и переназначать роль для пользователя с ролью администратора Системы.

4.2.2.2. Ресурсные роли

Ресурсные роли ограничивают права доступа пользователей к разделам Системы, экранам, атрибутам объектов и т.д. Список ресурсных ролей содержится в разделе «Администрирование» → «Ресурсные роли». Над таблицей со списком присутствует фильтр для поиска ролей по различным атрибутам.

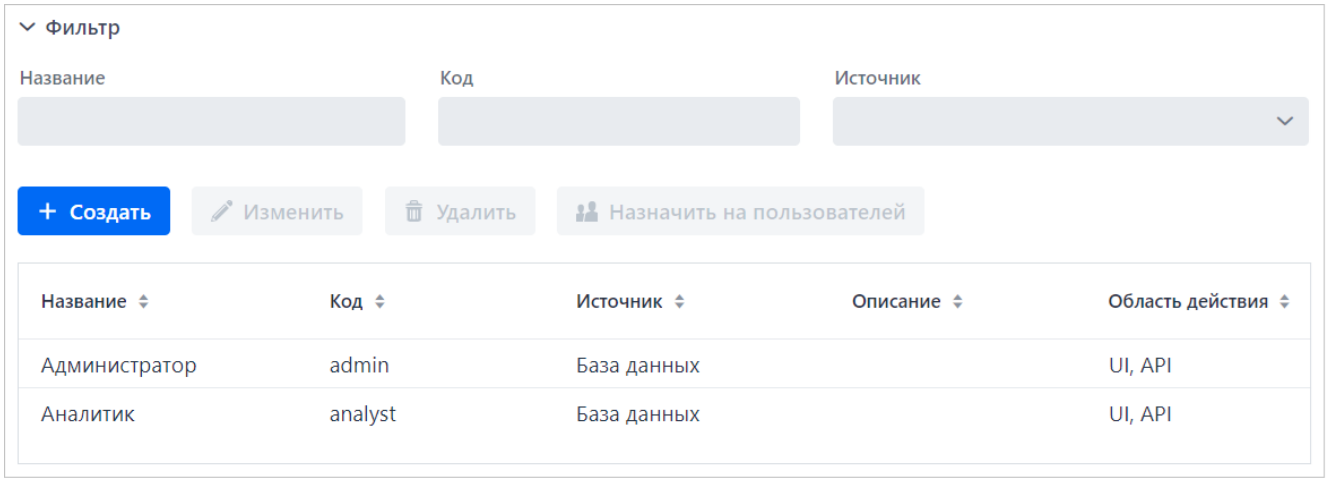

Рисунок 56 – Подраздел «Ресурсные роли»

Для просмотра или изменения ресурсной роли необходимо выбрать ее из списка, нажать кнопку «Изменить», внести изменения и нажать кнопку «ОК».

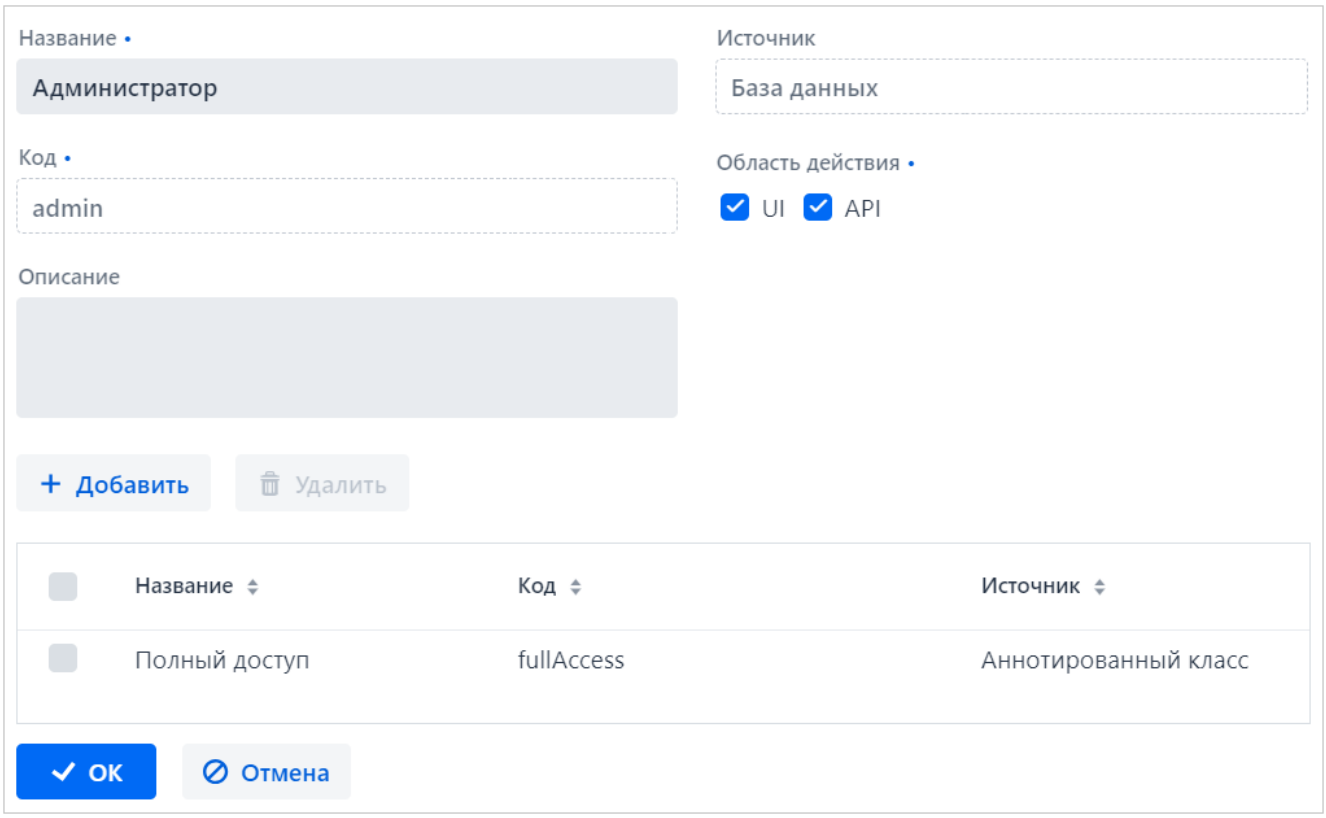

Рисунок 57 – Карточка ресурсной роли

Для удаления ресурсной роли необходимо выбрать ее из списка, нажать кнопку «Удалить» и подтвердить удаление в появившемся окне.

Для создания ресурсной роли используется кнопка «Создать» в разделе Системы «Администрирование» → «Ресурсные роли». В карточке роли необходимо заполнить обязательные поля:

- «Название» – наименование роли;
- «Код» – системное наименование роли;
- «Область действия» – возможность доступа роли к функциям Системы через интерфейс пользователя или API.

Название •

Заполните поле "Название"

Источник

База данных

Код •

Заполните поле "Код"

Область действия •

UI API

Описание

+ Добавить Удалить

Название	Код	Источник

OK Отмена

Рисунок 58 – Карточка ресурсной роли при создании

Для добавления прав ресурсной роли необходимо нажать кнопку «Добавить» в ее карточке – откроется окно со списком для выбора. Над таблицей со списком присутствует фильтр для поиска прав по названию и коду. Необходимо установить флажки напротив нужных прав из списка и нажать кнопку «Выбрать» – права отобразятся в карточке ресурсной роли.

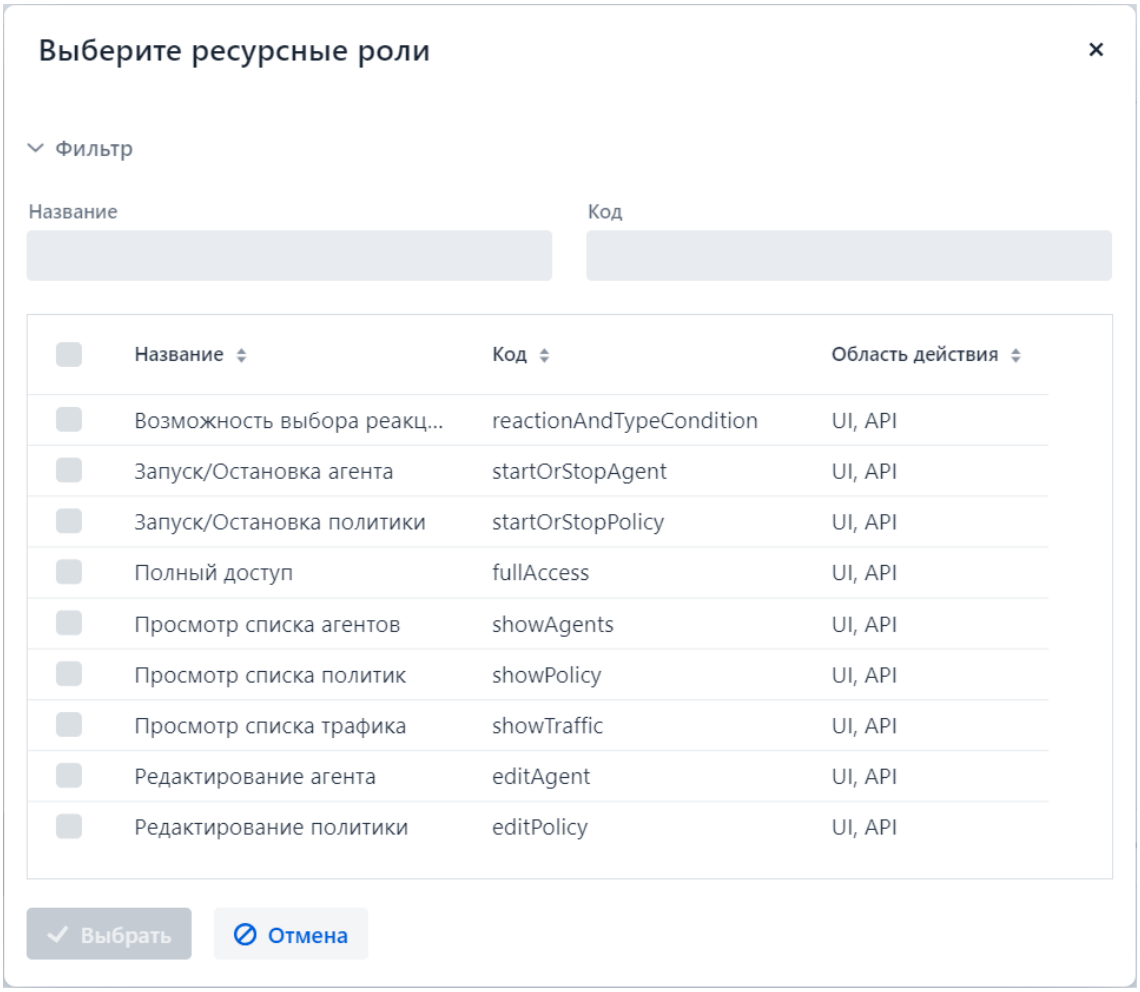

Рисунок 59 – Добавление прав ресурсной роли

Для сохранения внесенных данных используется кнопка «ОК» в карточке ресурсной роли.

4.2.2.3. Роли уровня строк

Роли уровня строк ограничивают для пользователей видимость отдельных записей в разделах Системы.

Список ролей уровня строк содержится в разделе «Администрирование» → «Роли уровня строк». Над таблицей со списком присутствует фильтр для поиска ролей по различным атрибутам.

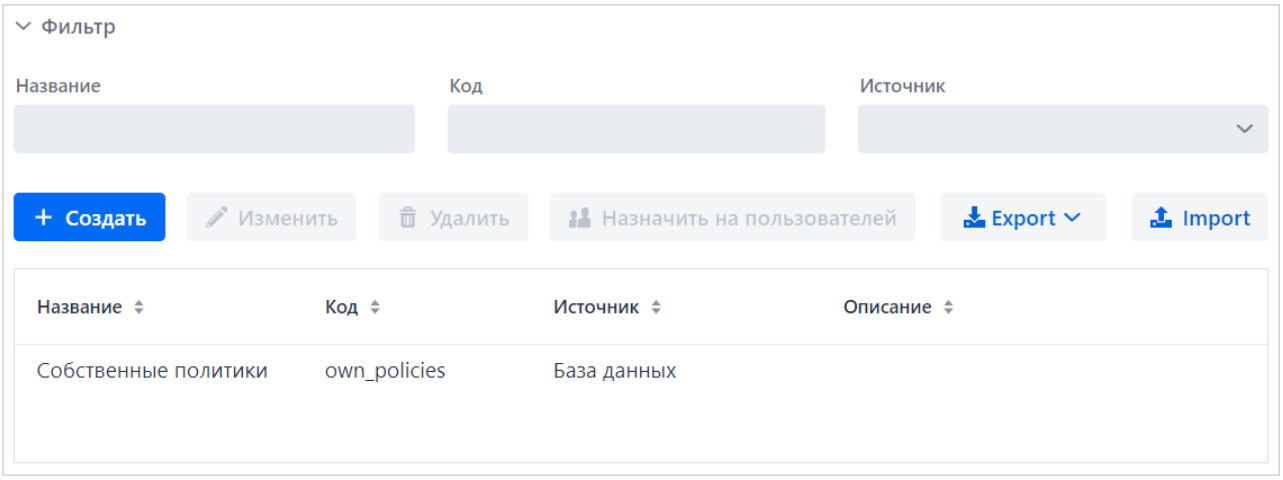

Рисунок 60 – Подраздел «Роли уровня строк»

Для просмотра или изменения роли уровня строк необходимо выбрать ее из списка, нажать кнопку «Изменить», внести изменения и нажать кнопку «ОК».

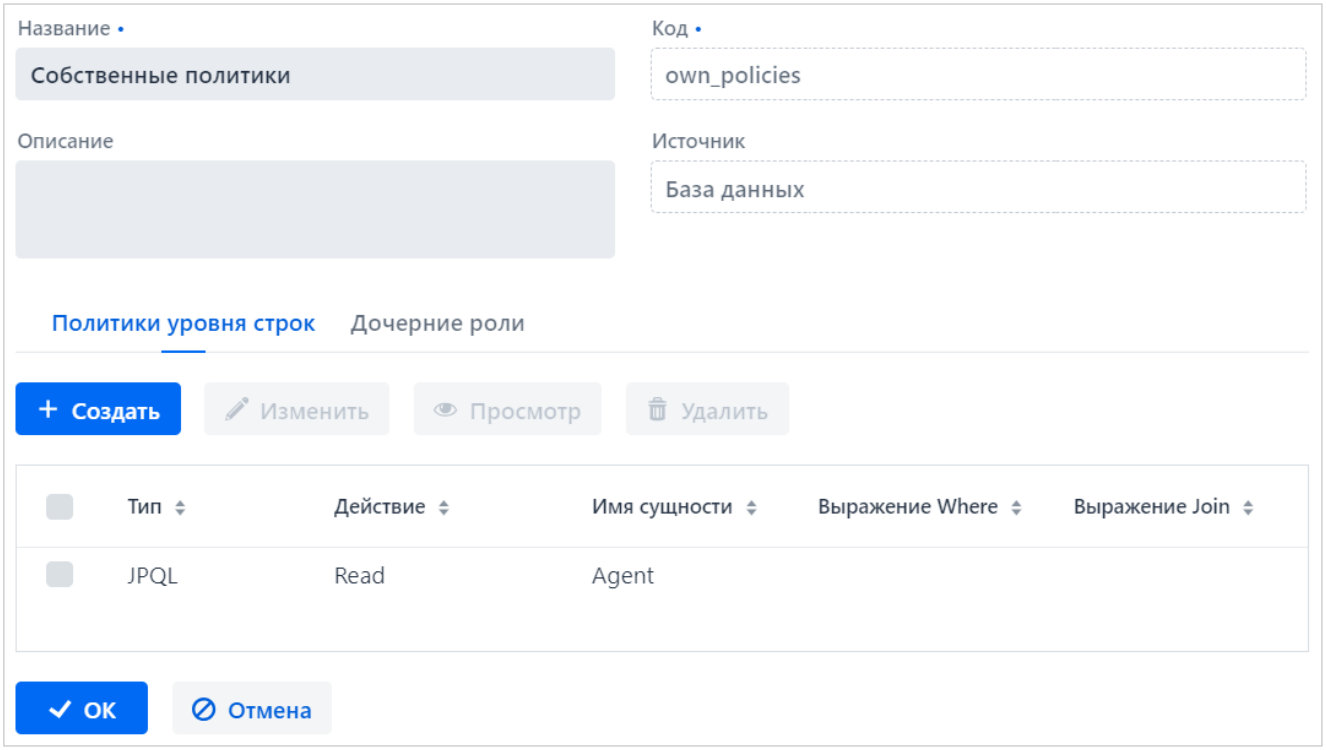

Рисунок 61 – Карточка роли уровня строк

Для экспорта и автоматического скачивания архива со списком ролей уровня строк используется «Export».

Для импорта ролей уровня строк используется кнопка «Import» над списком. Если в файле импорта содержится роль с именем, уже существующим в Системе, она не будет загружена повторно.

Для удаления роли уровня строк необходимо выбрать ее из списка, нажать кнопку «Удалить» и подтвердить удаление в появившемся окне.

Для создания роли уровня строк используется кнопка «Создать» в разделе Системы «Администрирование» → «Роли уровня строк». В карточке роли необходимо заполнить обязательные поля:

– «Название» – наименование роли;
– «Код» – системное наименование роли.

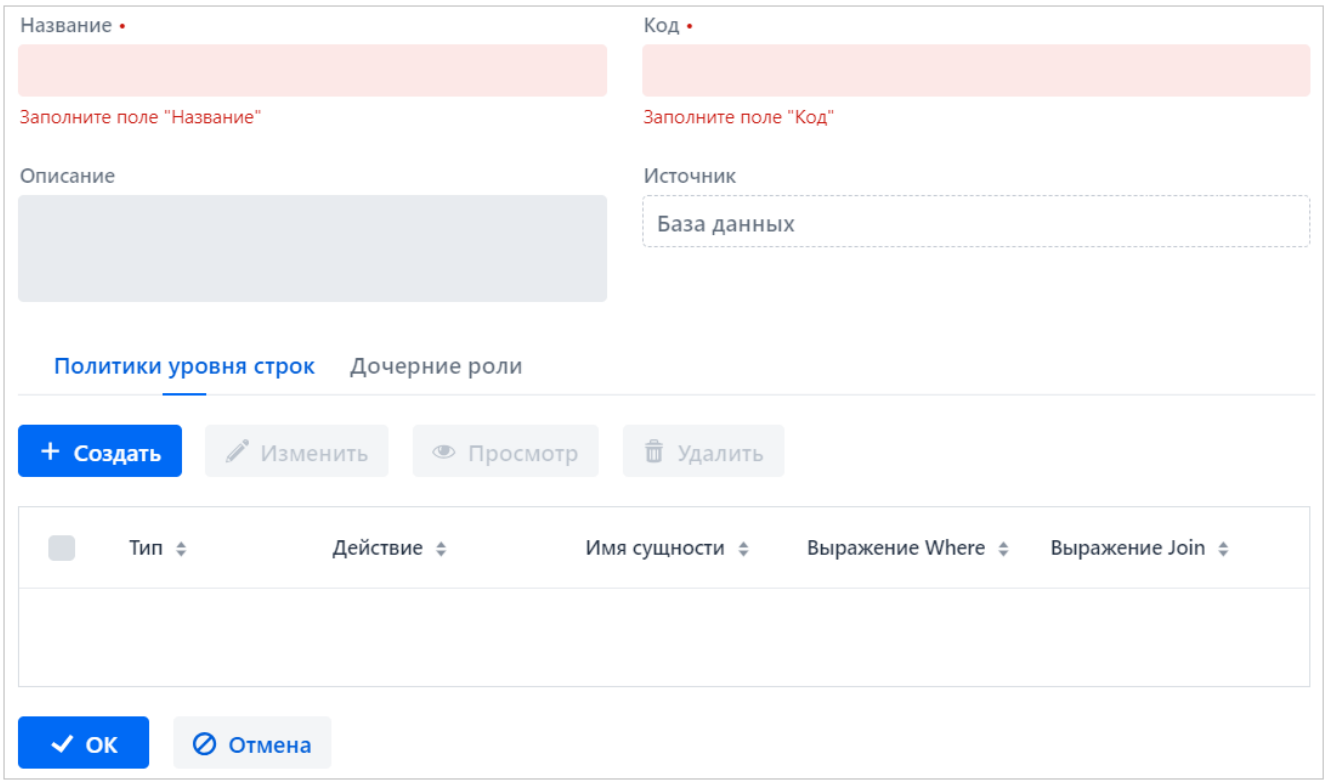

Рисунок 62 – Карточка роли уровня строк при создании

Для роли уровня строк должны быть заданы политики уровня строк, определяющие параметры доступа к записям в разделах Системы. Для создания политики используется кнопка «Создать» на вкладке «Политики уровня строк». В окне создания политики необходимо ввести ее имя, выбрать ее тип и задать выражения «Join» и «Where». Для проверки введенных скриптов используется кнопка «Check syntax». Для сохранения политики используется кнопка «ОК» в окне ее создания.

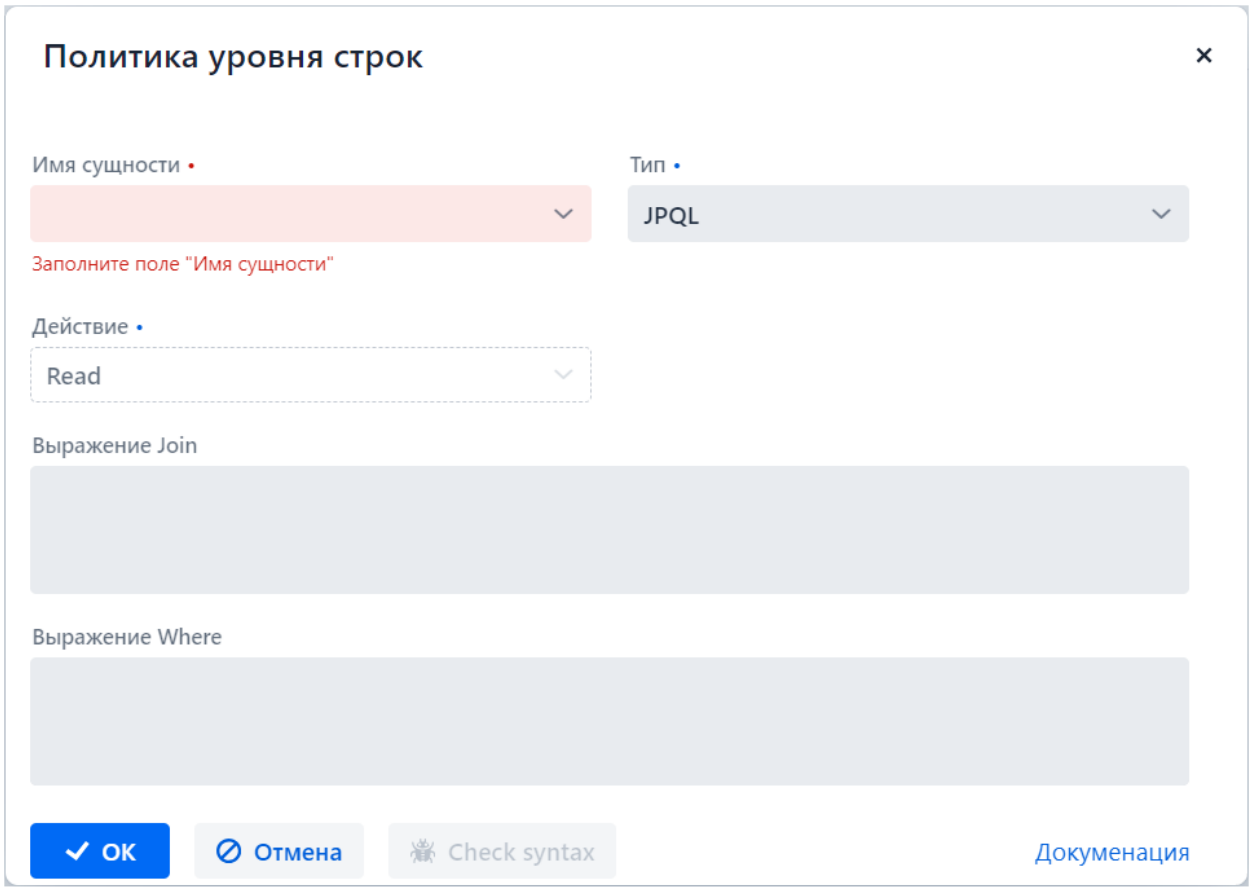

Рисунок 63 – Добавление политики уровня строк

Для роли уровня строк могут быть добавлены дочерние роли, от которых будут наследоваться политики уровня строк. Для этого используется кнопка «Добавить» на вкладке «Дочерние роли». В окне добавления дочерней роли доступны для выбора все существующие в Системе роли уровня строк. Необходимо установить флажки напротив нужных ролей из списка и нажать кнопку «Выбрать».

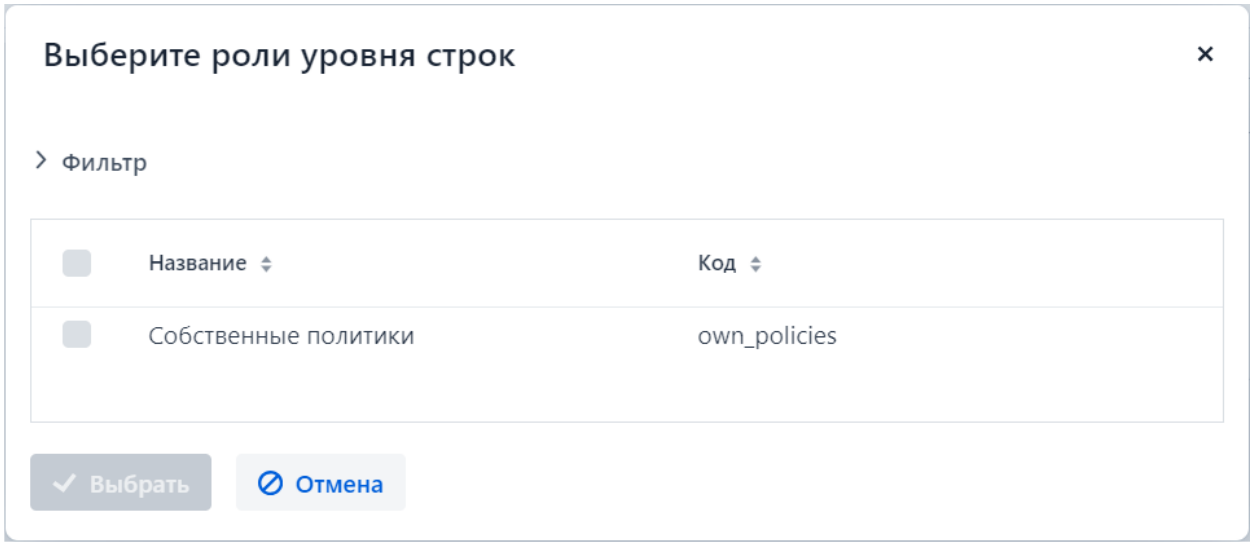

Рисунок 64 – Добавление дочерних ролей

Для сохранения введенных данных используется кнопка «ОК» в карточке роли уровня строк.

4.2.2.4. Назначение ролей

Для работы в Системе пользователю должна быть назначена ресурсная роль и при необходимости может быть назначена роль уровня строк. Роли могут быть назначены пользователю через подразделы с ролями или через подраздел «Пользователи».

В первом варианте назначение ролей осуществляется в разделах «Администрирование» → «Ресурсные роли» или «Администрирование» → «Роли уровня строк». Необходимо выбрать роль из списка и нажать кнопку «Назначить на пользователей» – откроется окно со списком пользователей Системы, которым еще не назначена выбранная роль. Необходимо выбрать учетные записи пользователей из списка и нажать кнопку «Выбрать» – указанным пользователям будут выданы права выбранной роли.

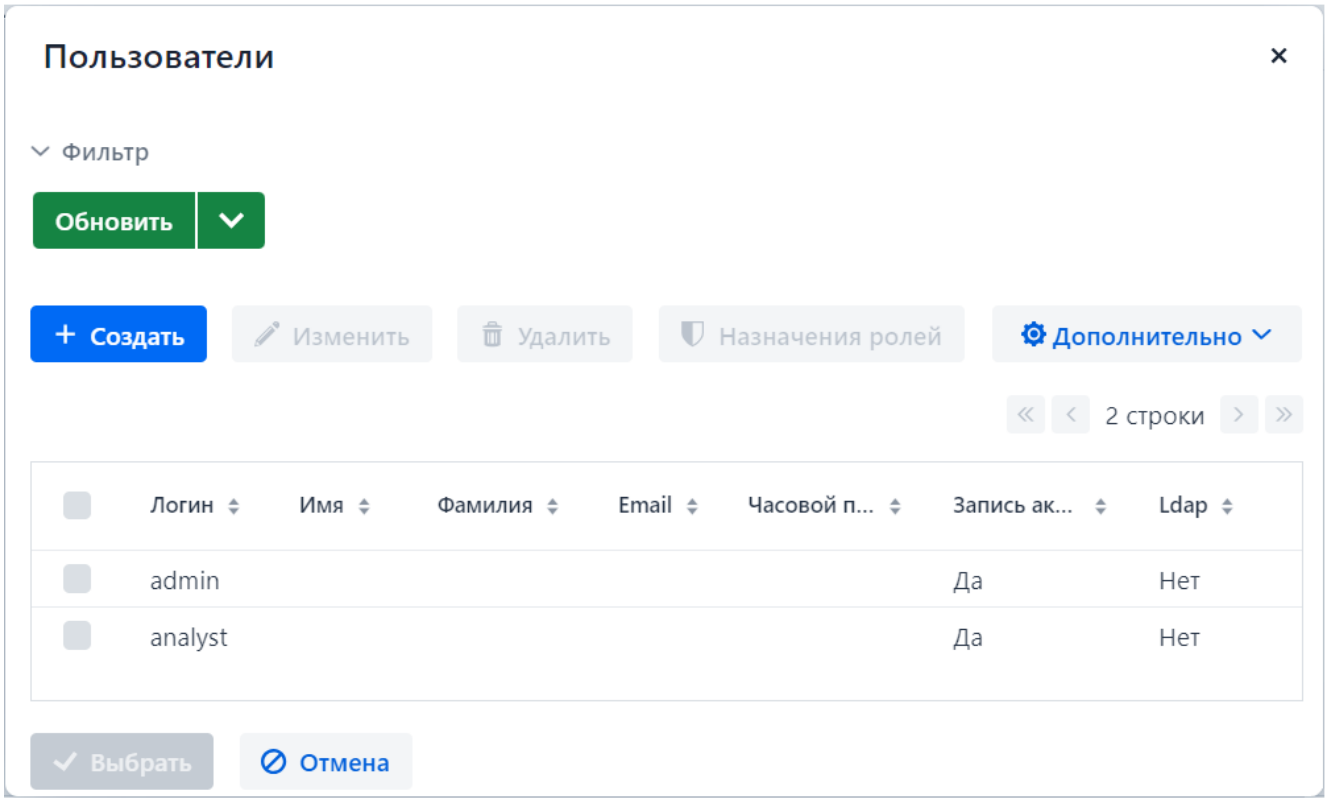

Рисунок 65 – Назначение роли пользователям

Во втором варианте назначение ролей осуществляется в разделе «Администрирование» → «Пользователи». Необходимо выбрать из списка учетную запись пользователя, которому необходимо назначить ресурсную роль, и нажать кнопку «Назначения ролей» над списком. На открывшейся странице с ресурсными разрешениями пользователя в списке будут представлены все ресурсные роли, уже назначенные этому пользователю.

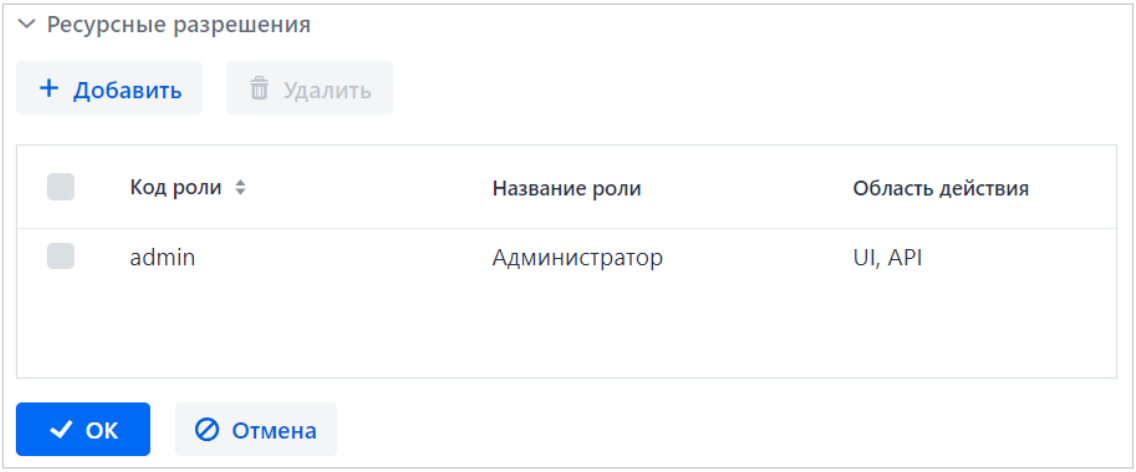

Рисунок 66 – Ресурсные роли, назначенные пользователю

Необходимо нажать кнопку «Добавить», в открывшемся окне выбрать из списка одну или несколько ресурсных ролей и нажать кнопку «Выбрать». Если из списка будут выбраны роли, уже назначенные пользователю, их выбор будет проигнорирован.

Для сохранения внесенных изменений используется кнопка «ОК» в окне с ресурсными разрешениями пользователя.

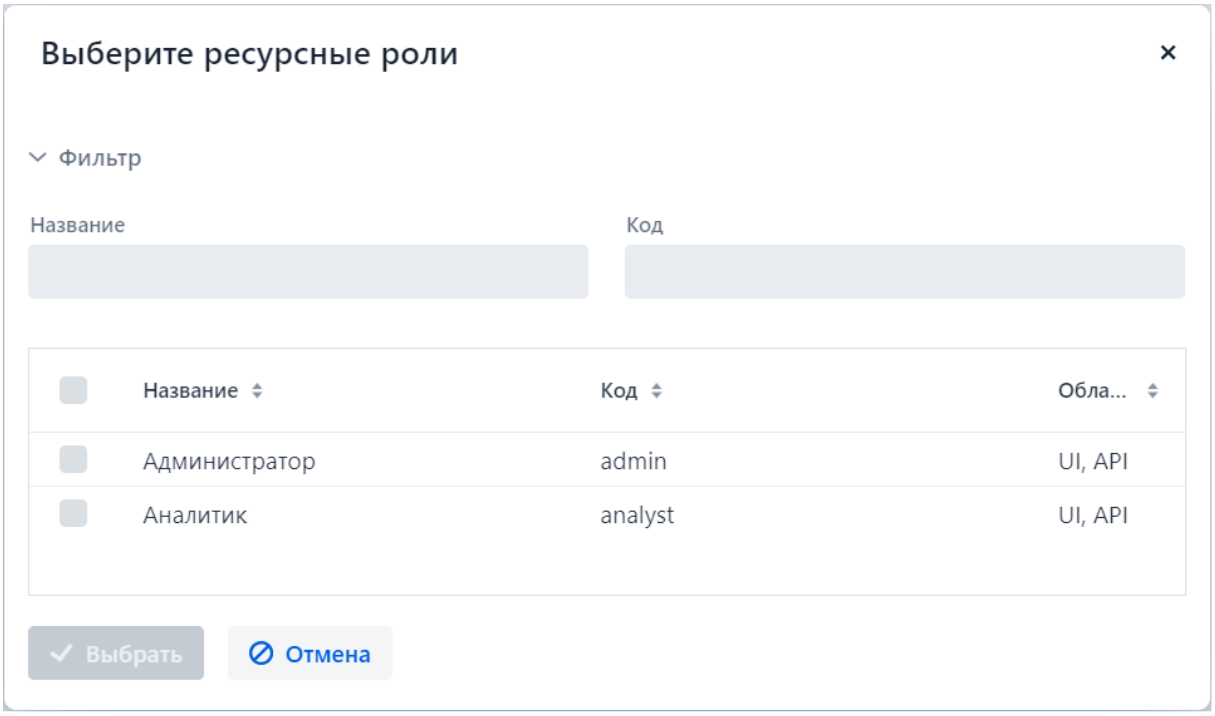

Рисунок 67 – Добавление ресурсных ролей пользователю

4.3. LDAP

В Системе присутствует встроенный компонент (аддон) LDAP, позволяющий использовать службу каталогов Active Directory. LDAP обеспечивает централизованное хранилище логинов и паролей, позволяя приложениям подключаться к LDAP-серверу для подтверждения доступа.

С помощью интеграции с LDAP происходит синхронизация пользователей. При первой попытке входа пользователя под своими доменными данными в Системе автоматически создается учетная запись этого пользователя. При этом пользователю не назначаются роли в Системе. Для предоставления пользователю доступа к работе с Системой администратор должен назначить ему соответствующую роль. После этого пользователь сможет работать в Системе в соответствии со своими полномочиями.

Параметры подключения к LDAP задаются в файле «application.properties» для модуля JMIX.

4.4. Логирование

4.4.1. Расположение и назначение журналов с логами

Просмотр системных журналов с логами возможен с помощью встроенных средств операционной системы. Например, для просмотра журнала в реальном времени можно воспользоваться командой «cat <*file_name*>» или «tail -f <*file_name*>», где <file_name> – это название файла. Команды вводятся в терминале.

Перечень директорий, содержащих системные журналы:

- «/opt/kafka/logs» – системные журналы «Kafka»;
- «/opt/ctds/collector/logs» – системные журналы «Collector»;
- «/opt/ctds/manager-api/logs» – системные журналы «Manager API»;
- «/opt/ctds/manager-ui/logs» – системные журналы «Manager UI»;
- «/opt/ctds/manager-ui/logs» – системные журналы «Clickhouse»;
- «/var/lib/pgsql/15/data/log» – системные журналы «Manager Repository» и «Collector Repository» (СУБД PostgreSQL);
- «/var/log/db-agent» – системные журналы агента.

4.4.2. Просмотр логов (аудит действий пользователя)

При взаимодействии пользователей с программным интерфейсом (API) Системы все действия фиксируются в системных журналах «Manager API», расположение которых указано в «Инструкции по эксплуатации экземпляра программного обеспечения, предоставленного для проведения экспертной проверки».

При взаимодействии пользователей с веб-интерфейсом Системы все действия фиксируются в системных журналах «Manager UI», расположение которых указано в «Инструкции по эксплуатации экземпляра программного обеспечения, предоставленного для проведения экспертной проверки».

5. ГЛОССАРИЙ

Термины и сокращения	Определение
Агент	Программное средство, выполняющее задачи в автономном режиме (например, сбор данных или мониторинг определенных событий)
Брокер	Компонент Системы, обеспечивающий асинхронный обмен информацией между другими компонентами, хранит в себе перехваченные и проанализированные данные
Коллектор	Компонент Системы, который собирает данные с агентов через брокер и систематизирует первичный трафик, хранит актуальные политики, проверяет трафик в соответствии с политиками, определяет необходимость блокировки трафика
Политика	Используется для автоматического определения нетипичного или вредоносного поведения при работе пользователей с внешними БД, применяется к трафику, идущему к отслеживаемым БД
СУБД	Система управления базами данных (совокупность программных средств, обеспечивающих управление созданием и использованием БД)