Программное обеспечение «Jay Data Files»

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

«Jay Data Files» – система, предназначенная для автоматического поиска, классификации и обезличивания чувствительных данных в загружаемых файлах.

Система позволяет устранить риски передачи конфиденциальной информации третьим лицам, определяя с помощью алгоритмов профилирования наличие в файлах чувствительных данных и преобразуя их по заданным правилам.

Основной целью Системы является обезличивание полученных данных в соответствии с настроенными алгоритмами маскирования.

Система решает следующие задачи:

- выявление в загруженных файлах конфиденциальных данных с помощью алгоритмов профилирования;
- обезличивание данных в соответствии с выбранным профилем с помощью алгоритмов маскирования;
- автоматизация и ускорение процесса проверки / деперсонализации данных;
- снижение рисков нарушения режима конфиденциальности.

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.

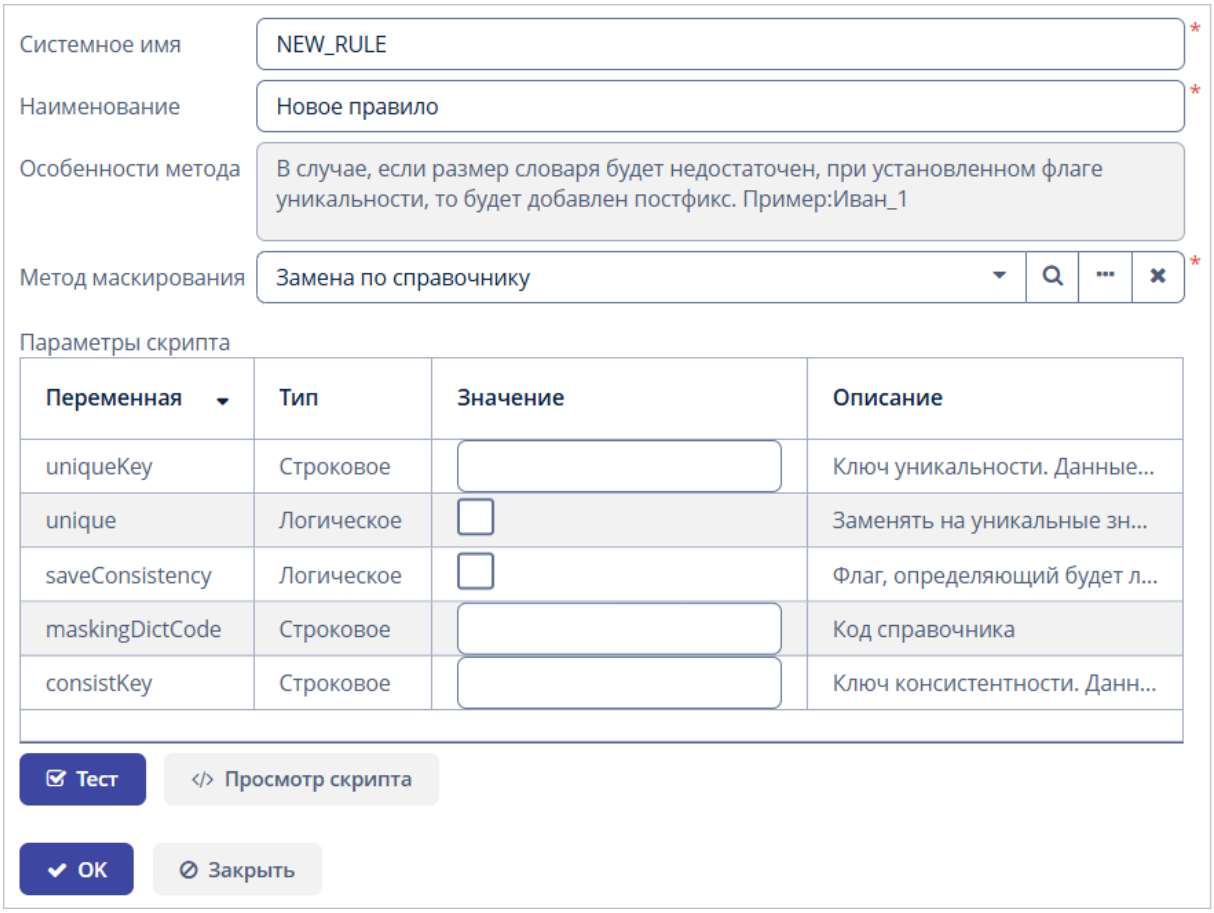

Рисунок 2 – Тип экрана: карточка

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 пагинации

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

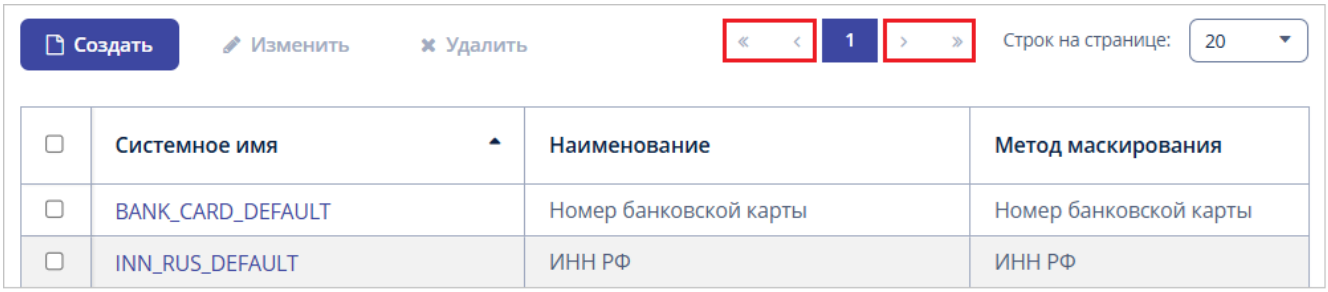

Рисунок 3 – Кнопки в области пагинации

2) 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.

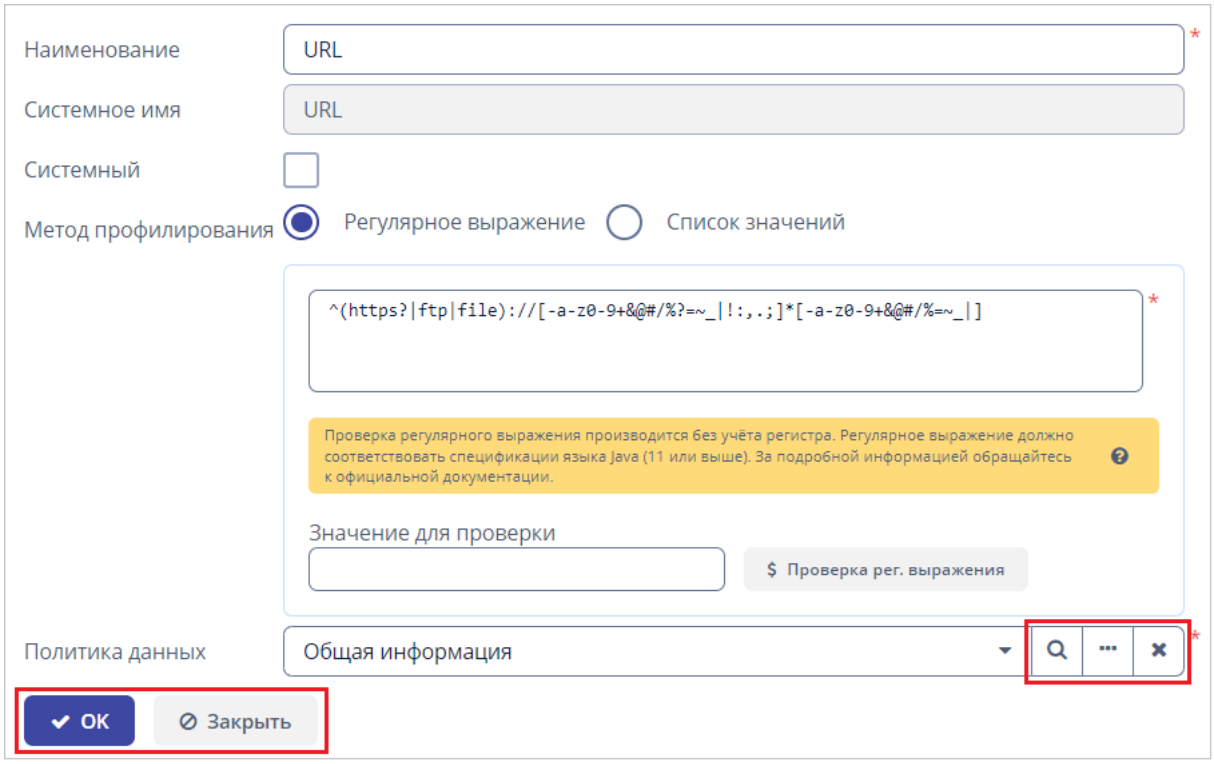

Рисунок 4 – Кнопки в карточке объекта

3) 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».

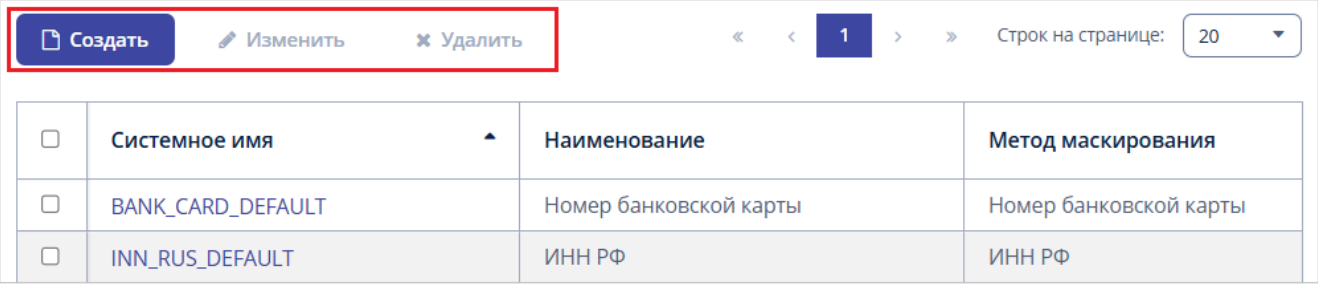

Рисунок 5 – Кнопки над списком объектов

2.3. Поля

1) Простое текстовое поле

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

Рисунок 6 – Поле для ввода текста

Обязательное незаполненное поле окрашивается в красный цвет.

Рисунок 7 – Незаполненное обязательное поле

Поле, недоступное для редактирования, светло-серого цвета.

Рисунок 8 – Поле, недоступное для редактирования

2) Редактор кода

   К данному типу полей относятся поля для отображения и ввода исходного кода.

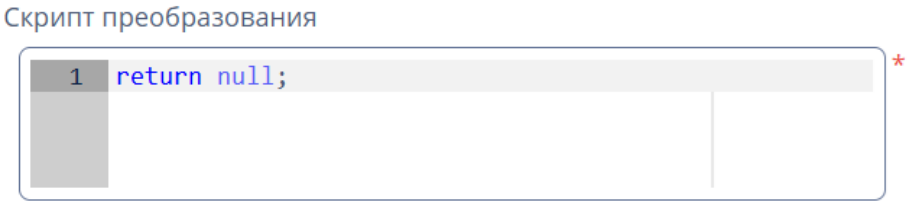

Рисунок 9 – Редактор кода

3) Поля выбора

   К данному типу полей относятся чекбоксы и радиокнопки.

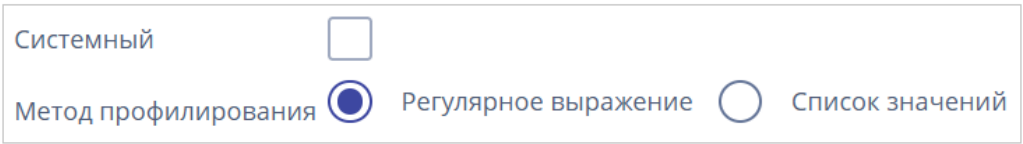

Рисунок 10 – Поля выбора

4) Список

К данному типу полей относятся выпадающие и комбинированные списки.

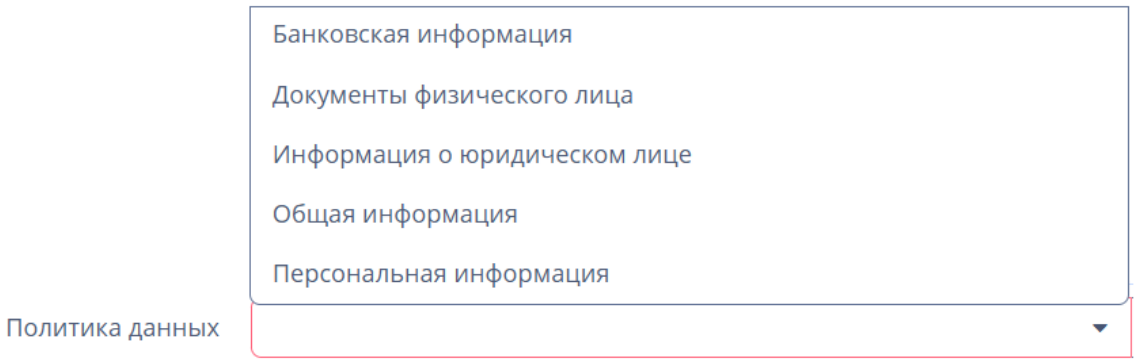

Рисунок 11 – Список

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».

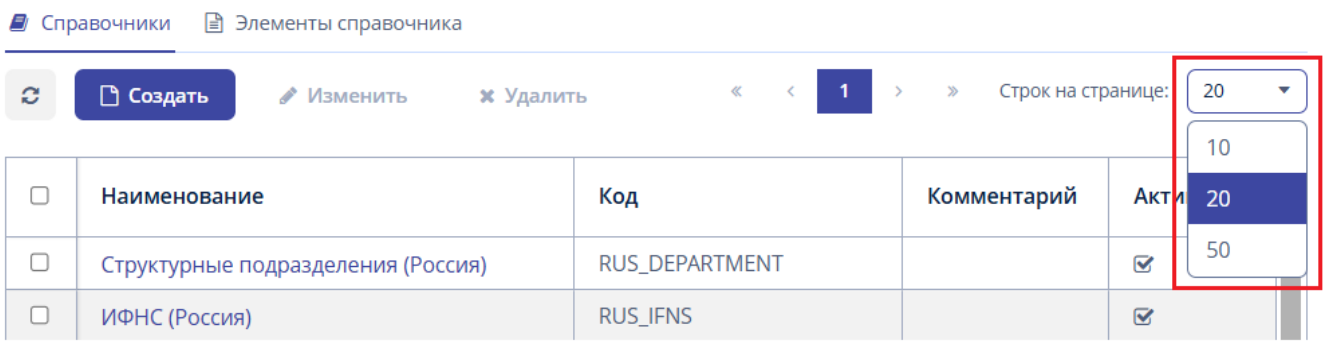

Рисунок 12 – Выбор количества записей на одной странице

Для переключения между страницами списка используются кнопки в области пагинации.

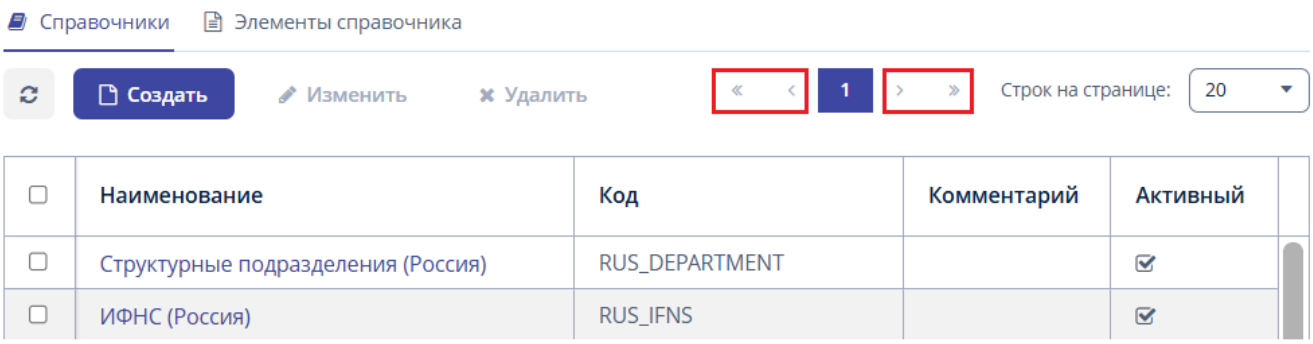

Рисунок 13 – Кнопки для переключения между страницами

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

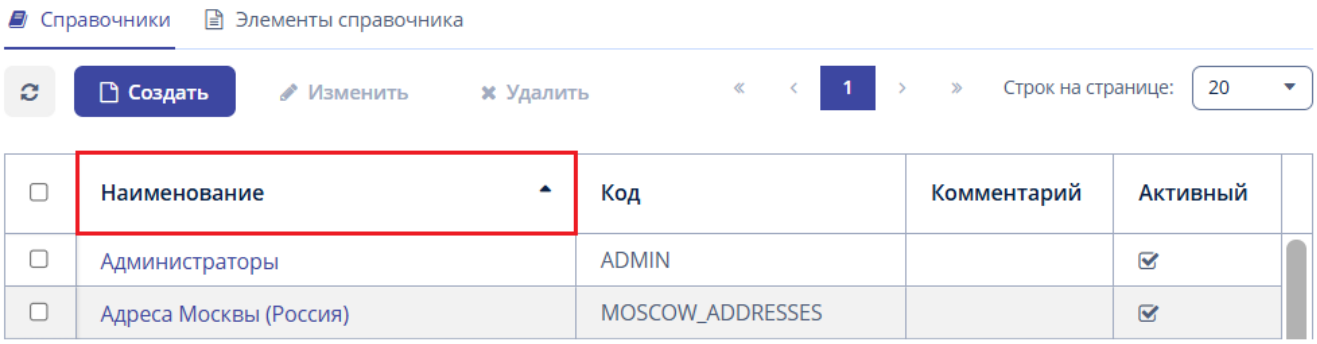

Рисунок 14 – Отсортированный список

Для изменения ширины столбца в списке необходимо навести курсор на его правую границу – он изменит свой вид на разделитель, нажать и удерживать, перемещая курсор влево или вправо.

Для изменения очередности расположения столбцов в списке необходимо нажать на заголовок столбца и, удерживая его, перемещать в нужное место.

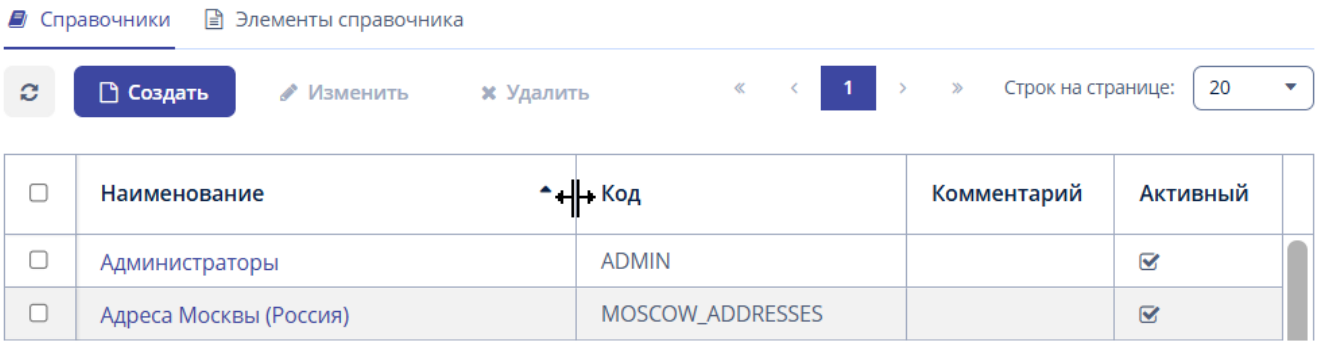

Рисунок 15 – Изменение ширины столбца

3. ИСПОЛЬЗОВАНИЕ СИСТЕМЫ

3.1. Вход в Систему

Для входа в Систему необходимо ввести в адресной строке браузера URL-адрес, по которому развернута Система. Для настройки объектов Системы и обезличивания файлов используются два отдельных URL-адреса. Необходимо ввести данные для входа и нажать кнопку «Войти». Для входа в Систему также могут использоваться доменные логин и пароль пользователя.

После входа пользователя в Систему для него становится доступной панель навигации для работы с разделами Системы.

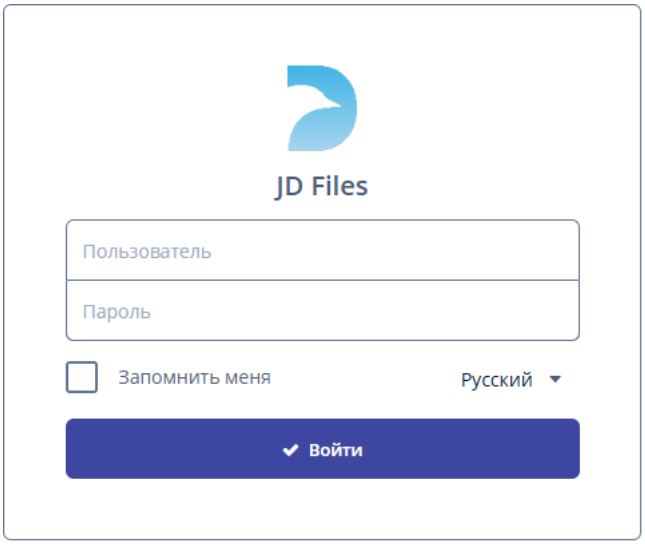

Рисунок 16 – Форма авторизации в Системе

3.2. Панель навигации

В левой части окна Системы расположена панель навигации, с помощью которой осуществляется доступ к разделам Системы. Разделы доступны пользователю, в зависимости от назначенной ему роли. Раздел «Администрирование» доступен администратору Системы.

Разделы раскрываются при нажатии на их название. При повторном нажатии раздел сворачивается. По умолчанию после входа пользователя в Систему панель навигации свернута.

В верхней части панели навигации располагается наименование Системы, в нижней – логин текущего пользователя, его часовой пояс и кнопка выхода из Системы. В зависимости от используемого URL-адреса Системы, панель навигации будет содержать разделы либо для настройки объектов Системы, либо для обезличивания файлов.

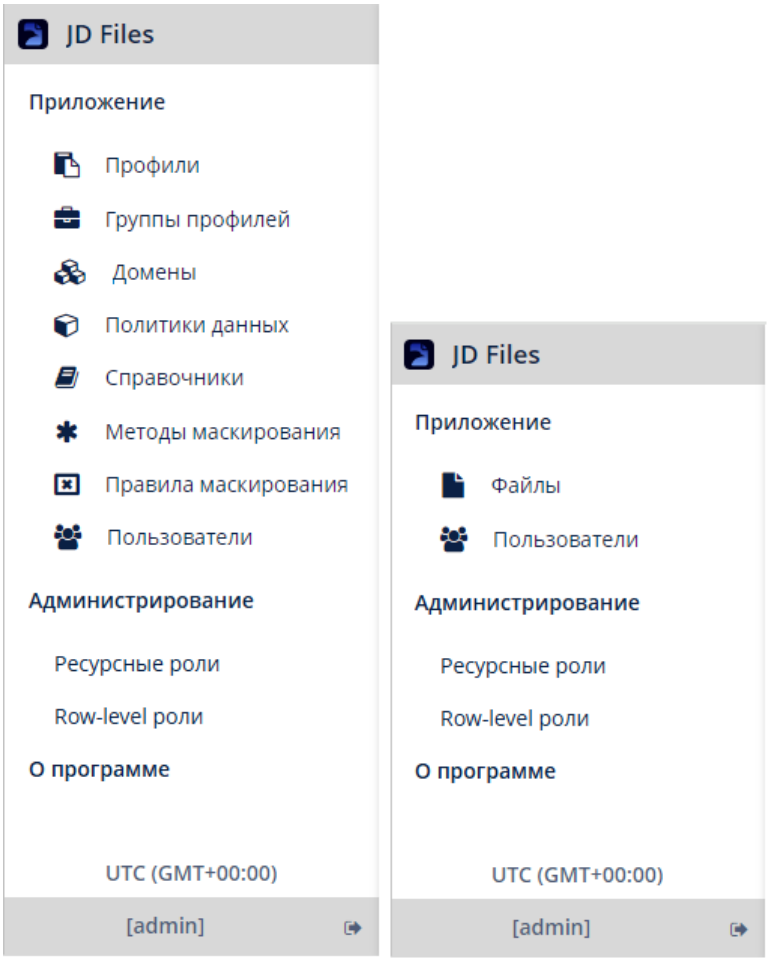

Рисунок 17 – Панель навигации Системы

При переходе к разделу «О программе» появляется окно с информацией о Системе.

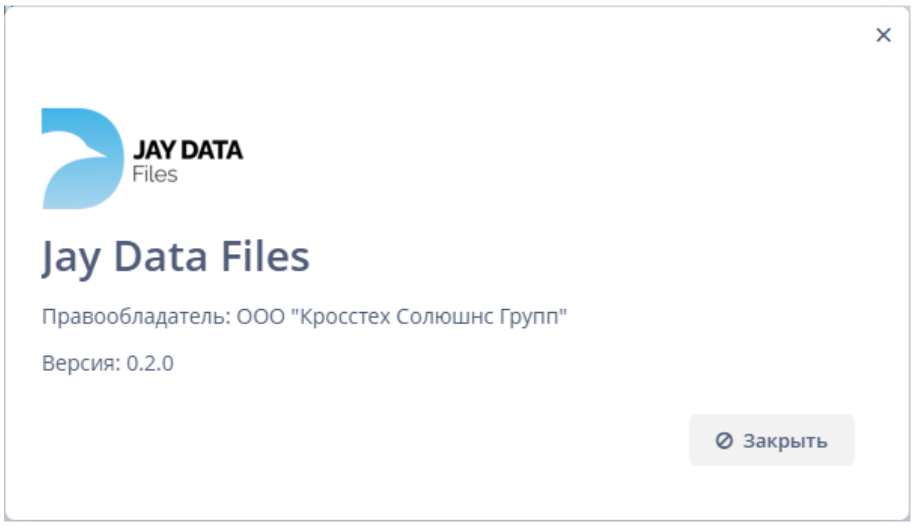

Рисунок 18 – Раздел «О программе» (пример)

3.3. Файлы

3.3.1. Общая информация

В разделе Системы «Приложение» → «Файлы» выполняется управление файлами, содержащими конфиденциальные данные.

Пользователь загружает файл с локального компьютера в Систему, Система вычисляет метаданные файла, пользователь отправляет файл на обезличивание, Система профилирует (выявляет в файле конфиденциальные данные и присваивает им домены) и маскирует файл, обезличенный файл становится доступным для скачивания. Исходный и обезличенный файлы сохраняются в отдельном защищенном хранилище, данные из файлов шифруются с помощью алгоритма AES-256.

Для скачивания исходного файла используется кнопка в столбце «Исходный». Для скачивания обезличенного файла (доступен только после выполнения обезличивания) используется кнопка в столбце «Результат».

Для удаления файла необходимо выбрать его из списка, нажать кнопку «Удалить» и подтвердить удаление в появившемся окне.

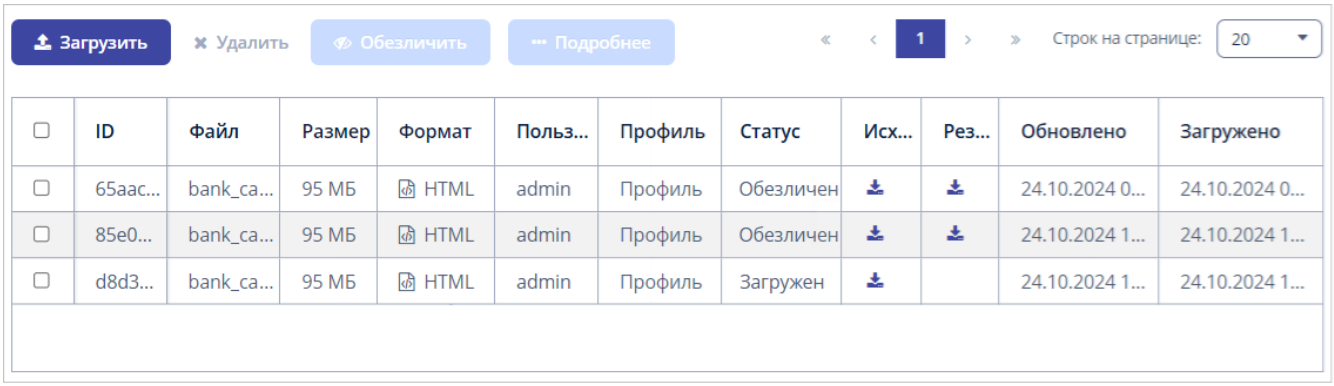

Рисунок 19 – Подраздел «Файлы»

3.3.2. Жизненный цикл файла

При выполнении каких-либо действий с файлом меняется его статус. Жизненный цикл файла состоит из следующих статусов: «Вычисление метаданных», «Загружен», «Обезличивание», «Новый» (виден только администратору Системы), «В работе» (виден только администратору Системы), «Обезличен».

Изменение статуса файла происходит в соответствии со следующими правилами.

1) Файл начинает отображаться в разделе Системы «Приложение» → «Файлы» только после завершения загрузки в Систему. Сразу после завершения загрузки файла автоматически начинается вычисление его метаданных (формат, размер, хэш-сумма), статус файла меняется на «Вычисление метаданных».
2) После успешного завершения вычисления метаданных файла его статус меняется на «Загружен».
3) После отправки файла на обезличивание его статус меняется на «Обезличивание». Данный статус отображается для пользователя Системы в подразделе «Файлы» при выполнении следующих последовательных процессов: ожидание обработки файла в очереди на автоматическое обезличивание, автоматическое обезличивание файла, ручная модерация файла (если в ней возникла необходимость), вычисление метаданных обезличенного файла.
4) Файл, отправленный на ручную модерацию, отображается для администратора Системы в разделе «Приложение» → «Ручная модерация» со статусом «Новый».

   Если администратор скачивает файл для локального обезличивания и отмечает в Системе взятие файла в работу, его статус меняется на «В работе».

   Если администратор возвращает файл со статусом «В работе» в очередь ожидания обработки, его статус меняется на «Новый».

   Если администратор загружает в Систему файл, обезличенный локально, и подтверждает его готовность, статус файла меняется на «Обезличен». Автоматически начинается вычисление метаданных обезличенного файла.

   Для пользователя в подразделе Системы «Файлы» статус файла в процессе его ручной модерации не изменяется.

После успешного завершения вычисления метаданных обезличенного файла процесс обезличивания считается завершенным, статус файла в подразделе «Файлы» меняется на «Обезличен».

3.3.3. Загрузка файлов

Для загрузки нового файла в Систему необходимо перейти в раздел Системы «Приложение» → «Файлы» и нажать кнопку «Загрузить» над списком. В появившемся окне нажать кнопку «Загрузить», в появившемся системном окне выбрать локальный файл с компьютера и подтвердить его загрузку.

Максимальный размер загружаемого текстового файла: 100 Мб. В Системе отсутствует ограничение на уникальность названий загружаемых файлов.

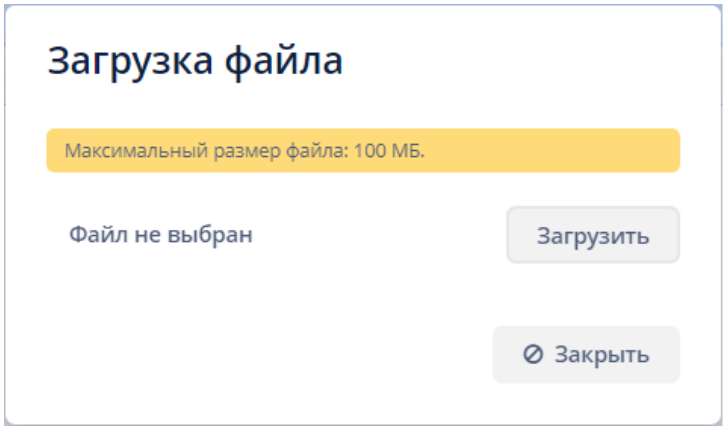

Рисунок 20 – Окно загрузки файла

При загрузке файла Система определяет его размер и формат. Если файл соответствует требованиям, начинается его автоматическая загрузка в Систему, появляется окно с прогрессом загрузки. Пока загрузка файла не завершена, ее можно отменить.

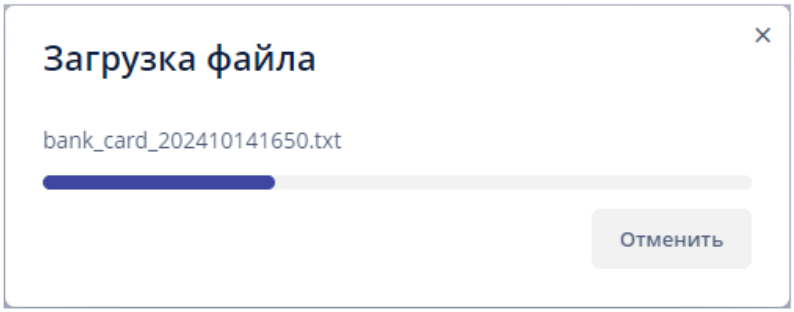

Рисунок 21 – Прогресс загрузки файла в Систему

После завершения загрузки файл появляется в списке и становится доступным для скачивания с помощью кнопки в столбце «Исходный». Каждому файлу присваивается уникальный идентификатор. Определенные Системой размер и формат файла отображаются в строке с файлом в соответствующих столбцах таблицы. Статус файла меняется на «Загружен».

3.3.4. Обезличивание файлов

Файл может быть отправлен на обезличивание только в том случае, если его обезличивание еще не проводилось. Для обезличивания может быть выбрано сразу несколько файлов. Для того, чтобы пользователь мог запустить обезличивание, ему должна быть назначена роль, входящая хотя бы в одну группу профилей обезличивания. В противном случае, Система выдаст ошибку.

Для запуска обезличивания файла необходимо выбрать его из списка и нажать кнопку «Обезличить» над списком. В появившемся окне из комбинированного списка необходимо выбрать профиль обезличивания, который будет использоваться при маскировании. В списке доступны профили, входящие в группы профилей, доступные роли пользователя. Если пользователю доступен только один профиль обезличивания, он будет установлен в поле по умолчанию.

Для запуска процесса обезличивания используется кнопка «Обезличить».

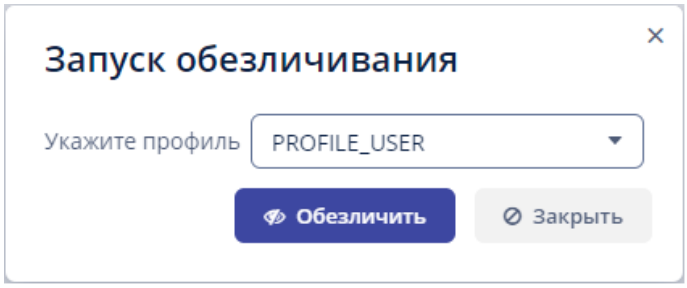

Рисунок 22 – Выбор профиля обезличивания

Статус файла, отправленного на обезличивание, меняется на «Обезличивание». После успешного завершения процесса обезличивания файла его статус меняется на «Обезличен», а в столбце «Результат» появляется кнопка для скачивания, при нажатии на которую выполняется автоматическое скачивание обезличенного файла на локальный компьютер пользователя.

Если формат файла не подходит для автоматического обезличивания, или его метаданные не были вычислены, или в процессе обезличивания возникла ошибка, файл отправляется на ручную модерацию.

3.3.5. Хэш-суммы файлов

Для загруженного и обезличенного файлов в Системе автоматически производится вычисление и хранение хэш-сумм, необходимых для проверки целостности данных. Хэш-суммы вычисляются с помощью алгоритма SHA-256.

Для просмотра вычисленных хэш-сумм необходимо выбрать один или несколько файлов из списка и нажать кнопку «Подробнее» над списком. В появившемся окне в табличной форме представлены выбранные файлы и вычисленные для них хэш-суммы.

Если хэш-сумма загруженного или обезличенного файла не была вычислена, ее значение устанавливается как «Не определена». Значение хэш-суммы обезличенного файла хранится в Системе даже после удаления этого файла. Если при вычислении хэш-суммы загруженного или обезличенного файла произошла ошибка, файл будет отправлен на ручную модерацию.

Для копирования значения хэш-суммы используется кнопка .

Для экспорта данных таблицы необходимо нажать кнопку «Экспорт в Excel» – файл с данными в формате .xlsx будет автоматически скачан на компьютер.

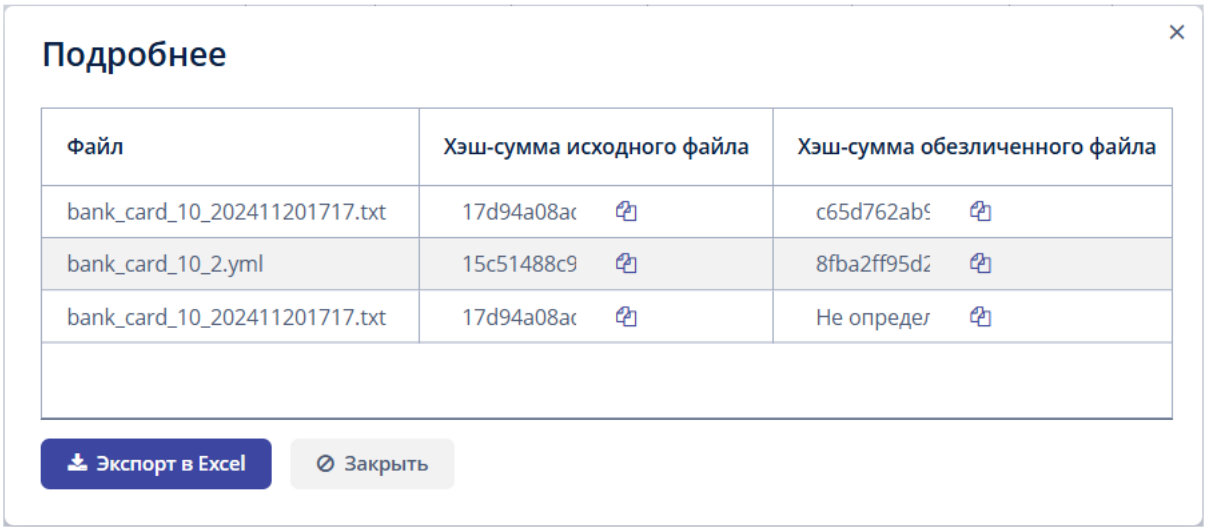

Рисунок 23 – Вычисление хэш-суммы файлов

3.3.6. Ручная модерация файлов

Ручная модерация файлов в Системе применяется для обеспечения точности и корректности процесса обезличивания. Файлы автоматически отправляются на ручную модерацию по следующим причинам:

– формат файла, отправленного на обезличивание, не подходит для автоматического обезличивания;
– в процессе автоматического обезличивания файла возникла ошибка;
– произошла ошибка при вычислении метаданных загруженного или обезличенного файла.

Все файлы, отправленные на ручную модерацию, отображаются в разделе Системы «Приложение» → «Ручная модерация». Пользователи, имеющие доступ к ручной модерации, видят все существующие в подразделе файлы, вне зависимости от того, кто занимается их локальным обезличиванием.

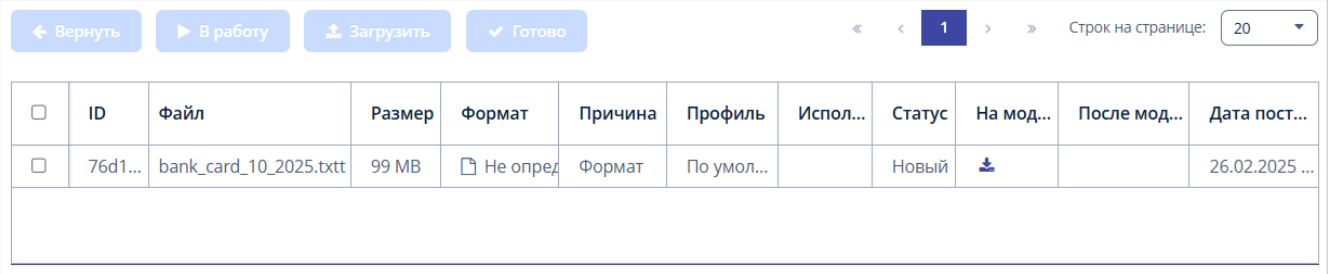

Рисунок 24 – Подраздел «Ручная модерация»

Для каждого файла в процессе его ручной модерации в столбцах таблицы отображается следующая информация:

– «ID» – уникальный идентификатор файла, загруженного в Систему;
– «Файл» – наименование файла, загруженного в Систему;
– «Размер» – размер файла, загруженного в Систему;
– «Формат» – формат файла, загруженного в Систему (отображается формат, не поддерживаемый Системой, или «Не определен» в случае неизвестного формата данных);
– «Причина» – причина отправки файла на ручную модерацию;
– «Профиль» – профиль обезличивания, выбранный для файла;
– «Исполнитель» – пользователь, взявший файл «В работу»;
– «Статус» – статус файла, находящегося на ручной модерации (при поступлении на модерацию для файла по умолчанию устанавливается статус «Новый»);
– «На модерацию» – содержит кнопку для скачивания файла на компьютер пользователя для проведения локального обезличивания;

– «После модерации» – содержит кнопку для скачивания обезличенного файла на компьютер пользователя (кнопка появляется после загрузки локально обезличенного файла в Систему);
– «Дата поступления» – дата и время поступления файла на ручную модерацию.

Для начала процесса локального обезличивания необходимо выбрать из списка файл со статусом «Новый» и нажать кнопку «В работу» – статус файла будет изменен на «В работе». В строке с файлом в столбце «Исполнитель» появится имя пользователя, взявшего файл в работу. Нельзя взять в работу файл, который находится в статусе «Обезличен» или «В работе» у другого пользователя.

Для отмены процесса локального обезличивания необходимо выбрать из списка файл со статусом «В работе» и нажать кнопку «Вернуть» – статус файла будет изменен на «Новый», файл вернется в очередь ожидания обработки. В строке с файлом будет очищено значение столбца «Исполнитель». Нельзя вернуть файл, который находится в статусе «Новый», «Обезличен» или «В работе» у другого пользователя.

В строке со взятым в работу файлом необходимо нажать на кнопку в столбце «На модерацию» – файл будет автоматически скачан на компьютер.

После локального обезличивания файла он должен быть загружен обратно в Систему. Необходимо выбрать из списка файл, для которого будет загружена его обезличенная версия, и нажать кнопку «Загрузить». В появившемся окне нажать кнопку «Загрузить» и выбрать обезличенный файл с компьютера. Нельзя загрузить обезличенную версию для файла, который находится в статусе «Новый», «Обезличен» или «В работе» у другого пользователя.

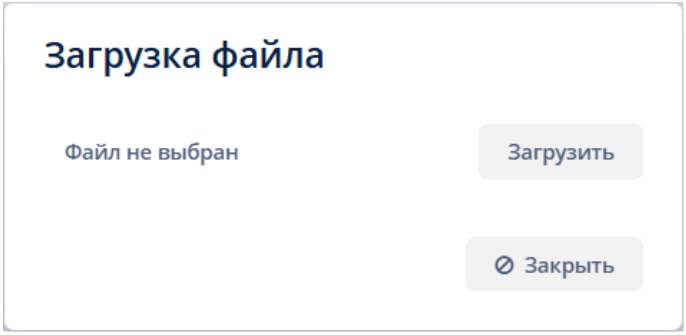

Рисунок 25 – Окно загрузки обезличенного файла

Перед загрузкой обезличенной версии файла Система проверяет его наименование и формат. Если формат и наименование файла совпадают с изначальными, начинается автоматическая загрузка данного файла в Систему, появляется окно с прогрессом загрузки. В противном случае, Система выдаст ошибку. Пока загрузка файла не завершена, ее можно отменить.

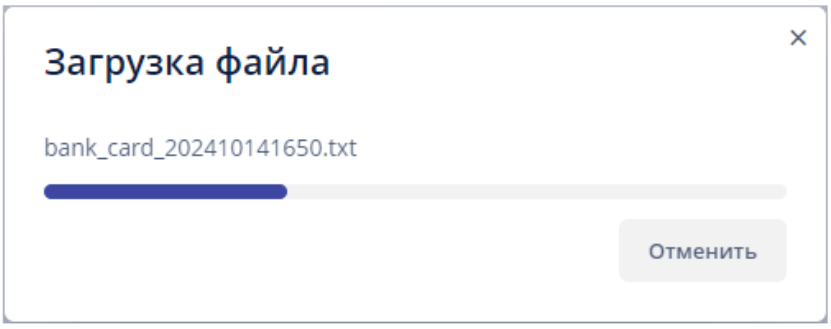

Рисунок 26 – Прогресс загрузки обезличенного файла

После завершения загрузки в строке с файлом в столбце «После модерации» появится кнопка для повторного скачивания обезличенной версии файла. Пока файл не переведен в статус «Обезличен», его обезличенная версия может быть повторно загружена в Систему неограниченное количество раз.

Для завершения процесса локального обезличивания необходимо выбрать из списка файл со статусом «В работе». Для файла предварительно должна была загружена его обезличенная версия. Далее нажать кнопку «Готово» – статус файла будет изменен на «Обезличен», автоматически начнется вычисление метаданных обезличенного файла. Нельзя завершить обезличивание файла, который находится в статусе «Новый», «Обезличен» или «В работе» у другого пользователя.

После завершения вычисления метаданных обезличенного файла процесс ручной модерации считается завершенным, обезличенный файл предоставляется конечному пользователю, инициировавшему процесс обезличивания.

3.4. Профили

3.4.1. Общая информация

Профили обезличивания предназначены для упрощения настройки процесса обезличивания и для создания различных сценариев обезличивания. Каждый профиль содержит список доменов, которые необходимо определять для чувствительных данных, и соответствующие каждому из них правила маскирования, по которым выполняется обезличивание файлов. Пользователь выбирает профиль обезличивания при отправке файла на обезличивание.

Список профилей содержится в разделе Системы «Приложение» → «Профили». Профиль может входить в одну или несколько групп профилей, список которых отображается в столбце «Группы».

Для просмотра профиля необходимо нажать на его наименование в списке.

Для изменения профиля необходимо выбрать его из списка и нажать кнопку «Изменить» над списком, внести изменения и сохранить их.

Для удаления одного или нескольких профилей необходимо выбрать их из списка и нажать кнопку «Удалить», в появившемся окне подтвердить удаление.

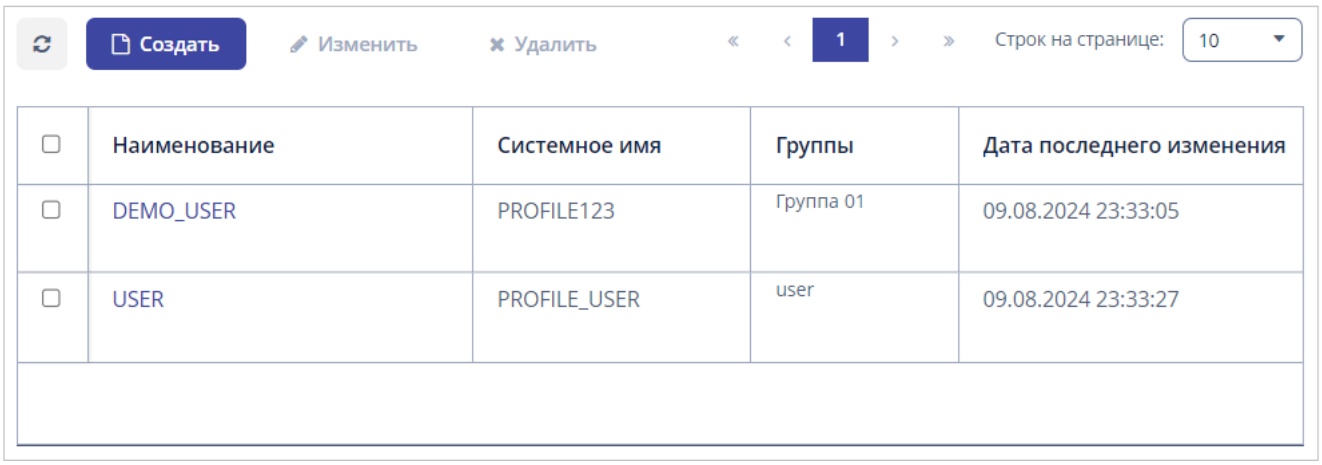

Рисунок 27 – Подраздел «Профили»

3.4.2. Создание профиля

Для создания профиля используется кнопка «Создать» в разделе Системы «Приложение» → «Профили».

На странице создания профиля необходимо заполнить поля:

– «Системное имя» – системный код профиля, с помощью которого он может быть идентифицирован в Системе (может содержать только заглавные латинские буквы и знаки подчеркивания, должен начинаться с буквы);
– «Наименование» – название профиля;
– «Описание» – краткое описание профиля.

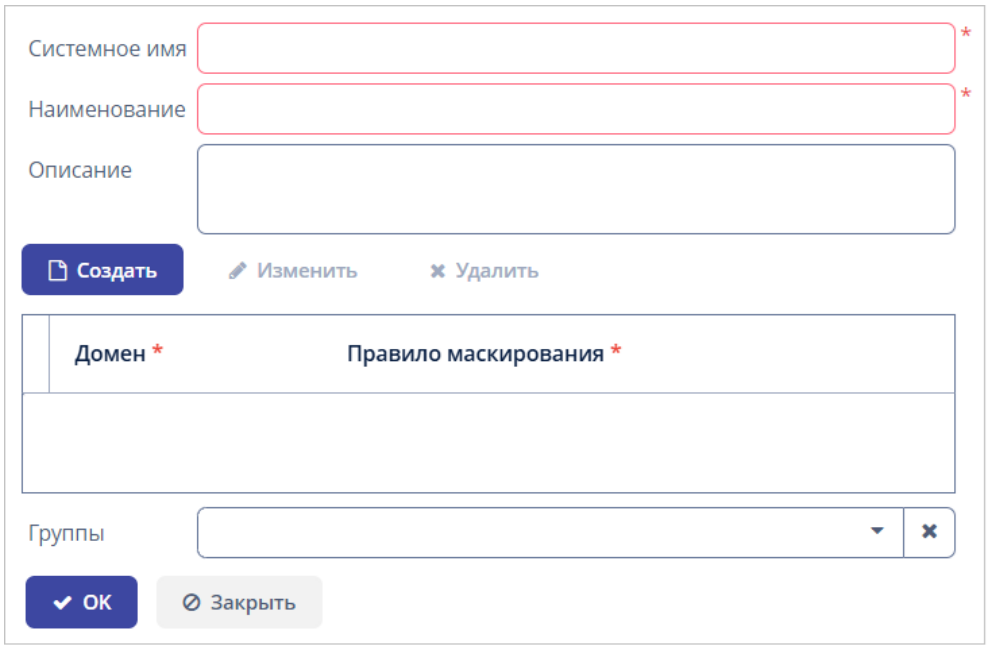

Рисунок 28 – Создание профиля

Для добавления в профиль связки «Домен – Правило маскирования» необходимо нажать кнопку «Создать» на странице создания профиля. Далее выбрать домен и связанное с ним правило маскирования из соответствующих комбинированных списков и нажать кнопку «ОК» – запись появится в таблице на странице создания профиля.

В рамках одного профиля связки «Домен – Правило маскирования» должны быть уникальными. В профиль должна входить хотя бы одна связка «Домен – Правило маскирования».

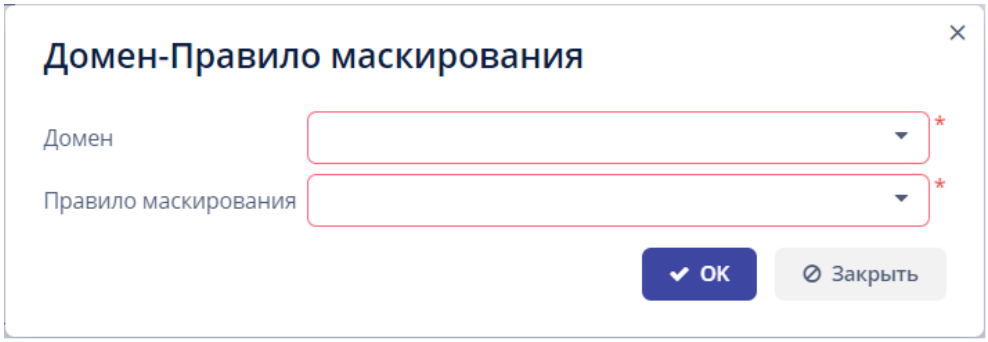

Рисунок 29 – Добавление связки «Домен – Правило маскирования»

Если профиль необходимо включить в группу профилей, необходимо выбрать группу из соответствующего комбинированного списка на странице создания профиля. Один профиль может быть включен в несколько групп.

Для сохранения профиля используется кнопка «ОК».

3.5. Группы профилей

3.5.1. Общая информация

Группы профилей предназначены для связывания профилей обезличивания с ролями пользователей. Группа профилей может содержать в себе один или несколько профилей. Если пользователю назначена роль, включенная в группу профилей, при отправке файла на обезличивание такому пользователю будут доступны все профили, включенные в данную группу профилей.

Список групп профилей содержится в разделе Системы «Приложение» → «Группы профилей».

Для просмотра группы профилей необходимо нажать на ее наименование в списке.

Для изменения группы профилей необходимо выбрать ее из списка и нажать кнопку «Изменить» над списком, внести изменения и сохранить их.

Для удаления одной или нескольких групп профилей необходимо выбрать их из списка и нажать кнопку «Удалить», в появившемся окне подтвердить удаление. Удаление групп профилей или профилей не влияют друг на друга.

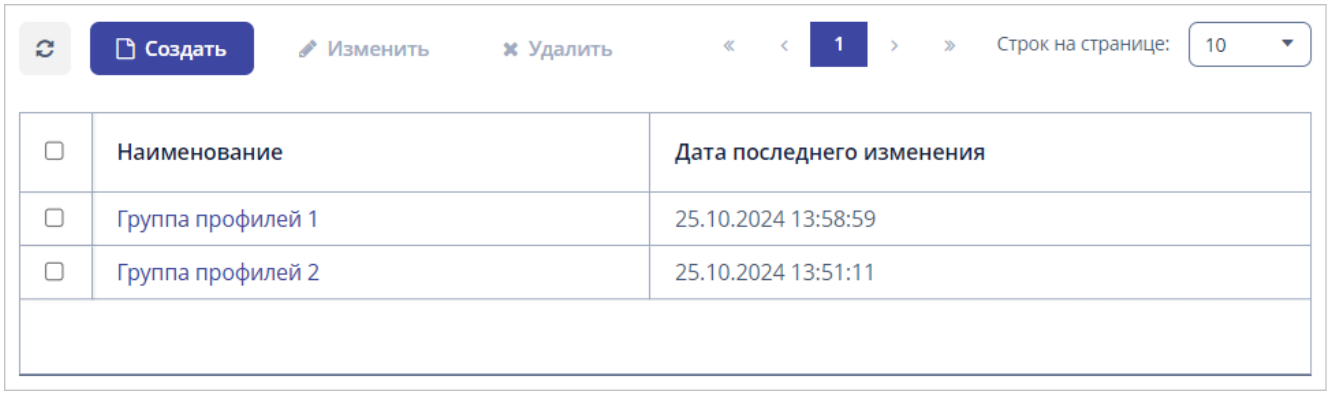

Рисунок 30 – Подраздел «Группы профилей»

3.5.2. Создание группы профилей

Для создания группы профилей используется кнопка «Создать» в разделе Системы «Приложение» → «Группы профилей».

На странице создания группы профилей необходимо заполнить поля:

– «Наименование» – название группы профилей;

– «Роли» – набор ресурсных ролей, назначаемых пользователям;

– «Профили» – профили обезличивания загружаемых в Систему файлов.

Для сохранения группы профилей используется кнопка «ОК».

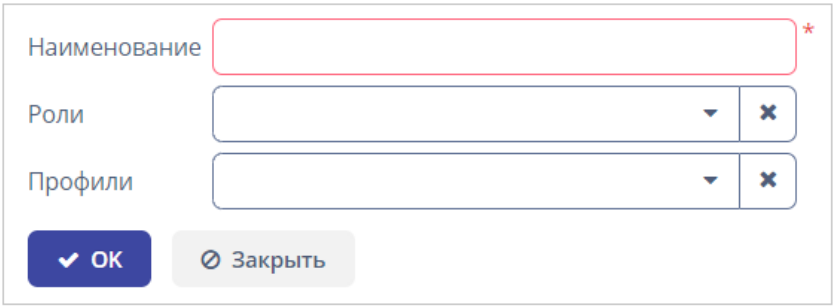

Рисунок 31 – Страница создания группы профилей

3.6. Домены

3.6.1. Общая информация

Домены определяют область информации, к которой относятся данные из загруженного в Систему файла. Если в процессе профилирования Система присвоила данным домен «_C_EMAIL», предполагается, что в них содержится информация об электронной почте пользователей.

Проверка на соответствие данных из файла какому-либо домену осуществляется с помощью регулярного выражения, определяющего этот домен. Для некоторых доменов в целях минимизации ложных срабатываний, помимо проверки по регулярному выражению, используются дополнительные методы проверки.

Список доменов содержится в разделе Системы «Приложение» → «Домены». Домены в списке сгруппированы по политикам данных, к которым они принадлежат. Домены делятся по типу на системные и пользовательские. Тип домена определяется наличием установленного флажка в столбце «Системный».

Для просмотра домена необходимо нажать на его наименование в списке.

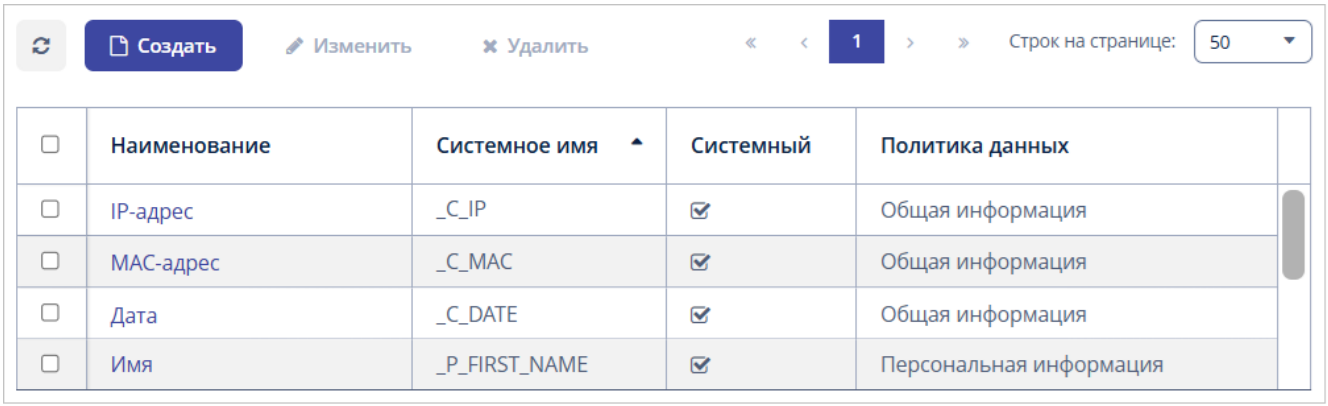

Рисунок 32 – Подраздел «Домены»

Для изменения домена необходимо выбрать его из списка и нажать кнопку «Изменить», внести изменения и сохранить их. Редактирование доменов нельзя выполнять при запущенном обезличивании файла. Если домен будет изменен во время обезличивания, результаты процесса окажутся недостоверными или будут содержать в себе ошибки.

При редактировании системного домена для изменения доступны только наименование домена и значение комбинированного списка «Политика данных». Содержание регулярного выражения скрыто. В отличие от параметров пользовательского домена, параметры системного домена содержат раздел «Доп. метод проверки» для проверки метода профилирования. Данное поле необходимо только для отображения информации о том, что в анализаторе данных для этого домена используется дополнительный метод проверки.

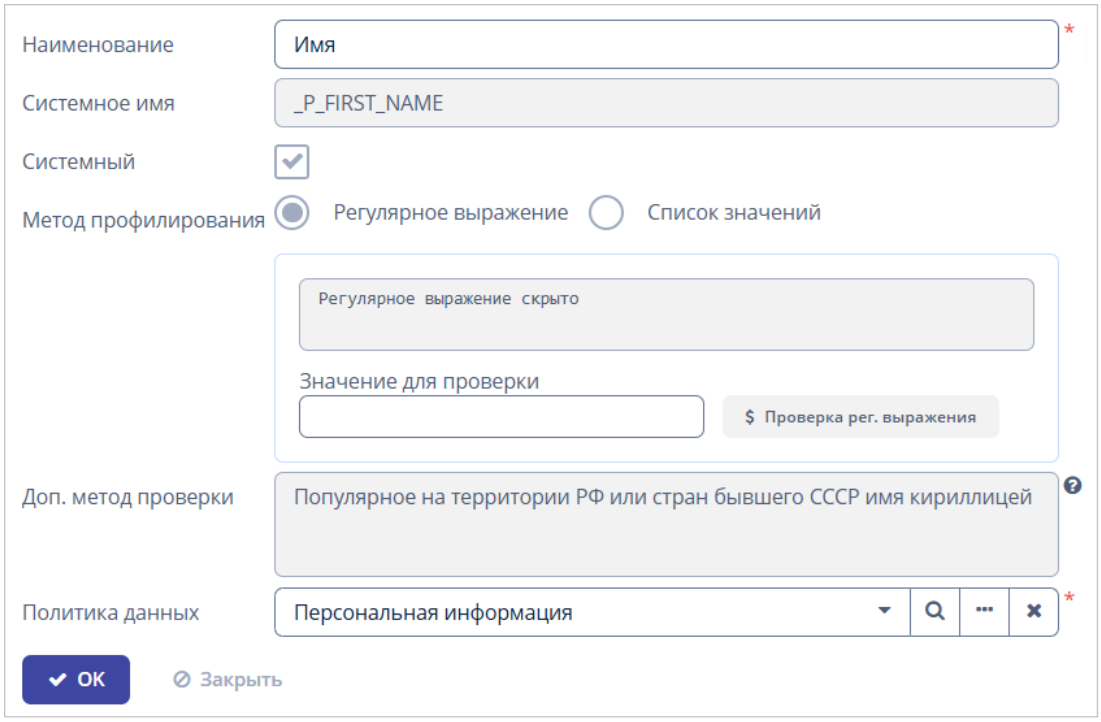

Рисунок 33 – Редактирование системного домена (пример)

При редактировании пользовательского домена для изменения доступны все параметры, кроме «Системного имени», заданного при создании домена. Пользовательский домен не может быть переведен в статус системного.

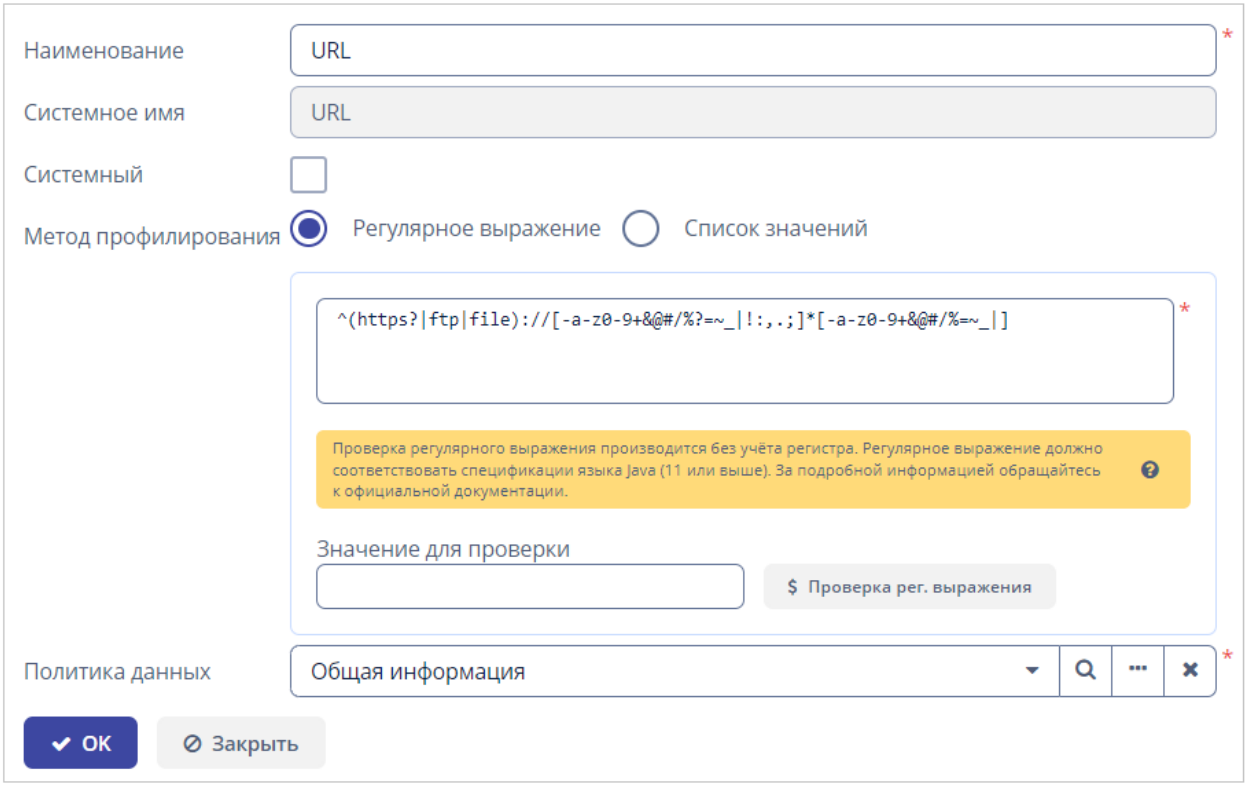

Рисунок 34 – Редактирование пользовательского домена (пример)

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

Системный домен не может быть удален.

3.6.2. Создание пользовательского домена

Пользовательские домены – домены, добавленные в Систему пользователями и содержащие проверки в соответствии с произвольными регулярными выражениями. Пользовательские домены определяют чувствительные данные, формат которых в разных компаниях может отличаться, например: имя хоста, серийный номер оборудования, логин пользователя, наименование / код проекта и т.д.

Пользовательский домен не может быть переведен в статус системного.

Для создания домена используется кнопка «Создать» в разделе Системы «Приложение» → «Домены».

На странице создания домена необходимо заполнить следующие поля и разделы.

1) Поле «Наименование»
   Название домена.
2) Поле «Системное имя»
   Системный код домена, с помощью которого он может быть идентифицирован в Системе (может содержать только заглавные латинские буквы и знаки подчеркивания, должен начинаться с буквы).
   При попытке создания пользовательского домена, наименование которого уже существует в Системе или не соответствует существующим ограничениям, появится сообщение об ошибке.
   После создания и сохранения пользовательского домена его системное имя изменению не подлежит.
3) Флажок «Системный»
   Признак, отвечающий за принадлежность домена к типу «Системный». Для пользовательских доменов данный признак недоступен для изменений.
4) Область «Метод профилирования»
   Определяет, каким образом происходит поиск конфиденциальных данных в анализаторе данных.
   Доступно два метода профилирования:
   – «Регулярное выражение»
     «Regexp», с помощью которого осуществляется проверка на принадлежность значения из загруженного в Систему файла какому-либо домену. Для некоторых доменов в целях минимизации ложных срабатываний, помимо проверки по регулярному выражению, используются дополнительные методы проверки (доступно только для системных доменов). По умолчанию

указывается регулярное выражение «^.*$», которое является универсальным (под него подходит любое значение).

– «Список значений»
  Список значений, с помощью которого осуществляется проверка на принадлежность значения из загруженного в Систему файла какому-либо домену. Происходит сравнение значения из указанного списка со значением из файла. В случае совпадения проставляется признак соответствия текущему домену.

Ниже области выбора метода профилирования находится поле для ввода соответствующей информации и поле для ввода значения для проверки. В зависимости от выбранного метода, справа от поля проверки будет присутствовать кнопка «Проверка рег. выражения» или «Проверка списка знач.».

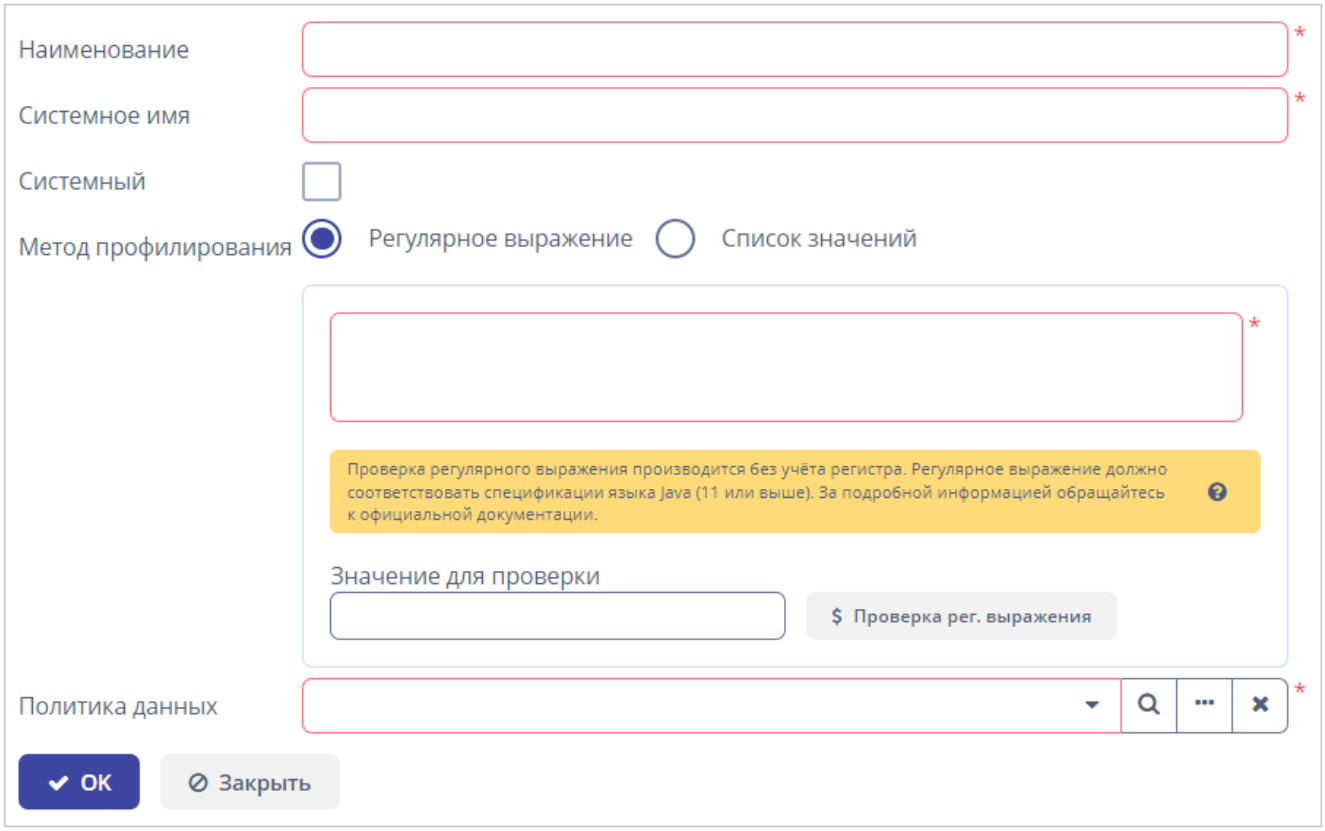

Рисунок 35 – Страница создания пользовательского домена

5) Комбинированный список «Политика данных»
   Политика данных, к которой относится данный домен.

Для сохранения домена используется кнопка «ОК».

3.6.3. Системные домены

Системные домены – домены, определяющие данные, формат которых регулируется стандартами (например, законами РФ или определенным форматом этих данных). Системные домены определяют общеизвестные категории конфиденциальной информации, которые могут быть полезны для всех организаций, например: ФИО, номер телефона, наименование организации.

Системный домен не может быть изменен или переведен в статус пользовательского.

Набор системных доменов является неизменяемым с точки зрения пользователя Системы. Системные имена системных доменов содержат префиксы, определяющие принадлежность домена какой-либо политике данных.
Ниже представлены наименования, описания и логика определения системных доменов, а также дополнительные методы проверки для некоторых из них.

3.6.3.1. _B_CARD_NUMBER (Номер банковской карты)

16-значный номер банковской карты для платежных систем «Мир», «American Express», «Visa» или «Mastercard».

Дополнительный метод проверки: алгоритм «Луна» для номера банковской карты.

Логика определения:

1) Домен определяет 16-значные номера банковских карт.
2) Первая цифра номера указывает на платежную систему.
   Домен определяет номера карт, первые цифры которых совпадают со значениями от 2 до 6.
   Слева и справа от номера не должно находиться цифр, но могут находиться буквы, специальные символы и пробелы.
   Например, домен обнаруживает номер карты в строке «номер_карты 4216 1111 2222 3333», а в строке «942161111222233339» – нет.
3) Домен определяет номера карт, в которых могут находиться разделители «-», « », «_» после каждого квартета чисел. Например, домен обнаруживает номер карты в строках «4216 1111 2222 3333», «4216_1111_2222_3333», а в строке «42-16 1111.2222_3_3_3_3» – нет.
4) Домен осуществляет проверку номера карты на его корректность с помощью алгоритма проверки контрольного числа «Луна».

3.6.3.2. _B_PAYMENT_ACCOUNT (Расчетный счет)

20-значный расчетный счет в одной из следующих валют: российский рубль, доллар США, евро, юань, фунт стерлингов, тенге, белорусский рубль, иена.

Логика определения:

1) Домен определяет 20-значные номера банковских (расчетных) счетов.
2) Слева и справа от номера не должно находиться цифр, но могут находиться буквы, специальные символы и пробелы.
3) Домен определяет номера счетов, первые три цифры которых совпадают со следующими значениями: от 401 до 425, 430.
4) Цифры на позициях 6, 7 и 8 указывают на код валюты той или иной страны.

   Домен определяет следующие коды валют:

   – 051 (Армения);
   – 156 (Китай);
   – 364 (Иран);
   – 376 (Израиль);
   – 392 (Япония);
   – 398 (Казахстан);
   – 408 (КНДР);
   – 417 (Киргизия);
   – 496 (Монголия);
   – 643, 810 (Россия);
   – 784 (ОАЭ);
   – 826 (Великобритания);
   – 840 (США);
   – 860 (Узбекистан);
   – 933 (Беларусь);
   – 934 (Туркменистан);
   – 941 (Сербия);
   – 944 (Азербайджан);
   – 949 (Турция);
   – 972 (Таджикистан);
   – 978 (Евросоюз).
5) Домен определяет номера счета, в которых могут находиться разделители «-», « », «_» после каждого квартета чисел.

3.6.3.3. _C_DATE (Дата)

Дата в формате «ДД.ММ.ГГ» или ее вариациях.

Логика определения:

1) Домен определяет даты в форматах «ДД.ММ.ГГГГ.», «ДД.ММ.ГГ.», «ГГГГ.ММ.ДД.», «ГГ.ММ.ДД».
2) Слева и справа от даты не должны находиться цифры, но могут находиться буквы, специальные символы и пробелы.
3) Домен определяет даты, в которых после числа и перед годом могут находиться наименования месяцев. Например, «31 декабря 1991 года».
4) Домен определяет даты, в которых между числом, месяцем и годом могут находиться разделители «/», «.», «-», « », «_». Например, домен обнаруживает дату строках «31.12.1999», «1999/12/31», а в строке «3\1.12,1991» – нет.

3.6.3.4. _C_EMAIL (Электронная почта)

Адрес электронной почты в соответствии с RFC 5322 с произвольным доменным именем сервера почтового ящика.

Логика определения:

1) Домен определяет адреса электронной почты с максимальной длиной в 254 символа (включая символ «@» и доменное имя).
2) Внутри адреса не должно находиться больше одного символа «@».
3) Наименование почтового ящика (до символа «@») должно состоять из букв, цифр, точек и символов «_». Левая граница наименования должна определяться пробелами или началом строки.
4) Доменное имя должно состоять из букв и одной точки. Правая граница доменного имени должна определяться цифрами, специальными символами или пробелами.
5) Домен определяет адреса, написанные латиницей как строчными, так и заглавными буквами.

3.6.3.5. _C_IP (IP-адрес)

IP-адрес версии IPv4 или IPv6.
Логика определения:

1) Домен определяет IP-адрес версии IPv4 и IPv6.
2) В случае IPv4 домен определяет адреса, состоящие из четырех групп символов, разделенных точкой. Каждая группа должна состоять из цифр в диапазоне от 0 до 255.
3) В случае IPv6 домен определяет адреса, состоящие из восьми групп символов, разделенных двоеточием. Каждая группа должна состоять из четырех символов, которые могут принимать значения: [0-9A-Fa-f].
4) Слева и справа от адреса не должно находиться цифр и букв, но могут находиться специальные символы и пробелы.

3.6.3.6. _C_LOCALITY (Населенный пункт)

Населенный пункт, город в России.
Логика определения:

1) Домен определяет наименования самых популярных городов России.
2) Слева и справа от наименования не должно находиться букв, но могут находиться цифры, специальные символы и пробелы.
3) Домен определяет наименования, написанные кириллицей как строчными, так и заглавными буквами.

3.6.3.7. _C_MAC (MAC-адрес)

MAC-адрес устройства.
Логика определения:

1) Домен определяет MAC-адрес устройства, состоящие из шести групп, разделенных дефисом или двоеточием.
2) Каждая группа адреса должна состоять из двух символов, которые могут принимать значения: [0-9A-Za-z].
3) Слева и справа от адреса не должно находиться цифр и букв, но могут находиться специальные символы и пробелы.

3.6.3.8. _C_PHONE (Номер мобильного телефона)

Номер мобильного телефона мобильного оператора России, начинающийся с +7, 7 или 8.

Логика определения:

1) Домен определяет 11-значные телефонные номера России. Слева и справа от номера не должно находиться цифр, но могут находиться буквы, специальные символы и пробелы.
2) Домен определяет номера, первые цифры которых совпадают с 7 и 8, а вторые цифры совпадают со значениями от 4 до 9.
3) Домен определяет номера, в которых вторая, третья и четвертая цифры находятся в круглых скобках. Например, «+7 (999) 123-45-67».
4) Домен определяет номера, в которых могут находиться разделители «-», « » между первой и второй, четвертой и пятой, седьмой и восьмой, девятой и десятой цифрами.

3.6.3.9. _D_MEDICAL_POLICY (Полис ОМС)

Номер полиса ОМС.

Логика определения:

1) Домен определяет 16-значные номера полисов ОМС.
2) Слева и справа от номера не должно находиться цифр, но могут находиться буквы, специальные символы и пробелы.
3) Домен определяет номера полисов, в которых первые две цифры совпадают со значениями от 01 до 84, одиннадцатые и двенадцатые цифры совпадают со значениями от 00 до 31 и от 50 до 81, а тринадцатые и четырнадцатые цифры – со значениями от 00 до 12.
4) Домен определяет номера полисов, в которых может находиться разделитель « » между шестой и седьмой цифрами.

3.6.3.10. _D_PASSPORT (Паспорт)

Номер паспорта гражданина РФ.

Логика определения:

1) Домен определяет 10-значные номера паспортов граждан России. Слева и справа от номера не должно находиться цифр, но могут находиться буквы, специальные символы и пробелы.
2) Первые две цифры номера паспорта указывают на код ОКАТО. Домен определяет номера, первые две цифры которых соответствуют кодам ОКАТО регионов России.
3) Домен определяет номера, в которых могут находиться разделители «№», « » между четвертой и пятой цифрами.

3.6.3.11. _D_TIN (ИНН физического лица)

12-значный ИНН физического лица с корректными контрольными суммами.

Дополнительный метод проверки: алгоритм проверки контрольной суммы 12-значного ИНН.

Логика определения:

1) Домен определяет 12-значный номер ИНН физического лица. Слева и справа от номера не должно находиться цифр, но могут находиться буквы, специальные символы и пробелы.
2) Первые четыре цифры номера указывают на коды ИФНС. Домен определяет номера, первые четыре цифры которых соответствуют кодам ИФНС.
3) Домен проводит анализ номера на его корректность с помощью проверки контрольного числа по алгоритму, утвержденному ФНС России.

3.6.3.12. _D_SNILS (СНИЛС)

Номер СНИЛС с корректной контрольной суммой.

Дополнительный метод проверки: алгоритм проверки контрольной суммы СНИЛС.

Логика определения:

1) Домен определяет 11-значные номера СНИЛС.
2) Слева и справа от номера не должно находиться цифр, но могут находиться буквы, специальные символы и пробелы.
3) Домен определяет номера, в которых могут находиться разделители «-», « », «_» между третьей и четвертой, шестой и седьмой, девятой и десятой цифрами.
4) Домен осуществляет проверку номера на его корректность с помощью проверки контрольного числа. Алгоритм проверки указан в п. 8 Приложения 1 информационного сообщения ПФ РФ от 21.02.2013 г. «Особенности представления страхователями в органы ПФР отчетности, начиная с отчетности с I квартала 2013 года».

3.6.3.13. _O_NAME (Наименование юридического лица)

Наименование юридического лица (ИП, АО, ПАО, ООО, ЗАО, ОАО, ОДО, ГУП или ГК).

Логика определения:

1) Домен определяет наименования юридических лиц, записанных после вида юридических лиц, т.е. после вида юридического лица должно быть записано хотя бы одно слово.
2) Домен определяет следующие виды юридических лиц (а также их сокращения, например: ИП, АО, ООО и т.д.):
   - индивидуальный предприниматель;
   - акционерное общество;
   - публичное акционерное общество;
   - общество с ограниченной ответственностью;
   - закрытое акционерное общество;
   - открытое акционерное общество;
   - общество с дополнительной ответственностью;
   - государственное унитарное предприятие;
   - госкорпорация / государственная корпорация.
3) Слева от наименования не должно находиться букв, но могут находиться цифры, специальные символы и пробелы.
4) Домен определяет виды юридических лиц, написанные как строчными, так и заглавными буквами.
5) Домен определяет наименования, в которых должны присутствовать от одного до пяти пробелов и одна или ни одной кавычки между видом юридического лица и наименованием (например, ООО «Рога и копыта»).

3.6.3.14. _O_TIN (ИНН юридического лица)

10-значный ИНН юридического лица с корректной контрольной суммой.

Дополнительный метод проверки: алгоритм проверки контрольной суммы 10-значного ИНН.

Логика определения:

1) Домен определяет 10-значный номер ИНН юридического лица. Слева и справа от номера не должно находиться цифр, но могут находиться буквы, специальные символы и пробелы.
2) Первые четыре цифры номера указывают на коды ИФНС. Домен определяет номера, первые четыре цифры которых соответствуют кодам ИФНС.
3) Домен проводит анализ номера на его корректность с помощью проверки контрольного числа по алгоритму, утвержденному ФНС России.

3.6.3.15. _P_EDUCATION_LEVEL (Уровень образования)

Уровень образования (в том числе академическая степень).

Логика определения:

1) Домен определяет уровни образования в России:
   - аспирант / аспирантура;
   - бакалавр / бакалавриат;
   - магистр / магистратура;
   - специалист / специалитет;
   - высшее;
   - дошкольное;
   - начальное общее;
   - основное общее;
   - среднее общее;
   - среднее профессиональное;
   - кандидат наук;
   - доктор наук.
2) Слева и справа от уровня не должно находиться букв, но могут находиться цифры, специальные символы и пробелы.
3) Домен определяет уровни, написанные как строчными, так и заглавными буквами.

3.6.3.16. _P_FIRST_NAME (Имя)

Популярное на территории РФ или стран бывшего СССР имя, написанное кириллицей.

Логика определения:

1) Домен определяет четыреста самых популярных мужских и женских имен в России, написанных кириллицей.
2) Слева и справа от имен не должно находиться букв, но могут находиться цифры, специальные символы и пробелы.
3) Домен определяет имена, написанные как строчными, так и заглавными буквами.

3.6.3.17. _P_LAST_NAME (Фамилия)

Популярная на территории РФ или стран бывшего СССР фамилия, написанная кириллицей.

Логика определения:

1) Домен определяет пятьсот пятьдесят самых популярных мужских фамилий в России, написанных кириллицей. Женские фамилии будут определяться соответственно мужским фамилиям, т.к. они образуются путем прибавления к мужской фамилии буквы «а».
2) Слева от фамилий не должно находиться букв, но могут находиться цифры, специальные символы и пробелы. Справа от фамилий не должно находиться букв, кроме одной буквы «а», также могут находиться цифры, специальные символы и пробелы.
3) Домен определяет фамилии, написанные кириллицей как строчными, так и заглавными буквами.

3.6.3.18. _P_MARITAL_STATUS (Семейное положение)

Семейное положение.

Логика определения:

1) Домен определяет семейное положение людей:
   – в разводе;
   – вдова / вдовец;
   – женат / не женат;
   – замужем / не замужем;
   – разведен / разведена;
   – холост.
2) Слева и справа от положения не должно находиться букв, но могут находиться цифры, специальные символы и пробелы.
3) Домен определяет положения, написанные как строчными, так и заглавными буквами.

3.6.3.19. _P_PATRONYMIC (Отчество)

Популярное на территории РФ или стран бывшего СССР отчество, написанное кириллицей.

Логика определения:

1) Домен определяет тысячу самых популярных мужских и женских отчеств в России, написанных кириллицей.
2) Слева и справа от отчеств не должно находиться букв, но могут находиться цифры, специальные символы и пробелы.
3) Домен определяет отчества, написанные как строчными, так и заглавными буквами.

3.7. Политики данных

3.7.1. Общая информация

Политики данных группируют домены по принадлежности к одной и той же области информации. Например, такие домены как «_P_LAST_NAME» (фамилия), «_P_PATRONYMIC» (отчество) и «_P_NATIONALITY» (национальность) объединяются в политику данных «_P _» (персональная информация).

Список политик данных содержится в разделе Системы «Приложение» → «Политики данных».

Для просмотра политики данных необходимо нажать на ее наименование в списке. Для изменения политики данных необходимо выбрать ее из списка и нажать кнопку «Изменить», внести изменения и сохранить их. Для удаления политики данных необходимо выбрать ее из списка и нажать кнопку «Удалить», в появившемся окне подтвердить удаление.

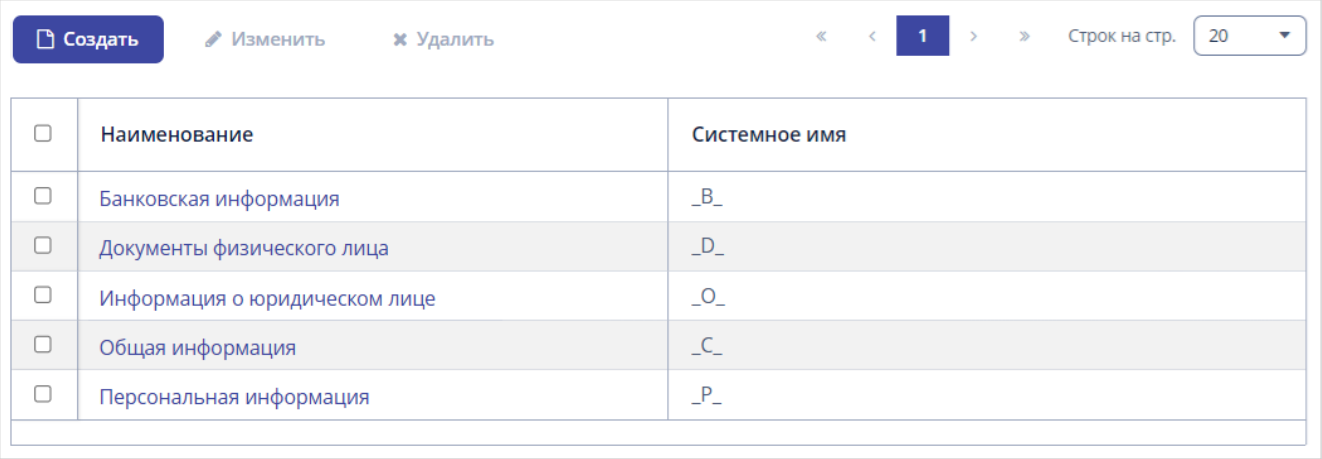

Рисунок 36 – Подраздел «Политики данных»

3.7.2. Создание политики данных

Для создания политики данных используется кнопка «Создать» в разделе Системы «Приложение» → «Политики данных».

На странице создания политики данных необходимо заполнить все поля. В качестве системного имени, как правило, используется префикс политики данных в формате «_буква_». При редактировании политики данных изменение системного имени будет недоступным. Для сохранения используется кнопка «ОК».

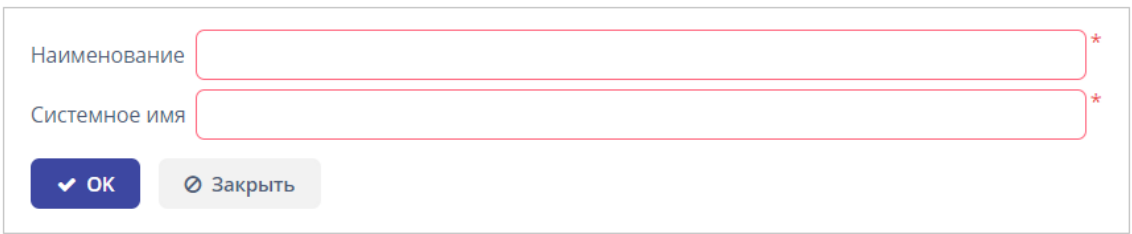

Рисунок 37 – Страница создания политики данных

3.8. Справочники

3.8.1. Общая информация

Справочник определяет наименование каталога с данными.

Справочники и их элементы могут использоваться в определенных методах маскирования, в которых исходное значение заменяется на другое. Например, коды справочников используются в качестве значений параметров в методе маскирования «Замена по справочнику».

Список справочников содержится в разделе Системы «Приложение» → «Справочники».

Для просмотра справочника необходимо нажать на его наименование в списке.

Для изменения справочника необходимо выбрать его из списка и нажать кнопку «Изменить», внести изменения и сохранить их.

Для удаления справочника необходимо выбрать его из списка и нажать кнопку «Удалить», в появившемся окне подтвердить удаление.

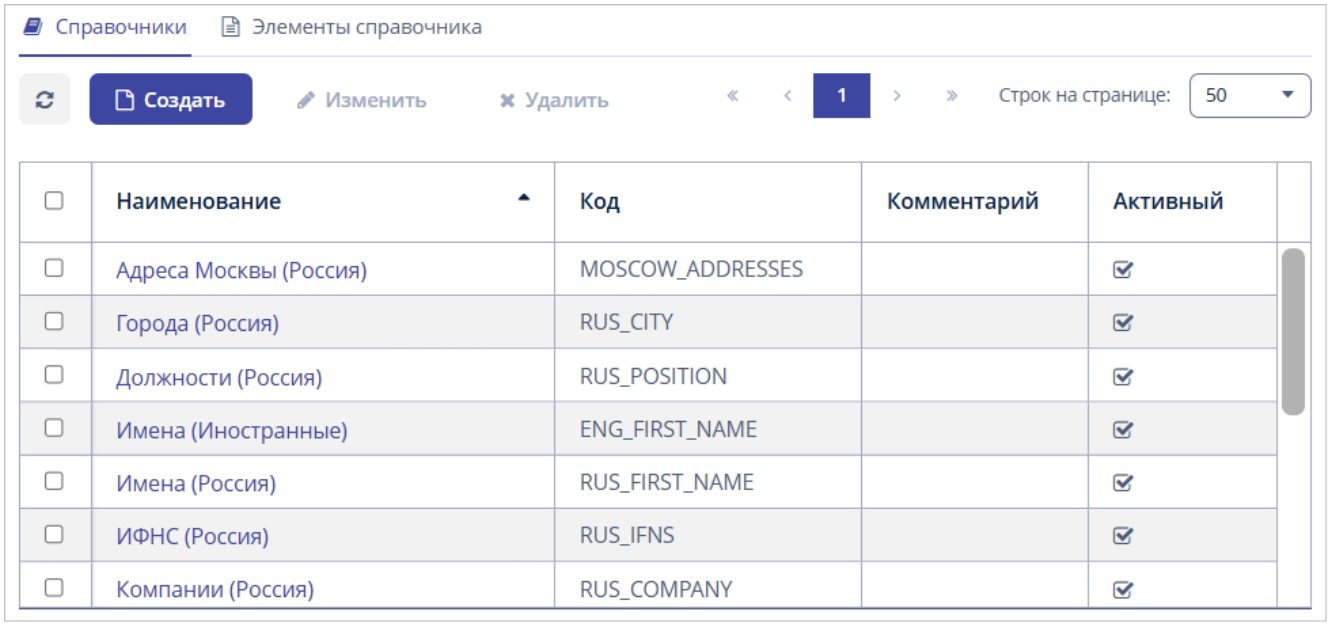

Рисунок 38 – Подраздел «Справочники»: вкладка «Справочники»

Справочники, существующие в Системе по умолчанию:

- «Адреса Москвы (Россия)» – список адресов г. Москвы;
- «Города (Россия)» – список городов России;
- «Должности (Россия)» – список должностей сотрудников;
- «Имена (Иностранные)» – список иностранных имен (записаны латинскими буквами);
- «Имена (Россия)» – список имен России (записаны кириллицей);
- «ИФНС (Россия)» – список случайно сгенерированных чисел, приведенных к формату ИФНС;

– «Компании (Россия)» – список несуществующих компаний;
– «Населенные пункты» – список населенных пунктов мира;
– «Несуществующие города (Россия)» – список несуществующих городов России;
– «Префиксы стран для международных номеров» – список префиксов стран, которые используются в международных банковских номерах;
– «Проекты (Россия)» – список проектов, в которых может участвовать организация;
– «Простые обезличенные значения (Россия)» – список простых обезличенных значений формата «Значение» + «Число»;
– «Структурные подразделения (Россия)» – структурные подразделения для организации;
– «Фамилии (Россия)» – список фамилий России (записаны кириллицей).

Список справочников и их элементов может пополняться администратором Системы.

3.8.2. Создание справочника

Для создания справочника используется кнопка «Создать» в разделе Системы «Приложение» → «Справочники».

На странице создания справочника необходимо заполнить поля:

– «Наименование» – наименование справочника;
– «Код» – системный код справочника для его идентификации в Системе;
– «Комментарий» – краткое описание содержимого справочника.

При снятии флажка «Активный» справочник будет недоступен для выбора при маскировании данных. Для сохранения используется кнопка «ОК».

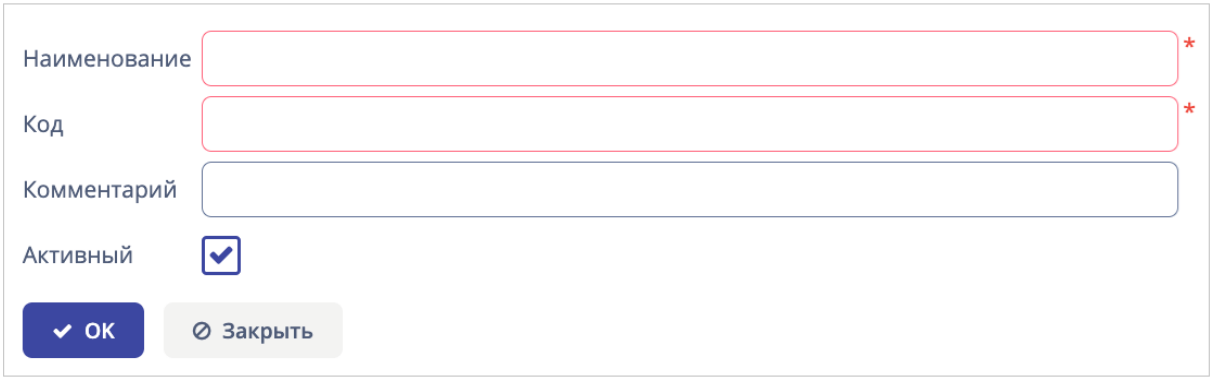

Рисунок 39 – Страница создания справочника

3.8.3. Элементы справочника

Элементы справочника – это однородные по своей сути объекты, входящие в один справочник.

Для просмотра списка элементов справочников необходимо перейти в раздел Системы «Приложение» → «Справочники», на вкладке «Справочники» выбрать один или несколько справочников из списка и перейти на вкладку «Элементы справочника» – на ней отобразятся элементы выбранных справочников. Если справочники не были выбраны, вкладка «Элементы справочника» будет пустой.

Для просмотра элемента справочника необходимо нажать на его наименование в списке.

Для изменения элемента справочника необходимо выбрать его из списка и нажать кнопку «Изменить», внести изменения и сохранить их.

Для удаления элемента справочника необходимо выбрать его из списка и нажать кнопку «Удалить», в появившемся окне подтвердить удаление.

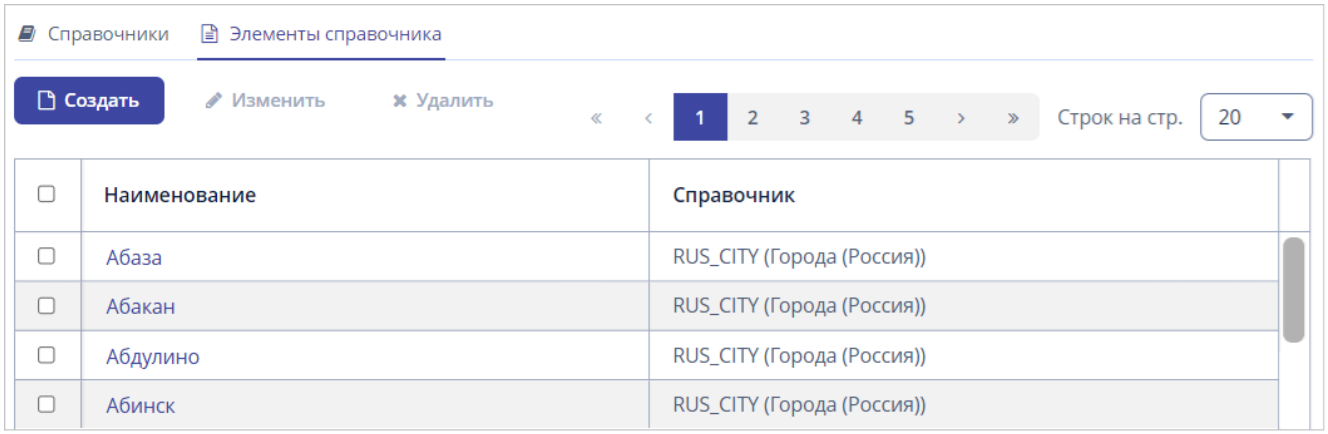

Рисунок 40 – Подраздел «Справочники»: вкладка «Элементы справочника»

Для создания элемента справочника необходимо перейти в раздел Системы «Приложение» → «Справочники» → вкладка «Элементы справочника» и нажать кнопку «Создать» над списком. На странице создания элемента справочника необходимо заполнить поля:

– «Наименование» – наименование элемента справочника;

– «Справочник» – справочник, для которого создается элемент.

Для сохранения используется кнопка «ОК».

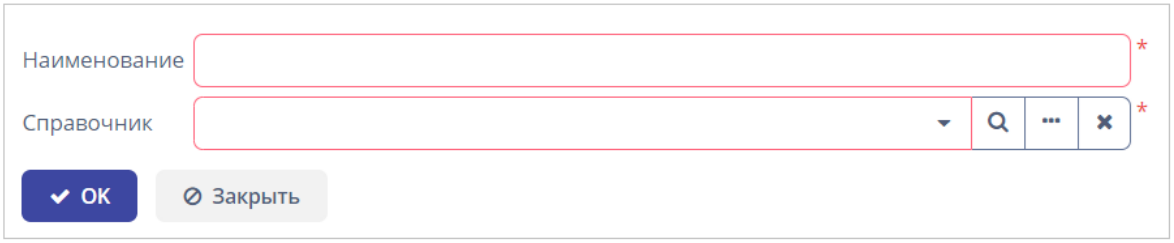

Рисунок 41 – Страница создания элемента справочника

3.9. Методы маскирования

3.9.1. Общая информация

Метод маскирования определяет логику преобразования данных при обезличивании. Существуют системные (поставляемые вместе с дистрибутивом Системы) и пользовательские (создаваемые пользователем Системы) методы маскирования. На их основе создаются правила маскирования, содержащие в себе значения параметров методов по умолчанию.

Список методов маскирования содержится в разделе Системы «Приложение» → «Методы маскирования».

Для просмотра метода маскирования необходимо нажать на его наименование в списке.

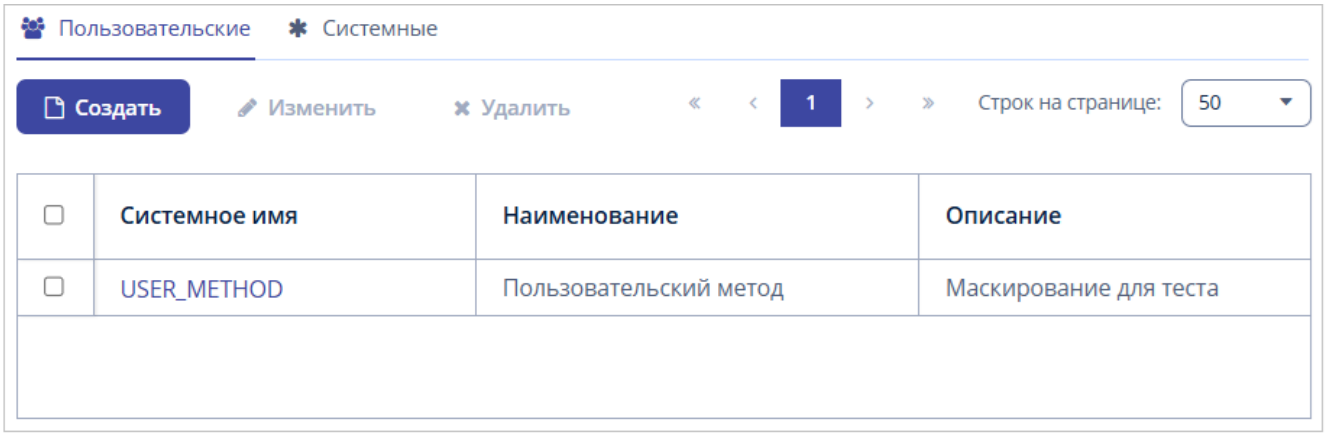

Рисунок 42 – Методы маскирования: вкладка «Пользовательские» (пример)

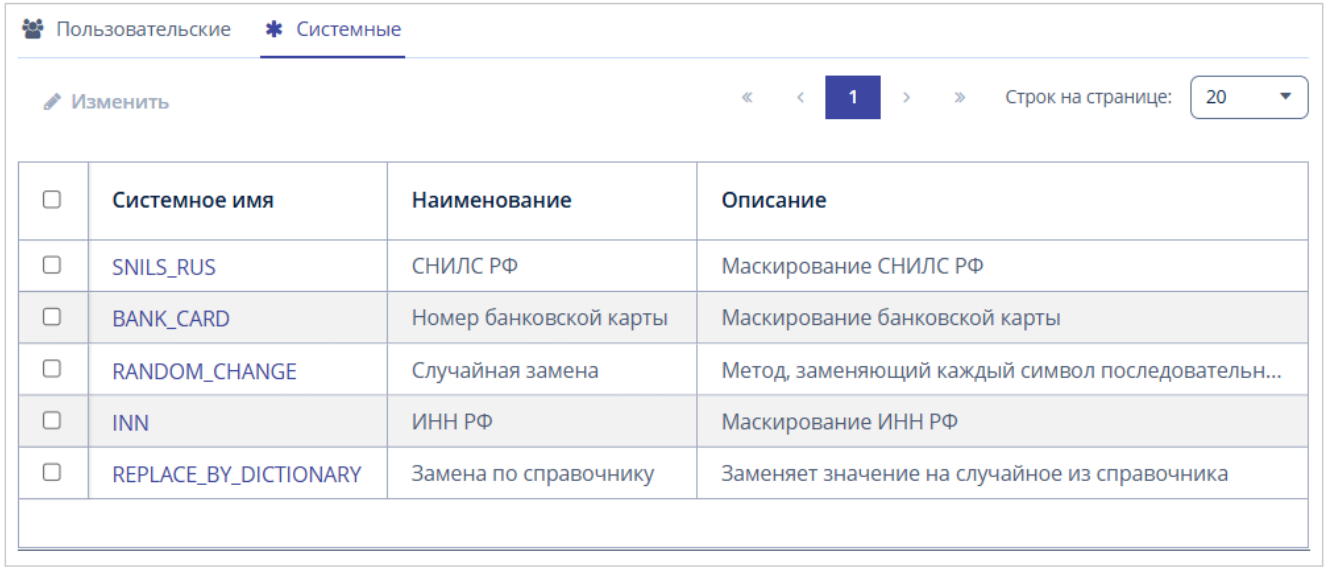

Рисунок 43 – Методы маскирования: вкладка «Системные»

Для изменения метода маскирования необходимо выбрать его из списка и нажать кнопку «Изменить». В отличие от пользовательского метода, для системного метода маскирования доступно изменение только его наименования.

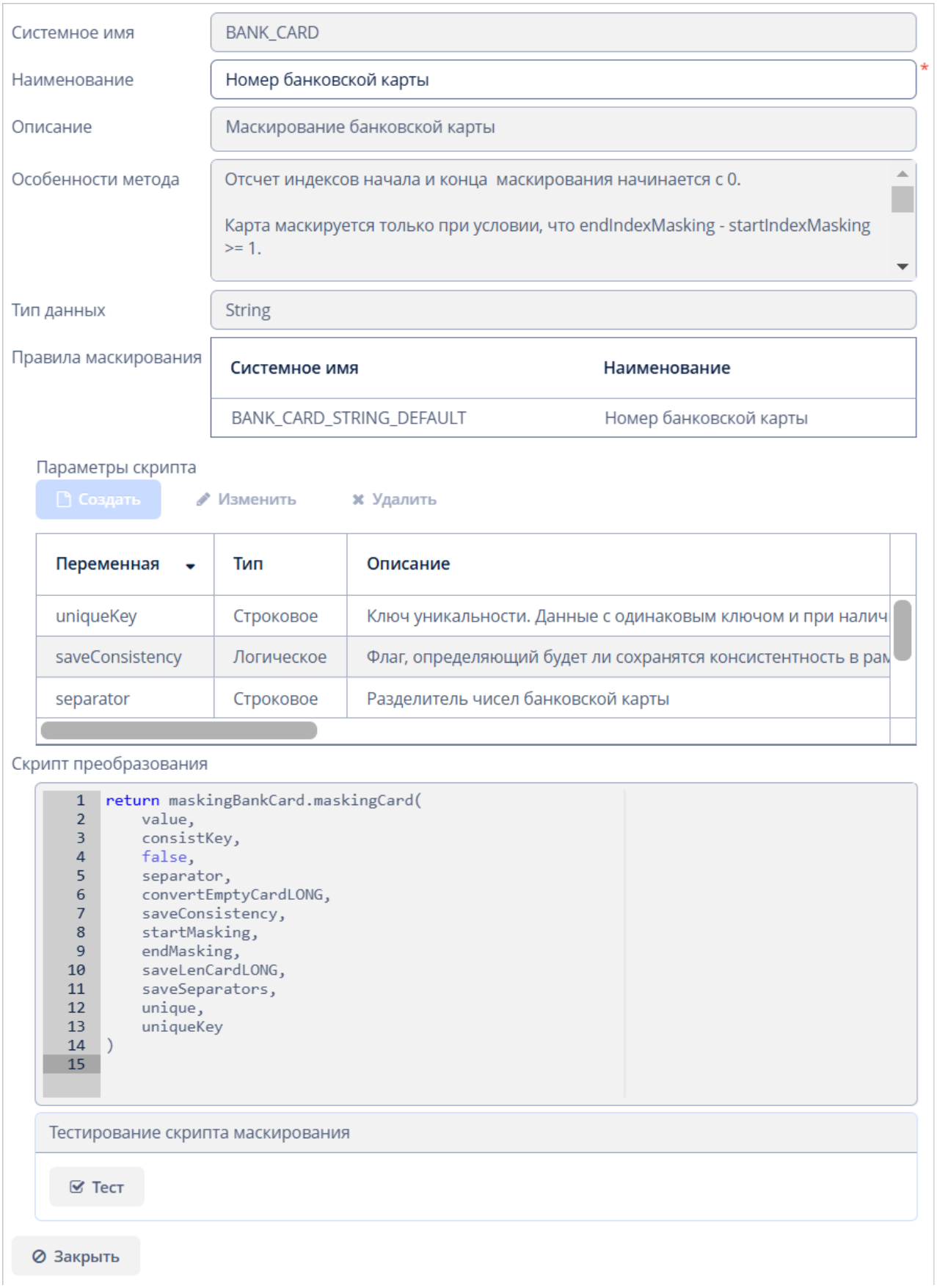

Рисунок 44 – Страница изменения системного метода маскирования (пример)

Для удаления пользовательского метода маскирования необходимо выбрать его из списка и нажать кнопку «Удалить», в появившемся окне подтвердить удаление. Системные методы маскирования не могут быть удалены.

Каждый метод маскирования может быть протестирован. Перед тестированием метода необходимо сохранить внесенные в него изменения. Для перехода к тестированию используется кнопка «Тест» в карточке метода.

При необходимости можно указать значения параметров скрипта метода. Для этого в поле «Входное значение» требуется ввести значение, предназначенное для тестирования, выбрать тип данных и нажать кнопку «Тест». Полученное в результате тестирования значение появится во всплывающем сообщении. Для возврата к карточке метода маскирования необходимо нажать на сообщение, затем нажать кнопку «Закрыть» в окне тестирования.

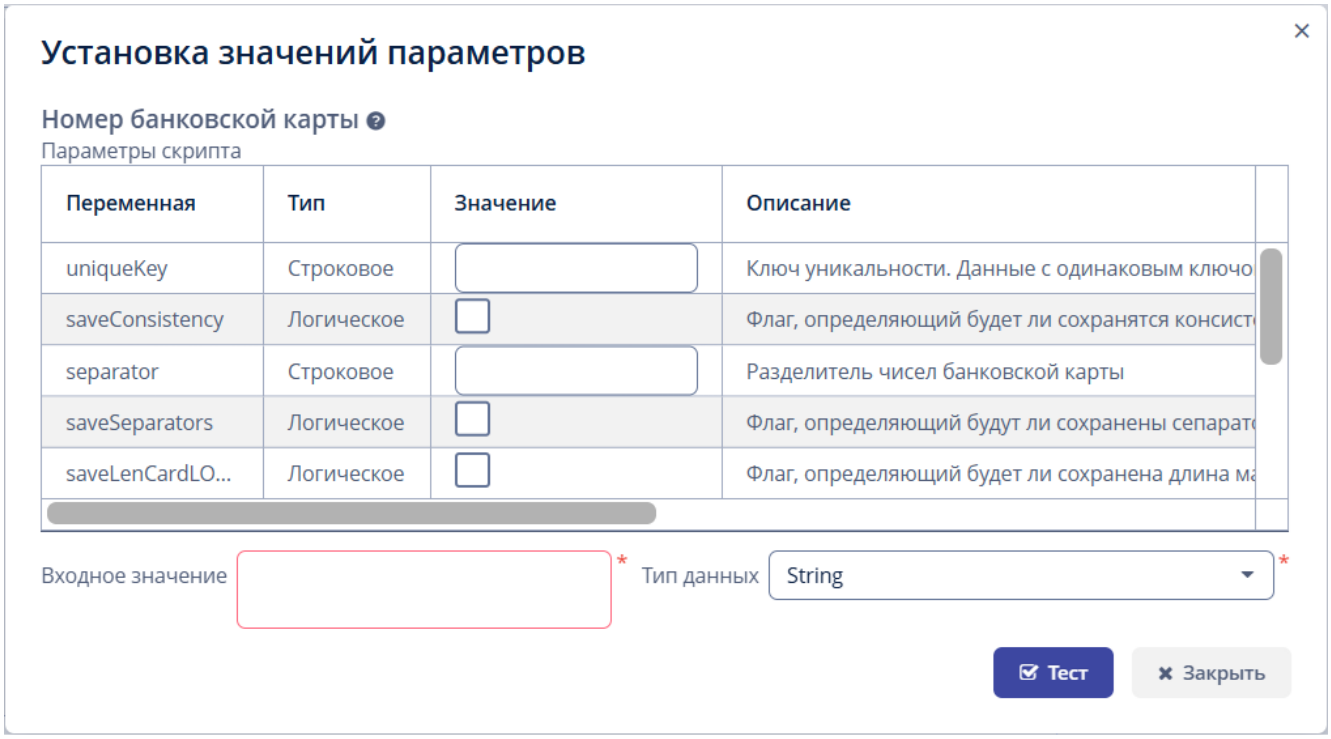

Рисунок 45 – Окно тестирования метода маскирования (пример)

Скрипт всегда использует для своей работы следующие данные.

1) Исходное значение (переменная «value»)
   Оригинальное значение из загруженного в Систему файла до его маскирования.
2) Переменные с названием параметра скрипта
   Значения параметров скрипта доступны в его переменных, которые называются, как сам параметр (например, «constantValue»). Тип переменной определяется типом параметра.

3.9.2. Создание пользовательского метода маскирования

Для создания пользовательского метода маскирования необходимо перейти в раздел «Приложение» → «Методы маскирования» и нажать кнопку «Создать» на вкладке «Пользовательские».

На странице создания пользовательского метода маскирования необходимо заполнить следующие поля и разделы.

1) «Системное имя»
   Системный код метода маскирования, с помощью которого он может быть идентифицирован в Системе.
2) «Наименование»
   Название метода маскирования.
3) «Описание»
   Краткое описание метода маскирования.
4) «Особенности метода»
   Описание работы метода маскирования.
5) «Тип данных»
   Тип данных, к которому привязан метод маскирования. К данным файла с типом «STRING» можно применить только методы маскирования, которые работают с типом данных «STRING».
6) «Правила маскирования»
   Правила маскирования, основанные на методе маскирования. Таблица заполняется, когда в карточке правила маскирования указывается метод, к которому оно привязано.
7) «Список параметров скрипта»
   Таблица с параметрами метода маскирования.
8) «Скрипт преобразования»
   Groovy-скрипт, определяющий логику преобразования исходного значения. Скрипт может использовать все возможности языка Groovy и доступен для изменения только наиболее опытным пользователям Системы, а также ее администраторам.
9) «Тестирование скрипта маскирования»
   Блок для проверки работы метода маскирования.

Для сохранения используется кнопка «ОК».

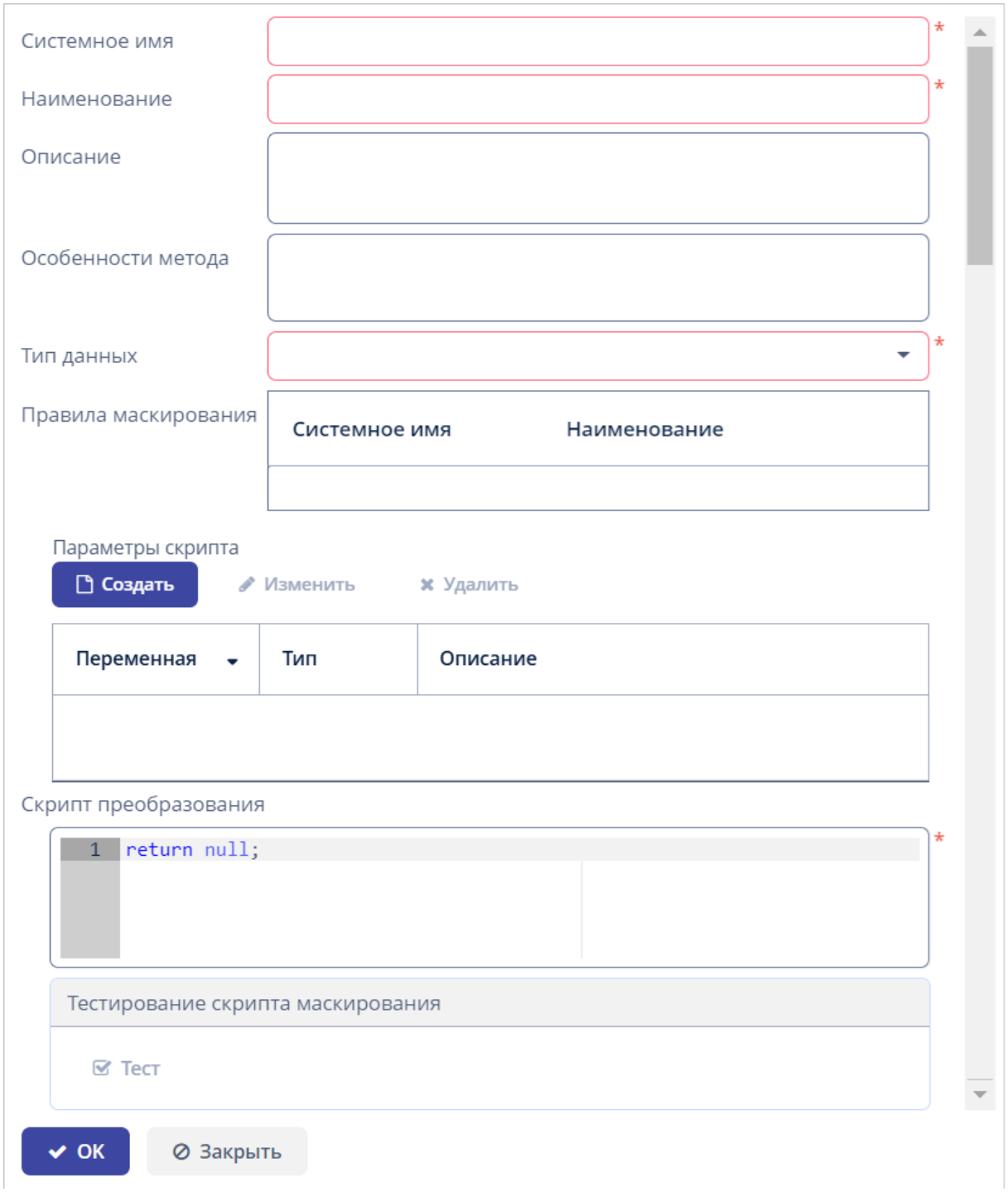

Рисунок 46 – Страница создания пользовательского метода маскирования

3.9.3. Параметры методов маскирования

3.9.3.1. Общая информация

Параметры методов маскирования – переменные, которые могут быть использованы в скрипте преобразования (Groovy-скрипте) метода маскирования.

В каждый метод маскирования передается свой уникальный набор параметров, который определяется при создании метода маскирования. При создании правила маскирования, основанного на методе, необходимо указать значения параметров для данного правила по умолчанию.

Например, при необходимости замены последних N букв в значении на служебные символы пользователь может воспользоваться любым из правил, основанном на соответствующем системном методе.

Примеры использования методов маскирования для замены символов.

При использовании метода «Замена 5 последних символов на ?», если значение параметра «количество символов» будет = «5», символ = «?», параметр «fromEnd» = «true», фамилия «Иванов» будет преобразована в «И?????».

При использовании метода «Замена 2 последних символов на #», если значение параметра «количество символов» будет = «2», символ = «#», параметр «fromEnd» = «true», фамилия «Иванов» будет преобразована в «Иван##».

Названия правил приведены для примера. Пользователь может создать свои собственные правила с индивидуальным набором параметров и называть их по-своему.

3.9.3.2. Создание параметра метода маскирования

Создание параметра метода маскирования (параметра скрипта) возможно только для пользовательского метода маскирования.

Для создания параметра необходимо перейти в раздел «Приложение» → «Методы маскирования», на вкладке «Пользовательские» выбрать метод маскирования из списка и нажать кнопку «Изменить».

На странице редактирования метода маскирования в разделе «Параметры скрипта» необходимо нажать кнопку «Создать».

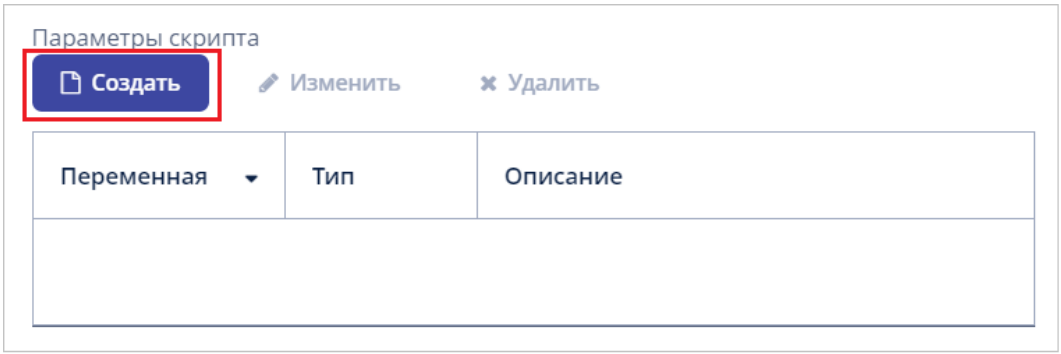

Рисунок 47 – Создание параметра скрипта

В открывшемся окне необходимо заполнить все поля и выбрать тип данных параметра из выпадающего списка «Тип». Параметры могут быть трех типов: строковые, логические и числовые.

Для сохранения параметра используется кнопка «ОК».

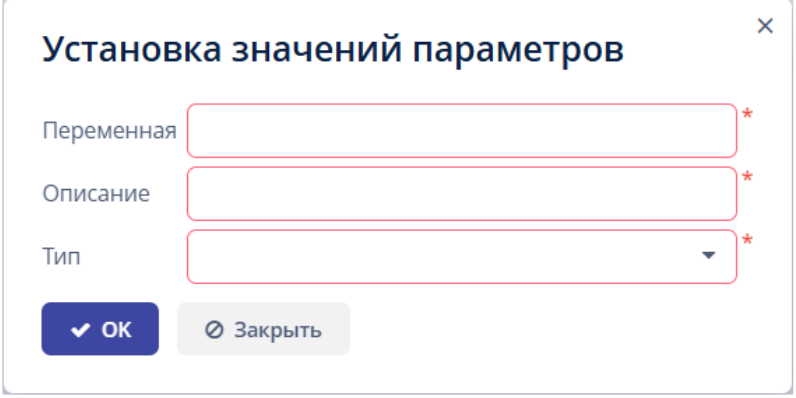

Рисунок 48 – Окно создания параметра скрипта

Для изменения параметра скрипта необходимо дважды нажать на его название в списке или выбрать его из списка и нажать кнопку «Изменить».

Для удаления параметра скрипта необходимо выбрать его из списка и нажать кнопку «Удалить», в появившемся окне подтвердить удаление.

3.9.4. Валидация в методах маскирования

Пользователь может создавать правила маскирования на основе методов, задавая разные значения параметров маскирования. Может возникнуть ситуация, при которой с указанными значениями параметров применение правила к данным из загруженного в Систему файла будет невозможным по какой-либо причине.

Одной из таких причин может быть слишком большое количество уникальных записей в маскируемом файле. В таком случае Система оповестит пользователя о том, что данное правило не может быть применено к данным из файла ввиду слишком маленькой мощности выборки. Мощность выборки – это количество возможных вариантов замаскированных значений при определенном наборе параметров правила.

Другой причиной может стать комбинация взаимоисключающих параметров или некорректные значения этих параметров.

Каждый метод маскирования имеет свой набор ограничений на значения и комбинации вводимых параметров в основанных на них правилах маскирования. Ограничения определяются индивидуально в каждом из методов с помощью Groovy-скрипта в разделе «Параметры скрипта». Для валидации (проверки) в методах маскирования существует скрипт проверки и сообщение об ошибке (в случае непрохождения валидации).

Также в каждом из методов маскирования могут присутствовать дополнительные ограничения, связанные со спецификой данных, хранящихся в загруженном в Систему файле (относящиеся к домену).

Например, в номерах банковских карт первые четыре цифры отвечают за принадлежность к определенному банку, часто повторяются и не могут быть случайными, что влияет на мощности выборки. Количество возможных вариантов написания ИНН также определено математической последовательностью, определенной законом, что может сокращать выборку.

3.9.5. Системные методы маскирования

В данном разделе приведены системные (встроенные) методы маскирования, поставляемые вместе с дистрибутивом Системы.

В текущей версии Системы в системных методах маскирования присутствуют, но не используются следующие параметры методов: «unique», «saveConsistency», «consistKey» и «uniqueKey».

3.9.5.1. Замена по справочнику

Заменяет исходное значение на элемент справочника. Метод используется для замены исходного значения на реалистичное, но отличное от оригинального. Работает только со строковыми значениями.

Особенности метода:

1) Если одновременно установлены параметры «unique» и «saveConsistency», маскирование будет происходить консистентно, а не уникально.
2) В случае, если размер словаря недостаточен при установленном параметре уникальности, будет добавлен числовой постфикс. Пример: если имя «Иван» уже было использовано, будет применено значение «Иван_1».

Параметры метода:

- «maskingDictCode» – указание кода справочника, на элементы которого будут маскироваться исходные данные;
- «saveConsistency» – признак, определяющий сохранение консистентности в рамках ключа консистентности;
- «consistKey» – ключ консистентности (применяется при активном параметре «saveConsistency»);
- «unique» – всегда заменяет исходное значение на уникальное выходное значение в рамках маскируемых данных из загруженного в Систему файла;
- «uniqueKey» – ключ уникальности (применяется при активном параметре «unique», данные с одинаковым ключом маскируются уникально).

Данный метод часто используется при маскировании фамилии или имени пользователей.

При наборе параметров, указанных в таблице 1, имя пользователя «Иван» изменится на «Андрей». При активном параметре сохранения консистентности, если в ходе маскирования имя пользователя «Иван» хотя бы раз заменилось на

«Андрей», все последующие имена «Иван» в рамках ключа консистентности будут заменены на «Андрей».

Таблица 1 – Пример параметров для метода «Замена по справочнику»

Название переменной	Значение
saveConsistency	активно
maskingDictCode	RUS_FIRST_NAME
consistKey	defaultFirstNameConsistKey
unique	активно
uniqueKey	DEFAULT_RUS_FIRST_NAME_UNIQUE

Количество записей в справочнике с указанным в параметре «maskingDictCode» кодом должно быть достаточным, чтобы выдержать консистентность. В данном случае при валидации проверяется количество записей в справочнике перед запуском маскирования, и маскирование не будет выполнено с консистентностью, если количество уникальных записей в загруженном в Систему файле превышает мощность выборки из справочника.

3.9.5.2. Номер банковской карты

Изменяет исходные цифры в номере банковской карты в соответствии с заданными параметрами, с проверкой контрольного числа. Работает только со строковыми значениями.

Особенности метода:

- если интервал маскирования недостаточен при маскировании с уникальными значениями, исходное значение будет замаскированно полностью;
- отсчет индексов начала и конца маскирования начинается с «0»;
- если одновременно установлены параметры «unique» и «saveConsistency», маскирование будет происходить консистентно, а не уникально;
- если значение параметра «startMasking» или «endMasking» равно нулю, считается, что значение не установлено;
- исходное значение маскируется только при условии «endMasking - startMasking ≥ 1»;
- если исходная последовательность цифр содержит менее 15 или более 19 символов, создается случайный номер банковской карты из 16 символов;
- если исходная строка не является числовой последовательностью, все знаки, не являющиеся сепараторами, будут заменены на цифры, и строка будет замаскирована как числовая последовательность;

– если в исходной последовательности цифр присутствовали разделители и не были удалены из-за их неверного указания в параметре, такая последовательность будет считаться нечисловой;
– разделители при их сохранении остаются на прежних местах (например, для последовательности «1234_1234_1234_1234» при установке параметра «saveLenCardNumber» = «false» и при сохранении сепараторов исходного номера банковской карты возможен результат «1234_1234_1234_12345»);
– разделители не являются индексируемым элементом (например, в номере «0123_4567_8901_2345» индекс цифры «4» = 4).

Параметры метода:

– «uniqueKey» – ключ уникальности (применяется при активном параметре «unique», данные с одинаковым ключом маскируются уникально);
– «saveConsistency» – отвечает за сохранение консистентности в рамках ключа консистентности (если номер карты в одной строчке «0000 0001 0000 0001» был заменен на «1111 1110 1111 1110», все карты с номером «0000 0001 0000 0001» будут заменены на «1111 1110 1111 1110»);
– «separator» – разделитель между цифрами банковской карты (пробел или специальный символ), значение по умолчанию «EMPTY» означает отсутствие разделителей;
– «saveSeparators» – отвечает за сохранение разделителей на тех же местах, на которых они находятся в исходных данных;
– «saveLenCardNumber» – отвечает за сохранение длины номера карты;
– «consistKey» – ключ консистентности (применяется при активном параметре «saveConsistency»);
– «startMasking» – индекс начала фрагмента маскирования (например, при указании параметра равным «4» маскирование будет производиться, начиная с пятой цифры исходного значения);
– «convertEmptyCardNumber» – определяет, будут ли пустые значения и последовательности, не состоящие из чисел, преобразовываться в номер банковской карты длиной 16 символов;
– «endMasking» – индекс окончания фрагмента маскирования (например, при указании параметра равным «4» маскирование будет производиться до пятой цифры исходного значения);
– «unique» – всегда заменяет исходное значение на уникальное выходное значение в рамках маскируемых данных из загруженного в Систему файла.

Если указать параметр «startMasking» = «5», номер карты «1111 2222 3333 4444» будет маскироваться, начиная с шестого символа. Первые пять символов останутся равными исходным значениям (при условии, что «endMasking» не указан).

При наборе параметров, указанных в таблице 2, номер карты «1111 2222 3333 4444» может быть преобразован в «1111 2648 8789 6786».

Таблица 2 – Пример использования параметра «startMasking» в методе «Номер банковской карты»

Название переменной	Значение
saveLenCardNumber	активно
saveSeparators	активно
startMasking	5
endMasking	0
convertEmptyCardNumber	активно
saveConsistency	неактивно
consistKey	defaultBankCardconsistKey
separator	пробел
unique	активно
uniqueKey	BANK_CARD_STRING_DEFAULT_UNIQUE

Если указать параметр «endMasking» = «3», в номере карты «1111 2222 3333 4444» замаскируются только три первые значения (при условии, что «startMasking» не указан).

При наборе параметров, указанных в таблице 3, номер карты «1111 2222 3333 4444» может быть преобразован в «6891 2222 3333 4444».

Таблица 3 – Пример использования параметра «endMasking» в методе «Номер банковской карты»

Название переменной	Значение
saveLenCardNumber	активно
saveSeparators	активно
startMasking	0
endMasking	3
convertEmptyCardNumber	активно
saveConsistency	неактивно
consistKey	defaultBankCardconsistKey
separator	пробел
unique	активно
uniqueKey	BANK_CARD_STRING_DEFAULT_UNIQUE

При наборе параметров, указанных в таблице 4, номер карты «1111 1111 1111 1111» может быть преобразован в «1111 2345 6781 1111».

Таблица 4 – Пример использования параметров «startMasking» и «endMasking» в методе «Номер банковской карты»

Название переменной	Значение
saveLenCardNumber	активно
saveSeparators	активно
startMasking	4
endMasking	11
convertEmptyCardNumber	активно
saveConsistency	неактивно
consistKey	defaultBankCardconsistKey
separator	пробел
unique	активно
uniqueKey	BANK_CARD_STRING_DEFAULT_UNIQUE

Если вместо номера банковской карты указано значение «карта отсутствует», при наборе параметров, указанных в таблице 5, может получиться результат «0101 0102 0203 0304».

Таблица 5 – Пример использования параметра «convertEmptyCardNumber» в методе «Номер банковской карты»

Название переменной	Значение
saveLenCardNumber	активно
saveSeparators	активно
startMasking	0
endMasking	0
convertEmptyCardNumber	активно
saveConsistency	неактивно
consistKey	defaultBankCardconsistKey
separator	пробел
unique	активно
uniqueKey	BANK_CARD_STRING_DEFAULT_UNIQUE

При наборе параметров, указанных в таблице 6, номер карты «0001_0001_0001_0001» может быть преобразован в «2110_3110_4110_5110».

Таблица 6 – Пример использования параметра «separator» в методе «Номер банковской карты»

Название переменной	Значение
saveLenCardNumber	активно
saveSeparators	активно
startMasking	0
endMasking	0
convertEmptyCardNumber	активно
saveConsistency	неактивно
consistKey	defaultBankCardconsistKey
separator	_
unique	активно
uniqueKey	BANK_CARD_STRING_DEFAULT_UNIQUE

Ниже приведены проверки в рамках валидации метода.

1) Проверка 1
   Значения «startMasking» ≥ 0, «endMasking» ≥ 0, «endMasking» > «startMasking».
2) Проверка 2
   Диапазон значений между «endMasking» и «startMasking» должен быть достаточным, чтобы выдержать консистентность. В данном случае валидация проверяет комбинацию значений указанных параметров правила маскирования перед запуском самого маскирования. Пользователь не сможет осуществить маскирование с консистентностью, если количество уникальных записей в загруженном в Систему файле больше, чем мощность выборки.
3) Проверка 3
   Параметр «convertEmptyValue» не должен быть установлен одновременно вместе с параметром «saveConsistency». Консистентность не может маскировать одинаковые значения, в том числе «null», в разные значения. Поэтому комбинация данных параметров не имеет практического смысла.

3.9.5.3. ИНН РФ

Данные исходного файла заменяются на случайно сгенерированные значения в формате ИНН РФ, с проверкой контрольного числа.

Особенности метода:

- если одновременно установлены параметры «unique» и «saveConsistency», маскирование будет происходить консистентно, а не уникально;
- в случае, если последовательность в исходном значении состоит не из 10 или 12 символов, или если строка не является числовой последовательностью, создается случайный ИНН из 12 символов.

Параметры метода:

- «saveConsistency» – отвечает за сохранение консистентности в рамках ключа консистентности;
- «consistKey» – ключ консистентности (применяется при активном параметре «saveConsistency»);
- «keyDictIfns» – код словаря ИФНС, берется из раздела «Справочники»;
- «convertEmptyInn» – отвечает за преобразование пустых значений в ИНН стандартного образца;
- «unique» – всегда заменяет исходное значение на уникальное выходное значение в рамках маскируемых данных из загруженного в Систему файла;
- «uniqueKey» – ключ уникальности (применяется при активном параметре «unique», данные с одинаковым ключом маскируются уникально).

При наборе параметров, указанных в таблице 7, значение «44570ак» может быть преобразовано в стандартный 10-значный ИНН «123451234».

Таблица 7 – Пример параметров для метода «ИНН РФ»

Название переменной	Значение
saveConsistency	неактивно
consistKey	INN_RUS
keyDictIfns	RUS_IFNS
convertEmptyInn	активно
unique	активно
uniqueKey	INN_NUMBER_DEFAULT_UNIQUE

3.9.5.4. СНИЛС РФ

Данные исходного файла заменяются на случайно сгенерированное значение в формате СНИЛС РФ, с проверкой контрольного числа. СНИЛС имеет вид «XXX-XXX-XXX YY», где «XXX-XXX-XXX» – номер, а «YY» – контрольное число.

Особенности метода:

- если одновременно установлены параметры «unique» и «saveConsistency», маскирование будет происходить консистентно, а не уникально;
- в случае, если последовательность в исходном значении состоит не из 11 символов, или если строка не является числовой последовательностью, создается случайный СНИЛС из 11 символов.

Параметры метода:

- «convertEmptySnils» – определяет, будут ли конвертироваться пустые значения;
- «saveSeparators» (только для строковой версии метода) – определяет, будет ли сохранен разделитель от исходного значения;
- «firstSeparator» (только для строковой версии метода) – первый тип разделителя, который может присутствовать в последовательности;
- «secondSeparator» (только для строковой версии метода) – второй тип разделителя, который может присутствовать в последовательности;
- «saveConsistency» – определяет, будет ли сохранена консистентность в рамках ключа консистентности;
- «consistKey» – ключ консистентности (применяется при активном параметре «saveConsistency»);
- «unique» – всегда заменяет исходное значение на уникальное выходное значение в рамках маскируемых данных из загруженного в Систему файла;
- «uniqueKey» – ключ уникальности (применяется при активном параметре «unique», данные с одинаковым ключом маскируются уникально).

При наборе параметров, указанных в таблице 8, СНИЛС «111-222-333 00» может быть преобразован в «324-432-368 56».

Таблица 8 – Пример параметров для метода «СНИЛС РФ»

Название переменной	Значение
saveConsistency	неактивно
consistKey	SNILS_RUS
convertEmptySnils	неактивно
saveSeparators	активно
firstSeparator	DEFAULT (или не заполнен)
secondSeparator	DEFAULT (или не заполнен)
unique	активно
uniqueKey	SNILS_RUS_NUMBER_DEFAULT_UNIQUE

Если в качестве разделителей в исходном значении вместо «-» и пробела используются другие служебные символы, их необходимо указать в параметрах «firstSeparator» и «secondSeparator». Метод не предусматривает работу с более чем двумя видами сепараторов.

При наборе параметров, указанных в таблице 9, значение СНИЛС «111#222#333 00» может быть преобразовано в «354#368#567 91».

Таблица 9 – Пример использования параметра «firstSeparator» в методе «СНИЛС РФ»

Название переменной	Значение
saveConsistency	неактивно
consistKey	SNILS_RUS
convertEmptySnils	неактивно
saveSeparators	активно
firstSeparator	#
secondSeparator	DEFAULT (или не заполнен)
unique	активно
uniqueKey	SNILS_RUS_NUMBER_DEFAULT_UNIQUE

При наборе параметров, указанных в таблице 10, значение СНИЛС «111#222&333 00» может быть преобразовано в «354#368&56791».

Таблица 10 – Пример использования параметров «firstSeparator» и «secondSeparator» в методе «СНИЛС РФ»

Название переменной	Значение
saveConsistency	неактивно
consistKey	SNILS_RUS
convertEmptySnils	неактивно
saveSeparators	активно
firstSeparator	#
secondSeparator	&
unique	активно
uniqueKey	SNILS_RUS_NUMBER_DEFAULT_UNIQUE

3.9.5.5. Случайная замена

Метод маскирования, позволяющий заменять данные исходного файла на случайно сгенерированное значение. Новое значение генерируется таким образом, что число заменяется на число, а буква заменяется на букву, при этом спецсимволы остаются без изменений. Работает только со строковыми значениями.

Особенности метода:

1) Если одновременно установлены параметры «unique» и «saveConsistency», маскирование будет происходить консистентно, а не уникально.
2) Замена символов происходит по следующим правилам:
   – заглавная русская буква – заменяется на случайную заглавную русскую букву;
   – прописная русская буква – заменяется на случайную прописную русскую букву;
   – заглавная английская буква – заменяется на случайную заглавную английскую букву;
   – прописная английская буква – заменяется на случайную прописную английскую букву;
   – цифра – заменяется на случайную цифру;
   – иные символы – остаются неизменными.
3) Исходное значение маскируется только при условии «endMasking - startMasking ≥ 1».
4) Отсчет индексов начала и конца маскирования начинается с «0».

Параметры метода «Случайная замена»:

- «saveConsistency» – определяет, будет ли сохранена консистентность в рамках ключа консистентности;
- «consistKey» – ключ консистентности (применяется при активном параметре «saveConsistency»);
- «convertEmptyValue» – определяет маскирование пустых значений;
- «startMasking» – индекс начала фрагмента маскирования (например, при указании параметра равным «4» маскирование будет производиться, начиная с пятой цифры исходного значения);
- «endMasking» – индекс окончания фрагмента маскирования (например, при указании параметра равным «4» маскирование будет производиться до пятой цифры исходного значения);
- «unique» – всегда заменяет исходное значение на уникальное выходное значение в рамках маскируемых данных из загруженного в Систему файла;
- «uniqueKey» – ключ уникальности (применяется при активном параметре «unique», данные с одинаковым ключом маскируются уникально).

При наборе параметров, указанных в таблице 11, исходное значение «123_a4b5» может быть преобразовано в «685_e2n1».

Таблица 11 – Пример параметров для метода «Случайная замена»

Название переменной	Значение
saveConsistency	неактивно
consistKey	randomChangeMaskingConsistKey
convertEmptyValue	неактивно
startMasking	0
endMasking	0
unique	активно
uniqueKey	RANDOM_CHANGE_STRING_DEFAULT_UNIQUE

Ниже приведены проверки в рамках валидации метода маскирования «Случайная замена».

1) Проверка 1

   Значения «startMasking» ≥ 0, «endMasking» ≥ 0, «endMasking» > «startMasking».

2) Проверка 2

   Диапазон значений между «endMasking» и «startMasking» должен быть достаточным, чтобы выдержать консистентность. В данном случае валидация проверяет комбинацию значений указанных параметров правила маскирования перед запуском самого маскирования. Пользователь не сможет осуществить маскирование с консистентностью, если количество уникальных записей в загруженном в Систему файле больше, чем мощность выборки.

3) Проверка 3

   Параметр «convertEmptyValue» не должен быть установлен одновременно вместе с параметром «saveConsistency». Консистентность не может маскировать одинаковые значения, в том числе «null», в разные значения. Поэтому комбинация данных параметров не имеет практического смысла.

3.10. Правила маскирования

3.10.1. Общая информация

Правила маскирования определяют метод маскирования, применяемый к данным из загруженного в Систему файла, и содержат в себе конкретные значения параметров метода, которые будут использоваться при маскировании.

Список правил маскирования содержится в разделе Системы «Приложение» → «Правила маскирования». Правила в списке сгруппированы по методам, на которых они основаны.

Для просмотра правила маскирования необходимо нажать на его наименование в списке. Для изменения правила маскирования необходимо выбрать его из списка и нажать кнопку «Изменить», внести изменения и сохранить их. Для удаления правила маскирования необходимо выбрать его из списка, нажать кнопку «Удалить» и в появившемся окне подтвердить удаление.

Рисунок 49 – Подраздел «Правила маскирования»

Для одного метода маскирования может быть создано несколько правил. Правила маскирования определяют набор параметров метода, с которыми может работать пользователь. Например, «REPLACE_BY_DICTIONARY» (замена по справочнику) – это метод маскирования, на котором могут быть основаны правила маскирования «Замена по справочнику городов РФ» и «Замена по справочнику компаний РФ».

В Системе для каждого системного метода маскирования заранее созданы правила с наиболее вероятными для использования значениями параметров. Сами правила не делятся на системные и пользовательские – они могут создаваться как для системных, так и для пользовательских методов.

В правиле маскирования для каждого параметра устанавливается значение по умолчанию – оно будет использовано, если пользователь Системы не переопределит его самостоятельно.

3.10.2. Создание правила маскирования

Для создания правила маскирования используется кнопка «Создать» в разделе Системы «Приложение» → «Правила маскирования».

На странице создания правила требуется заполнить обязательные поля и из списка «Метод маскирования» выбрать метод, на котором будет основано правило. Если выбранный метод обладает набором параметров, они отобразятся в разделе «Параметры скрипта». Необходимо установить значения параметров в соответствующих полях и чекбоксах.

Для просмотра скрипта правила маскирования используется кнопка «</> Просмотр скрипта» – скрипт отобразится в отдельном окне.

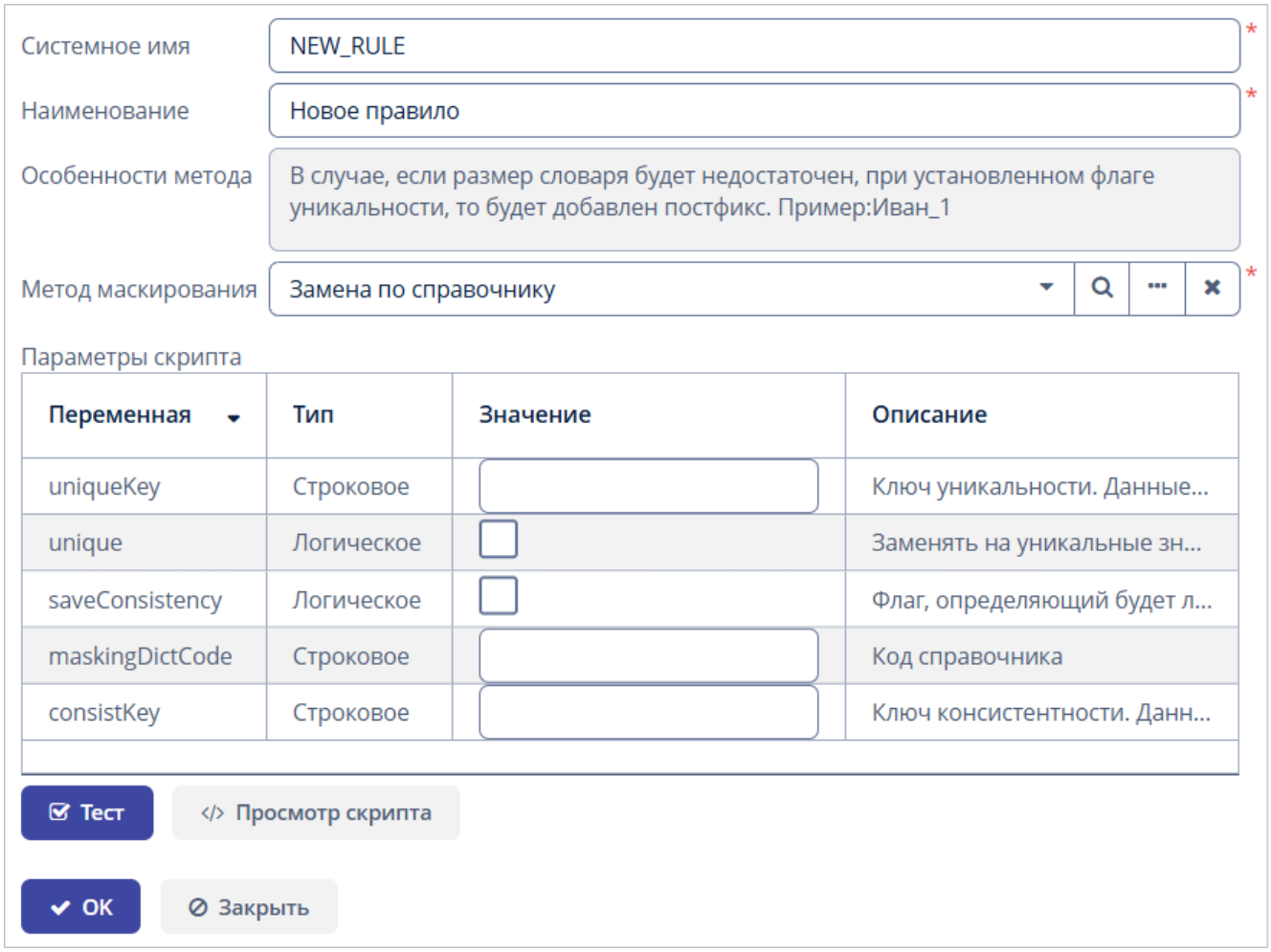

Рисунок 50 – Страница создания правила маскирования (пример)

Для перехода к тестированию правила маскирования используется кнопка «Тест» в карточке правила. Требуется ввести оригинальное значение в поле «Входное значение», выбрать тип данных и нажать кнопку «Тест». Полученное в результате тестирования значение появится во всплывающем сообщении. Для возврата к параметрам правила маскирования необходимо нажать на сообщение, затем – кнопку «Закрыть».

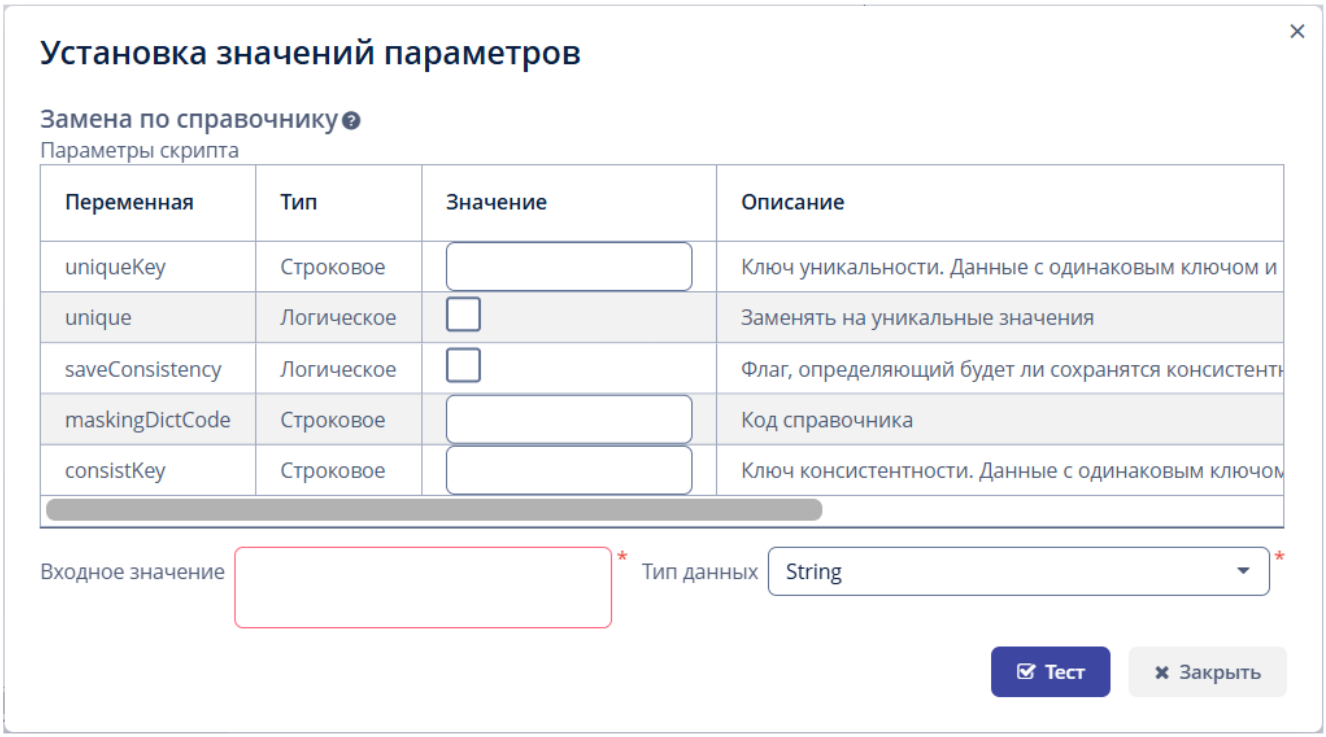

Рисунок 51 – Окно тестирования правила маскирования

Для сохранения правила маскирования используется кнопка «ОК» на странице создания правила.

4. АДМИНИСТРИРОВАНИЕ

4.1. Пользователи

4.1.1. Общая информация

При входе пользователя в Систему с локальной учетной записью корректность введенных логина и пароля проверяется самой Системой. Для учетной записи пользователя можно сбросить или сменить пароль, сбросить токен «Запомнить меня», а также деактивировать учетную запись.

Список пользователей содержится в разделе Системы «Приложение» → «Пользователи». В верхней части страницы расположен фильтр для поиска пользователей.

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

Для удаления учетной записи пользователя необходимо выбрать ее из списка и нажать кнопку «Удалить». В окне подтверждения удаления нажать кнопку «Удалить».

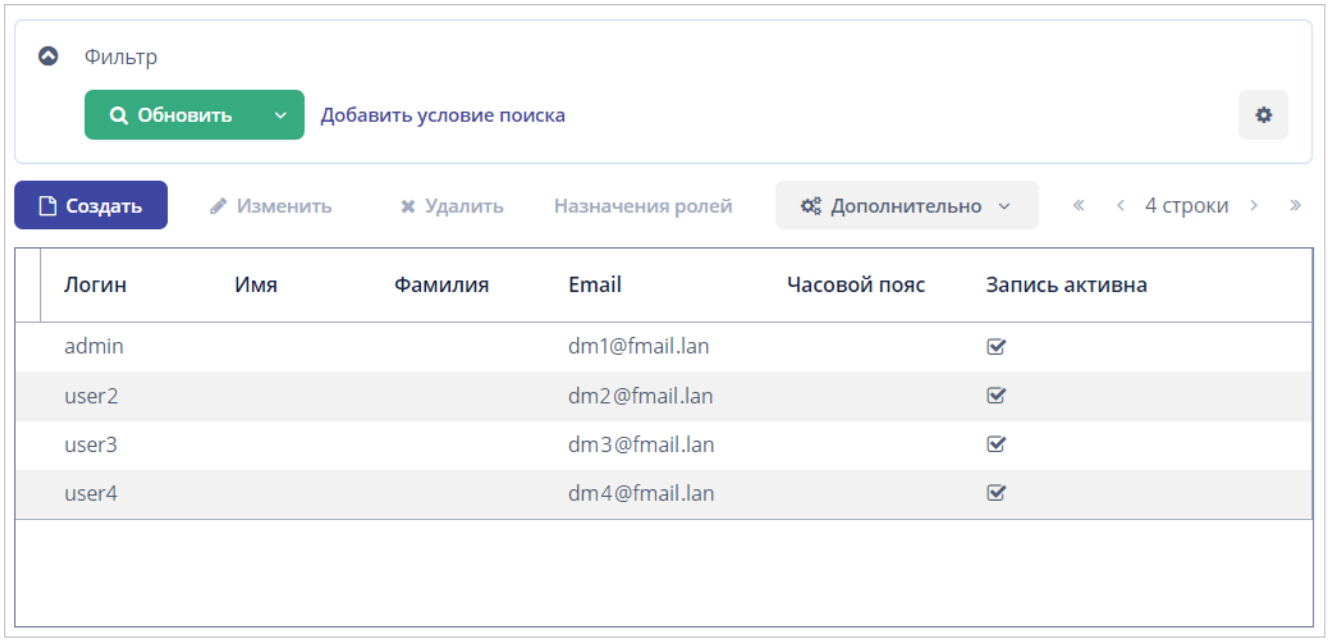

Рисунок 52 – Подраздел «Пользователи»

4.1.2. Создание локального пользователя

Создавать пользователя в Системе может только администратор Системы.

Для создания пользователя используется кнопка «Создать» в разделе Системы «Приложение» → «Пользователи».

На странице создания пользователя необходимо заполнить поля:

- «Логин» – логин пользователя, используемый для входа в Систему;
- «Пароль» – пароль для входа в Систему;
- «Подтвердить пароль» – повторный ввод пароля для входа в Систему;
- «Имя» – имя пользователя в Системе;
- «Фамилия» – фамилия пользователя в Системе;
- «Email» – электронная почта пользователя;
- «Часовой пояс» – часовой пояс пользователя;
- «Запись активна» – признак, активирующий или отключающий учетную запись пользователя в Системе (если учетная запись неактивна, вход в Систему будет невозможен).

Для сохранения используется кнопка «ОК».

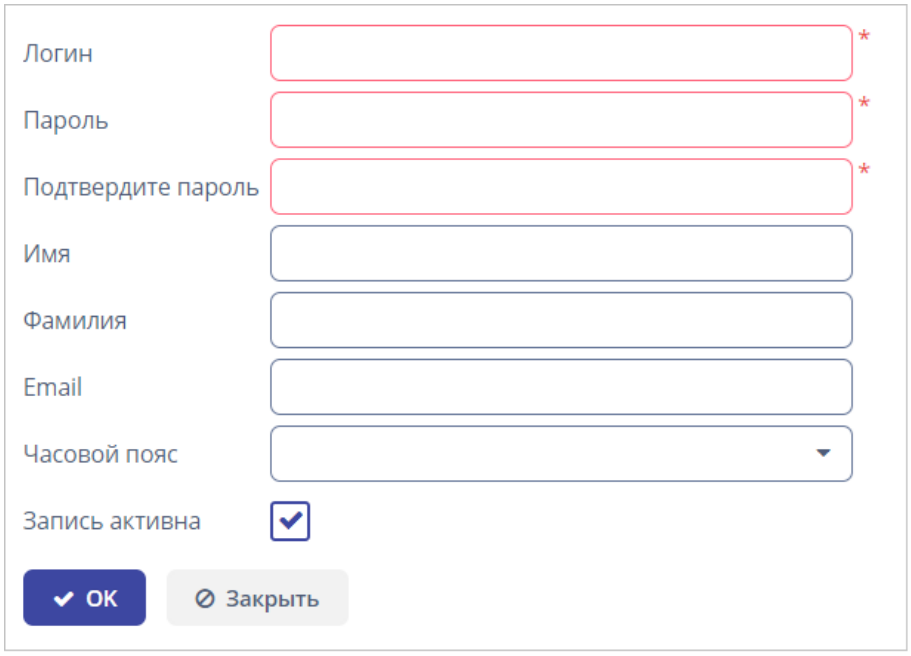

Рисунок 53 – Страница создания пользователя

По умолчанию после создания учетной записи пользователя в Системе ему не назначена никакая роль, поэтому при попытке авторизации такого пользователя Система сообщит об отсутствии доступа. Необходимо назначить пользователю роль, после чего работа в Системе станет для него возможной.

4.1.3. Редактирование локального пользователя

Для редактирования локального пользователя необходимо выбрать его из списка в разделе «Приложение» → «Пользователи» и нажать кнопку «Изменить» над списком.

Для изменения доступно меньше параметров, чем при создании пользователя. После внесения изменений необходимо нажать кнопку «ОК».

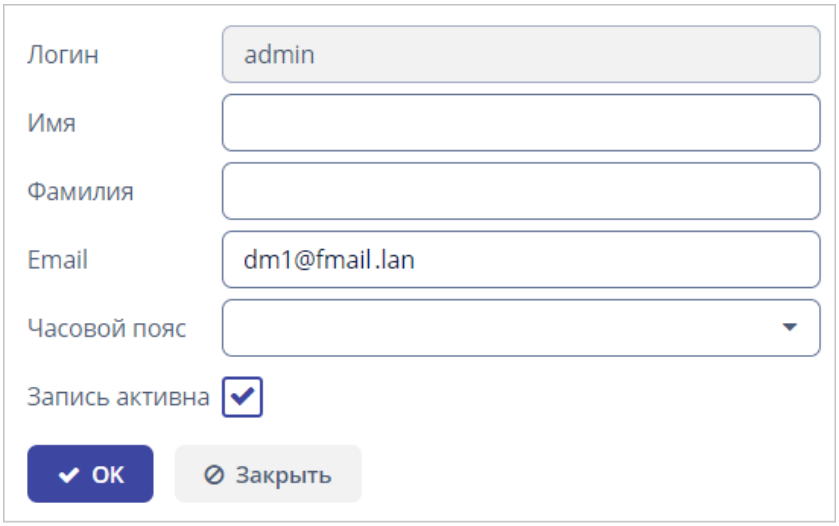

Рисунок 54 – Страница изменения параметров локального пользователя

4.2. Ролевая модель управления доступом

4.2.1. Общая информация

В Системе используется преднастроенная ролевая модель управления доступом. В Системе могут быть созданы ресурсные роли (ограничивают права доступа к разделам Системы, экранам, атрибутам и т.д.) и роли уровня строк (row-level роли) (ограничивают доступ к отдельным записям в разделах Системы).

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

Если ресурсная роль не назначена пользователю, у него не будет прав на ресурсы, к которым дает доступ эта роль. Если роль уровня строк не назначена пользователю, у него будет доступ ко всем записям.

Список ресурсных ролей содержится в разделе Системы «Администрирование» → «Ресурсные роли». В верхней части страницы расположен фильтр для поиска ролей.

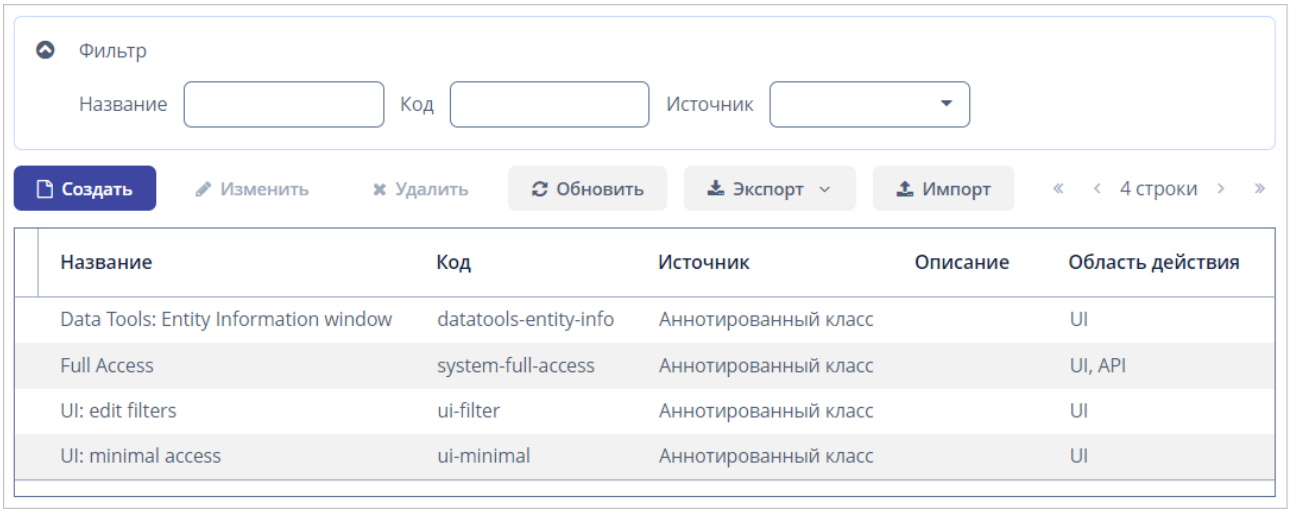

Рисунок 55 – Подраздел «Ресурсные роли» (пример)

Список ролей уровня строк содержится в разделе Системы «Администрирование» → «Row-level роли». В верхней части страницы расположен фильтр для поиска ролей.

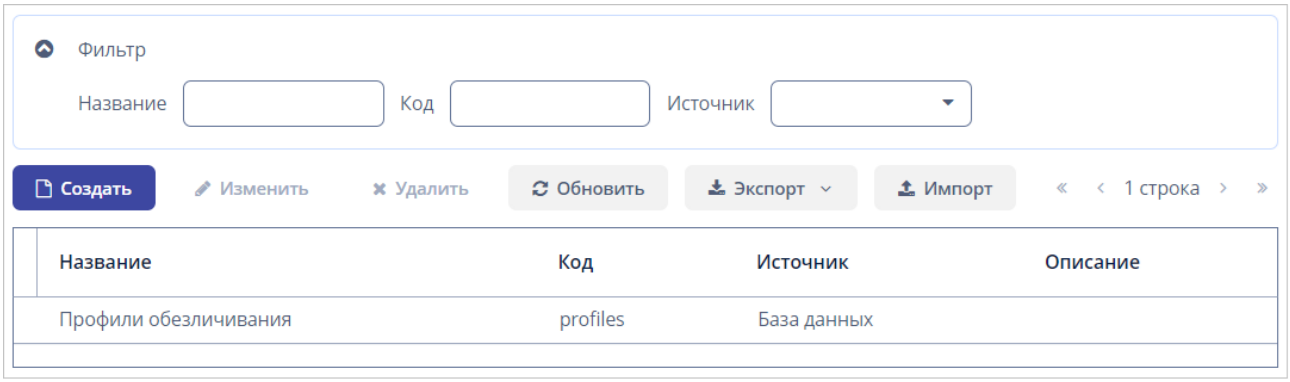

Рисунок 56 – Подраздел «Row-level роли» (пример)

4.2.2. Создание ресурсной роли

Для создания ресурсной роли используется кнопка «Создать» в разделе Системы «Администрирование» → «Ресурсные роли».

На странице создания ресурсной роли необходимо заполнить поля:

– «Название» – название роли;
– «Код» – системное название роли для ее идентификации в Системе;
– «Описание» – краткое описание роли;
– «Область действия» – область, на которую будет распространяться действие роли (интерфейс или API).

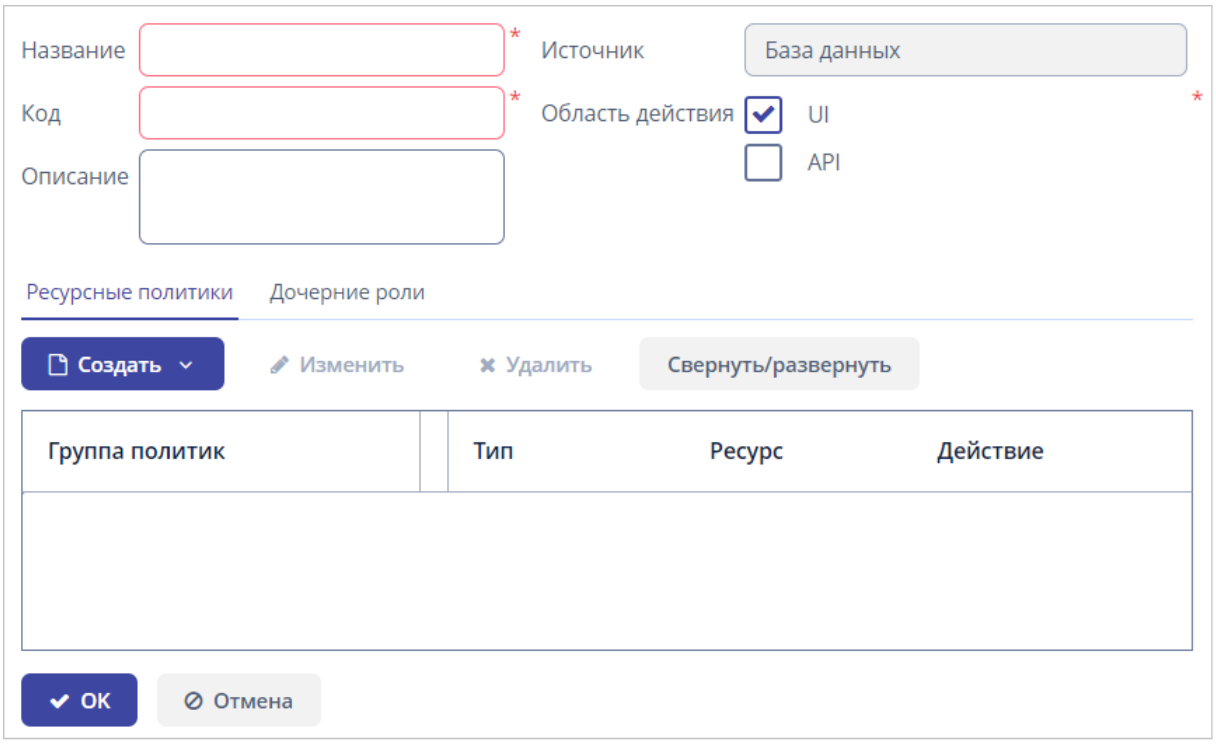

Рисунок 57 – Страница создания ресурсной роли

Ресурсные роли содержат в себе политики, описывающие ресурсы с разрешенными типами доступа к ним. Ресурсная роль может включать в себя любое количество политик. Для добавления политики необходимо раскрыть меню «Создать» на вкладке «Ресурсные политики» и выбрать один из следующих пунктов.

1) «Политика меню»
   Определяет пункт панели навигации (меню) Системы, который будет доступен пользователю для просмотра. При выборе названия пункта меню из комбинированного списка «Ресурс» поля «Группа политик» и «Экран» заполняются автоматически. Чтобы пункт меню отображался в навигационной панели, необходимо установить флажок «Выдать права на пункт меню». Для сохранения нажать кнопку «ОК».

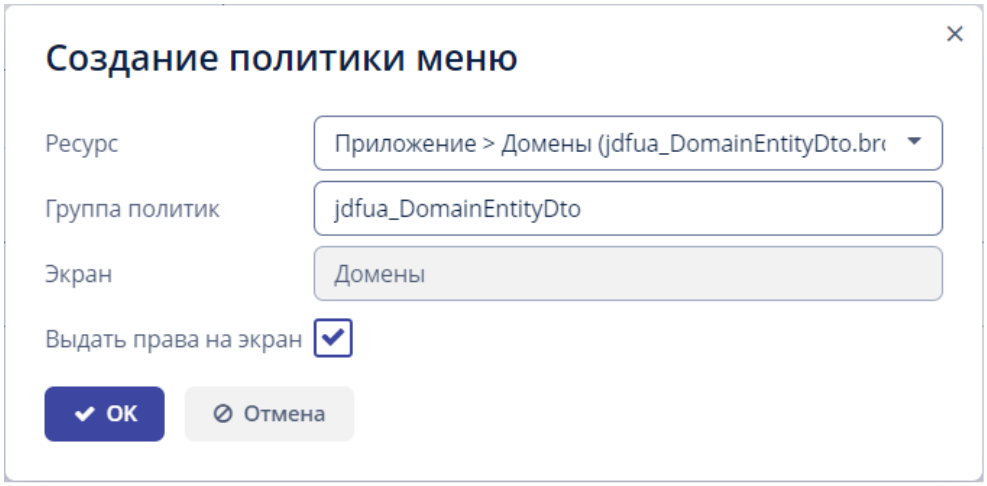

Рисунок 58 – Создание политики меню (пример)

2) «Политика экранов»
Определяет экран Системы, который будет доступен пользователю для просмотра. При выборе названия экрана из комбинированного списка «Ресурс» поля «Группа политик» и «Пункт меню» заполняются автоматически. Чтобы экран стал доступен для просмотра, необходимо установить флажок «Выдать права на экран». Для сохранения нажать кнопку «ОК».

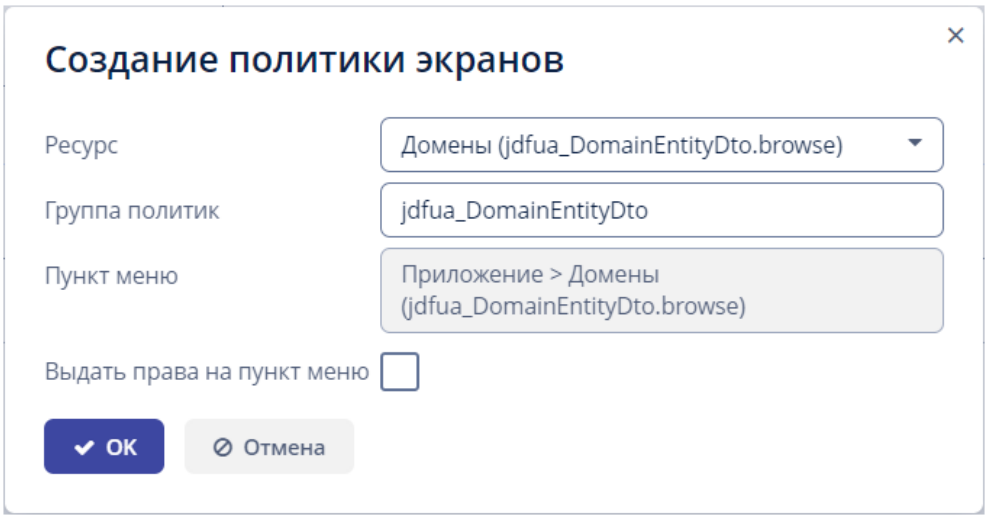

Рисунок 59 – Создание политики экранов (пример)

3) «Политика сущностей»
Определяет набор действий (создание, чтение, изменение, удаление) над сущностью (объектом) Системы, доступных пользователю. При выборе объекта из комбинированного списка «Сущность» поле «Группа политик» заполняется автоматически.
В блоке «Действия» необходимо установить флажки напротив действий, которые будут доступны пользователю над выбранным объектом. При установке флажка «Все действия» пользователю будут доступны все виды действий над выбранным объектом.

Для сохранения нажать кнопку «ОК».

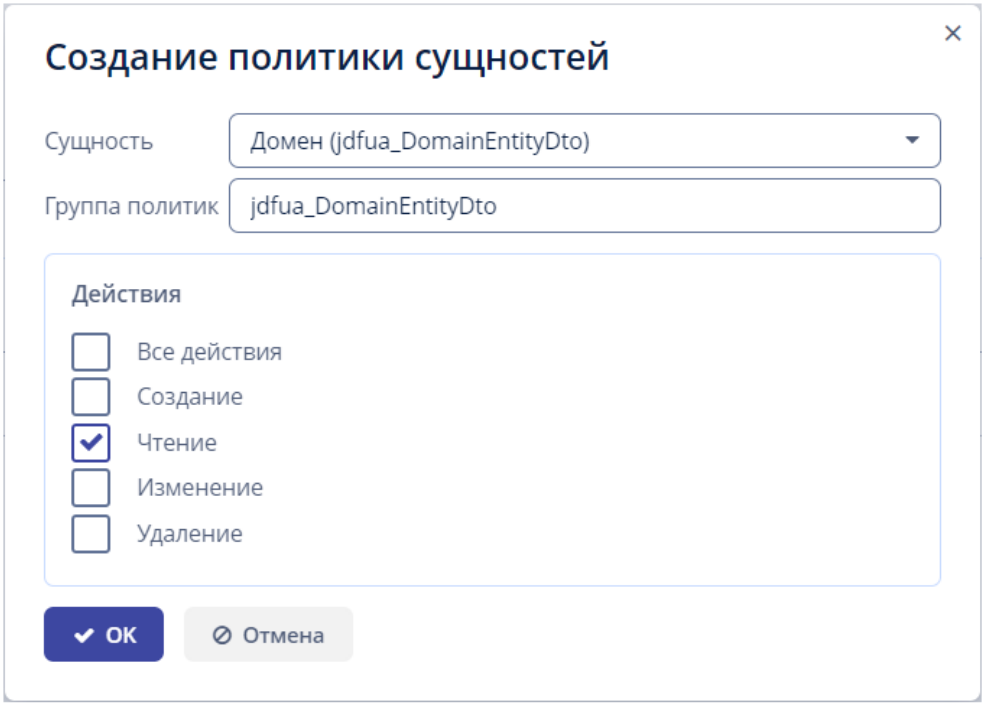

Рисунок 60 – Создание политики сущностей (пример)

4) «Политика атрибутов сущностей»
Определяет, какие атрибуты сущности (объекта) Системы пользователь сможет просматривать и изменять.
При выборе объекта из комбинированного списка «Сущность» поле «Группа политик» заполняется автоматически, а в таблице «Атрибуты» отображаются все атрибуты выбранного объекта.
В таблице «Атрибуты» необходимо установить флажки в столбцах «Просмотр» и/или «Изменение» напротив атрибутов, которые будут доступны пользователю для просмотра и/или изменения соответственно. При установке флажка «Все атрибуты» пользователю будет доступен просмотр/изменение всех атрибутов выбранного объекта.
Для сохранения нажать кнопку «ОК».

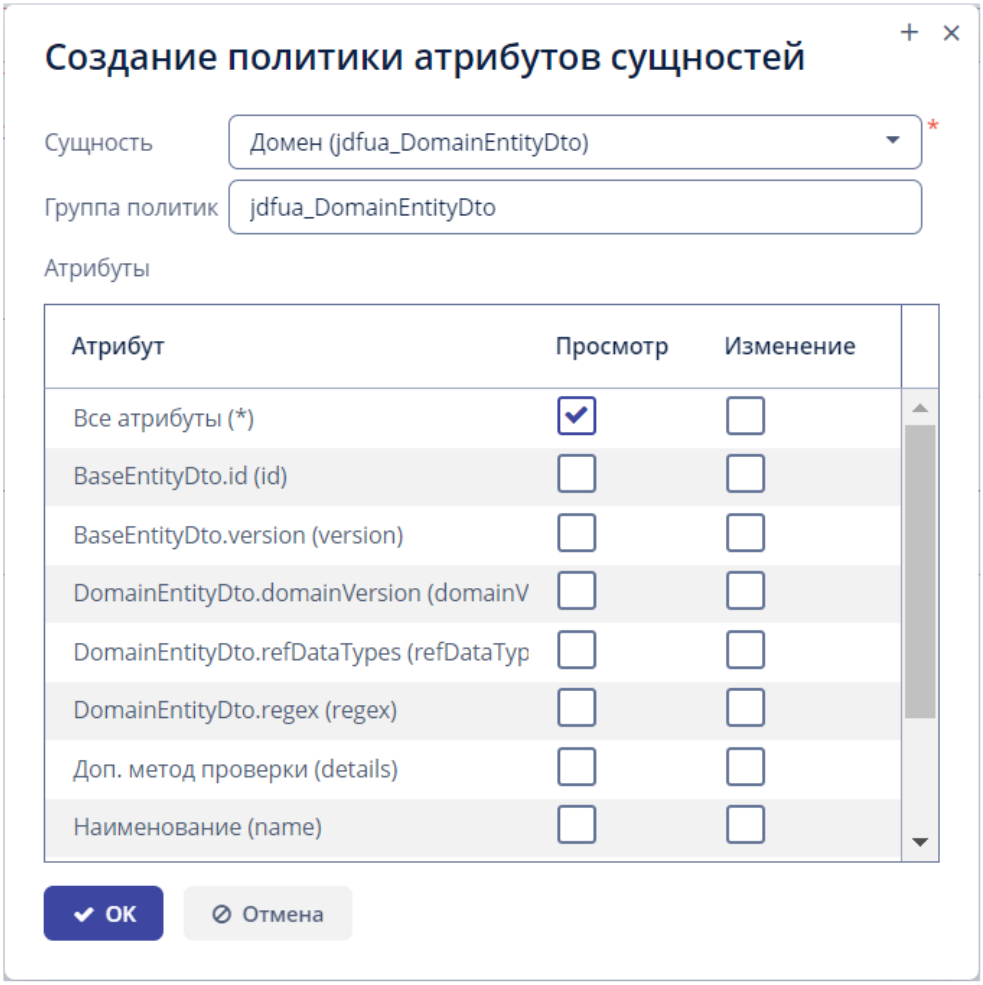

Рисунок 61 – Создание политики атрибутов сущностей (пример)

5) «Специальная политика»

Используется для разграничения доступа пользователя к различным функциям Системы, например, к авторизации в Системе.

Необходимо выбрать функцию из комбинированного списка «Ресурс» и определить группу политик, к которой будет отнесена данная специальная политика. Для сохранения нажать кнопку «ОК».

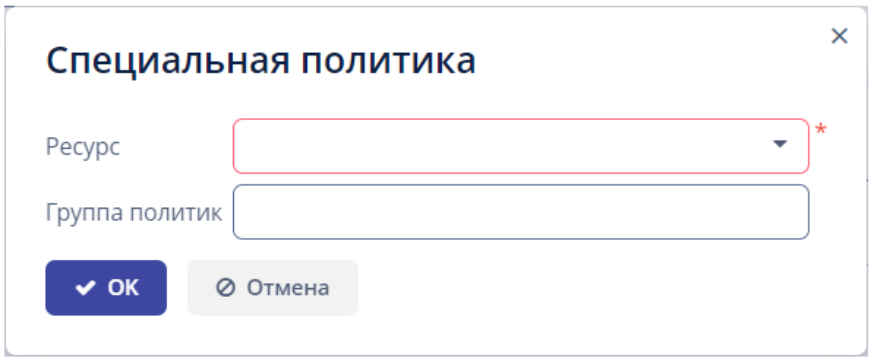

Рисунок 62 – Создание специальной политики

На вкладке «Дочерние роли» для создаваемой роли могут быть добавлены уже существующие в Системе ресурсные роли, от которых будут наследоваться их права. Необходимо нажать кнопку «Добавить», в открывшейся форме выбрать одну или несколько ролей и нажать кнопку «Выбрать».

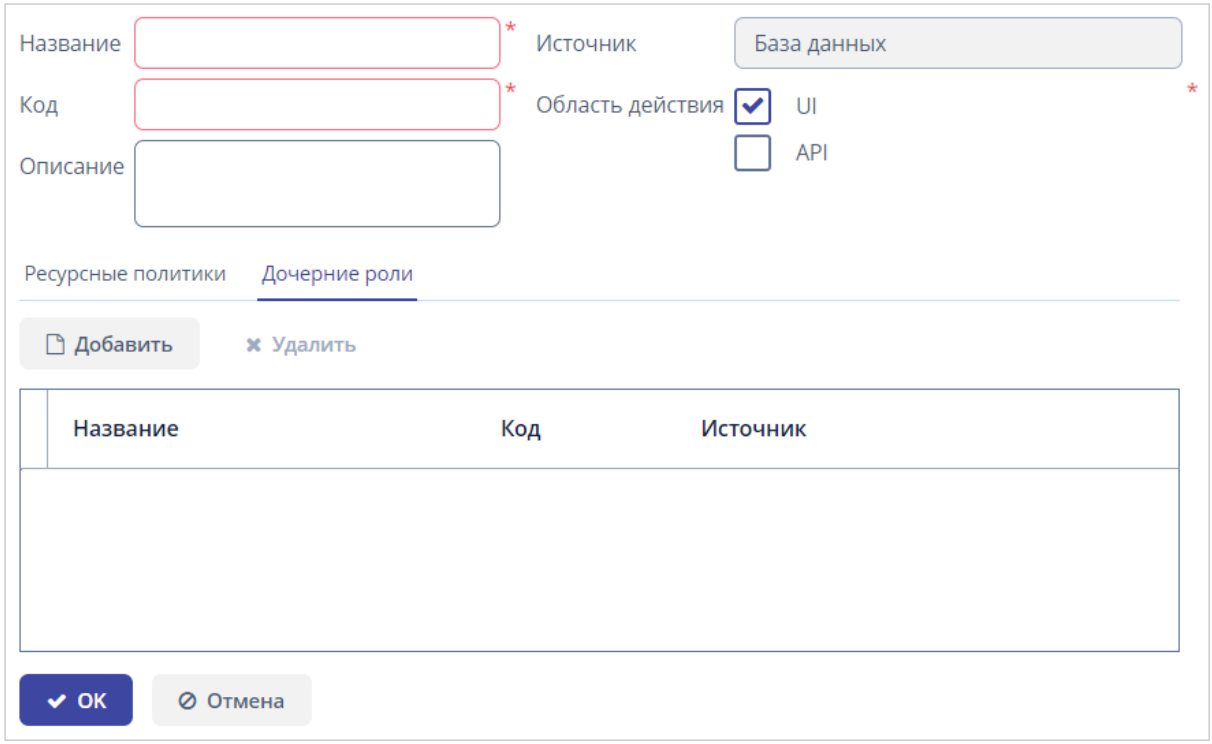

Рисунок 63 – Страница создания ресурсной роли: вкладка «Дочерние роли»

Для сохранения ресурсной роли используется кнопка «ОК» на странице ее создания. После сохранения роли она становится доступной для назначения пользователям.

4.2.3. Создание роли уровня строк

Для создания роли уровня строк используется кнопка «Создать» в разделе Системы «Администрирование» → «Row-level роли».

На странице создания роли уровня строк необходимо заполнить поля:

– «Название» – название роли;
– «Код» – системное название роли для ее идентификации в Системе;
– «Описание» – краткое описание роли.

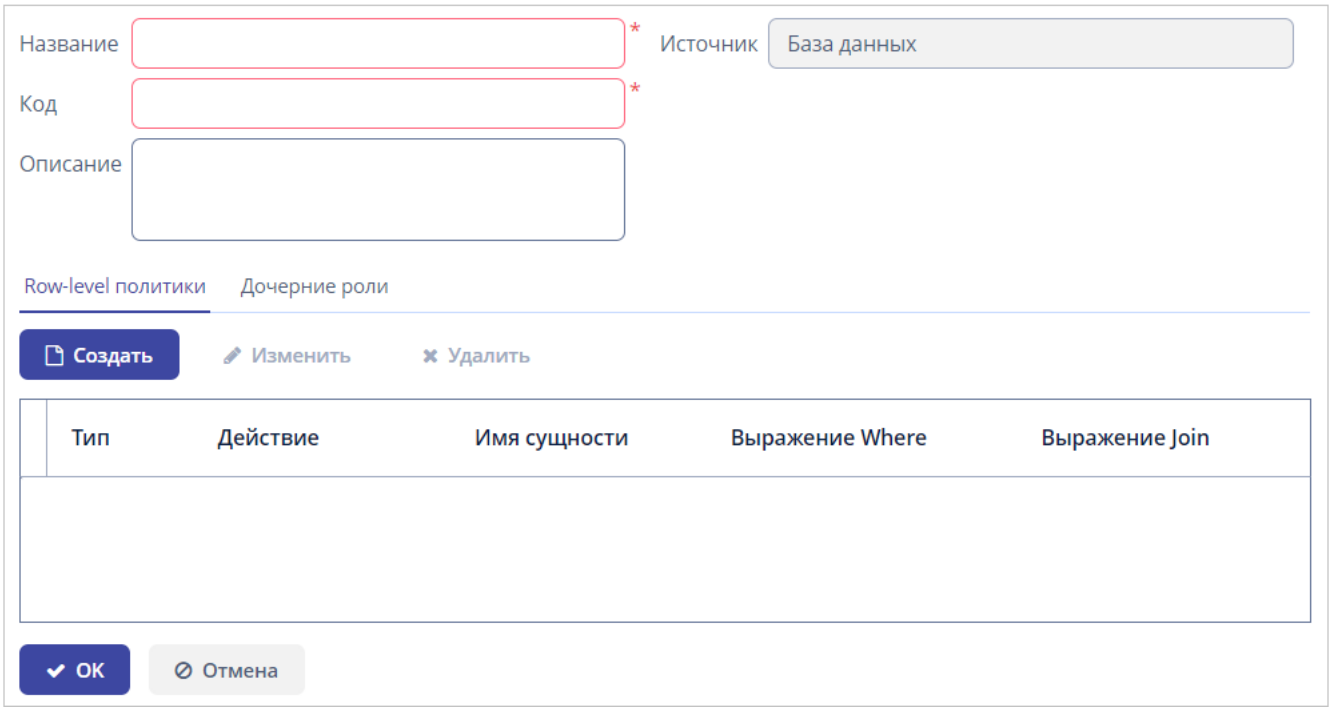

Рисунок 64 – Страница создания роли уровня строк

Роли уровня строк содержат в себе row-level политики, описывающие доступ к сущностям (объектам) Системы. Роль уровня строк может включать в себя любое количество политик. Для добавления политики необходимо нажать кнопку «Создать» на вкладке «Row-level политики».

Политика для роли уровня строк может быть двух типов.

1) «JPQL»
   Указывает выражения Where и/или Join, которые будут использоваться при загрузке сущности, преобразует оператор JPQL и отфильтровывает запрещенные экземпляры сущности на уровне БД.
2) «Predicate»
   Определяет предикат, который проверяется при выполнении различных действий с сущностью. Если предикат возвращает значение «true», данное действие разрешается для данного экземпляра сущности.

Предикатные политики можно определить для следующих действий: создание (CREATE), чтение (READ), изменение (UPDATE), удаление (DELETE).

Предикат READ проверяется при загрузке сущности из БД для корневой сущности и всех вложенных коллекций вплоть до графа загруженных объектов. Если сущность может быть загружена как коллекция в графе объектов другой сущности, нужно определить для нее как JPQL, так и предикатные политики.

Предикаты CREATE, UPDATE, DELETE проверяются перед созданием, обновлением или удалением экземпляра сущности из БД.

В зависимости от выбранного типа политики, форма ее создания будет отличаться и может содержать следующие поля:

– «Имя сущности» – сущность, для которой необходимо разграничить доступ;
– «Тип» – тип политики;
– «Действие» – вид действия, применяемый к сущности (доступно для редактирования только для типа политики «Predicate»);
– «Выражение Join» – выражение JPQL, которое будет добавлено в секцию «from» в запросе к источнику данных;
– «Выражение Where» – выражение JPQL, которое будет добавлено в условие «where» в запросе к источнику данных;
– «Скрипт» – Groovy скрипт, выполняющийся для каждого объекта проверяемого графа объектов (если объект не соответствует условиям, он отфильтровывается из графа объектов).

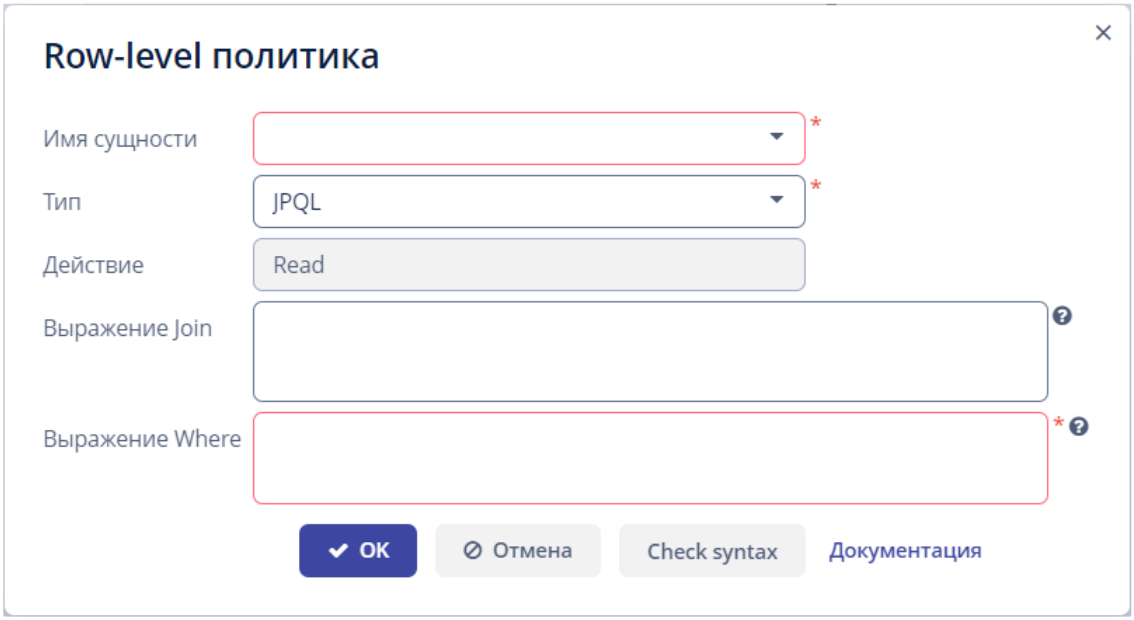

Рисунок 65 – Создание row-level политики с типом «JPQL»

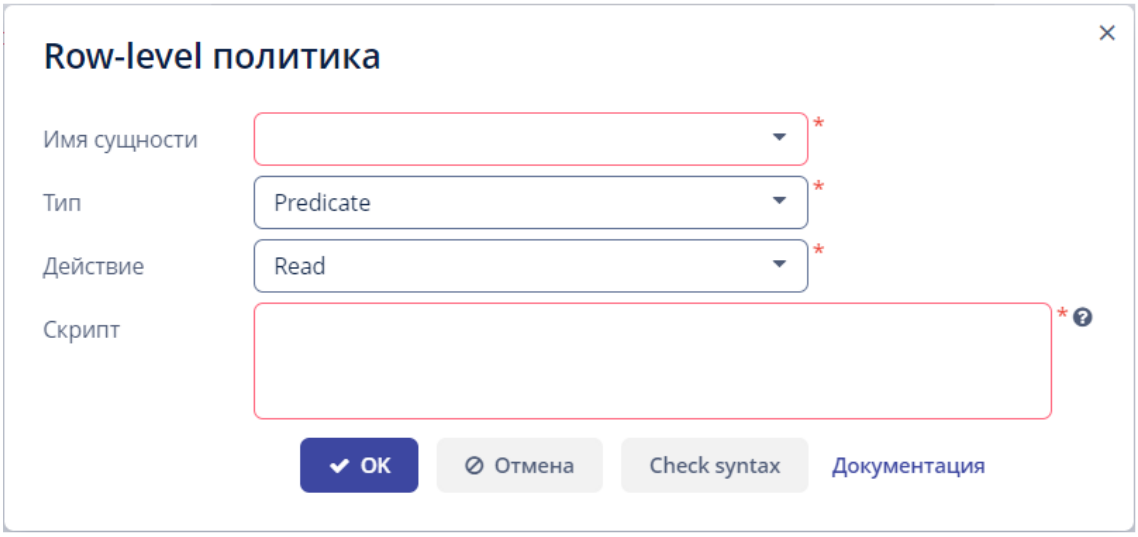

Рисунок 66 – Создание row-level политики с типом «Predicate»

На вкладке «Дочерние роли» для создаваемой роли могут быть добавлены уже существующие в Системе роли уровня строк, от которых будут наследоваться их права. Необходимо нажать кнопку «Добавить», в открывшейся форме выбрать одну или несколько ролей и нажать кнопку «Выбрать».

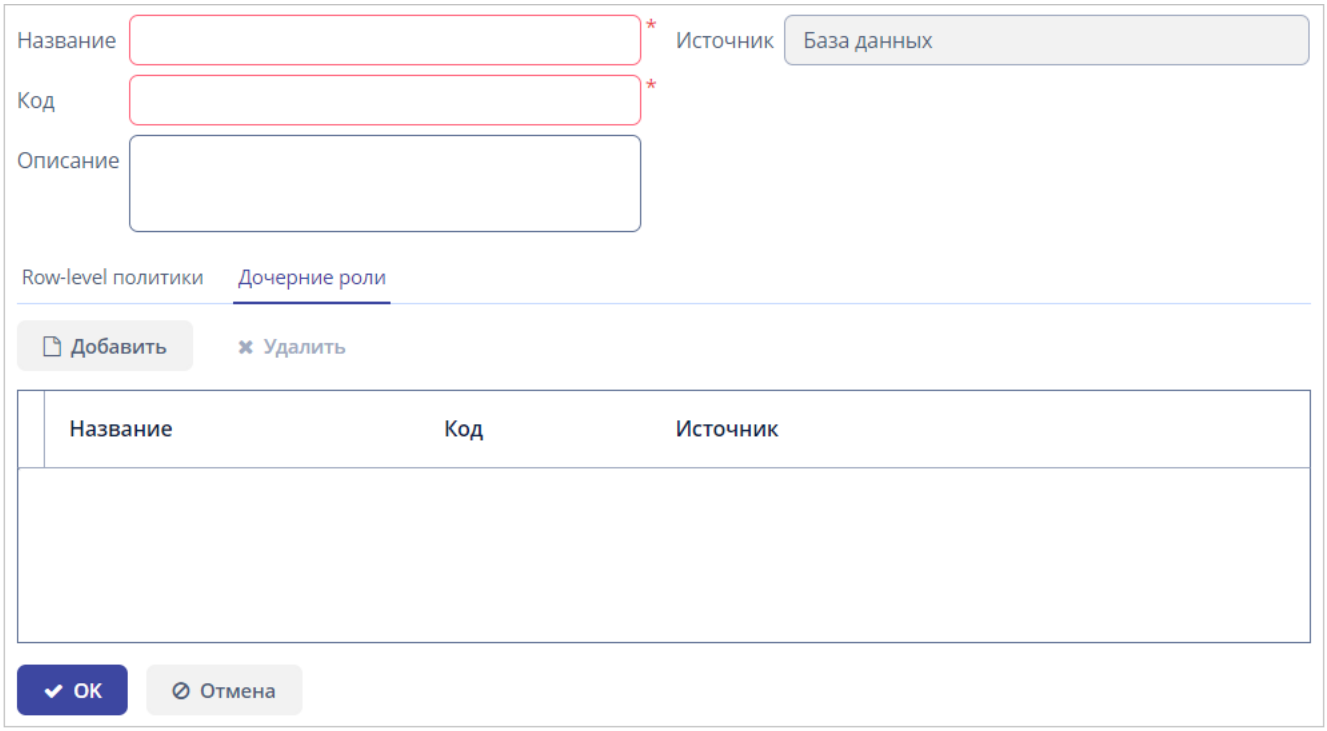

Рисунок 67 – Страница создания роли уровня строк: вкладка «Дочерние роли»

Для сохранения роли уровня строк используется кнопка «ОК» на странице ее создания. После сохранения роли она становится доступной для назначения пользователям.

4.2.4. Назначение ролей пользователям

Для назначения пользователю роли через интерфейс Системы необходимо перейти в раздел «Приложение» → «Пользователи», выбрать пользователя из списка и нажать кнопку «Назначения ролей» над списком.

Пользователю может быть назначено любое количество ролей.

На открывшейся странице необходимо:

– нажать кнопку «Добавить» в разделе «Ресурсные разрешения» для назначения пользователю ресурсных ролей;

– нажать кнопку «Добавить» в разделе «Row-level ограничения» для назначения пользователю row-level ролей.

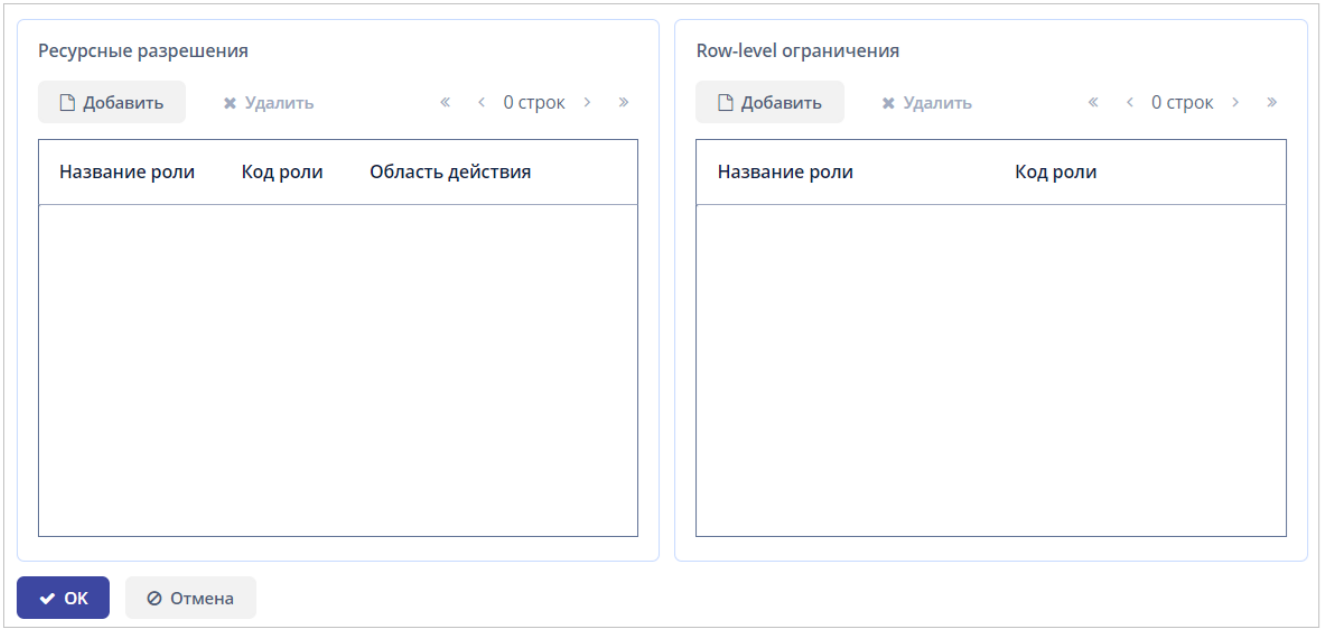

Рисунок 68 – Страница назначения ролей для пользователя

В появившемся окне требуется выбрать роль из списка и нажать кнопку «Выбрать». Для выбора нескольких ролей из списка необходимо удерживать «Ctrl». Выбранные роли отобразятся в списке назначенных пользователю ролей.

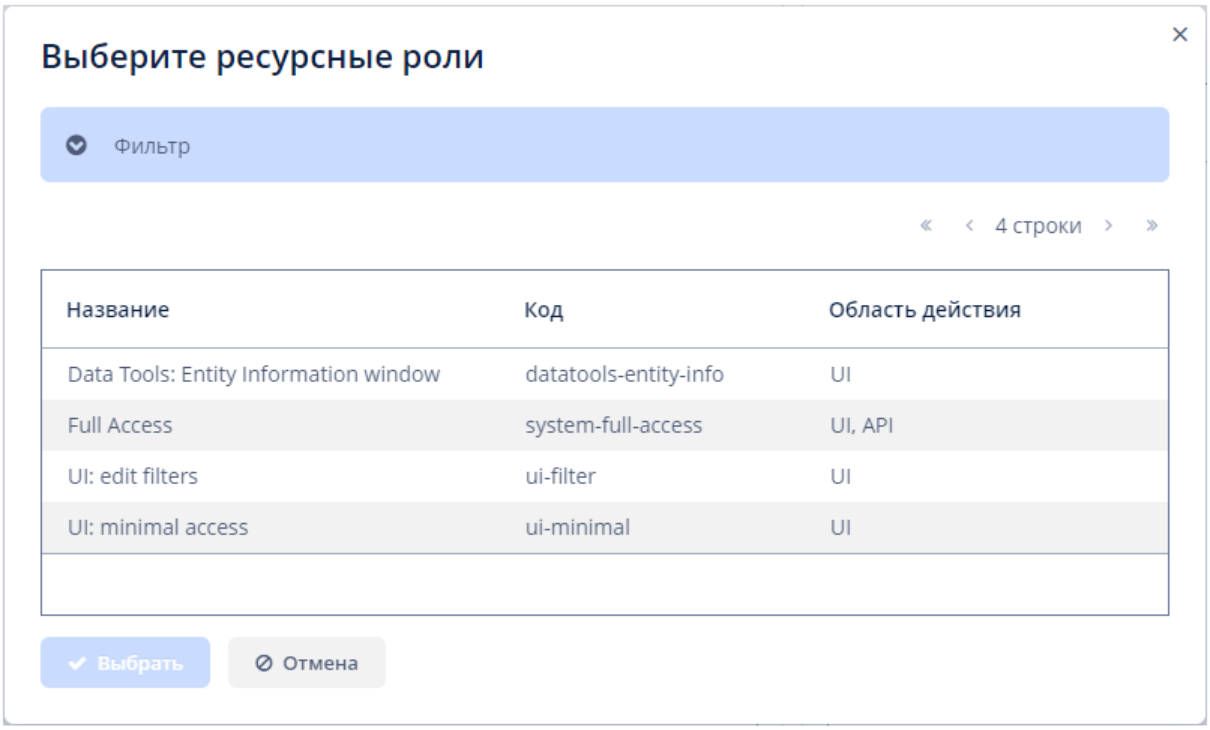

Рисунок 69 – Окно для назначения ресурсных ролей

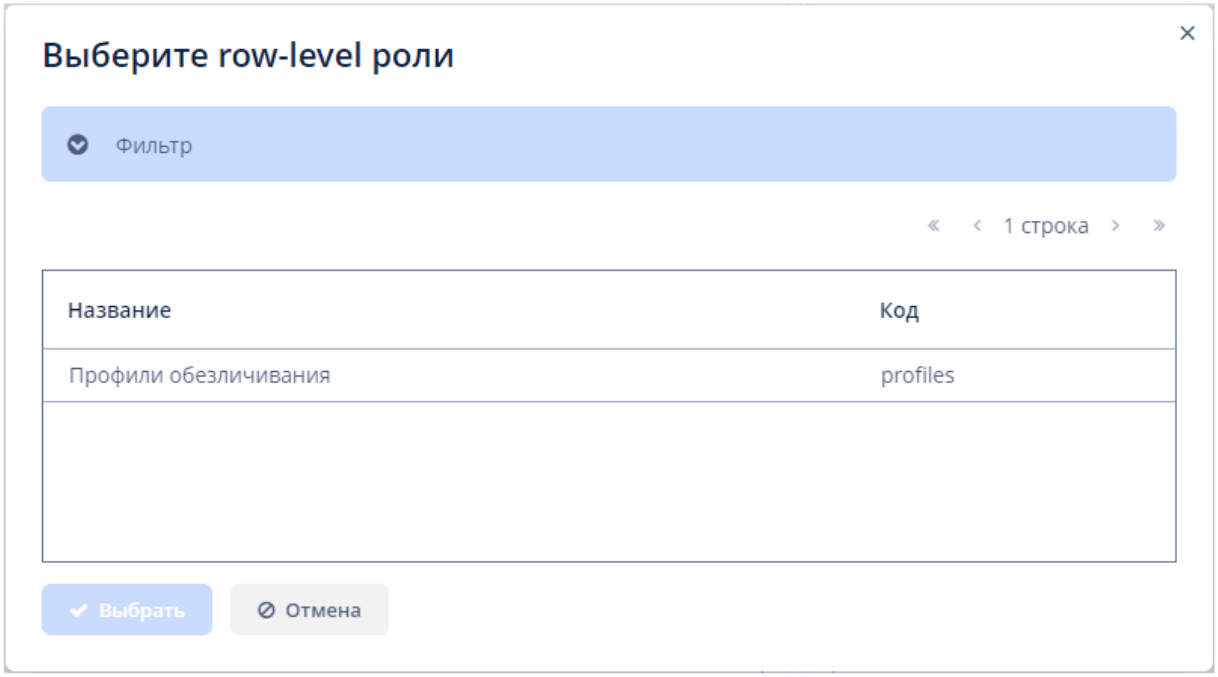

Рисунок 70 – Окно для назначения row-level роли

Для удаления назначенной роли необходимо выбрать ее из списка и нажать кнопку «Удалить». Для сохранения изменений нажать кнопку «ОК».

4.3. Логирование

Подразумевается, что развертывание Системы производилось в директорию «/opt/».

Директория, в которой расположены лог-файлы: «/opt/jdfserver/logs/».

Лог файл каждого из микросервисов Системы доступен в директории:

«/opt/jdfserver /logs/<*название_мс*>.log»

где <*название_мс*> – название микросервиса.

Доступ к журналам с логами на запись предоставляется только администратору Системы.

Примеры директорий с лог-файлами микросервисов Системы.

/opt/ jdfserver /logs/analyzer_entities.log
/opt/ jdfserver /logs/masking.log
/opt/ jdfserver /logs/fileprocessor.log.log

Настройки логирования содержатся в файлах конфигурации «application.properties» каждого микросервиса, находящихся в директории:

«/opt/jdfserver/<*название_мс*>/application.properties»

где <*название_мс*> – название микросервиса.

Для изменения настроек логирования необходимо внести изменения в значения параметров файлов конфигурации и перезапустить соответствующие им микросервисы. Перечень параметров приведен в таблице 12.

Таблица 12 – Параметры файлов конфигурации для настройки логирования

Имя настройки	Описание	Значение по умолчанию
logging.file.path	Путь к директории с логами (сам по себе ни на что не влияет, но может быть использован в качестве переменной для подстановки в другие значения)	logs
logging.file.name	Путь к файлу системных логов	/opt/jdfserver/logs/<*название_мс*>.log
logging.level.root	Уровень логирования*	INFO
logging.logback.rollingpolicy.file-name-pattern	Шаблон имени архива системных логов	/opt/jdfserver/logs/archive/<*название_мс*>-<ГГГГ-ММ-ДД>.<N>.log.gz
logging.pattern.file	Шаблон сообщения системного лога (не должен меняться)	${HOSTNAME:${spring.application.name}} %d{yyyy-MM-dd HH:mm:ss} [%thread] %-5level %logger{36} - %msg%n

где:

- <*название_мс*> – название микросервиса;
- <*N*> – номер, присваивается автоматически по возрастанию файлам одного микросервиса за одну и ту же дату;
- * – не рекомендуется устанавливать значение параметра «Уровень логирования» выше INFO, все сообщения аудита (CEF-логи) имеют данный уровень, и при повышении уровня логирования Система прекратит их запись.

В Системе осуществляется автоматическое архивирование и удаление файлов системных логов и журналов аудита (CEF-логов) для уменьшения занимаемого логами объема дискового пространства.

Архивирование производится при превышении заданного размера файла логов (по умолчанию равен 50 Мб).

Удаление файлов логов производится при:

- превышении суммарного размера всех файлов (по умолчанию равно 1 Гб, только для системных логов);
- истечении срока хранения (по умолчанию равно 30 дням для системных логов, 1096 дней – для журналов аудита).

Настройки архивирования и удаления могут быть изменены отдельно для каждого микросервиса. Для этого необходимо выполнить следующие действия:

- открыть на сервере файл «/opt/jdfserver/<*название_мс*>/application.properties»;
- изменить значения необходимых настроек (см. таблицу 13);
- сохранить файл и перезапустить соответствующий микросервис.

Таблица 13 – Параметры файлов конфигурации для настройки архивирования и удаления файлов системных логов и журналов аудита

Имя настройки	Описание	Значение по умолчанию
logging.logback.rollingpolicy.max-file-size	Максимальный размер файла системных логов до создания нового файла	1 Мб
logging.file.total-size-cap	Максимальный суммарный размер всех файлов системных логов	-

5. ГЛОССАРИЙ

Термины и сокращения	Определение
Деперсонализация данных	Процесс замены или удаления конфиденциальной информации, в результате которого устраняется связь между данными и субъектом (например, замена или удаление имен и адресов из БД)
Домен	Категория конфиденциальной информации, которая подлежит обезличиванию (например, имя, номер телефона, адрес электронной почты и т.д.)
Маскирование	Скрытие данных или части данных определенными параметрами, заложенными в правилах маскирования
Метод маскирования	Определяет логику преобразования данных при обезличивании
Политика данных	Группирует домены по принадлежности к одной и той же области информации
Правило маскирования	Определяет метод маскирования, применяемый к данным из загруженного в Систему файла, и содержит конкретные значения параметров метода, которые будут использоваться при маскировании
Профилирование	Процесс, в ходе которого определенным данным из загруженного файла в автоматическом режиме присваиваются найденные домены
Профиль	Упрощает настройку процесса обезличивания. Содержит список доменов, которые необходимо определять для чувствительных данных, и соответствующие каждому из них правила маскирования, в соответствии с которыми производится обезличивание загруженных в Систему файлов
Справочник	Каталог с данными для маскирования