ИНФОСИСТЕМЫ
ДЖЕТ

JET DETECTIVE

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

2022

АННОТАЦИЯ

В руководстве пользователя приведены сведения о назначении и функциональных возможностях программной платформы Jet Detective, а также описаны операции, которые выполняют пользователи при работе с платформой и её настройке.

СОДЕРЖАНИЕ

1 Введение 7

1.1 Область применения 7
1.2 Краткое описание возможностей 7
1.3 Уровень подготовки пользователей 8

2 Назначение Jet Detective 9

3 Структура Jet Detective 10

3.1 Перечень функциональных модулей 10
3.2 Модуль Фабрика данных 10
3.3 Модуль Анализ событий 11
3.4 Модуль Расследование 11
3.5 Модуль Документооборот 12
3.6 Модуль Списки 12
3.7 Модуль Агрегаты 12
3.8 Модуль Отчеты 13
3.9 Модуль Авторизация 13

4 Подготовка к работе 14

4.1 Вход в Jet Detective 14
4.2 Выход из Jet Detective 14
4.3 Порядок проверки работоспособности 14
4.4 Описание интерфейса пользователя 15
4.4.1 Окно веб-приложения 15
4.4.2 Типовые элементы управления 17
4.4.3 Индикация полей при вводе данных 19
4.4.4 Работа с табличными списками 19
4.4.5 Работа с иерархическими списками 25
4.4.6 Отказ от сохранения изменений 26
4.5 Профиль пользователя 26
4.5.1 Шаблоны профилей 26

5 Расследование инцидентов 30

5.1 Общие сведения 30
5.2 Графики на Рабочем столе 30
5.2.1 Общее описание рабочего стола 30
5.2.2 Настройка графиков на рабочем столе 31

5.2.3 Интерактивные возможности графиков на рабочем столе 32
5.2.4 Управление списком допустимых графиков в справочнике 32
5.2.5 Управление списком допустимых периодов для графиков 33
5.3 Управление инцидентами 34
5.3.1 Просмотр записи группировки инцидента 34
5.3.2 Создание записи управления инцидентами 36
5.3.3 Редактирование записи управления инцидентами 39
5.3.4 Удаление записи управления инцидентами 39
5.4 Работа с пользовательскими объектами 39
5.4.1 Общие сведения 39
5.4.2 Просмотр записи объекта 40
5.4.3 Добавление записи объекта 41
5.4.4 Редактирование записи объекта 42
5.4.5 Удаление записи объекта 42
5.5 Рабочий стол оператора 43
5.5.1 Общие сведения 43
5.5.2 Открытие и закрытие рабочего стола оператора 44
5.5.3 Изменение периода обновления списка инцидентов 44
5.5.4 Создание инцидента вручную 45
5.5.5 Быстрая фильтрация инцидентов 46
5.5.6 Назначение исполнителя инцидента 47
5.5.7 Смена статуса инцидентов 48
5.5.8 Открытие карточки инцидента 49
5.5.9 Карточка инцидента на рабочем столе оператора 49

6 Администрирование Jet Detective 59

6.1 Общие данные для администрирования 59
6.1.1 Размещение компонентов Jet Detective 59
6.2 Фабрика данных 60
6.2.1 Общие сведения 60
6.2.2 Просмотр объекта 63
6.2.3 Описание полей таблицы объекта 64
6.2.4 Подтверждение конфигурации объекта (создание таблицы в БД) 65
6.2.5 Редактирование конфигурации объекта 65
6.2.6 Управление табличным представлением и формой объектов 66
6.3 Обогащение данных 67

6.3.1 Общие сведения 67
6.3.2 Типы действий для процесса обогащения событий 67
6.3.3 Настройка обогащения 68
6.4 Модели документооборота 70
6.4.1 Просмотр модели документооборота 70
6.4.2 Создание модели документооборота 71
6.4.3 Настройка модели документооборота 72
6.5 Модель распределения прав доступа 74
6.5.1 Механизмы управления доступом 74
6.5.2 Разрешения 75
6.5.3 Инструменты для формирования наборов разрешений 76
6.5.4 Владения 77
6.6 Настройка механизмов управления доступом 80
6.6.1 Общие сведения 80
6.6.2 Дерево разрешений 81
6.6.3 Дерево владений 86
6.6.4 Дерево ролей 89
6.7 Управление учётными записями 94
6.7.1 Просмотр списка пользователей и учётной записи пользователя 94
6.7.2 Создание учётной записи пользователя 95
6.7.3 Порядок настройки прав доступа пользователя 96
6.7.4 Формирование набора разрешений пользователя 97
6.7.5 Формирование схемы владения пользователя 99
6.7.6 Редактирование учётной записи пользователя 101
6.7.7 Блокировка и разблокировка учётной записи пользователя 101
6.7.8 Управление паролем учётной записи пользователя 102
6.7.9 Удаление учётной записи пользователя 103
6.8 Отчеты 103
6.8.1 Общие сведения 103
6.8.2 Шаблоны отчетов 103
6.8.3 Запрошенные отчеты 109
6.8.4 Расписание отчетов 113
6.9 Служебные справочники 117
6.9.1 Серверы обработки 117
6.9.2 Действия 120
6.9.3 Переменные 124

6.9.4 Объекты поиска 126
6.9.5 Регулярные выражения 129
6.9.6 Справочник e-mail 131
6.9.7 Справочник директорий 133
6.9.8 Конфигурация сервисов 135
6.9.9 Архивация 138
6.9.10 Управление стилями таблиц объектов 139
6.10 Мониторинг процессов ETL 143
6.10.1 Общие сведения 143
6.10.2 Просмотр списка ETL-процессов 144
6.10.3 Просмотр ETL-процесса 144
6.10.4 Редактирование ETL-процесса 149
6.10.5 Запуск ETL-процесса 150
6.10.6 Остановка ETL-процесса 150
7 Настройка механизмов выявления аномалий 151
7.1 Правила и политики выявления аномалий 151
7.1.1 Общие сведения 151
7.1.2 Настройка правил выявления 152
7.1.3 Настройка политик выявления 173
7.2 Расчет агрегатов 181
7.2.1 Общие сведения 181
7.2.2 Просмотр управления агрегатом 181
7.2.3 Добавление управления агрегатом 182
7.2.4 Редактирование управления агрегатом 187
7.2.5 Удаление управления агрегатом 187
7.2.6 Запуск расчета агрегата 187
7.2.7 Остановка расчета агрегата 188
7.2.8 Просмотр истории расчета 189
7.2.9 Расчет агрегата за прошедшие периоды 190
7.2.10 Пересчет отдельных слепков 191
Список сокращений 192
Глоссарий 193

1 ВВЕДЕНИЕ

1.1 ОБЛАСТЬ ПРИМЕНЕНИЯ

Универсальная программная платформа Jet Detective (далее – Jet Detective) разработана для применения в организациях и на предприятиях любых отраслей: банки, предприятия розничной торговли, промышленные предприятия и др.

Jet Detective предназначена для создания систем, автоматизирующих анализ и выявление аномалий в данных, поступающих в режиме реального времени из множества разнородных, не связанных между собой источников.

Автоматизированные системы на базе Jet Detective обеспечивают:

- минимизацию времени принятия человеком экспертного решения при расследовании выявленных аномалий;
- применение для обнаружения известных аномалий экспертных правил выявления;
- гибкость настройки и расширения модели данных;
- масштабируемость решения пропорционально увеличению количества источников и объемов поступающих данных.

1.2 КРАТКОЕ ОПИСАНИЕ ВОЗМОЖНОСТЕЙ

Jet Detective принимает данные из множества разнородных источников. Эти данные очищаются, обогащаются, агрегируются, связываются и накапливаются в виде *объектов*, представляющих собой взаимосвязанные бизнес-сущности, такие как «клиенты», «платежи», «устройства», «действия» и любые другие.

Средствами Jet Detective проводится кросс-канальный анализ входящего потока данных в режиме реального времени, целью которого является выявление *аномалий* – нарушений, отклонений от обычного поведения; состояний, выходящих за пороговые значения; подозрительных или мошеннических действий.

Выявленные аномалии фиксируются в виде *инцидентов*. Jet Detective предоставляет пользователю необходимые инструменты для проведения расследования инцидентов: графические средства анализа связей, графические средства кросс-канального расследования, получение любых срезов данных.

1.3 УРОВЕНЬ ПОДГОТОВКИ ПОЛЬЗОВАТЕЛЕЙ

Требования к уровню подготовки пользователей Jet Detective основных категорий приведены в таблице 1.

Таблица 1 – Требования к уровню подготовки пользователей

Категория пользователей	Основное действие	Требование к уровню подготовки
Расследователи	Расследование инцидентов	▪ Базовые навыки работы с операционными системами семейства Microsoft Windows ▪ Базовые навыки работы с интернет-обозревателями ▪ Знание предметной области, в которой применяется Jet Detective, – в части выявления аномалий
Администраторы	Настройка взаимодействия Jet Detective с внешними системами; настройка модели данных; управление учётными записями и правами доступа пользователей	▪ Знание и опыт работы с ETL-системами ▪ Знание и опыт использования SQL-подобных языков запросов данных ▪ Понимание принципов, на которых базируется ролевая модель доступа
Аналитики	Настройка экспертных правил выявления аномалий;	▪ Знание предметной области, в которой применяется Jet Detective, – в части выявления аномалий ▪ Знание и опыт использования SQL-подобных языков запросов данных

2 НАЗНАЧЕНИЕ JET DETECTIVE

Универсальная программная платформа Jet Detective реализует следующие функции:

- получение и накопление информации транзакционного и не транзакционного характера, поступающей из множества разнородных источников;
- обработка данных, которая включает в себя очистку, обогащение, агрегацию, связывание информации;
- кросс-канальный анализ потоков данных в режиме реального времени с целью выявления аномалий, которые могут быть связаны:
- с мошенническими или подозрительными действиями;
- нарушением бизнес-процессов и регламентов;
- отклонениями от обычного поведения участников бизнес-процессов;
- нарушениями работоспособности компонентов сложных систем;
- состояниями, выходящими за пороговые значения;
- обнаружением скомпрометированных сущностей;
- проведение пользователем расследования инцидентов, связанных с выявленными аномалиями, в том числе с использованием графических инструментов кросс-канального расследования и анализа связей, получения любых срезов данных;
- настройка схемы хранения данных с применением конструктора модели объектов, основанной на концепции модели бизнес-объектов (Business Object Model);
- настройка интеграционного взаимодействия Jet Detective с системами-источниками и системами-потребителями;
- настройка алгоритмов выявления аномалий и прогнозирование потенциальных аномалий;
- настройка информирования пользователей и настройка действий, которые должны выполняться автоматически по факту выявления аномалий.

3 СТРУКТУРА JET DETECTIVE

3.1 ПЕРЕЧЕНЬ ФУНКЦИОНАЛЬНЫХ МОДУЛЕЙ

Jet Detective состоит из следующих функциональных модулей:

- **Фабрика данных**;
- **Анализ событий**;
- **Расследование инцидентов**;
- **Документооборот;**
- **Списки**;
- **Авторизаци**;
- **Агрегаты**;
- **Отчеты**;
- **Интеграция**.

3.2 МОДУЛЬ ФАБРИКА ДАННЫХ

Модуль **Фабрика данных** предназначен для управления данными и реализует следующие функции:

- настройка модели объектов, основанной на концепции модели бизнес-объектов (Business Object Model);
- сбор данных объектов из различных источников;
- баз данных;
- файлов различных типов;
- файлов протоколов серверов;
- интеграционных компонентов смежных систем и прочих;
- трансформация данных: очистка, обогащение, агрегация, связывание данных.

Модуль включает в себя:

- интерфейс пользователя конструктора объектов для настройки объектов нескольких видов (события, справочники, агрегаты);
- интерфейсы пользователя для просмотра, поиска, анализа и манипулирования данными в виде форм, таблиц, графов;
- приложение для настройки ETL-процессов и правил трансформации данных;
- приложение, реализующее ETL-процессы;
- приложение, реализующее логику настройки объектов и управления данными объектов;
- систему хранения на платформе традиционной реляционной системы управления базами данных (СУБД);

- систему хранения, которая обеспечивает быстрый доступ к большим данным, реализованную с помощью нереляционных распределенных баз данных;
- репозиторий, представленный файловым хранилищем, который предназначен для конфигурационной информации.

3.3 МОДУЛЬ АНАЛИЗ СОБЫТИЙ

Модуль **Анализ событий** предназначен для обработки входящих потоков данных и реализует следующие функции:

- настройка и испытание правил и политик выявления аномалий;
- применение правил и политик выявления к потокам данных;
- реагирование на выявленные аномалии:
- инициация процесса создание инцидентов;
- информирование пользователей;
- формирование ответа, отправляемого в источник данных; выполнение программных сценариев и прочее.

Модуль включает в себя:

- интерфейс пользователя для настройки правил и политик выявления, включающих в себя экспертные правила выявления аномалий;
- интерфейс пользователя для испытаний и сравнения политик и правил выявления;
- приложение, которое применяет правила и политики выявления к потокам данных, выполняет действия, обусловленные результатом применения политик и правил;
- систему оперативного хранения, которая предназначена для предоставления данных, используемых в анализе событий, а также реализует быстрый доступ и специальную стратегию обновления.

3.4 МОДУЛЬ РАССЛЕДОВАНИЕ

Модуль **Расследование** предназначен для проведения расследования выявленных инцидентов и реализует инструменты расследования, позволяющие проводить анализ инцидентов и связанных с ними объектов.

Модуль включает в себя интерфейс пользователя:

- рабочего стола оператора. Используется в процессе анализа условий сработавших правил и политик выявления аномалий;
- анализа связей инцидента с объектами;
- проведения кросс-канального расследования цепочек событий;
- анализа досье объектов.

3.5 МОДУЛЬ ДОКУМЕНТООБОРОТ

Модуль **Документооборот** предназначен для создания и настройки модели документооборота, которой будут подчиняться выбранные объекты Jet Detective.

Модуль реализует следующие функции:

- настройка моделей документооборота в части: модели смены статуса, действий при переходах и логики определения ответственного;
- связь модели с объектом Jet Detective;
- перевод объекта по статусам;
- инициация действий при переходе;
- определение ответственного для события в соответствии с выполняемым переходом.

Модуль включает в себя интерфейс для настройки модели документооборота.

3.6 МОДУЛЬ СПИСКИ

Модуль **Списки** предназначен для ведения и настройки списков, для которых будет необходима проверка на вхождение с возможностью использования полнотекстового поиска.

Модуль реализует следующие функции:

- настойка структуры списочных данных и логики их загрузки;
- предоставление механизма поиска по спискам, включая возможность полнотекстового поиска.

Отдельный интерфейс для работы с данным модулем нет. Структура списков и логика загрузки настраивается через интерфейсы модуля **Фабрика данных** (см. раздел 6.1). Настройка параметров поиска выполняется при настройке правил в модуле **Анализ событий** (см. раздел 6.9.4).

3.7 МОДУЛЬ АГРЕГАТЫ

Модуль **Агрегаты** предназначен для настройки логики расчета агрегатов и выполнения этих вычислений по заданному расписанию.

Модуль реализует следующие функции:

- настройка логики расчета агрегата;
- настройка расписания расчета агрегата;
- выполнение вычислений агрегата по настроенному расписанию, с учетом всех параметров настройки;
- сохранение результатов расчета.

Модуль включает в себя интерфейсы:

- для настройки параметров вычисления агрегатов;
- настройки расписания расчетов агрегатов;
- просмотра рассчитанных значений агрегатов.

3.8 МОДУЛЬ ОТЧЕТЫ

Модуль **Отчеты** предназначен для хранения шаблонов отчётов загруженных в Jet Detective, формирования отчётов в различных форматах, а также их последующего сохранения и отправки на e-mail.

Модуль реализует следующие функции:

- хранение шаблонов отчетов;
- формирование отчёта по шаблону с указанием входных параметров для него;
- формирование отчёта в разных форматах;
- отправка сформированного отчета на e-mail;
- размещение сформированного отчета в папку;
- сохранение сформированного отчета на компьютере пользователя;
- формирование отчета по шаблону согласно заданному по расписанию;
- сохранение истории запросов отчета со значениями входных параметров, по которым он был сформирован;
- повторное получение ранее сформированного отчета.

Модуль включает в себя интерфейсы:

- для работы с шаблонами отчетов;
- работы со списком ранее запрошенных отчетов;
- создания и настройки расписания формирования отчета.

3.9 МОДУЛЬ АВТОРИЗАЦИЯ

Модуль **Авторизация** предназначен для организации доступа пользователей к функциям и данным Jet Detective и реализует следующие функции:

- настройка справочников доступа: разрешения, владения, роли пользователей, учётные записи пользователей;
- аутентификация и авторизация пользователя;
- применение настройки прав доступа к действиям пользователей.

Модуль включает в себя:

- интерфейс для настройки разрешений, владений, ролей пользователей и учётных записей пользователей;
- интерфейс для идентификации пользователя;
- приложение для авторизации пользователя;
- систему хранения для справочников доступа.

4 ПОДГОТОВКА К РАБОТЕ

4.1 ВХОД В JET DETECTIVE

Чтобы войти в Jet Detective:

1) В адресной строке интернет-обозревателя (далее – обозреватель) укажите адрес Jet Detective.
2) В открывшемся окне авторизации укажите регистрационное имя и пароль пользователя (Рисунок 1).
3) Нажмите кнопку **Войти**.

Откроется окно веб-приложения Jet Detective. Описание интерфейса пользователя см. в разделе 4.4.

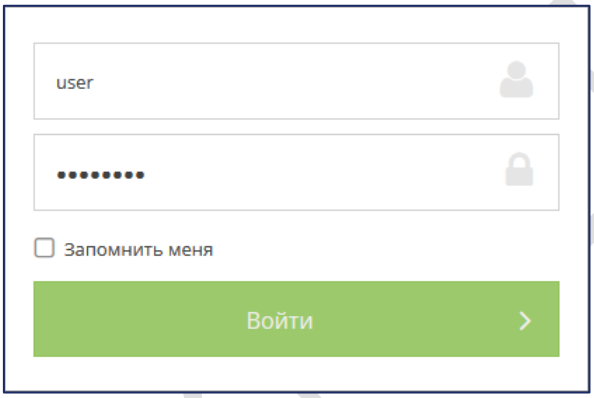


Рисунок 1 – Вход в Jet Detective

4.2 ВЫХОД ИЗ JET DETECTIVE

Чтобы выйти из Jet Detective, на вспомогательной панели веб-приложения нажмите кнопку **Выход из системы** (находится в правом верхнем углу).

4.3 ПОРЯДОК ПРОВЕРКИ РАБОТОСПОСОБНОСТИ

Jet Detective готова к работе, если:

1) В процессе авторизации не получены сообщения об ошибках.
2) Успешно прошло обновление веб-приложения, если оно требовалось.
3) В результате авторизации открылось окно веб-приложения (см. раздел 4.4.1).

4.4 ОПИСАНИЕ ИНТЕРФЕЙСА ПОЛЬЗОВАТЕЛЯ

4.4.1 Окно веб-приложения

Окно веб-приложения Jet Detective (Рисунок 2) содержит следующие основные элементы интерфейса:

- панель меню (далее *Меню*);
- рабочую область;
- вспомогательную панель.

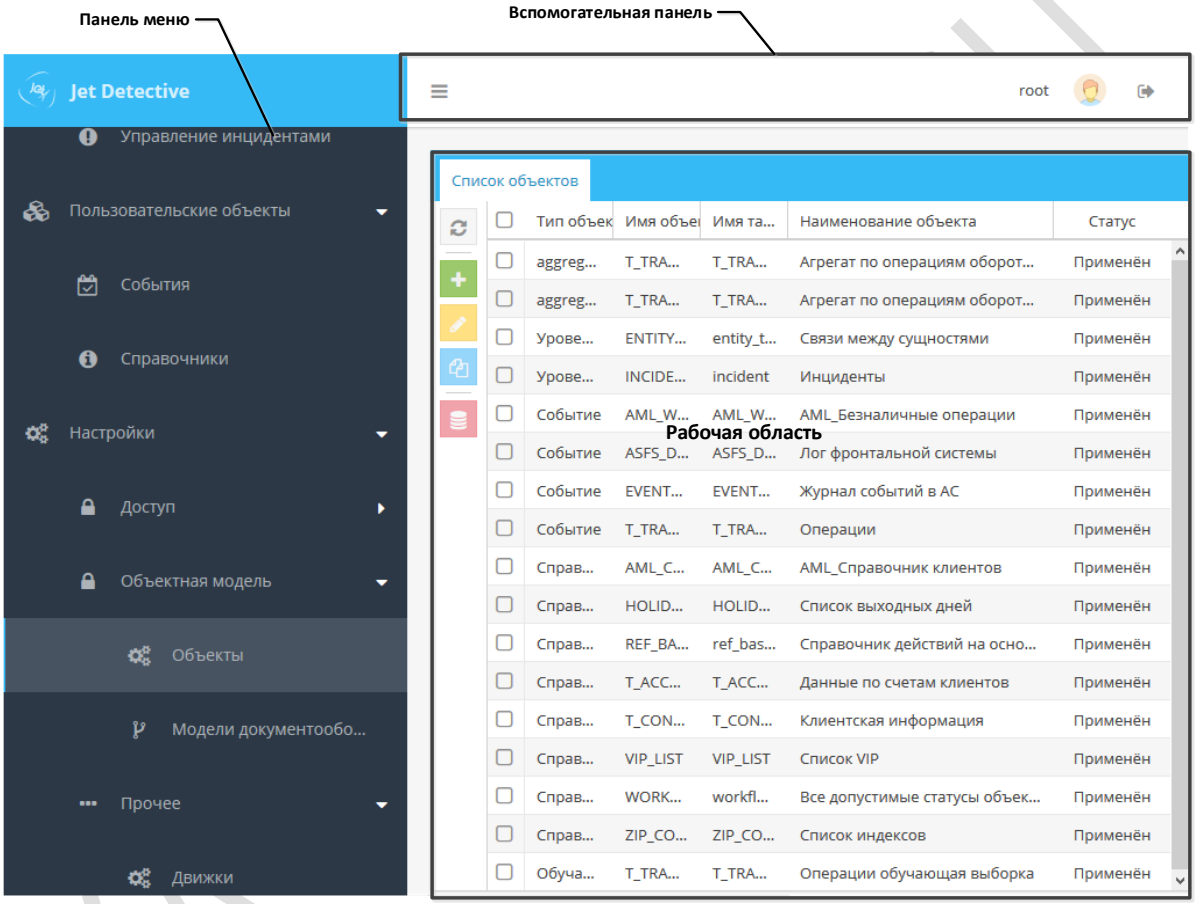


Рисунок 2 – Общий вид окна веб-приложения

Интерфейс веб-приложения устроен единообразно – в *рабочей области* по умолчанию отображается вкладка со списком сущностей, соответствующих выбранному пункту меню, и вкладки с формой самих сущностей, которые открывает пользователь. Исключение составляет интерфейс **Рабочего стола**.

Например:

- если выбрать пункт меню **Настройки** – **Объекты**, отобразится вкладка со списком конфигураций объектов Jet Detective;
- если выбрать пункт меню **Пользовательские объекты** – **События**, отобразится вкладка со списком объектов с типом **События** (Рисунок 3) и т. п.

Список сущностей отображается в виде таблицы, изменение параметров отображения таблиц описано в разделе 4.4.4.

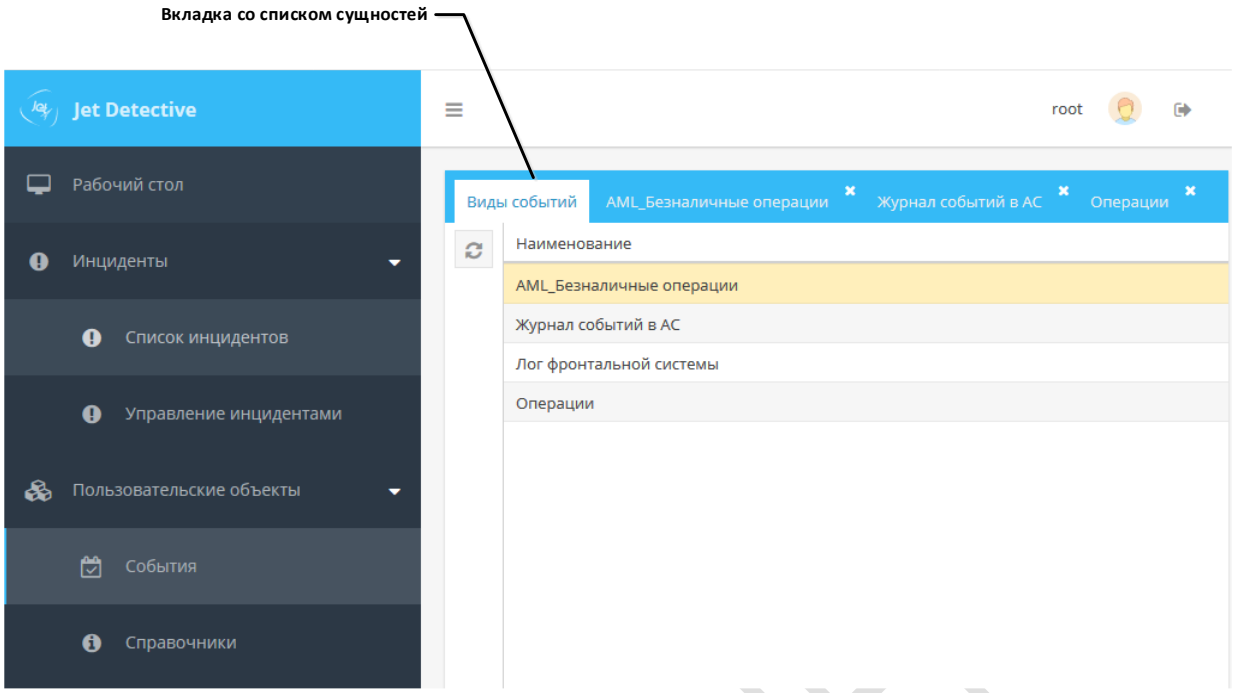


Рисунок 3 – Пример списка экземпляров объекта с типом **События**

Чтобы просмотреть информацию о какой-либо сущности, на вкладке со списком дважды щёлкните по соответствующей строке. Экранная форма откроется на отдельной вкладке в рабочей области (Рисунок 4).

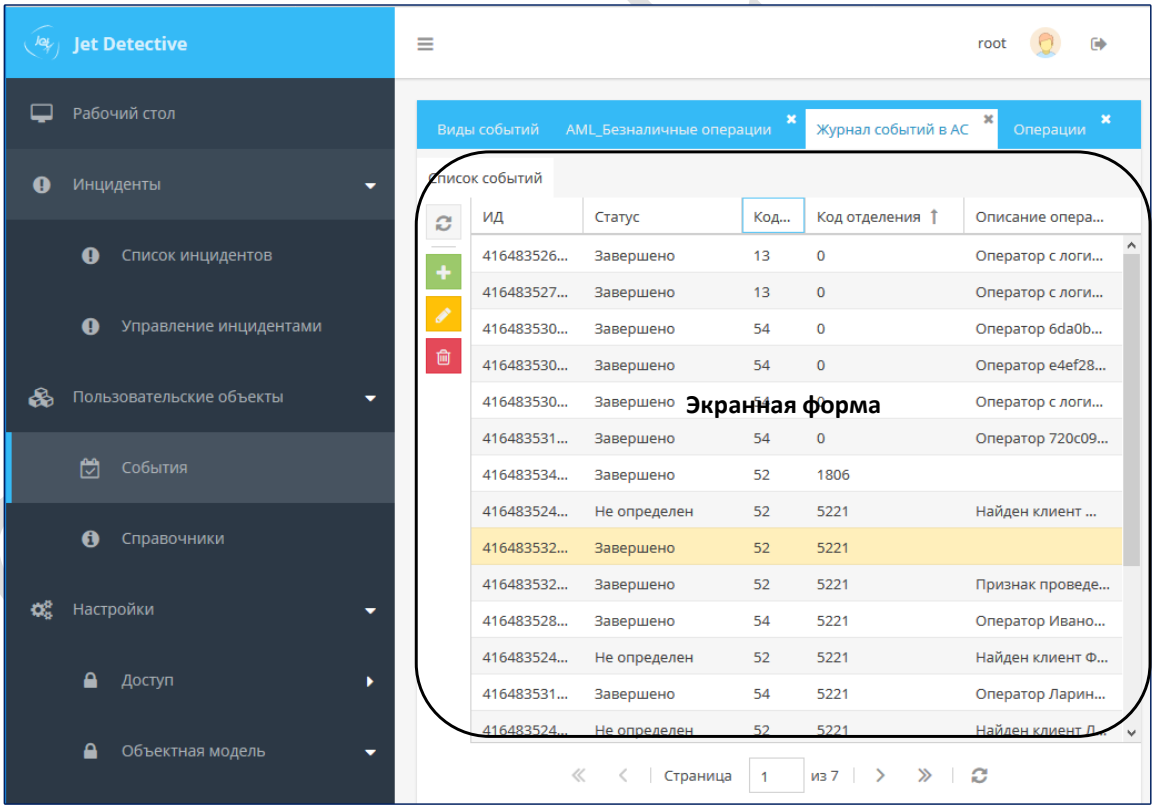


Рисунок 4 – Пример вкладки с экранной формой выбранной сущности

Если открытая сущность также является списочной, то для просмотра информации какой-либо из них, дважды щелкните по ней в списке. Экранная форма конкретной записи откроется во втором уровне вкладок (Рисунок 5)

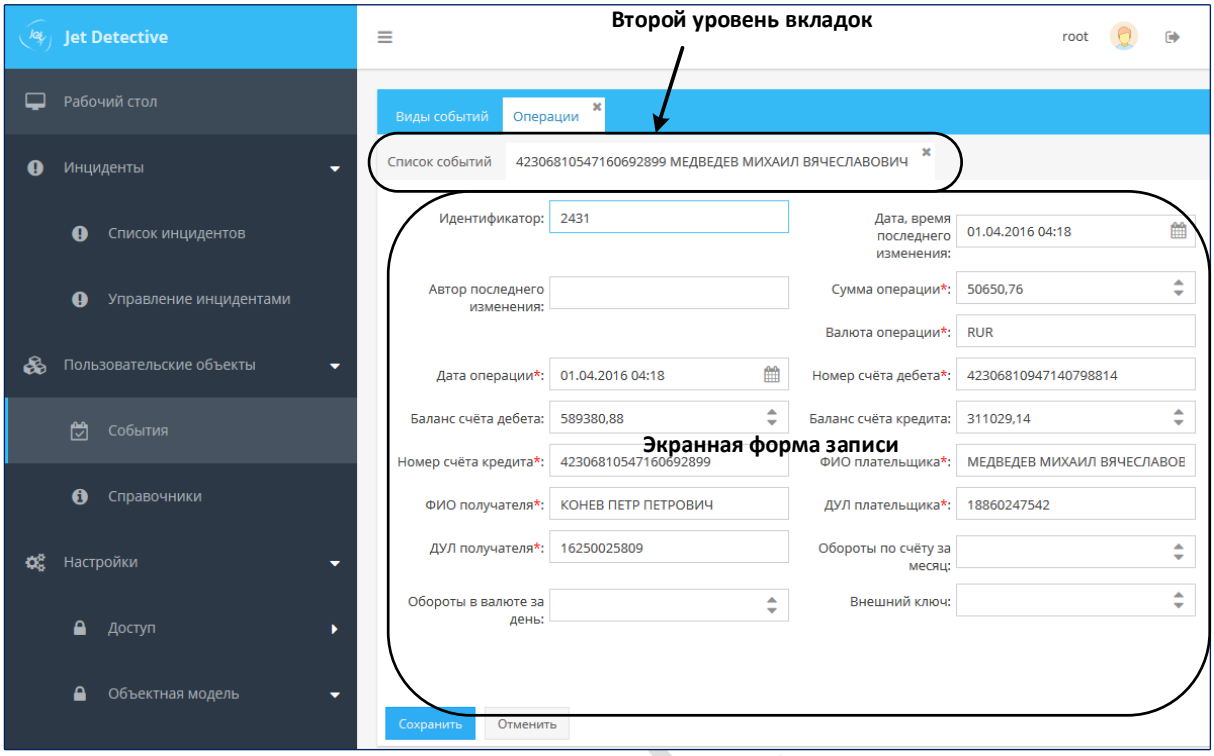


Рисунок 5 – Пример рабочей области с двумя уровнями вкладок

Описание элементов вспомогательной панели приведено в таблице 2.

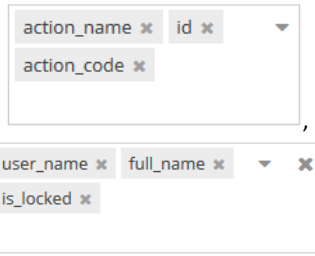
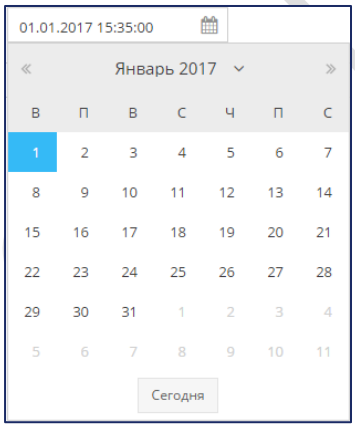
Таблица 2 – Описание вспомогательной панели

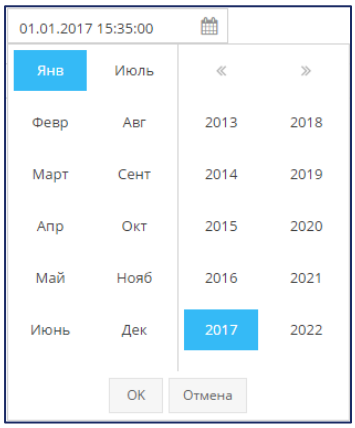
Элемент интерфейса	Тип	Описание элемента и его применения
	Кнопка	Сворачивание (раскрытие) панели меню
9/3080	Кнопка	Открывает рабочий стол оператора (см. раздел 5.5)
	Кнопка	Раскрытие меню с пунктами: **Профиль пользователя** (см. раздел 4.5); **История событий**; **Изменить пароль**; **О системе** Слева от кнопки отображается регистрационное имя пользователя авторизованного в Jet Detective в настоящее время
	Кнопка	Выход из Jet Detective

4.4.2 Типовые элементы управления

В таблице 3 приведены сведения о назначении типовых элементов управления, расположенных в рабочей области и диалоговых окнах веб-приложения Jet Detective.

Таблица 3 – Типовые элементы управления

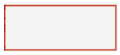
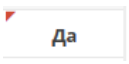
Элемент управления	Тип или название	Описание элемента и его применения
	Кнопка **Обновить**	Обновление отображаемой информации, поступающей с сервера Jet Detective
	Поле	Поле с раскрывающимся списком и множественным выбором элементов. Чтобы заполнить поле, выберите в раскрывающемся списке одно или несколько значений. Для выбора нескольких значений используйте клавишу Ctrl. Чтобы удалить из поля указанное ранее значение, нажмите кнопку  (находится в правой части поля). Чтобы в одно действие удалить все указанные значения, нажмите кнопку . *Примечание.* такая возможность доступна не для всех полей
	Кнопка **Добавить**	Добавление данных
	Кнопка **Добавить**	Добавление данных с возможностью выбора их вида
	Кнопка **Удалить**	Удаление данных
	Кнопка **Открыть**	Открытие экранной формы выбранной в списке сущности (объекта, учётной записи пользователя и т. д). Экранную форму можно также открыть двойным щелчком по строке в списке сущностей
	Кнопка **Копировать**	Создание сущности с копированием параметров выбранной в списке сущности
	Поле с календарём	Дату в поле можно указать как вручную, так и с помощью раскрывающегося календаря. Используемый формат – ДД.ММ.ГГГГ. Время можно указать только вручную, формат – чч:мм:сс. По умолчанию время автоматически устанавливается в значение 00:00:00. При необходимости его можно изменить. Чтобы раскрыть календарь, нажмите кнопку  . Отобразится дата, выбранная ранее, или текущая дата – если поле с датой не заполнено. Чтобы перейти к любому месяцу и году: нажмите кнопку в верхней части календаря; в раскрывшемся списке выберите месяц и год; нажмите ОК. Для перехода к предыдущему или последующему месяцу используйте кнопки  и  . Или: нажмите клавиши Ctrl+ ← или Ctrl+→.

Элемент управления	Тип или название	Описание элемента и его применения
		Для перехода к предыдущему или последующему году нажмите клавиши Ctrl+↓ или Ctrl+↑. Для выбора даты, соответствующей сегодняшнему дню, нажмите кнопку Сегодня или клавишу пробела
	Поле	Поле с раскрывающимся списком
	Поле	Поле с блоком кнопок для увеличения/уменьшения численного значения. Значение можно указать введом с клавиатуры

4.4.3 Индикация полей при вводе данных

При вводе данных в поля экранных форм используется индикация полей (Таблица 4).

Таблица 4 – Индикация полей

Элемент интерфейса	Описание
*	Обязательное для заполнения поле
	Обязательное для заполнения поле, которое не было заполнено
	Ячейка таблицы, значение которой изменено пользователем, но еще не сохранено
	Предупреждение. При наведении указателя мыши на значок отображается текст предупреждения
	Подсказка. При наведении указателя мыши на значок отображается текст подсказки

4.4.4 Работа с табличными списками

4.4.4.1 Упорядочивание строк

В интерфейсе пользователя списки сущностей отображаются в табличном виде.

Под упорядочиванием строк таблицы понимается сортировка по содержимому ячеек того или иного столбца или по числовым значениям. Сортировка возможна как по возрастанию, так и по убыванию.

Стрелка справа от названия какого-либо столбца (↓ или ↑) указывает на установленный порядок сортировки.

Чтобы отсортировать список, щёлкните левой кнопкой мыши по заголовку столбца. Повторный щелчок по заголовку вызывает обратную сортировку.

Другой способ сортировки списка:

1) Наведите курсор на заголовок столбца, по которому необходимо выполнить сортировку.

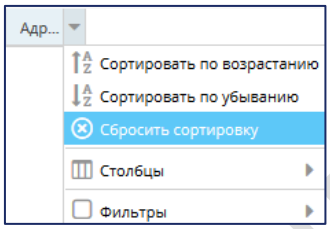
   В правой части заголовка отобразится кнопка 

2) Нажмите на кнопку и выберите пункт **Сортировать по возрастанию** или **Сортировать по убыванию**

Чтобы сбросить примененную сортировку:

3) Наведите курсор на заголовок столбца, где применена сортировка (в заголовке стрелка вверх или вниз).

В правой части заголовка отобразится кнопка 



4) Нажмите кнопку и выберите пункт **Сбросить сортировку**.

4.4.4.2 Настройка табличного представления

Можно включать столбцы в таблицу и исключать их.

Доступны два способа настройки.

Способ первый.

Чтобы настроить отображение столбцов:

1) Наведите курсор на заголовок любого столбца.

В правой части заголовка отобразится кнопка  (Рисунок 6).

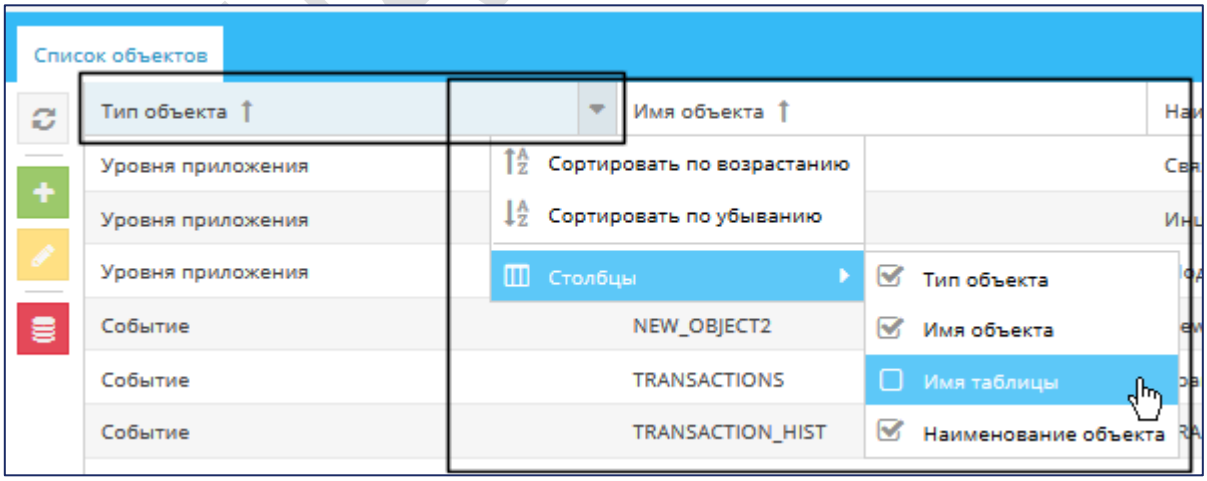


Рисунок 6 – Настройка отображения столбцов

2) Нажмите кнопку и в раскрывшемся меню наведите указатель на пункт **Столбцы**.

Раскроется список с названиями столбцов. Рядом с названиями столбцов, которые уже отображаются в таблице, установлены флажки.

3) Установите флажки у тех столбцов, которые следует отображать, и снимите флажки, у столбцов, которые нужно скрыть.
4) Для завершения настройки щёлкните левой кнопкой мыши по любой области окна.

Чтобы изменить порядок следования столбцов в таблице, с помощью мыши перетащите заголовок столбца в другое место шапки таблицы.

Способ второй

1) Нажмите на кнопку **Настроить** 

   Откроется модальное окно со списком атрибутов объекта. Возле атрибутов, которые уже отображаются в таблице, установлен флаг (Рисунок 7).
2) Отметьте флажками те атрибуты, которые необходимо отобразить в таблице.
3) Измените порядок атрибутов в таблице. Для этого кликнув на строку и удерживая ее перетащите ее на нужную позицию.
4) Нажмите кнопку **Применить**

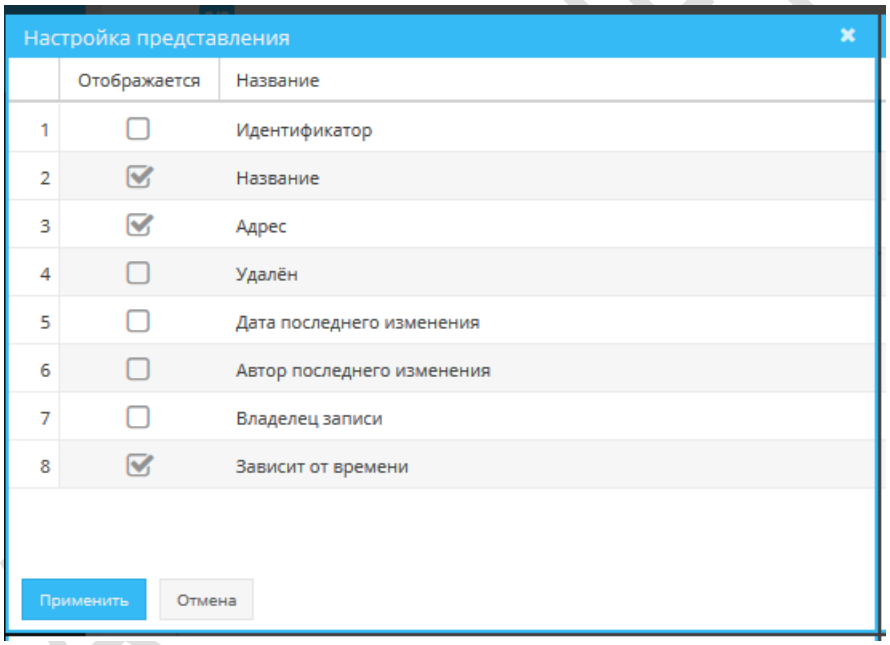


Рисунок 7 – Модально окно с настройками табличного представления

4.4.4.3 Фильтрация столбцов

Чтобы отфильтровать значения в табличном списке:

1) Наведите курсор на заголовок любого столбца таблицы.

В правой части заголовка отобразится кнопка  (Рисунок 8).

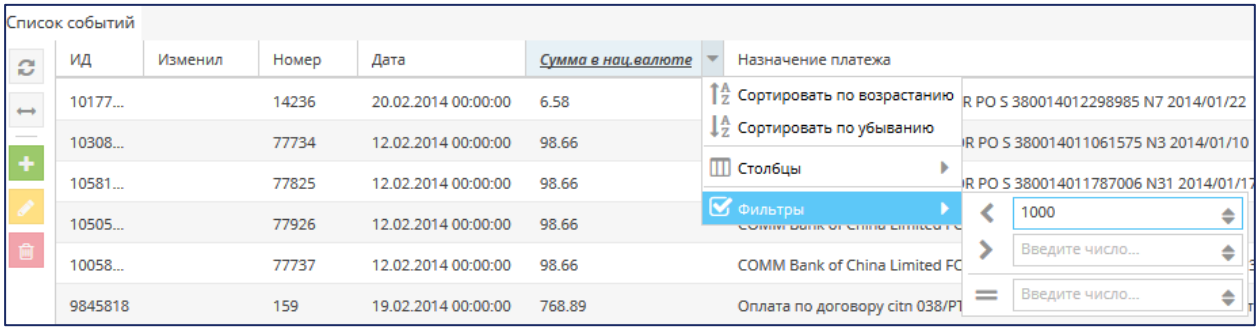
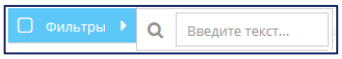
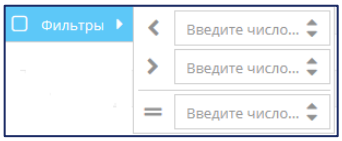
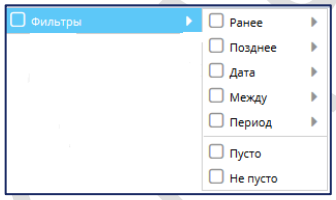


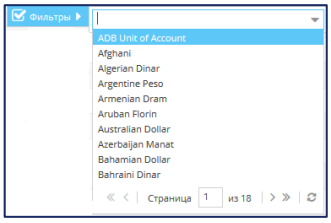
Рисунок 8 – Настройка фильтрации значений таблицы

2) Нажмите кнопку и в раскрывшемся меню наведите указатель на пункт **Фильтры** – отображается, если для выбранного столбца доступна фильтрация значений.

Отобразится список полей с доступными параметрами фильтрации. Состав списка зависит от типа данных выбранного столбца (Таблица 5).

Таблица 5 – Описание полей фильтрации для различных типов данных

Поле	Тип данных	Описание фильтра и его применения
	Текстовый	Полнотекстовый поиск значения в столбце. При этом регистр не учитывается. Введите значение для поиска
	Числовой	Поиск числового значения. Укажите значения: введите числа с клавиатуры или используйте стрелки  При этом: ▪ Если указано условие «<», будут найдены значения меньше указанного. ▪ Если указано условие «>», будут найдены значения больше указанного. ▪ Если указаны оба условия – «>» и «<», будут найдены значения для промежутка чисел. ▪ Если после указания условий «**<**» и «**>**» **введено значение в поле «=», поля условий очистятся**
	Дата/время	Поиск даты: ▪ **Ранее** – дата, которая меньше указанной даты; ▪ **Позднее** – дата, которая больше указанной даты; ▪ **Дата** – конкретная дата. Указать можно одно значение; ▪ **Между** – промежуток дат, между которыми должно быть найдено значение. Указывается одно значение для каждой границы; ▪ **Период** – поиск дат, отстоящих от текущего момента времени на заданное значение. Список доступных периодов поиска задается через справочник **Все допустимые периоды для дашбордов** (см. раздел 5.2.5). ▪ **Пусто** – фильтрует все записи, где поле даты пустое ▪ **Не пусто** – фильтрует все записи, где поле даты имеет какое-то значение. **Поля Ранее** и **Позднее** могут использоваться совместно, для поиска диапазона дат

Поле	Тип данных	Описание фильтра и его применения
	Логический	Выбор логического значения: **Да** или **Нет**
	Ссылочный (REF-атрибут)	Поиск выбранного значения справочника, на который ссылается атрибут. Раскрывающийся список поля содержит значения справочника, на который ссылается атрибут. Доступен полнотекстовый поиск. Введите значение в поле и выберите запись в списке

3) Укажите параметры фильтрации.

4) Для завершения настройки щёлкните левой кнопкой мыши по любой области окна.

Заголовок столбца, для которого установлен фильтр, выделится полужирным курсивом (Рисунок 9).

Рисунок 9 – Отображение столбца «Дата», на котором применен фильтр

Отфильтровать значения табличного списка можно для нескольких столбцов одновременно. Для этого повторите пункты 1)–4) для других столбцов.

Чтобы отфильтровать по конкретному значению из ячейки таблицы:

1) В таблице на ячейки, по значению которой необходимо применить фильтр, нажмите правой клавишей мыши.

2) В контекстном меню выберите пункт **Отфильтровать по значению ячейки**

Чтобы сбросить все примененные фильтры:

1) В таблице на любом месте нажмите правой клавишей мыши.

2) В появившемся контекстном меню выберите пункт **Сбросить фильтры.**

4.4.4.4 Изменение ширины столбцов

Чтобы настроить ширину столбца таблицы, при помощи мыши перетащите границу между столбцами в шапке таблицы.

Чтобы автоматически подобрать ширину столбца по содержимому ячеек:

1) Подведите указатель мыши, например, к правой границе столбца в шапке таблицы.

Когда курсор примет вид двухсторонней стрелки, дважды щёлкните по границе столбца.

Ширина столбца, расположенного слева, будет подобрана автоматически.

Чтобы установить ширину столбцов автоматически по значению содержимого столбцов:

1) Нажмите на кнопку **Автоматически выставить ширину у столбцов**

4.4.4.5 Счетчик записей в таблице

В заголовке каждой таблице присутствует счетчик, который показывает количество полученных из базы данных записей (Рисунок 10). За один раз может быть получено не более 150 записей. По мере прокручивания загруженных записей выполняются повторные загрузки для увеличения числа записей.

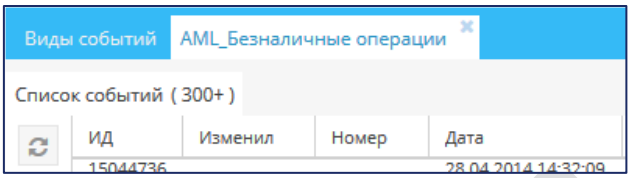


Рисунок 10 – Заголовок таблицы, где указано количество загруженных записей (300+)

4.4.4.6 Проиндексированные столбцы

В табличном представлении пользовательских объектов в заголовке колонок, которые имеют индекс, стоит значок «звездочка». Фильтрация по колонкам с таким значком выполняется быстрее, чем по колонкам без него.

4.4.4.7 Выгрузка в EXCEL

Чтобы выгрузить данные табличного представления в Excel:

1) На табличном представлении, данные которого необходимо выгрузить в Excel, вызовите контекстное меню (нажатием правой клавиши мыши)
2) Выберите пункт **Выгрузить в Excel**

   Примечание: При выгрузке учитываются все примененные фильтры и сортировки.
3) В появившемся модальном окне укажите количество выгружаемых записей (Рисунок 11).

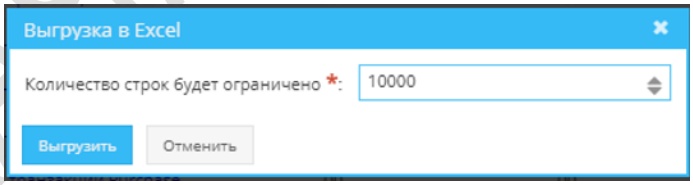


Рисунок 11 – Модальное окно для указания количества выгружаемых в Excel записей

Примечание: Количество не может превышать 10 000.

4) Нажмите кнопку **Выгрузить**

4.4.4.8 Кнопки перехода к страницам таблицы

Для некоторых таблиц в нижней части рабочей области отображается панель с кнопками управления страницами таблицы (Таблица 5).

Таблица 6 – Кнопки перехода к страницам таблицы

Элемент управления	Тип или название	Описание элемента и его применения
«	Кнопка **Первая страница**	Переход к первой странице таблицы
‹	Кнопка **Предыдущая страница**	Переход к предыдущей странице таблицы
Страница 3 из 7	Поле	Переход к странице, номер которой указан в поле. Чтобы перейти к странице таблицы: 1) укажите в поле номер страницы (справа от поля ввода указано общее количество страниц); 2) нажмите клавишу Enter
›	Кнопка **Следующая страница**	Переход к следующей странице таблицы
»	Кнопка **Последняя страница**	Переход к последней странице таблицы

4.4.5 Работа с иерархическими списками

В интерфейсе пользователя ряд сущностей представлен иерархическими списками в виде *дерева*. Согласно общепринятой терминологии, узлы дерева, не имеющие дочерних элементов, называются *листьями*, а узлы, имеющие дочерние элементы, – *внутренними узлами*.

Узлы дерева отмечены специальными значками, характеризующими тип узла. Например, в дереве разрешений узлы с типом **Папка** отмечены значком или . Описания типов узлов приводятся в разделах, посвященных работе с соответствующими деревьями.

Чтобы развернуть внутренний узел дерева, в левой части узла нажмите кнопку . Она примет вид

Чтобы свернуть внутренний узел дерева, нажмите кнопку .

Чтобы развернуть все внутренние узлы дерева, нажмите кнопку **Развернуть дерево** . Отобразятся все уровни иерархии (Рисунок 12).

Чтобы свернуть все внутренние узлы дерева до корневого узла, нажмите кнопку **Свернуть дерево** .

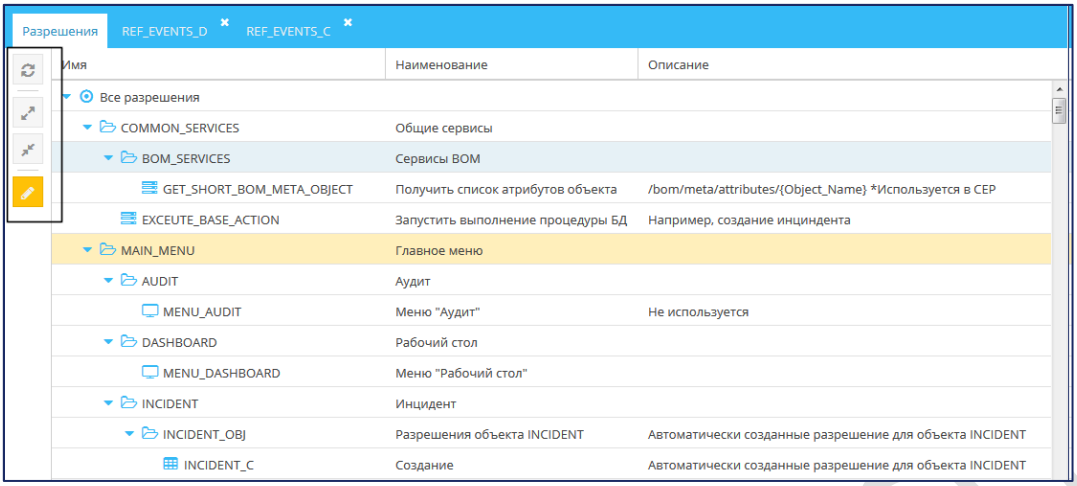


Рисунок 12 – Кнопки управления и пример полностью развернутого дерева разрешений

4.4.6 Отказ от сохранения изменений

Существует два способа отказаться от сохранения внесенных изменений:

- закрыть вкладку с экранной формой;
- нажать кнопку **Отменить** (находится в нижней части вкладки).

После этого вкладка с экранной формой закроется, а внесённые изменения не сохранятся.

4.5 ПРОФИЛЬ ПОЛЬЗОВАТЕЛЯ

Профиль пользователя состоит из двух вкладок:

- **Шаблоны профилей** – сохраненные состояния табличных представлений объектов системы.
- **События сессии** – история всех всплывающих сообщений, которые формировались в рамках текущей сессии пользователя

4.5.1 Шаблоны профилей

Шаблон профилей используется для настройки индивидуального рабочего пространства пользователя в системе. Шаблоны позволяют настроить и запомнить, выбранный вид табличных представлений для каждого пользователя.

Шаблон профиля включает в себя:

- набор видимых колонок в табличном представлении объекта;
- порядок колонок в табличном представлении объектов;
- установленные фильтры в табличном представлении объекта (там, где они есть);
- установленные сортировки в табличных представлениях объектов (там, где они есть);
- ширину колонок в табличном представлении объектов.

Шаблон профиля распространяется на отображение следующих объектов:

- табличные представления пользовательских объектов (меню **Пользовательские объекты,** см. раздел 5.4);
- табличное представление Список инцидентов, Связанные события, История событий и История инцидентов на рабочем столе оператора (см. раздел 5.5);

- другие табличные представления системы, поддерживающие функцию сохранения состояния.

  Примечание. Исключения при сохранении шаблона профиля: Связанные события, История событий и История инцидентов на рабочем столе оператора – не сохраняется сортировка и фильтры (там, где они есть).

4.5.1.1 Просмотр шаблонов профилей

Чтобы посмотреть список шаблонов профилей:

1) Нажмите на вспомогательной панели на иконку  и выберите меню пункт меню **Профиль пользователя**.

В рабочей области отобразится две вкладки:

- **Шаблоны профилей** (см. Рисунок 13)
- **События сессии** (см. Рисунок 14)

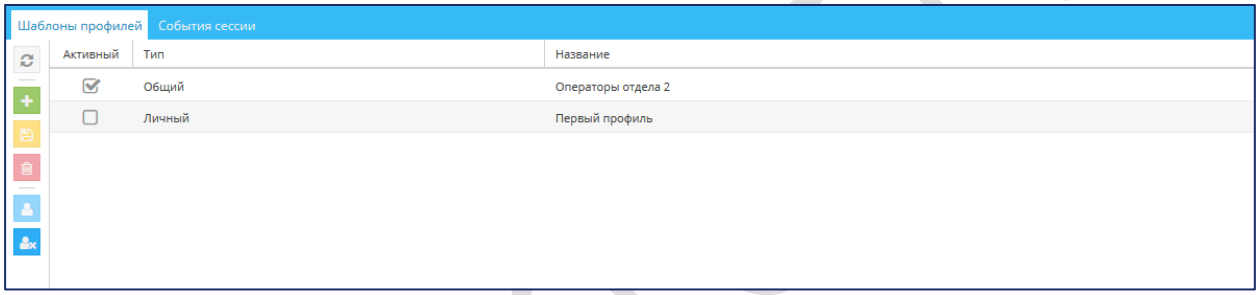


Рисунок 13 – Вкладка с перечнем шаблонов профилей

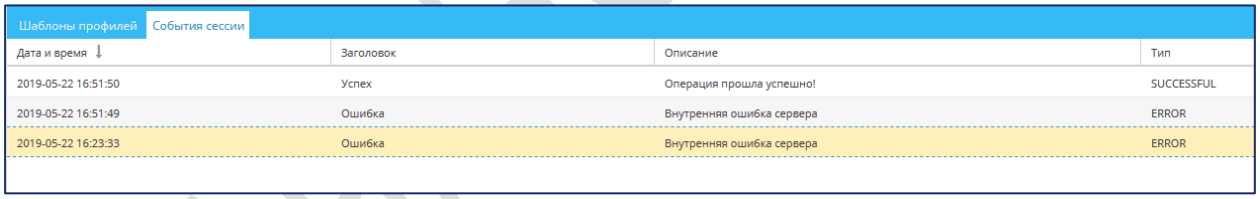


Рисунок 14 – Вкладка с перечнем событий сессии

4.5.1.2 Добавление шаблона профиля

Чтобы добавить в систему шаблон профиля:

1) Настройте табличные представления, так как необходимо сохранить в профиле.
2) Откройте список шаблонов профилей (см. раздел 4.5.1.1).
3) Нажмите кнопку **Добавить**  (Рисунок 13).

Откроется модальное окно **Создание шаблона профиля** (Рисунок 15).

4) Заполните поля окна:

- **Тип** – выберите один из доступных типов:
  - **Личный** – доступен для использования, редактирования и удаления только создавшему ему пользователю;

- **Общий** – доступен для использования всем пользователям системы. Создавать, редактировать и удалять профили такого типа могут пользователи с отдельным разрешением;

- **Название** – текстовое поле для имени профиля для его отображения в списке;
- Флаг **Сделать активным.** Если флаг установлен, то после сохранения профиля, он назначается активным для авторизованного пользователя. Если флаг снят, то профиль создается, но не назначается активным для пользователя;

4) Нажмите кнопку **Сохранить**.

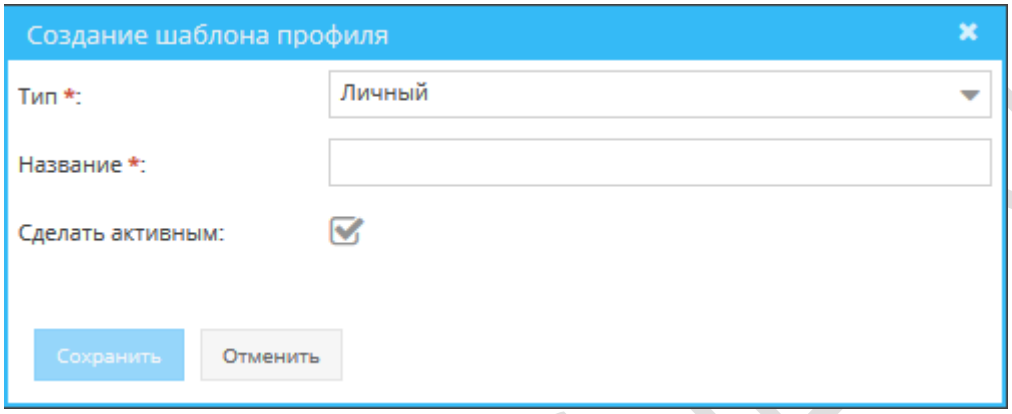


Рисунок 15 – Форма **Создание шаблона профиля**

4.5.1.3 *Редактирование шаблонов профилей*

Чтобы отредактировать шаблон профиля:

1) Настройте табличные представления, так как необходимо сохранить в профиле.
2) Откройте список шаблонов профилей (см. раздел 4.5.1.1).
3) Выберите в списке шаблон, который хотите изменить и сохранить в нем настроенное представление.
4) Нажмите кнопку **Сохранить** (Рисунок 13).

4.5.1.4 *Копирование шаблонов профилей*

Чтобы скопировать шаблон профиля:

1) Откройте список шаблонов профилей (см. раздел 4.5.1.1).
2) Назначьте шаблон профиля, который необходимо скопировать, как активный (см. раздел 4.5.1.6).
3) Нажмите кнопку Добавить (Рисунок 13). И далее повторите шаги необходимые для добавления шаблона профиля (см. раздел 4.5.1.2).

4.5.1.5 *Удаление шаблонов профилей*

Чтобы удалить шаблон профиля:

1) Откройте список шаблонов профилей (см. раздел 4.5.1.1).
2) Выберите в списке шаблон, который хотите удалить.

3) Нажмите кнопку **Удалить**  (Рисунок 13).

4.5.1.6 Активный шаблон профиль

Активный шаблон профиля – это те настройки табличных представлений системы, которые применяются для пользователя при начале сессии.

Чтобы назначить активный уже существующий шаблон профиля:

1) Откройте список шаблонов профилей (см. раздел 4.5.1.1).
2) Выберите в списке шаблон профиля, который хотите назначить как активный.
3) Нажмите кнопку **Назначить активным**  (Рисунок 13).

   Как только шаблон станет активным, он автоматически будет применятся к действующему состоянию системы.

4.5.1.7 Сбросить активный шаблон профиля

Чтобы сбросить активный шаблон профиля и вернуть отображение табличных представлений к виду по умолчанию:

1) Откройте список шаблонов профилей (см. раздел 4.5.1.1).
2) Нажмите кнопку **Сбросить активным**  (Рисунок 13).

   После того, как активный шаблон профиля сбрасывается, табличные представления приводятся к стандартному виду.

5 РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

5.1 ОБЩИЕ СВЕДЕНИЯ

Средствами Jet Detective автоматически выполняется кросс-канальный анализ входящего потока данных, целью которого является выявление аномалий. Анализ проводится в соответствии со специальными правилами и политиками выявления аномалий.

Выявленные аномалии фиксируются в виде инцидентов. *Инцидент* – это информационная запись, обладающая следующими свойствами:

- запись связана с событиями, в которых были выявлены аномалии;
- запись связана со сработавшими правилами и политиками выявления;
- в записи хранится информация о результате процесса выявления;
- в записи хранится информация о статусе и результатах расследования.

Расследователи анализируют каждый инцидент и по результатам принимают решение, к какой категории отнести инцидент. Пример категорий при расследовании мошеннических действий: мошеннический, подозрительный или легитимный.

5.2 ГРАФИКИ НА РАБОЧЕМ СТОЛЕ

5.2.1 Общее описание рабочего стола

На **Рабочем столе** размечена область для отображения четырех графиков. Изменение границ этих областей недоступно.

Любой пользователь может выбрать графики, которые следует отображать на своем рабочем столе (Рисунок 16). Графики периодически обновляются в автоматическом режиме.

Чтобы перейти к просмотру, выберите пункт меню **Рабочий стол**.

Рисунок 16 – Отображение настроенных графиков на рабочем столе

5.2.2 Настройка графиков на рабочем столе

Чтобы настроить отображение графиков на рабочем столе:

1) Выберите пункт меню **Рабочий стол.**

Откроется экранная форма рабочего стола с размеченными границами для отображения графиков или графики, настроенные пользователем ранее.

> *Примечание.* Выбранные графики и периоды их отображения сохраняются в кеше браузера, в котором работает пользователь.

2) Выберите график в первом раскрывающемся списке – он расположен над областью отображения первого графика (Рисунок 17). Этот список содержит значения справочника **Все допустимые дашборды** (см. раздел 5.2.4).

3) Выберите значение периода во втором раскрывающемся списке, если график зависит от времени.

4) Повторите шаги 2) и 3) для остальных трех областей отображения графиков.

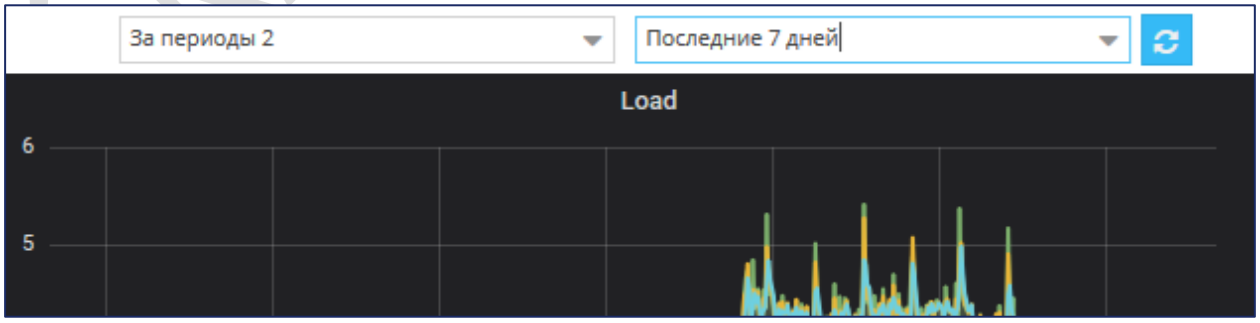


Рисунок 17 – Настройка графика. Поля с раскрывающимися списками

5.2.3 Интерактивные возможности графиков на рабочем столе

Все графики на рабочем столе являются интерактивными: при наведении на график появляется подсказка со значениями отрезка графика, а также доступно масштабирование части графика.

Для масштабирования части графика выделите интересующую часть графика или дважды щелкните по ней.

Фрагмент графика увеличится (см. Рисунок 18).

Если масштаб графика был изменен, то автоматическое обновление данных на графике перестает работать до тех пор, пока пользователь не нажмет кнопку **Обновить** рядом с графиком (см. Рисунок 17), либо пока не обновится страница браузера.

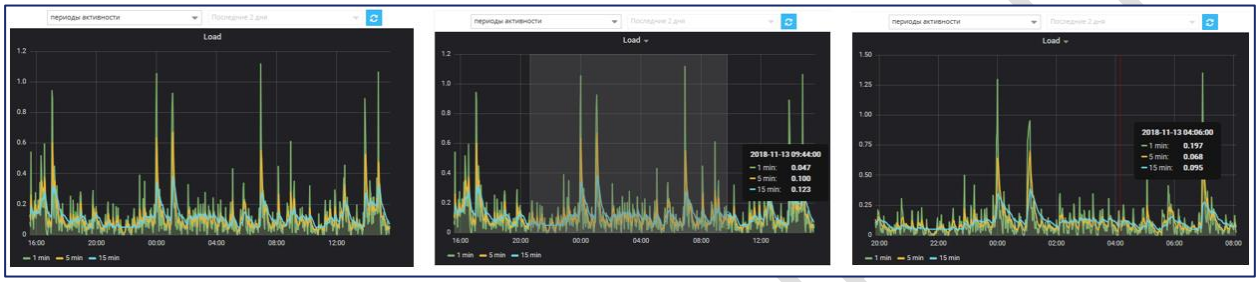


Рисунок 18 – Последовательность шагов при масштабировании части графика: первоначальный вид графика; выделенный фрагмент; итоговый вид графика после масштабирования)

5.2.4 Управление списком допустимых графиков в справочнике

Чтобы графики можно было использовать на рабочем столе (см. раздел 5.2.2), их следует добавить в список допустимых графиков Jet Detective – справочник **Все допустимые дашборды.** Этот справочник является объектом **Фабрики данных** и подчиняется всем правилам этого модуля.

Для работы с записями справочника **Все допустимые дашборды** откройте меню **Пользовательские объекты – Справочники** и в списке справочников перейдите к **Все допустимые дашборды.**

Просмотр, добавление, редактирование и удаление записей этого справочника описано в разделах 5.4.2–5.4.5.

Поля с параметрами справочника **Все допустимые дашборды** описаны в таблице 7.

Таблица 7 – Описание полей записи справочника **Все допустимые дашборды**

Поле	Описание
Название	Имя графика, которое будет отображаться на рабочем столе в раскрывающемся списке выбора графика
Адрес	Адрес созданного графика. Адрес следует копировать из параметров графика на вкладке Embed. При копировании необходимо удалить тег «iframe». **Пример адреса:** *<iframe src="http://xxx.xxxx.su:3000/xxxxxx-xxxxxx xxxxx xxxxxxxxxxx width="450" height="200" frameborder="0"></iframe>* **Пример адреса, после удаление тега «iframe»:** *http://xxx.xxxx.su:3000/xxxxxx-xxxxxx xxxxx xxxxxxxxxxx width="450" height="200" frameborder="0"*

Поле	Описание
Флаг **Зависит от времени**	Если **флаг установлен**, то для указанного графика будет доступен выбор периода, за который будут отображаться данные при настройке на рабочем столе (см. раздел 5.2.2). Одна шкала такого графика должна быть временно́й. Если **флаг снят**, то график от времени не зависит и для него будет недоступен выбор периода отображения при настройке на рабочем столе (см. раздел 5.2.2)

5.2.5 Управление списком допустимых периодов для графиков

Для управления списком допустимых периодов для графиков на рабочем столе предназначен справочник Jet Detective – **Все допустимые периоды для дашбордов.** Этот справочник является объектом **Фабрики данных** и подчиняется всем правилам этого модуля.

Для работы с записями справочника **Все допустимые периоды для дашбордов** откройте меню **Пользовательские объекты – Справочники** и в списке справочников перейдите к **Все допустимые периоды для дашбордов.**

Просмотр, добавление, редактирование и удаление записей этого справочника описано в разделах 5.4.2–5.4.5.

Поля с параметрами справочника **Все допустимые периоды для дашбордов** описаны в таблице 8.

Таблица 8 – Описание полей записи справочника **Все допустимые периоды для дашбордов**

Поле	Описание	Пример заполнения
Название	Имя периода, которое будет отображаться на рабочем столе в раскрывающемся списке выбора периода отображения графика	Период 2 дня
Начало периода	Формула определения начала периода. В формуле используются обозначения	now-2d
Конец периода	Формула определения конца периода. В формуле используются обозначения	now

Таблица 9 – Условные обозначения используемые при написании формулы начала и окончания периода в справочнике Все допустимые периоды для дашбордов

Условное обозначение	Описание
Now	Настоящий момент времени
M	Минуты
H	Часы
D	Дни
W	Недели
M	Месяцы
Y	Годы

5.3 УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

Инструмент управления инцидентами позволяет группировать инциденты по настроенным признакам. Таким образом, например, можно настроить формирование одного инцидента для одного клиента, вместо отдельных инцидентов по каждому из его событий, которые определены Jet Detective как аномалии.

Если в результате анализа события в политике необходимо сформировать инцидент (в настройках политики указано действие **Сформировать инцидент**), то проводится поиск настроенной группировки признаков инцидента для связки **Политика** – тип **События**:

- Если такая группировка найдена, то инцидент создаётся с учетом настроек этой группировки.
- Если такой группировки не найдено, то инцидент создаётся со значениями по умолчанию для группировки.
- Если в процессе добавления событий к инциденту (по параметру группировки), количество событий достигает 950 штук, то последующие события будут группироваться в новый инцидент.

При создании инцидента вручную (см. раздел 5.5.4) и добавлении события к инциденту (см. раздел 5.5.9.2.2) действует такая же логика.

5.3.1 Просмотр записи группировки инцидента

Чтобы посмотреть запись группировки инцидента:

1) Выберите пункт меню Инциденты – **Управление инцидентами**.

В рабочей области отобразится одна или несколько вкладок:

- **Управление инцидентами** – табличный список записей (Рисунок 19);
- Записи управлений инцидентами, открытые в этой сессии.

2) На вкладке со списком дважды щёлкните по строке записи

Экранная форма записи управления инцидентами откроется на отдельной вкладке (Рисунок 20).

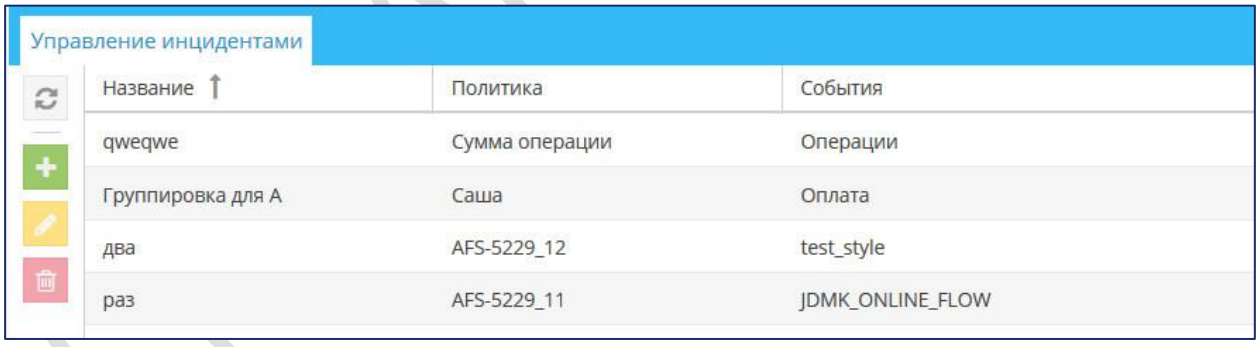


Рисунок 19 – Список записей управлений инцидентами

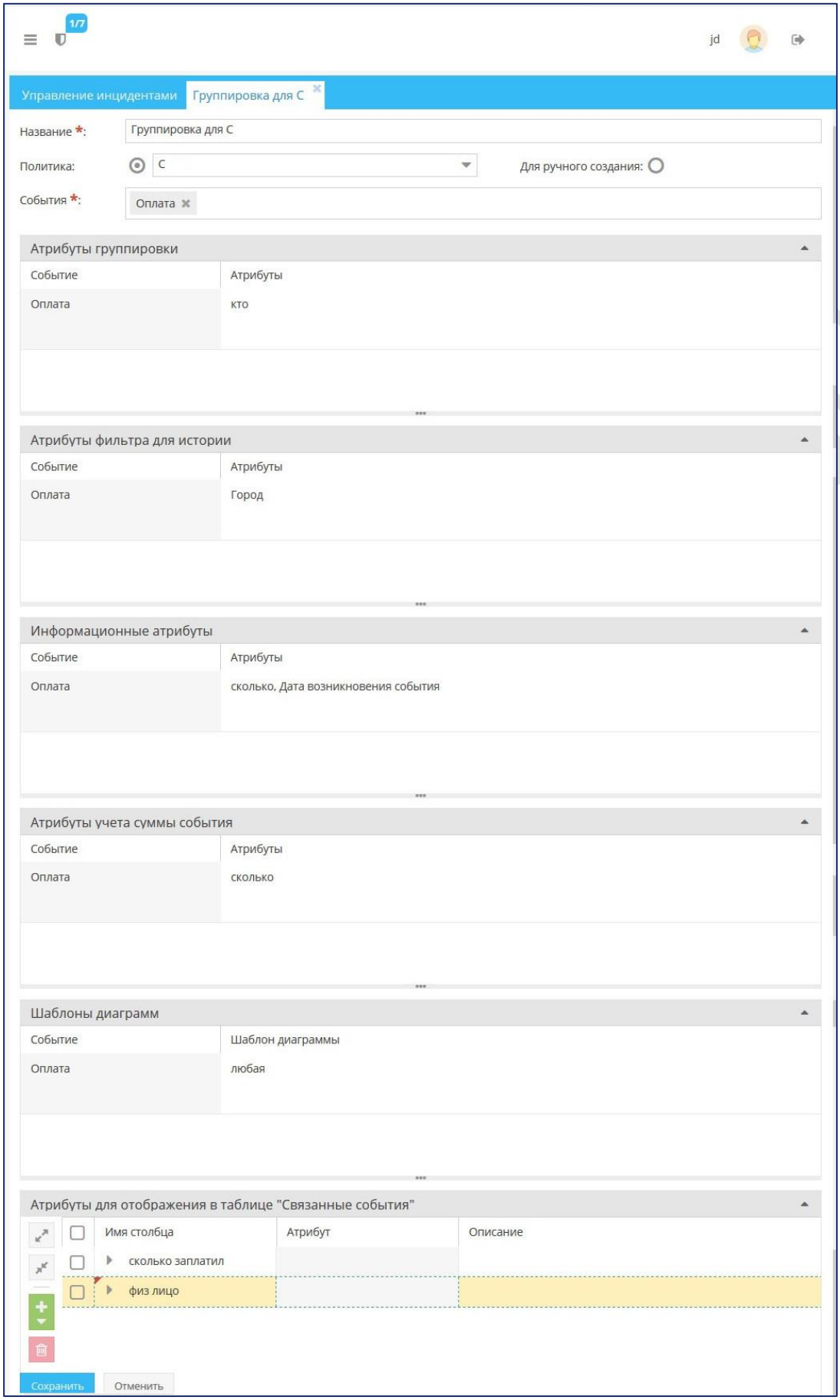


Рисунок 20 – Форма просмотра записи управления инцидентами

5.3.2 Создание записи управления инцидентами

Чтобы создать новую запись группировки:

1) На вкладке **Управление инцидентами** (Рисунок 19) нажмите кнопку **Добавить**  .

Откроется новая вкладка **Создание группировки инцидента** (Рисунок 21).

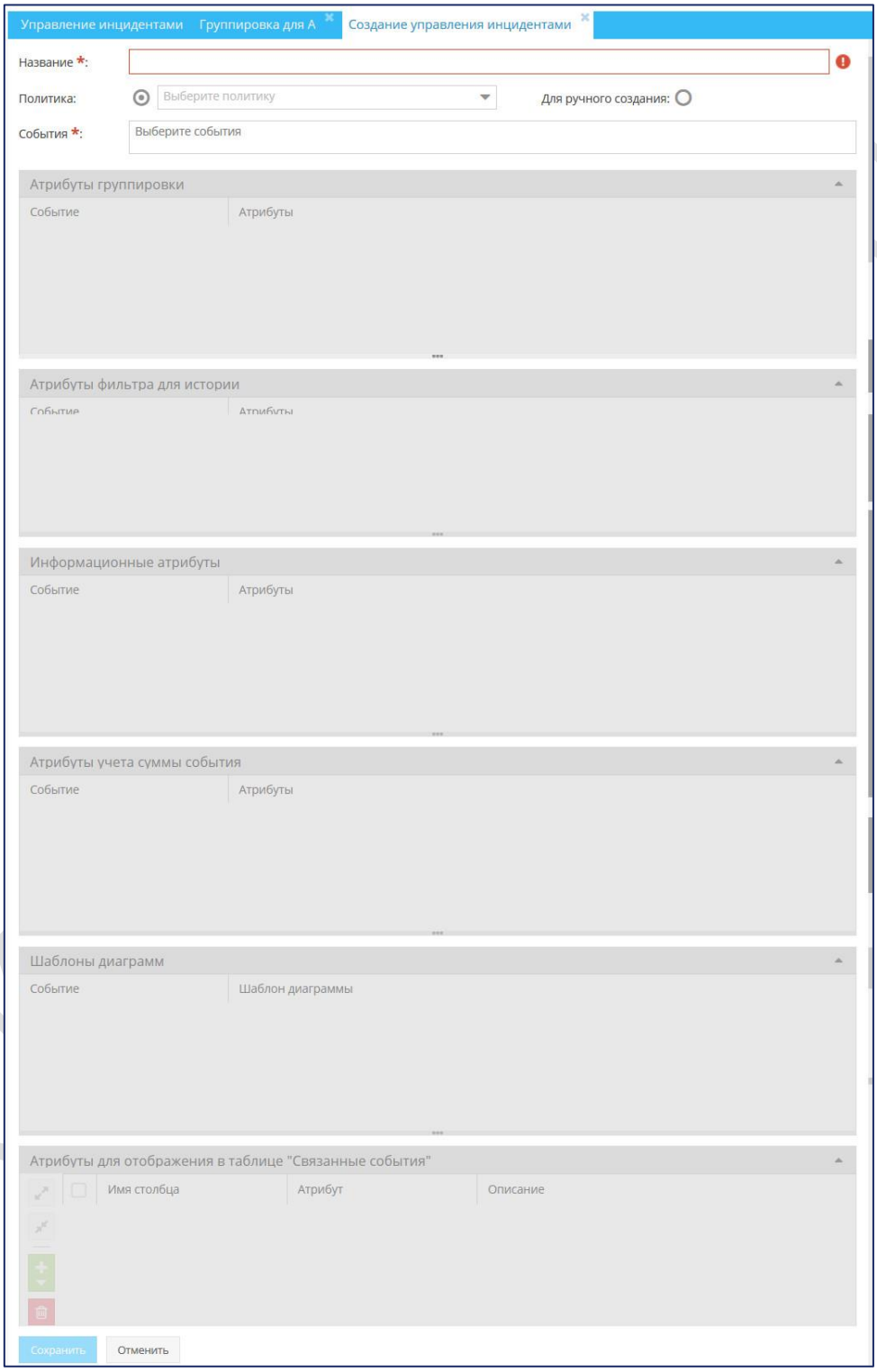


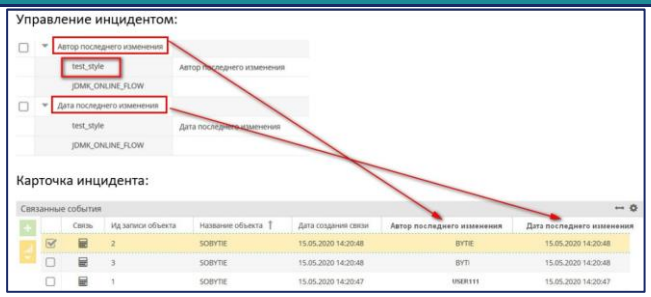
Рисунок 21 – Экранная форма вкладки **Создание управления инцидентами**

2) Заполните поля формы (Таблица 10).

Таблица 10 – Описание элементов вкладки **Создание управления инцидентами**

Элемент интерфейса	Описание элемента и его применения
Поле **Название**	Наименование управления инцидентами
Поле **Политика**	Выбор в раскрывающемся списке политики, для которой будет актуально создаваемое управление инцидентами. Поле недоступно для редактирования, если установлен флаг **Для ручного создания**
Флаг **Для ручного создания**	По умолчанию флаг снят. Если флаг установлен, то заданные параметры управления инцидентами будут использоваться при ручном создании инцидентов (см. раздел 5.5.4) и добавлении события в инцидент (см. раздел 5.5.9.2.2 и 5.5.9.4.1). Если **флаг снят**, то управление инцидентами будет использоваться при срабатывании политики, которая указана в поле **Политика**
Поле **События**	При ручном создании – выбор в раскрывающемся списке события, к которому будет применяться создаваемое управление инцидентами в результате срабатывания выбранной политики. При указании политики события указаны по умолчанию и недоступны для редактирования. Если указано несколько событий, то поля **Информационные атрибуты**, **Атрибуты группировки**, **Атрибуты учета суммы события** содержат блоки по каждому из событий
Поле **Атрибуты группировки**	Набор атрибутов выбранного события, которые позволяют группировать события и объединять в одном инциденте. Например, группировка по счету или по ИНН. События группируются в рамках одного инцидента до тех пор, пока он находится в состоянии **create** или **init**. Если в процессе добавления событий к инциденту по параметру группировки, количество событий достигает 950 штук, то последующие события будут группироваться в новый инцидент. Если параметр не заполнен, по умолчанию в роли атрибута связи используется атрибут **Идентификатор объекта**, т.е. для каждого аномального события создается отдельный инцидент. Поле не отображается, если установлен флаг **Для ручного создания**, т. к. в этом случае пользователь сам выбирает события, которые необходимо группировать в рамках одного инцидента. Выбранные атрибуты события добавляются в атрибут **group_object** инцидента в виде записи в формате JSON
Поле **Атрибуты учета суммы события**	Атрибут, который используется для подсчета суммы ущерба всего инцидента. Выбранные атрибуты события добавляются в атрибут **event_amount** инцидента в виде рассчитанного значения
Поле **Информационные атрибуты**	Набор атрибутов выбранного события, которые добавляются в карточку инцидента для информации. Если поле не заполнено, то никакие дополнительные данные в карточку инцидента не добавляются. Выбранные атрибуты события добавляются в атрибут **extra_info** инцидента в виде записи в формате JSON
Поле **Атрибуты для отображения в таблице «Связанные события»**	Параметры таблицы отвечают за то, какие атрибуты событий будут выводиться с блоке **Связанные события** на рабочем столе оператора (см. раздел 5.5.9.2). Функционал необходим для того, чтобы в одну таблицу выводить данные из разных типов событий. Указанные атрибуты будут добавляться в таблицу ENTITY_TO_ENTITY в виде JSON. Общая логика работа этой таблицы: ▪ в таблице задаются столбцы, которые необходимо добавить в таблицу **Связанных событий** (см. раздел 5.5.9.2); ▪ для каждого столбца задается имя, которое будет заголовкой для него в таблице **Связанных событий** (см. раздел 5.5.9.2); ▪ для каждого типа события указывается, какие атрибуты необходимо выводить в соответсвующих столбцах.

Элемент интерфейса	Описание элемента и его применения



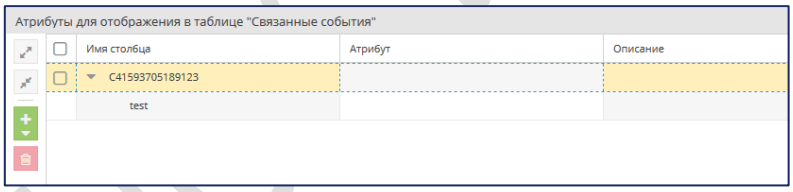
Добавление новых столбцов для таблицы **Связанные события**:

Нажмите кнопку Добавить  . Далее есть возможность добавить столбцы по одному или сразу несколько:

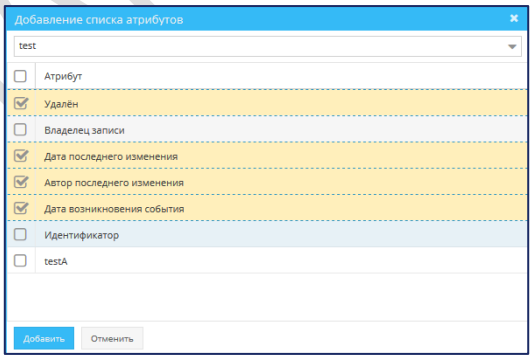
- Пункт **Столбец** – добавляет одну новую запись в таблицу для настройки. В столбце **Имя столбца** сформировано уникальное имя. Чтобы изменить его, кликните на имя и введите нужное значение.
- При необходимости укажите описание столбца в колонке **Описание**, в строке с именем столбца.

К строке с именем столбца автоматически добавляются дочерние строки с именами типов событий, которые указаны в поле **События.**

Для каждого типа события в столбце **Атрибут** выберите из раскрывающегося списка атрибут, который будет добавляться в новый столбец в таблице **Связанные события.**



- Пункт **Список столбцов –** в открывшемся модальном окне **Добавление списка атрибутов**, выберите тип события, из атрибутов которго необходимо сформировать столбцы.



Отметьте флагом те атрибуты, которые необходимо добавить, как столбцы в таблицу настройки. Нажмите **Добавить.**

В таблицу настройки для каждого выделенного атрибута добавится строка с **Именем столбца** равным наименованию атрибута. Для каждой строки с именем столбца добавятся дочение строки с типами событий, которые указаны в поле **События.**

У типа события, которое было выбрано в модальном окне, для каждого добавленного имени столбца в колонке Атрибут указан соответсвующий атрибут.

Далее колонки **Имя столбца**, **Атрибуты** и **Описание** редактируются так же, как и при добавлении одного столбца в таблицу.

Примечание: если атрибут не добавлен в таблицу настройки, значит в таблице уже есть имя столбца, которое совпадает с наименованием атрибута

3) Нажмите кнопку **Сохранить**.

Запись управления инцидентом создана.

5.3.3 Редактирование записи управления инцидентами

Чтобы отредактировать запись группировок:

1) Откройте экранную форму списка записей управления инцидентами (см. раздел 5.3.1).
2) На вкладке **Управление инцидентами** дважды щёлкните по строке, соответствующей записи.

Откроется вкладка выбранной записи. (Рисунок 19).

3) Измените значения параметров.
4) Нажмите кнопку **Сохранить**.

5.3.4 Удаление записи управления инцидентами

Чтобы удалить запись управления инцидентами:

1) Откройте экранную форму списка записей группировок инцидентов (см. раздел 5.3.1).
2) Выберите запись на вкладке **Управление инцидентами** (Рисунок 19).
3) Нажмите кнопку **Удалить**  .
4) Нажмите кнопку **Да** в появившемся запросе на удаление.

5.4 РАБОТА С ПОЛЬЗОВАТЕЛЬСКИМИ ОБЪЕКТАМИ

5.4.1 Общие сведения

Под работой с пользовательскими объектами понимается просмотр, редактирование и создание экземпляров объектов следующих типов:

- *Событие* – данные событий, поступающих из внешних систем. Примеры событий: платежная операция, вход пользователя в систему дистанционного банковского обслуживания.
- *Справочник* – справочные данные, которые используются для обогащения данных поступающих событий. Примеры справочников: справочник клиентов, справочник счетов, справочник сотрудников.
- *Агрегат* – данные, рассчитываемые в Jet Detective на основе данных поступающих событий. Например, можно создать агрегат по платежам, в котором будут храниться максимальные, минимальные и средние значения платежей того или иного вида.

Каждый объект характеризуется набором своих атрибутов. В интерфейсе пользователя объект отображается в виде таблицы, столбцы которой соответствуют атрибутам объекта, а строки – экземплярам объекта (Рисунок 22). Другими словами:

- экземпляр объекта с типом **Событие** – это запись о событии, имеющем определенный набор атрибутов;
- экземпляр объекта с типом **Агрегат** – это запись об агрегате, имеющем определенный набор атрибутов;

- экземпляр объекта с типом **Справочник** – это запись со справочными данными в определенном справочнике.

Для каждого объекта один из атрибутов выполняет функции уникального идентификатора записей. Значение идентификатора используется в интерфейсе пользователя в качестве названия вкладки, на которой отображается экранная форма объекта.

Настроить атрибут для идентификатора записи можно двумя способами:

- создать атрибут по умолчанию, который представляет собой уникальную последовательность чисел, поддерживаемую Jet Detective;
- указать любой атрибут объекта в качестве уникального идентификатора записи.

К одному типу объектов в общем случае относится множество объектов, сходных по характеру использования в Jet Detective, но отличающихся наборами атрибутов. Например, могут быть созданы объекты «платеж» и «перемещение материальных средств». Оба этих объекта относятся к типу **Событие**, но имеют разные наборы атрибутов.

Примечание. Состав атрибутов объекта определяется настройкой, реализованной в Jet Detective.

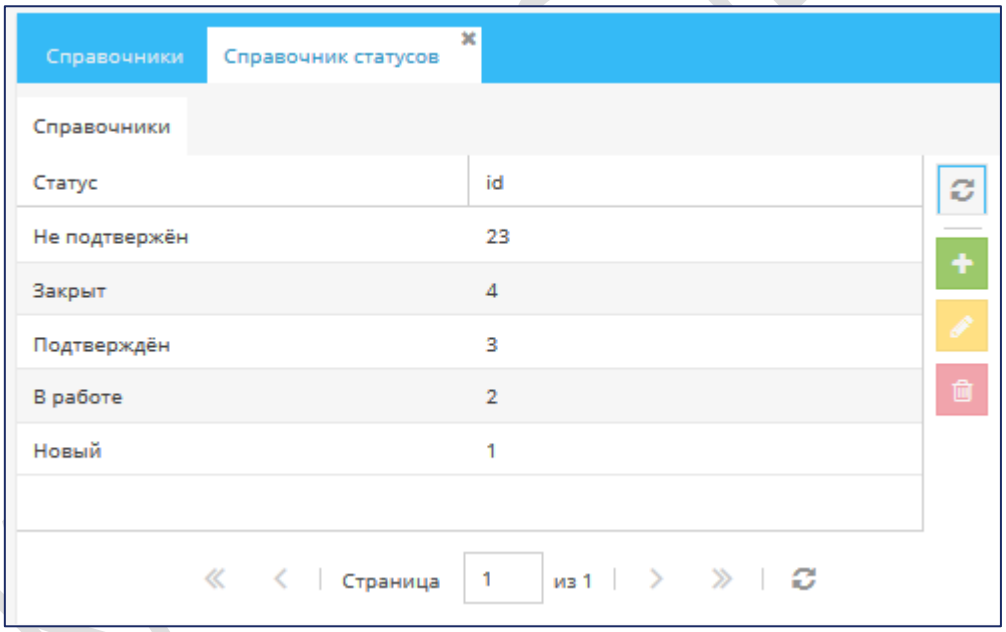


Рисунок 22 – Отображение объекта в виде таблицы

Ниже на примере справочника описаны процедуры создания, редактирования, удаления и просмотра записей объектов.

5.4.2 Просмотр записи объекта

Чтобы посмотреть запись справочника:

1) Выберите пункт меню П**ользовательские объекты** – **Справочники**.

В рабочей области отобразится одна или несколько вкладок:

- списка справочников (Рисунок 23);
- справочников, открытых в этой сессии.

2) На вкладке со списком дважды щёлкните по строке справочника.

Экранная форма справочника откроется на отдельной вкладке (Рисунок 24).

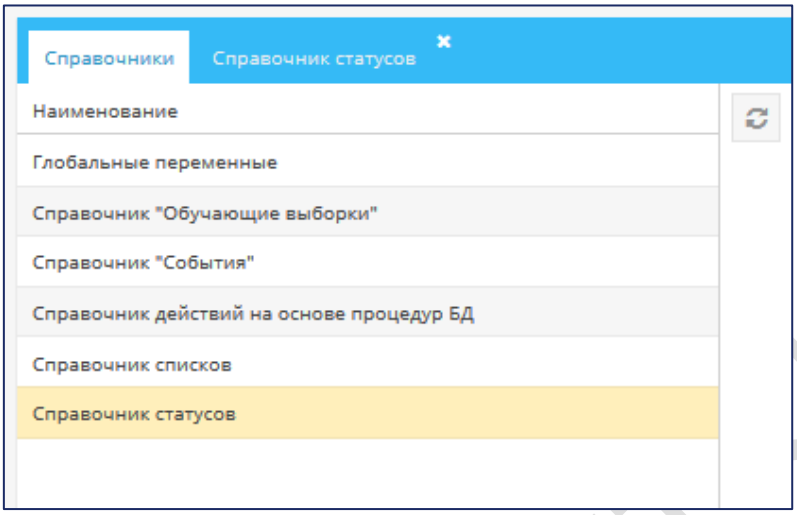


Рисунок 23 – Вкладка со списком справочников

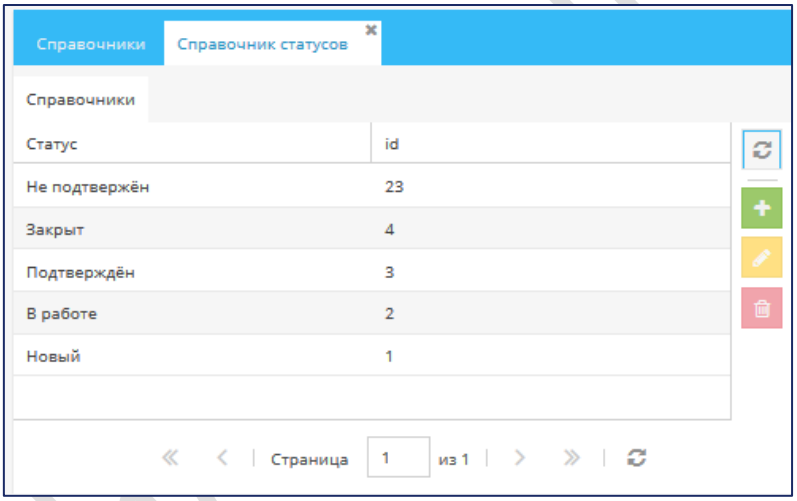


Рисунок 24 – Вкладка с экранной формой справочника

5.4.3 Добавление записи объекта

Чтобы добавить запись в справочник:

1) Откройте экранную форму справочника (см. раздел 5.4.2).

2) На вкладке **Справочники** нажмите кнопку **Добавить**  (Рисунок 24).

Откроется вкладка **Добавление новой записи** выбранного справочника (Рисунок 25).

3) Введите значения атрибутов.

Для атрибута **id** (уникальный идентификатор записи) автоматически установится вре́менное значение. Действительное значение присвоится автоматически после сохранения изменений.

4) Нажмите кнопку **Сохранить**.

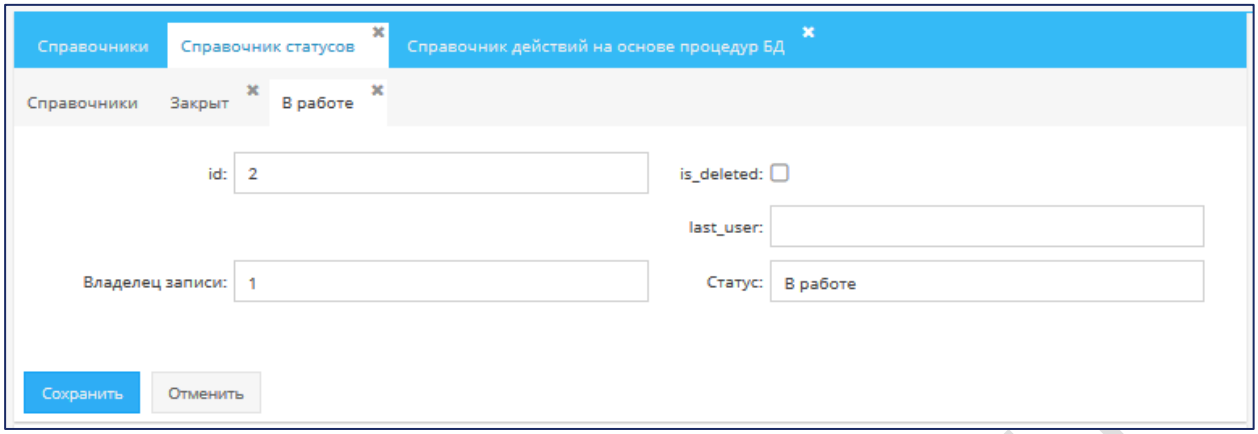


Рисунок 25 – Добавление записи в справочник

5.4.4 Редактирование записи объекта

Чтобы отредактировать запись в справочнике:

1) Откройте экранную форму справочника (см. раздел 5.4.2).
2) На вкладке **Справочники** дважды щёлкните по строке, соответствующей записи.

На экранной форме справочника откроется вкладка выбранной записи. (Рисунок 26). Поля, флажки и прочие элементы этой вкладки соответствуют атрибутам справочника.

3) Измените значения атрибутов.
4) Нажмите кнопку **Сохранить**.

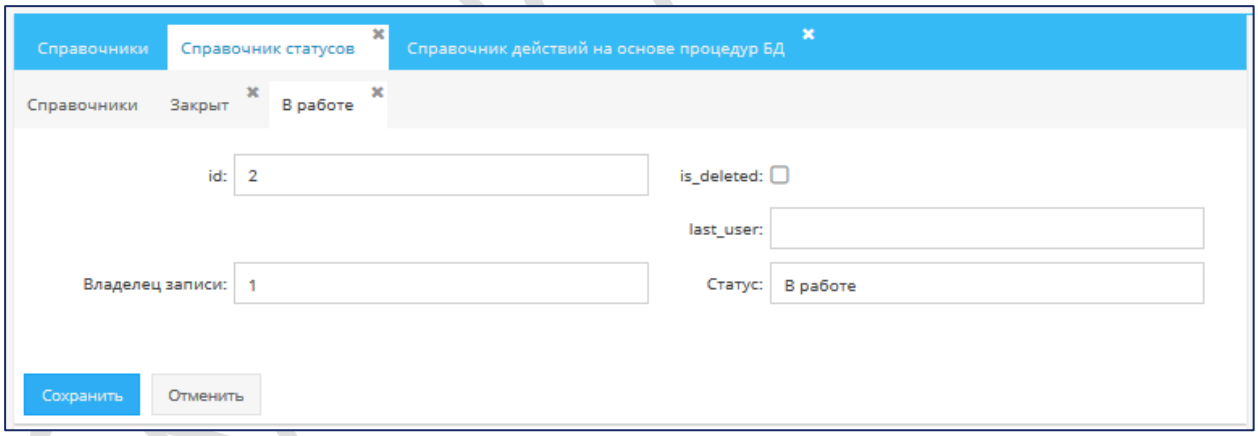


Рисунок 26 – Справочник статусов. Пример экранной формы записи **В работе**

5.4.5 Удаление записи объекта

Чтобы удалить запись из справочника:

1) Откройте экранную форму справочника (см. раздел 5.4.2).
2) Выберите запись на вкладке **Справочник**.
3) Нажмите кнопку **Удалить**  .
4) Нажмите кнопку **Да** в появившемся запросе на удаление.

5.5 РАБОЧИЙ СТОЛ ОПЕРАТОРА

5.5.1 Общие сведения

Выявленные аномалии фиксируются в Jet Detective в виде инцидентов. *Инцидент* – это информационная запись, которая:

- связана с событиями, в которых были выявлены аномалии;
- отображает информацию о сработавших политиках и правилах выявления;
- отображает информацию о статусе расследования и результатах расследования.

Jet Detective автоматически создаёт записи инцидентов, после чего они доступны для анализа на рабочем столе оператора. Первоначальный статус инцидента соответствует модели документооборота (см. раздел 6.4), которая привязана к объекту INCIDENT. Дальнейшие переходы статуса инцидента также подчиняются этой модели.

Рабочий стол оператора предназначен для отображения в одном окне информации по инцидентам. Такое представление данных позволяет пользователю за короткое время проанализировать информацию и принять решение по отработке инцидента.

Рабочий стол оператора состоит из двух частей (Рисунок 27):

- *Список инцидентов*. В списке инцидентов пользователь может:
  - изменить период обновления списка инцидентов (см. раздел 5.5.3);
  - создать инцидент в ручном режиме (см. раздел 5.5.4);
  - выбрать инциденты для работы (см. раздел 5.5.5);
  - назначить себе инцидент для анализа и принятия решения (см. раздел 5.5.6);
  - переназначить инцидент на другого пользователя(см. раздел 5.5.6);
  - сменить статус инцидента в соответствии с моделью документооборота инцидентов (см. раздел 5.5.7, подробнее о моделях документооборота описано в разделе 6.4);
  - посмотреть карточку инцидента (см. раздел 5.5.8).
- *Раздел детализации*. В разделе детализации пользователь может открыть для работы несколько вкладок одного из видов:
  - карточка инцидента (см. раздел 5.5.9);
  - форма события, связанного с инцидентом;
  - форма сработавшего правила, связанного с инцидентом;
  - форма любого объекта, которая открывается при переходе по ссылке соответствующего параметра в карточке инцидента.

При первом входе в Jet Detective на рабочем столе оператора по умолчанию применен быстрый фильтр **Мои в работе**.

Чтобы на рабочем столе оператора свернуть/развернуть список инцидентов, щёлкните по заголовку списка.

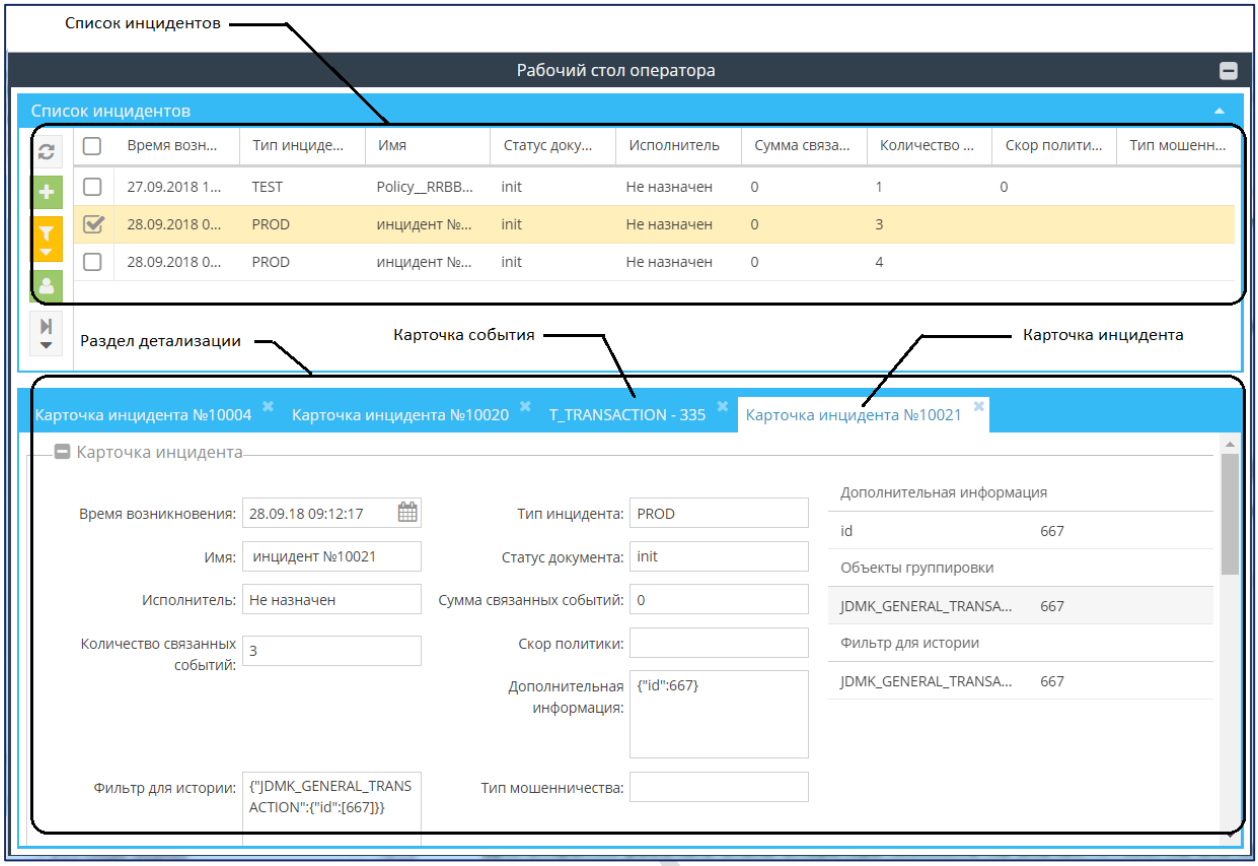


Рисунок 27 – Рабочий стол оператора

5.5.2 Открытие и закрытие рабочего стола оператора

Чтобы открыть рабочий стол оператора на вспомогательной панели, щёлкните по значку или индикатору 0/2. Первое число на индикаторе отображает количество незавершённых инцидентов, назначенных авторизованному пользователю, а второе – количество незавершённых инцидентов, для которых не назначены исполнители.

Чтобы закрыть рабочий стол оператора, нажмите кнопку , расположенную в правом верхнем углу окна рабочего стола, или нажмите клавишу Esc.

> *Примечание.* После закрытия окна состояние и данные рабочего стола оператора сохраняются. Не зависимо от дальнейших действий пользователя в любой момент (в рамках одной сессии) он может вернуться к рабочему столу оператора и продолжить работу с того места, на котором остановился.

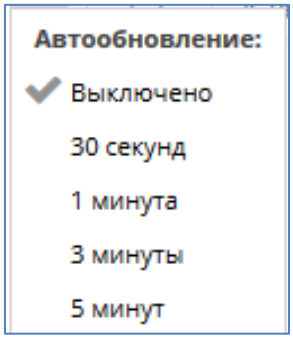
5.5.3 Изменение периода обновления списка инцидентов

Чтобы изменить период обновления или полностью отключить обновление списка инцидентов:

1) Откройте рабочий стол оператора (см. раздел 5.5.2).

2) В списке инцидентов нажмите стрелочку под кнопкой **Обновить** .

Откроется раскрывающийся список доступных периодов обновления. Активный периодов автообновления отмечен галочкой:



3) Выберите период автообновления списка инцидентов.

5.5.4 Создание инцидента вручную

Чтобы создать инцидент вручную:

1) Откройте рабочий стол оператора (см. раздел 5.5.2).

2) В списке инцидентов нажмите кнопку **Создать инцидент** .

Откроется форма **Добавление событий в инцидент** (Рисунок 28).

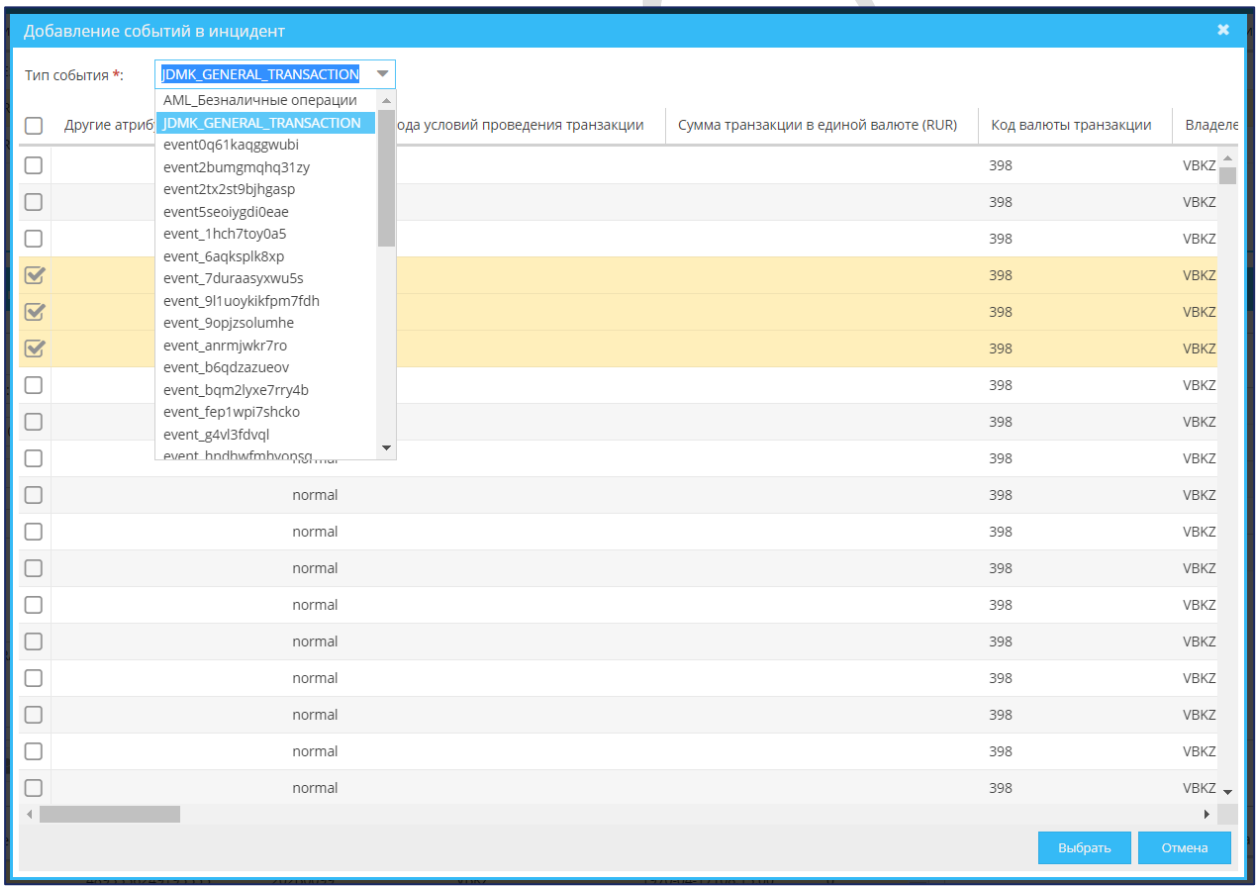


Рисунок 28 – Форма выбора событий для инцидента

3) В раскрывающемся списке выберите тип события.

   В форме **Добавление событий в инцидент** появится список объектов типа **Событие** из **Фабрики данных** Jet Detective. В списке отображаются только те объекты, которые хотя бы один раз применялись.

4) Установите флажки для тех событий, которые должны быть связаны с инцидентом.

5) Для отмены создания инцидента нажмите кнопку **Отмена**, или нажмите кнопку **Выбрать** для завершения создания инцидента.

Если была нажата кнопка **Выбрать**, в списке инцидентов появятся новый инцидент. В разделе детализации появится вкладка с карточкой созданного инцидента (Рисунок 29).

При создании инцидента вручную группировка инцидента работает по настроенному управлению инцидентами для выбранного типа события с флагом «для ручного создания».

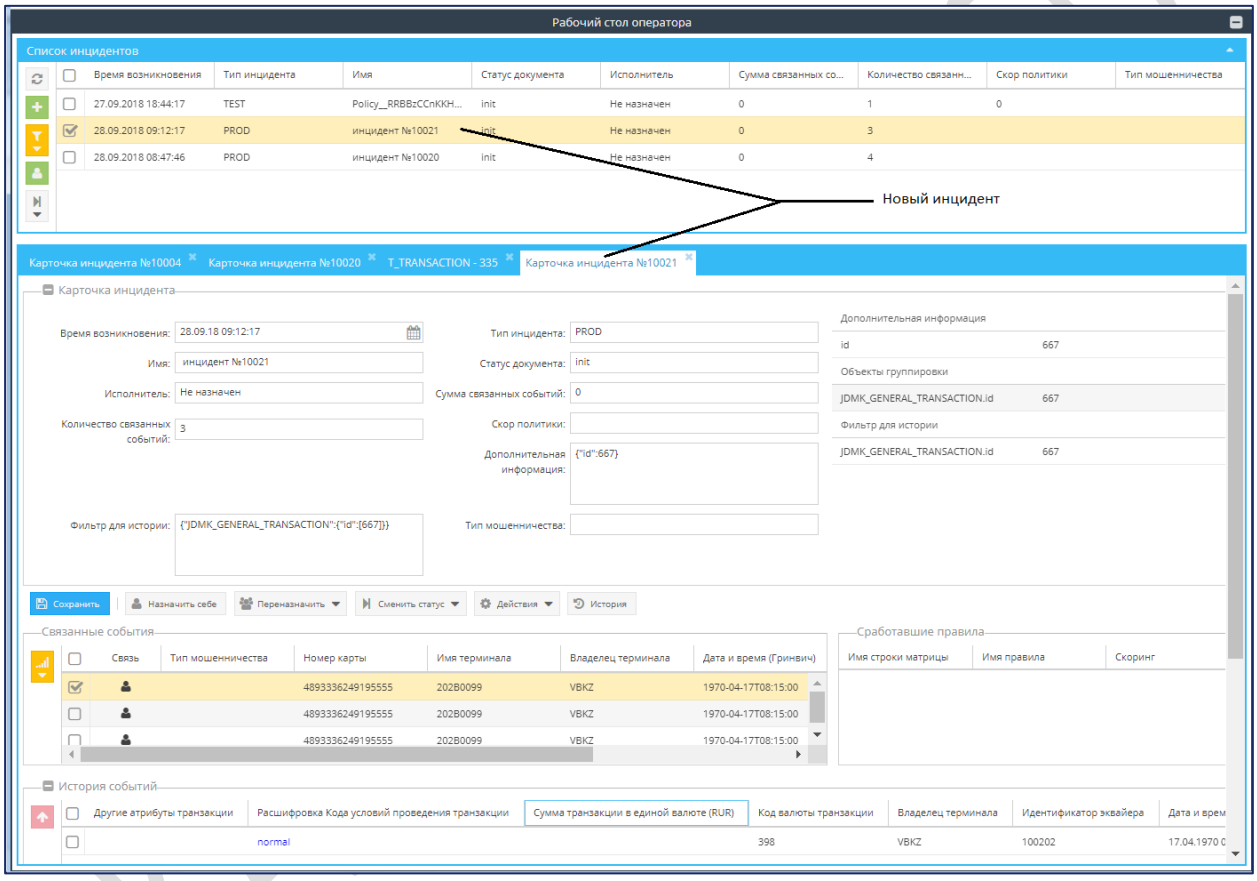


Рисунок 29 – Рабочий стол оператора. Новый инцидент

5.5.5 Быстрая фильтрация инцидентов

Состав колонок списка инцидентов аналогичен списку, приведённому на рисунке 27 в разделе 5.5.1. В заголовке списка инцидентов отображается, какой быстрый фильтр применен.

Чтобы выбрать инцидент:

1) Откройте рабочий стол оператора (см. раздел 5.5.2).

2) В списке инцидентов воспользуйтесь **Быстрым фильтром**: нажмите кнопку  (Рисунок 30).

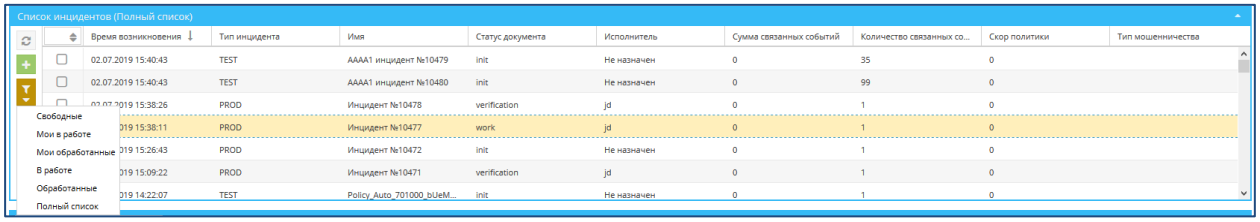


Рисунок 30 – Использование быстрого фильтра в списке инцидентов

Появится раскрывающееся меню для выбора следующих видов фильтров:

- **Мои открытые** – отображение незакрытых инцидентов, которые назначены пользователю, работающему с Jet Detective в настоящий момент (все статусы, кроме «Закрыт»)
- **В работе** – отображение незакрытых инцидентов (статус «В работе»), которые назначены пользователю, работающему с Jet Detective в настоящий момент;
- **Мои обработанные** – отображение закрытых инцидентов (статус «Закрыт»), которые назначены пользователю, работающему с Jet Detective в настоящий момент;
- **Свободные** – все инциденты в статусе **Начальный статус** и не назначенные ни одному пользователю;
- **Обработанные** – все инциденты в статусе **Закрыт;**
- **Полный список** – отображение полного списка инцидентов независимо от статуса и исполнителя;
- **Тестовые** – все тестовые инциденты (Тип инцидента = TEST).

Примечание: в фильтрах **Мои в работе**, **Мои обработанные**, **Свободные**, **В работе**, **Обработанные**, **Полный список** участвуют только инциденты на реальных данных (тип инцидента = PROD).

3) Выберите фильтр.

Список инцидентов изменится в соответствии с выбранным фильтром. В заголовке списка инцидентов отобразится название выбранного фильтра.

5.5.6 Назначение исполнителя инцидента

5.5.6.1 Назначение исполнителя из списка инцидентов

Чтобы назначить исполнителя инцидента:

1) Откройте рабочий стол оператора (см. раздел 5.5.2).
2) Установите флажки для инцидентов, которым необходимо назначить исполнителя (Рисунок 31).
3) В зависимости от того, какого пользователя необходимо назначить исполнителем для выбранных инцидентов, нажмите одну из следующих кнопок:

- **Назначить себе** или **Назначить себе и перейти в «Мои открытые»**  – назначение пользователя, работающего с Jet Detective в настоящий момент. При выборе **Назначить себе и перейти в «Мои открытые»** после назначения пользователя отобразится список инцидентов с

фильтром «Мои открытые». Выбранное значение этой кнопки сохранится на период рабочей сессии пользователя;

- **Назначить исполнителя** – назначение пользователя из раскрывающегося списка.

  Примечание: При назначении инцидента на себя, если статус инцидента был равен конечному статусу первого перехода модели документооборота (см. раздел 6.4), то перевод из этого статуса в следующий выполняется автоматически (при условии, что возможен только один переход по модели документооборота).

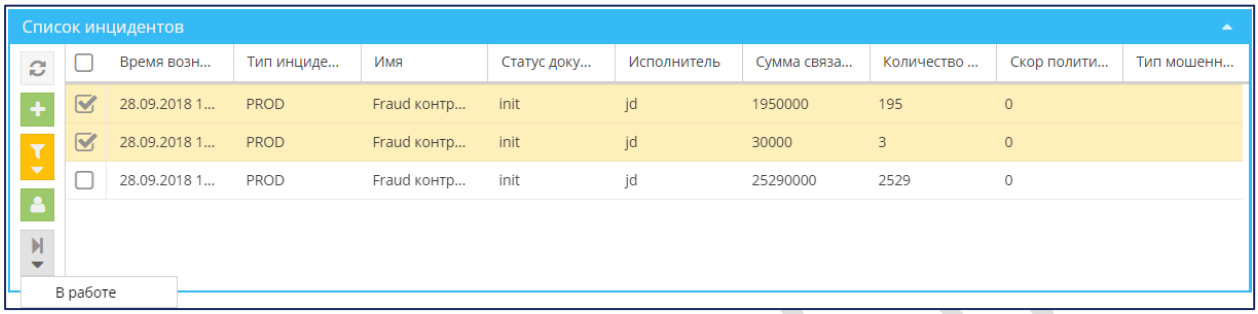


Рисунок 31 – Выбор нескольких инцидентов

5.5.6.2 Назначение исполнителя из карточки инцидента

Чтобы сменить назначить исполнителя из карточки инцидента:

1) Откройте карточку инцидента (см. раздел 5.5.8).
2) В зависимости от того, какого пользователя необходимо назначить исполнителем для инцидента, нажмите соответствующую кнопку:

- **Назначить себе** – назначение пользователя, работающего с Jet Detective в настоящий момент (кнопка будет недоступна, если исполнителем инцидента уже является работающий пользователь);

- **Переназначить** – назначение пользователя – выбор записи в раскрывающемся списке.

5.5.7 Смена статуса инцидентов

5.5.7.1 Смена статуса инцидента из списка инцидентов

Чтобы сменить статус инцидента из списка инцидентов:

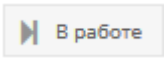
1) Откройте рабочий стол оператора (см. раздел 5.5.2).
2) Отметьте флажками инциденты с одинаковым статусом (Рисунок 31).
3) Нажмите кнопку **Сменить статус** и выберите статус для перехода.

Для выбранных инцидентов статус поменяется. Назначенный статус соответствует следующему доступному статусу по настроенной модели документооборота после статуса, который был у выбранных инцидентов.

5.5.7.2 Смена статуса инцидента из карточки инцидента

Чтобы сменить статус инцидента из карточки инцидента:

1) Откройте карточку инцидента, где исполнитель равен авторизованному пользователю (см. раздел 5.5.8).

2) Нажмите кнопку 

. Название кнопки соответствует следующему доступному статусу по настроенной модели документооборота после статуса, который был у выбранного инцидента.

Статус инцидента изменится, карточка инцидента и список инцидентов обновятся.

5.5.8 Открытие карточки инцидента

Чтобы открыть инцидент:

1) Откройте рабочий стол оператора (см. раздел 5.5.2).

2) Установите флаг в строке инцидента.

В разделе детализации появится вкладка с карточкой инцидента.

5.5.9 Карточка инцидента на рабочем столе оператора

Карточка инцидента располагается на вкладке раздела детализации рабочего стола оператора (см. рисунок 27 в разделе 5.5.1). Эта вкладка состоит из следующих блоков:

- Карточка инцидента (см. раздел 5.5.9.1);
- Связанные события (см. раздел 5.5.9.2);
- Сработавшие правила (см. раздел 5.5.9.3);
- История событий (см. раздел 5.5.9.4);
- История инцидентов (см. раздел 5.5.9.5).

5.5.9.1 Блок Карточка инцидента

Экранная форма этого блока приведена на рисунке 32.

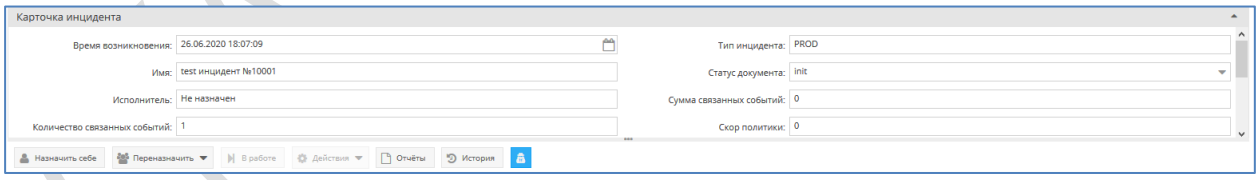


Рисунок 32 – Блок **Карточка инцидента**

В левой части блока расположены общие сведения об инциденте – их описание приведено в таблице 11. Набор полей и возможность их редактирования можно изменить при настройке объекта **INCIDENT** в **Фабрике данных** Jet Detective (см. раздел 6.2).

Таблица 11 – Описание полей вкладки **Карточка инцидента**

Поле	Описание
Количество связанных событий	Количество событий, входящих в инцидент (события из блока **Связанные события**)
Тип инцидента	Тип инцидента: PROD – инцидент сформирован на реальных данных; TEST – инцидент сформирован при тестировании
Статус документа	Статус инцидента в соответствии со связанной моделью документооборота
Скор политики	Балльная оценка выполнения политики выявления. Является суммой скорингового балла правил из блока **Сработавшие правила**
Исполнитель	Логин пользователя, ответственного за расследование инцидента
Фильтр связанных событий	Текстовое поле с описанием настроек, применённых при формировании инцидента – на основе группировки в **Управлении инцидентами** (см. раздел 5.3). Указанные критерии являются фильтром для событий и инцидентов в блоках **История событий** и **История инцидентов**
Время возникновения	Время создания инцидента
Сумма связанных событий	Сумма связанных с инцидентом событий. Суммирование выполняется по атрибутам, указанным в группировке в **Управлении инцидентами** (см. раздел 5.3)
Дополнительная информация	Текстовое поле, в котором отображается дополнительная информация, заданная в группировке в **Управлении инцидентами** (см. раздел 5.3)
Имя	Наименование инцидента

В правой части блока **Карточка инцидентов** представлена дополнительная информация, собранная в соответствии с настройкой группировки инцидентов. Подробная информация о настройке группировки инцидентов приведена в разделе 5.3. Если дополнительной информации по инциденту нет, то правая часть блока скрыта.

В нижней части блока **Карточка инцидентов** расположены кнопки:

- **Назначить себе**, **Переназначить** – описание работы этих кнопок приведено в разделе 5.5.6.2;
- **Сменить статус** – описание работы этих кнопок приведено в разделе 5.5.7.2;
- **Действие** – выбор дополнительного действия из справочника действий с параметром **Применение** равным «Рабочий стол оператора» (см. раздел 6.9.2);
- **Отчеты** – выбор отчета для формирования и способ его получения. Описание работы с функционалом формирования отчетов смотрите в разделе 6.8.2.5;
- **История** – отображение и ведение истории изменений инцидента (см. описание в разделе 5.5.9.1.2);
- **Открыть инструмент расследования –** открывается модальное окно с инструментом расследования (см. описание в разделе 5.5.9.1.4)

Чтобы свернуть/развернуть блок карточки инцидента, щёлкните по заголовку блока Карточка инцидента.

5.5.9.1.1 Выполнение действия

Чтобы выполнить дополнительное действие:

1) Нажмите кнопку **Действие**
2) Выберите из раскрывающегося списка действие, которое не обходимо выполнить
3) В открывшемся модальном окне (Рисунок 33) проверьте выбранное действие и заполните входные параметры для него (если требуется).

   Параметры действия заполняются автоматически, если они совпадают с атрибутом **Объект группировки** инцидента или (если не найден в **Объекте группировки**) по параметру **Имя** с атрибутами инцидента, с карточки которого вызвано действие.
4) Нажмите **Выполнить.** Действие будет выполняться в фоновом режиме.

   Результат выполнения действия отобразится во всплывающем сообщении.

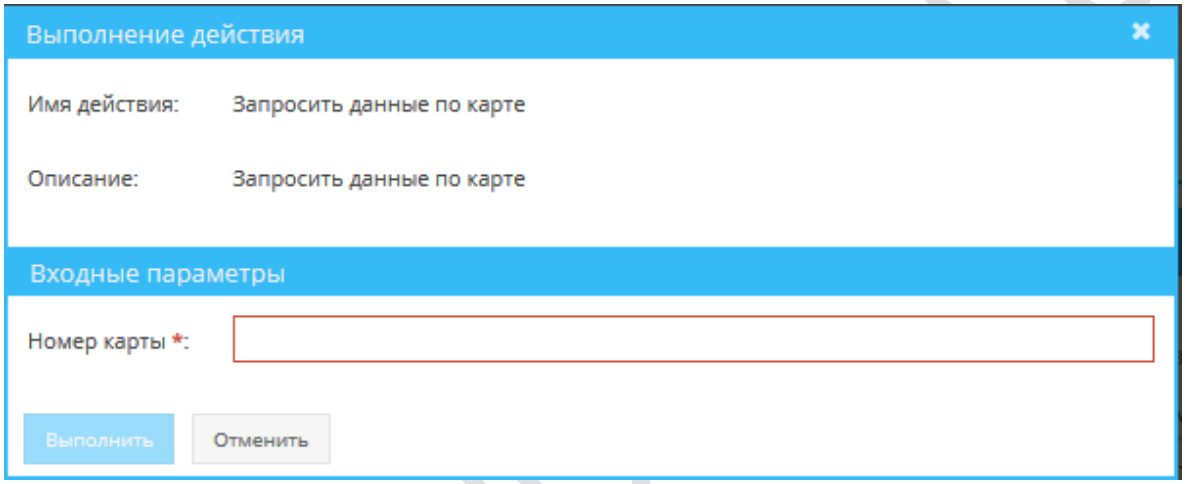


Рисунок 33 – Модальное окно выполнения действия

5.5.9.1.2 Просмотр истории изменений

На вкладке **История изменений** можно добавить комментарии к записи инцидента, а также посмотреть историю ранее оставленных комментариев и изменений инцидента (Рисунок 34).

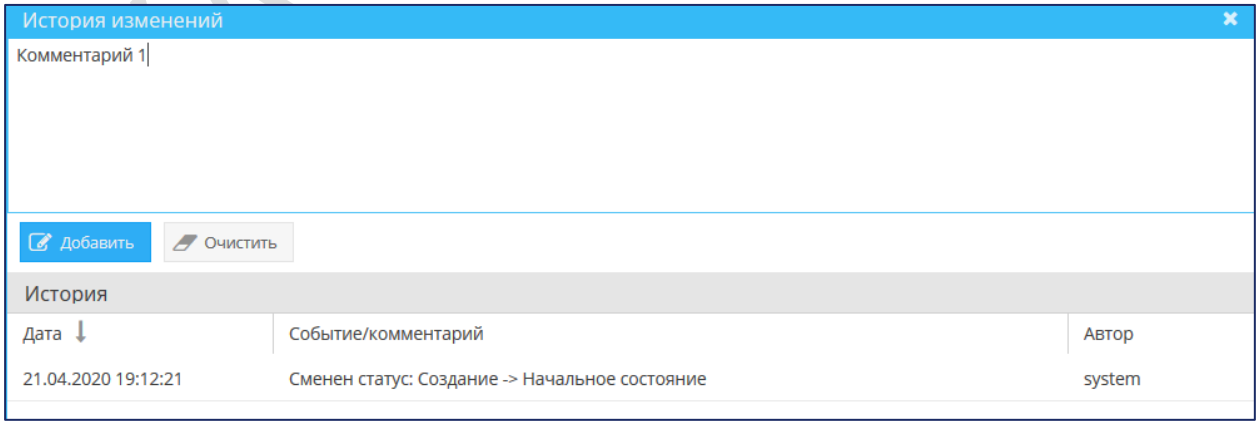


Рисунок 34 – Инциденты. Окно **История изменений**

Чтобы добавить новый комментарий:

1) Откройте запись инцидента (см. раздел 5.5.8).

2) Нажмите на кнопку **История** в блоке общей информации об инциденте.

Откроется модальное окно истории изменений (Рисунок 33).

3) Заполните поле **Комментарий**. Для очищения поля с комментарием нажмите кнопку **Очистить**.

4) Нажмите кнопку **Добавить.**

Комментарий будет добавлен в табличный список **История**.

5.5.9.1.3 Формирование отчёта

Чтобы сформировать отчёт:

1) Нажмите кнопку **Отчеты**.

2) В открывшемся модальном окне (Рисунок 35), выберите шаблон отчёта для формирования.

   2.1) Нажмите **Сформировать и отправить**, если необходимо быстрое формирование отчета без проверки параметров формирования. Входные параметры отчета так же автоматически подставляются – как и в случае нажатия на кнопку **Выбрать.** Если каких-то параметров для формирования отчета недостаточно, то формирование завершается ошибкой.

   2.2) Нажмите **Выбрать**, если необходимо перед формированием отчета проверить его параметры.

Откроется модальное окно, такое же как при формировании отчета через **Шаблоны отчетов** (см. раздел 6.8.2.5).

Поля формы входных параметров отчета заполняются автоматически, если имена входных параметров совпадают с атрибутами внутри **Объекта группировки, Фильтр для истории** или **Дополнительная информация** в блоке **Карточка инцидента** или совпадают с именами атрибутов инцидента.

3) Нажмите кнопку **Сформировать**.

Примечание. Отчёт формируется в фоновом режиме. После этого в зависимости от выбранной опции:

- файл отчёта сохранится в сетевой папке в соответствии с настройкой отчёта;
- отчёт отправится по электронной почте на адреса, указанные в настройке отчёта;
- слепок сформированного отчета сохранится в Запрошенных отчетах (см. раздел 6.8.3).

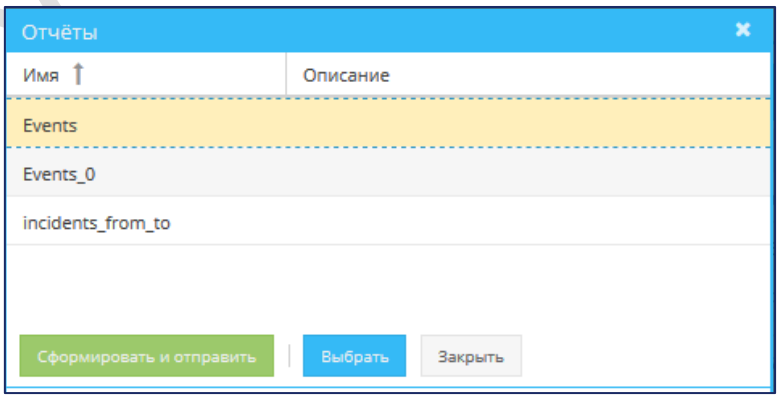


Рисунок 35 – Модальное окно формирования отчета из инцидента

5.5.9.1.4 Инструмент расследования

Инструмент находится в окне **Расследование**. Перейти к нему можно из **Карточки инцидента**.

Чтобы перейти к инструменту расследования со вкладки **Карточка инцидента** экранной формы записи инцидента:

1) Откройте карточку инцидента (см. раздел 5.5.8).

2) На вкладке **Карточка инцидента** нажмите кнопку **Открыть инструмент расследования** .

Откроется модальное окно с инструментом расследования.

В окне **Расследование** (Рисунок 36) отобразится:

- Панель кросс-канального расследования – графическое отображение событий;
- *Список событий* – табличный список событий;
- Панель информации о событии – атрибуты события.

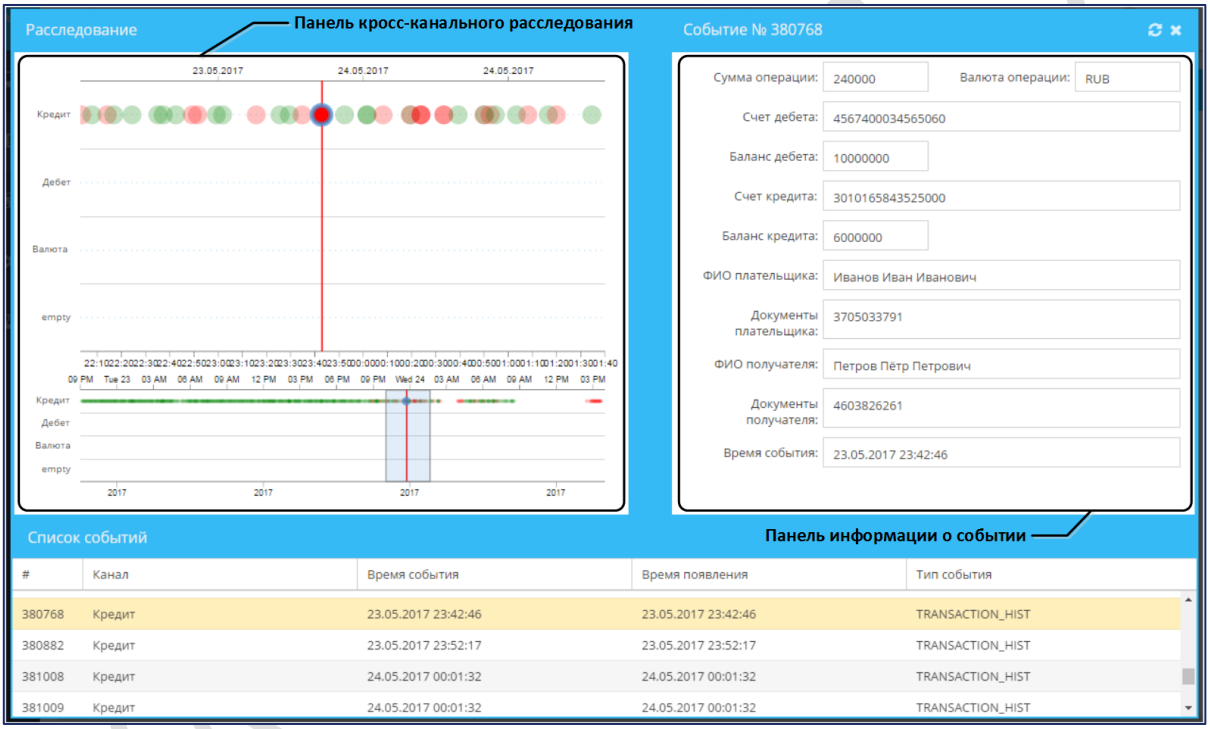


Рисунок 36 – Инциденты. Окно **Расследование**

Панель кросс-канального расследования состоит из двух частей (Рисунок 37):

- *График событий* – события за промежуток времени, входящие в область выделения на графике всех событий (находится в нижней части);
- График всех событий.

Графики имеют временны́е шкалы и шкалы каналов.

События отображаются кругами: неаномальные – зелёного цвета; аномальные – красного.

При открытии окна **Расследование** в начальной точке графиков находятся:

- *Область выделения* – полупрозрачный прямоугольник на графике всех событий. Обозначает промежуток времени, за который отображаются события на графике событий;
- *Указатель* – красная вертикальная линия на обоих графиках. Указывает на выбранное событие.

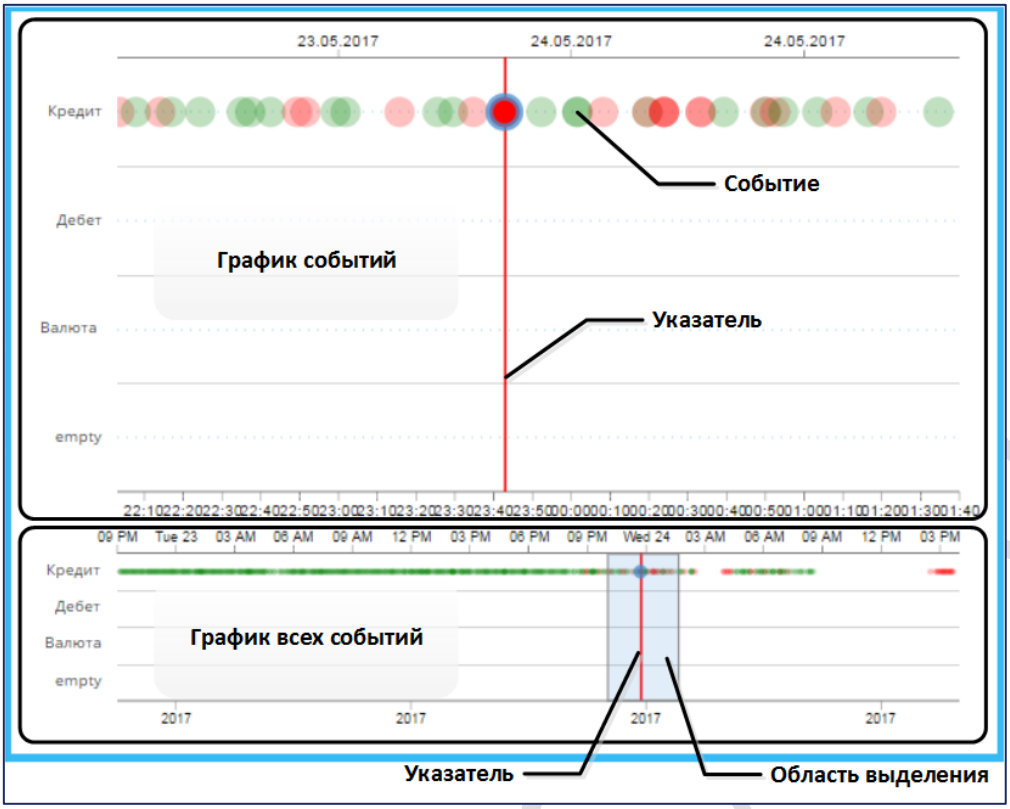


Рисунок 37 – Панель кросс-канального расследования

Область выделения можно перемещать в любое место графика всех событий. Для этого щёлкните по месту в графике, куда следует переместить область, или:

1) Наведите курсор на область выделения.
2) Когда курсор примет вид четырёхсторонней стрелки, с помощью мыши перетащите область выделения.

Можно изменить границы области выделения и тем самым изменить промежуток времени, за который события отображаются на графике событий. Для этого:

1) Наведите курсор на правую или левую границу области выделения.
2) Когда курсор примет вид двухсторонней стрелки, с помощью мыши потяните границу в сторону.

Чтобы выбрать и посмотреть событие щелкните по кругу на графике событий или по строке списка событий. При этом:

- указатель переместится на выбранное событие;
- в списке событий выделится строка события;
- на панели информации о событии отобразятся его атрибуты.

5.5.9.2 Блок Связанные события

Блок **Связанные события** представлен на рисунке 38.

События в индиденте группируются в соответствии с настройкой атрибутов группировки (см. раздел 5.3).

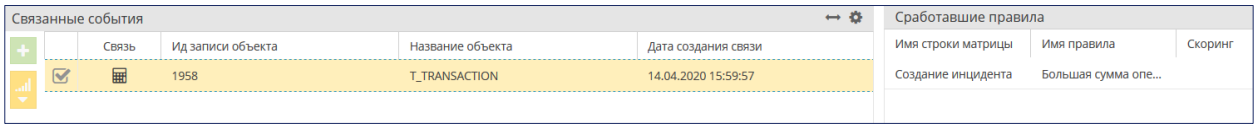


Рисунок 38 – Блок связанных событий

Группировка событий в один инцидент происходит по заданному параметру до тех пор, пока статус этого инцидента Create или Init.

В таблице связанных событий могут отображаться события разных типов.

В списке связанных событий имеются:

- Столбец с флагами, которые предназначены для пометки записей связанных событий.
- Столбец **Связь**:
- значок – индикатор событий, автоматически связанных с инцидентом;
- значок – индикатор событий, которые добавил пользователь;
- значок – индикатор событий, которые были добавлены в инцидент из «окна агрегата» при работе агрегативного правила (см. раздел 7.1.2.6)
- Столбцы с параметрами связи события и инцидента (таблица Entity_to_Entity). По этим столбцам доступна фильтрация и сортировка.
- Дополнительные столбцы с параметрами события, которые настраиваются через управление инцидентами (поле **Атрибуты для отображения в таблице Связанные события**, см. раздел 5.3.2). По этим столбцам доступна фильтрация и сортировка (только для типов данных: число, строка, дата и время, логический).

Для детального просмотра информации о событии дважды щёлкните по строке события. В отдельной вкладке раздела детализации откроется форма с информацией о событии. Пример окна приведен на рисунке 39.

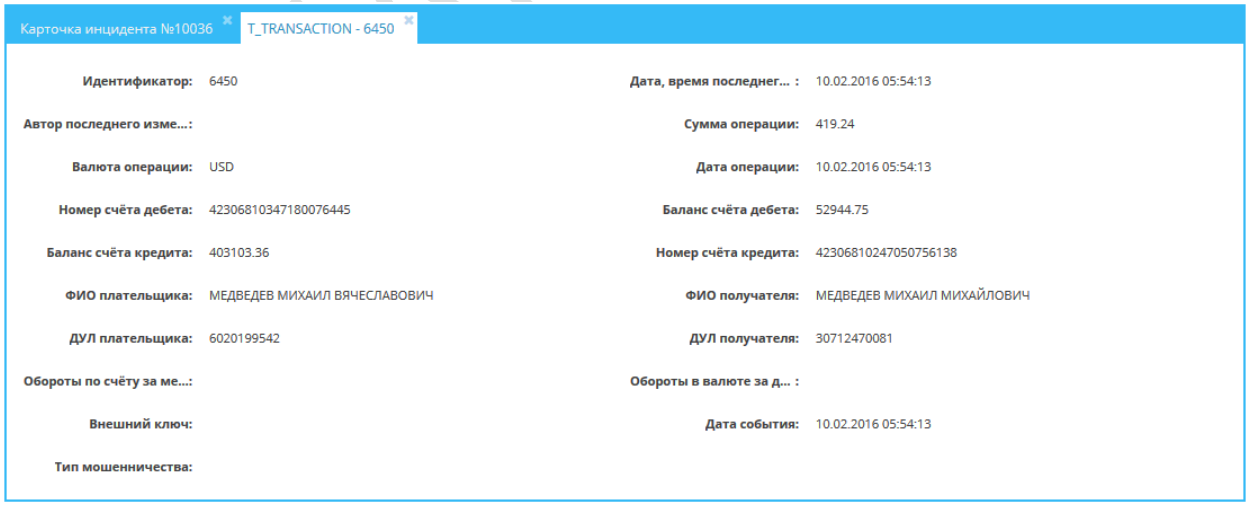


Рисунок 39 – Окно **Информация о событии**

5.5.9.2.1 Присвоение класса связанным с инцидентом событиям

Кнопка **Присвоить класс**  используется для присвоения выбранным событиям класса мошенничества. Для этого:

1) Выберите события в блоке связанные события – установите флажки.
2) В блоке связанных событий карточки инцидента нажмите кнопку **Присвоить класс**.
3) В раскрывающемся списке выберите нужный тип мошенничества. Список типов мошенничеству соответствует справочнику **Типы мошенничества** в **Фабрике данных** (см. раздел 6.2).

Для помеченных событий столбец **Тип мошенничества** заполнится кодом выбранного типа мошенничества.

5.5.9.2.2 Добавление события к инциденту

Чтобы добавить событие к существующему инциденту:

1) Откройте рабочий стол оператора (см. раздел 5.5.2);
2) Выберите инцидент в строке.
3) В списке связанных событий карточки инцидента нажмите кнопку **Добавить**  **.**
4) В открывшемся модальном окне выберите нужные события – так же, как при создании инцидента вручную (см. раздел 5.5.4). Список событий, доступных для выбора, ограничен атрибутом **Объект группировки** инцидента и типами связанных событий. Если, атрибут группировки в инциденте является идентификатором события, то список доступных для добавления событий ограничен только типами событий.
5) Нажмите **Выбрать**.

Выбранные события добавились в связанные события инцидента.

5.5.9.3 Блок Сработавшие правила

В правой части блока связанных событий расположен список сработавших правил, поля списка приведены в таблице 12.

Таблица 12 – Описание столбцов списка сработавших правил

Столбец	Описание
Имя строки матрицы	Имя строки матрицы срабатывания
Имя правила	Имя правила
Скоринг	Балльная оценка

В списке сработавших правил отображается все правила, которые привели к добавлению событий в инцидент. При выборе записи в блоке **Связанные события**, в блоке **Сработавшие правила** выделяются цветом те правила, которые сработали на выбранном событии.

Для просмотра описания правила дважды щёлкните по строке правила.

Откроется форма с параметрами настройки правила – на новой вкладке раздела детализации рабочего стола оператора.

5.5.9.4 Блок История событий

Блок **История событий** представлен на рисунке 40. Связь событий инцидента с историей событий устанавливается в соответствии со значением атрибутов связи – атрибута **Фильтр для истории** инцидента. Атрибут **Фильтр для истории** формируется согласно параметрам, настроенным в группировки в **Управлении инцидентов** (см. раздел 5.3)**.** На форме представленной на рисунке 40 атрибутом связи является Владелец терминала.

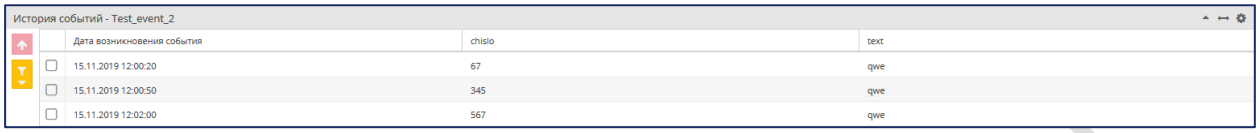


Рисунок 40 – Блок истории событий

История событий соответствует табличному представлению объекта, выбранного в таблице связанных событий (табличное представление объекта настраивается в **Фабрике данных** в параметре **Атрибуты для табличного представления** (см. раздел 6.2).

Для детального просмотра информации о событии дважды щёлкните по строке события.

На отдельной вкладке раздела детализации рабочего стола оператора откроется форма с информацией о событии.

Чтобы свернуть/развернуть блок истории событий, щёлкните по заголовку блока История событий.

5.5.9.4.1 Перемещение событий в блок Связанные события

Чтобы переместить событие из блока **История событий** в блок **Связанные события** карточки инцидента:

1) Откройте карточку инцидента (см. раздел 5.5.8).
2) В блоке **История событий** отметься флагом события, которые необходимо перенести в блок **Связанные события**.
3) Нажмите кнопку **Пометить как фрод** . В блоке связанных событий перемещённые пользователем события отмечены значком (см. раздел 5.5.9.2).

5.5.9.4.2 Изменение типа событий в блоке История событий

Чтобы в блоке История событий изменить тип отображаемого события:

1) Откройте карточку инцидента (см. раздел 5.5.8).
2) В блоке История событий нажмите кнопку Фильтр по типу события
3) В раскрывающемся списке выберите тип события, по которому необходимо отобразить историю.

Блок **История событий** обновится. История обновляется согласно фильтрам, сформированным в атрибуте **Фильтр для истории** инцидента.

Примечание: в раскрывающемся списке событий доступны только те типы событий, которые есть в блоке связанных событий.

5.5.9.5 *Блок История инцидентов*

Блок **История инцидентов** представлен на рисунке 41.

Рисунок 41 – Блок истории инцидентов

Блок истории инцидентов представляет собой список инцидентов, связанных с просматриваемым инцидентом. Связь определяется по атрибуту **Фильтр для истории.** Чтобы инцидент попал в историю к другому инциденту, необходимо, чтобы значение в атрибуте **Фильтр для истории** совпадало хотя бы для одного типа события.

Для детального просмотра информации по инциденту дважды щёлкните по строке инцидента.

В отдельной вкладке раздела детализации рабочего стола оператора откроется карточка инцидента.

Чтобы свернуть/развернуть блок истории инцидентов, щёлкните по заголовку блока История инцидентов.

6 АДМИНИСТРИРОВАНИЕ JET DETECTIVE

6.1 ОБЩИЕ ДАННЫЕ ДЛЯ АДМИНИСТРИРОВАНИЯ

Соответствие сервисов системы и функциональных модулей представлено в таблице 13.

Таблица 13 – Соответствие сервисов и модулей системы

Сервис	Модуль / Функция
config-service	**Конфигурация сервисов**
Jd-afs-workflow	**Модели документооборота**
Jd-aggragate	**Агрегаты**
Jd-archive-service	**Архивация**
Jd-auth	**Авторизация**
Jd-bom	**Фабрика данных**
Jd-cep-cooridnator	**Анализ событий**
Jd-cep-engine	**Анализ событий**
jd-changelog-service	Предоставляет информацию о версии установленных сервисов и изменениях в них
Jd-dictionary-service	**Поиск по спискам**
Jd-email-service	Отвечает за отправку email сообщений
Jd-enrichment-online	**Обогащение данных**
Jd-enrichment	**Обогащение данных**
Jd-etl-publisher	**Мониторинг ETL**
Jd-event-service	Сервис отвечает за взаимосвязь интерфейсной и сервисной частей
Jd-portation-service	**Импорт и экспорт правил**
Jd-report-service	**Отчеты**
Jd-scheduler-service	Отвечает за расписание запусков расчета агрегатов и формирования отчетов

6.1.1 Размещение компонентов Jet Detective

6.1.1.1 Типы хостов

Условно узлы, на которых исполняется Jet Detective, можно подразделить на следующие типы:

- **Worker host** – здесь размещаются основные сервисы, исполняющие бизнес-логику, которые реализуют интеграционное взаимодействие и взаимодействие сервисов, а также веб-сервер для взаимодействия с пользователями;
- **Management host** – здесь размещаются дополнительные сервисы, реализующие эксплуатационные задачи: аудит, мониторинг.
- **Database host** * – здесь размещаются СУБД, используемые системой для хранения оперативных данных

Примечание:

**- сервисы БД должны быть настроены и запущены до установки Jet Detective. Они могут не входить в контур эксплуатации системы, и поддерживаться собственными командами администрирования.*

Узлы могут сочетать в себе функции друг друга. Так, на одном узле могут быть развернуты одновременно и СУБД, и эксплуатационные и бизнес-компоненты. Однако в таком случае нельзя гарантировать отказоустойчивость и производительность системы.

6.1.1.2 Структура каталогов

Сервисы и компоненты Jet Detective развертываются на узлах типа worker и management. Они находятся в корневом каталоге приложения $JD_HOME – по умолчанию **/opt/afs.**

Все сервисы и компоненты на этих узлах управляются не привилегированным прикладным пользователем **afs**. Создание каталога, пользователя, назначение прав и первичная настройка выполняется установкой пакета **jd-config**.

После установки системы домашний каталог должен содержать следующие подкаталоги файлы:

- **jdctl –** скрипт запуска, остановки всех сервисов Jet Detective;
- **bin** – каталог. Содержит ссылки на скрипты запуска сервисов Jet Detective;
- **conf** – каталог. Содержит ссылки на базовые настройки и настройки логирования сервисов Jet Detective;
- **install** – каталог. Содержит набор конфигурационных файлов и утилит, которые используются сервисами Jet Detective при установке;
- **logs** – каталог. Содержит лог-файлы всех сервисов и компонентов Jet Detective;
- **data-integration** – каталог. Содержит компоненты ETL-инструментария;
- **reports** – каталог выгрузки отчётов, настроенный по умолчанию;
- **rollback** – технический каталог, необходимый для проведения процедуры отката БД при проведении обновлений;
- **www** – каталог. Содержит файлы необходимые для работы вебинтерфейса;
- **jd-*** – ряд каталогов. Содержат бинарные файлы и базовые настройки сервисов Jet Detective – полный список каталогов в «Карте портов и настроек по умолчанию»;
- .**kettle** – каталог. Содержит конфигурационные файлы для запуска ETL-сервера Carte;

6.2 ФАБРИКА ДАННЫХ

6.2.1 Общие сведения

Операции в Jet Detective выполняются с экземплярами *объектов* и их *атрибутами*. Объект является логическим представлением отдельной бизнес-сущности. Каждому объекту Jet Detective соответствует таблица базы данных (далее – *таблица объекта*), атрибуту объекта – одно или несколько полей этой таблицы, а каждому экземпляру объекта – отдельная запись в таблице.

Настройка объектов выполняется средствами модуля **Фабрика данных**, который оснащен конструктором объектов, основанном на концепции модели бизнес-объектов (Business Object Model). Объекты используются для формирования моделей данных.

Конструктор объектов позволяет создать модель данных для любой предметной области. Для полей таблиц объектов поддерживаются наиболее распространенные типы данных: строковый, числовой, логический, дата-время и др.

В Jet Detective реализована возможность создания таблиц объектов в различных системах хранения. Это могут быть как реляционные СУБД (например, Oracle).

Существуют следующие типы объектов:

- ***Событие***. Объекты этого типа используются для хранения данных о событиях, поступающих из внешних систем. Только для объектов этого типа можно настроить правила и политики выявления аномалий. Мастер-система для таких объектов – внешняя система.

  Объекты можно посмотреть в меню **Пользовательские объекты** – **События**.

- ***Справочник***. Справочные данные используются для обогащения поступающих событий. Возможна как загрузка из внешней системы, так и редактирование справочника через интерфейс Jet Detective.

  Объекты можно посмотреть в меню **Пользовательские объекты** – **Справочники**.

- ***Список***. Объекты, необходимые для формирования списков. В объектах этого типа реализована функция полнотекстового поиска на вхождение. Для полей, в которых требуется использовать эту функцию, при создании объекта должен быть указан индекс.

  Объекты можно посмотреть в меню **Настройки** – **Прочее** – **Объекты поиска.**

- ***Агрегат***. Объект для хранения рассчитанных значений агрегата, полученных по результатам работы **Модуля Агрегатов**. Значения этого объекта используются в правилах выявления, если выбран тип выражения **Агрегаты OFFLINE**. Правила расчета агрегата задаются при управлении агрегатом (см. раздел 7.2).

  Объекты можно посмотреть в меню **Пользовательские объекты** – **Агрегаты.**

- ***Уровень приложения***. Объекты этого типа относятся к служебным и встроены в Jet Detective. К объектам уровня приложения относятся инциденты, модели, связи между объектами. Добавленные объекты такого типа в интерфейсе посмотреть нельзя.

Настройка объекта заключается в создании и изменении конфигурации объекта. *Конфигурацией объекта* называется совокупность всех свойств объекта, таких как:

- атрибуты объекта;
- поля объекта;
- дополнительные опции объекта;
- модель документооборота.

После первого сохранения конфигурации:

- в базе данных создаётся её таблица;
- запись конфигурации появляется в списке объектов.

Таблица объекта создаётся в базе данных автоматически после подтверждения конфигурации (см. раздел 6.2.4).

После того как конфигурация объекта создана, необходимо настроить процессы заполнения этого объекта данными. Для этого используются ETL-процессы (см. раздел 6.10).

6.2.1.1 Статусы объектов

Объекты в модуле **Фабрика данных** имеют свой жизненный цикл. Статусы объектов представлены в таблице 14.

Таблица 14 – Статусы объектов в модуле **Фабрика данных**

Статус	Отображение в списке	Отображение в экранной форме объекта	Описание
Новый, готов к применению	Новый (зеленый)	 Новый, готов к применению	Все объекты создаются в этом статусе. Также в этом статусе создается первичная конфигурация объекта. Если для объекта установлен этот статус: ▪ конфигурация объекта валидна; ▪ объект ни разу не применен и нигде не виден; ▪ объект существует только в редакторе объектов
Новый, не готов к применению	Новый (красный)	 Новый, не готов к применению	Этот статус устанавливается, если: ▪ в объект в статусе «Новый, готов к применению» внесли корректировки; ▪ не выполнены условия проверки объекта на полноту и возможность применения. Если для объекта установлен этот статус: ▪ изменения сохранены, но объект в таком статусе применить нельзя; ▪ объект существует только в редакторе объектов
Изменен, готов к применению	Изменен (зеленый)	 Изменён, готов к применению	Этот статус устанавливается, если: ▪ объект уже был ранее применен, но в него внесли изменения; ▪ изменения валидны, объект можно применить. Если для объекта установлен этот статус: ▪ в Jet Detective используется в работе предыдущая версия объекта; ▪ все внесенные изменения сохранены и видны только в редакторе объектов
Изменен, не готов к применению	Изменен (красный)	 Изменён, не готов к применению	Этот статус устанавливается, если: ▪ объект уже был ранее применен, но в него внесли изменения; ▪ изменения не валидны, объект в таком статусе применить нельзя. Если для объекта установлен этот статус: ▪ в Jet Detective используется предыдущая версия объекта; ▪ Все внесенные изменения сохранены и видны только в редакторе объектов
Применён	Применен	 Применён	Если для объекта установлен этот статус: ▪ в Jet Detective для анализа и работы используется объект, соответствующий настроенному объекту в статусе «Применен»; ▪ в пользовательских объектах объект отображается с учетом изменений; ▪ созданы/изменены поля и атрибуты в базе данных

6.2.2 Просмотр объекта

Чтобы посмотреть объект:

1) Выберите пункт меню **Настройки** – **Объектная модель** – **Объекты**.

В рабочей области отобразится одна или несколько вкладок:

- **Список объектов** (Рисунок 42);
- конфигураций объектов, открытых в этой сессии.

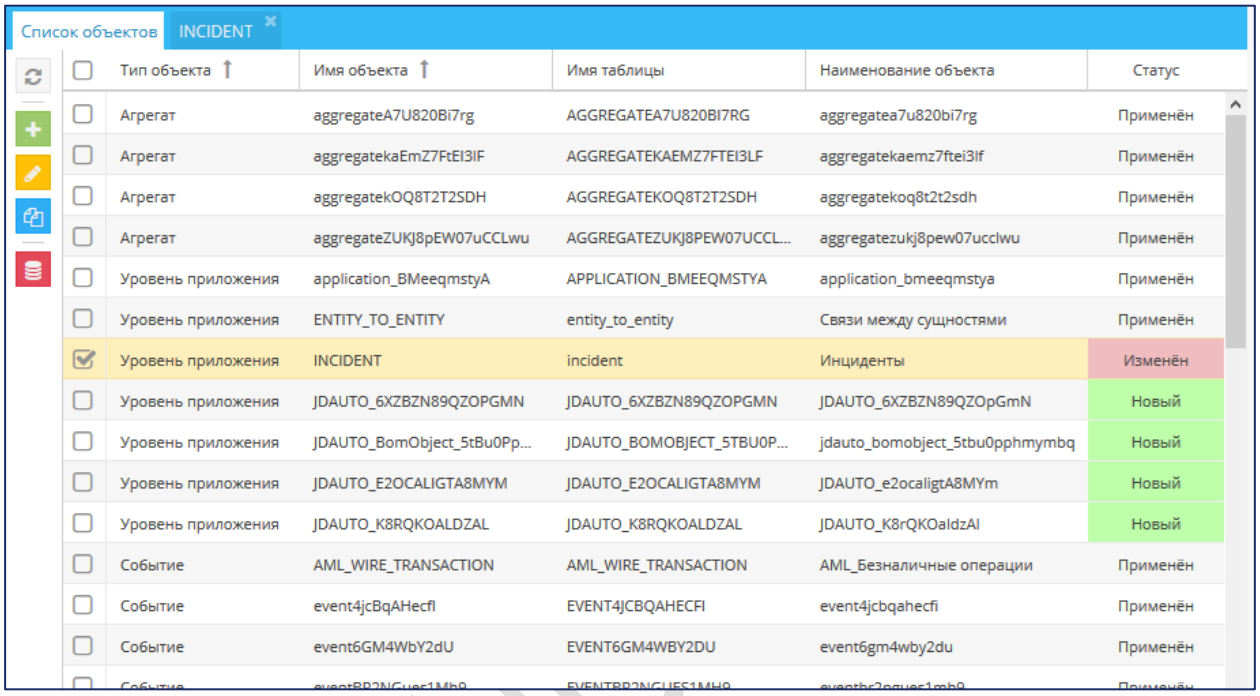


Рисунок 42 – Пример списка объектов

2) На вкладке **Список объектов** дважды щёлкните по строке объекта.

Экранная форма конфигурации объекта откроется на вкладке **Объект** (Рисунок 43).

Сведения о конфигурации объекта распределены по нескольким вкладкам (Таблица 15).

Таблица 15 – Краткое описание вкладок на экранной форме с конфигурацией объекта

Вкладка	Описание
Объект	Общие сведения об объекте
Атрибуты	Сведения об атрибутах объекта и инструменты для настройки атрибутов и соответствующих им полей таблицы объекта
Поля	Сведения о полях таблицы объекта и инструменты для настройки полей (см. раздел 6.2.3)
Дополнительные опции	Инструменты для настройки дополнительных опций объекта
Визуализация	Вкладка всегда недоступна для пользователя
Документооборот	Инструмент для связи объекта с моделью документооборота (см. раздел 6.4)

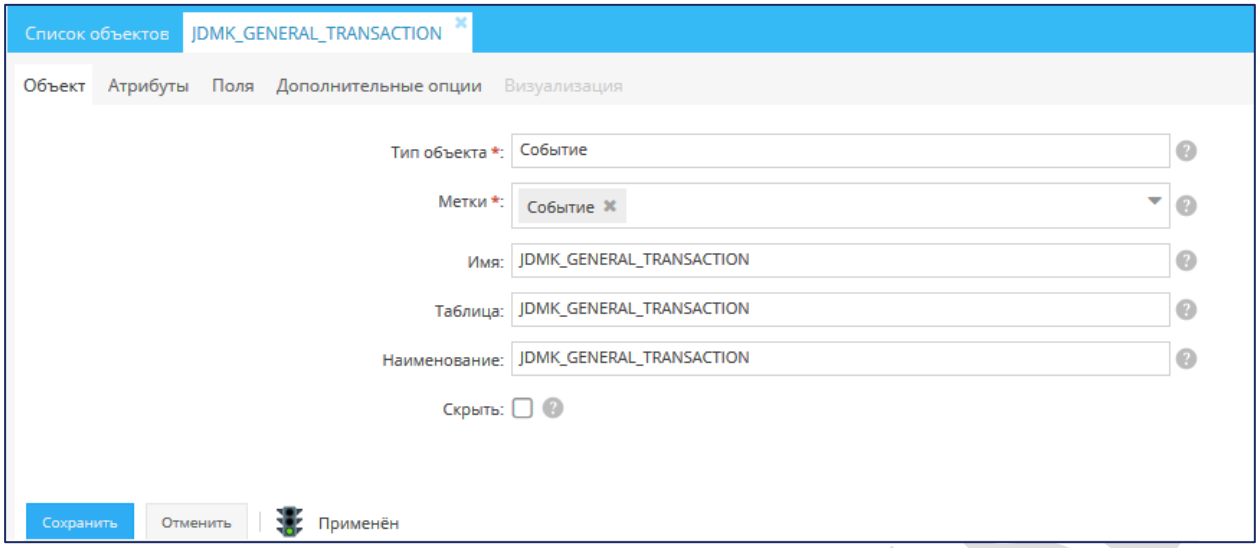


Рисунок 43 – Экранная форма конфигурации объекта. Вкладка **Объект**

6.2.3 Описание полей таблицы объекта

6.2.3.1 Общие сведения

Формирование таблицы объекта включает в себя следующие действия:

- составление описаний полей, которые необходимы для отображения в БД всех атрибутов объекта;
- установка для каждого атрибута соответствия между атрибутом и одним или несколькими описаниями полей.

Описание полей таблицы объекта отображается на вкладке **Поля** экранной формы с конфигурацией объекта (Таблица 16, Рисунок 44).

Таблица 16 – Свойства поля

Свойство	Описание
Имя	Имя поля
Используется в атрибутах	Соответствие поля тому или иному атрибуту объекта
Тип	Тип хранимых в поле данных
Размер	Максимальный размер хранимых в поле данных
Точность	Количество знаков после запятой, до которого следует округлять числовое значение
Список	Список возможных значений поля
По умолчанию	Значение поля по умолчанию
Индексы	Индексы полей. В частности, они необходимы для объектов с типом **Список** (см. описание типов в разделе 6.2.1). Полнотекстовый поиск по полю будет выполняться только при наличии индекса

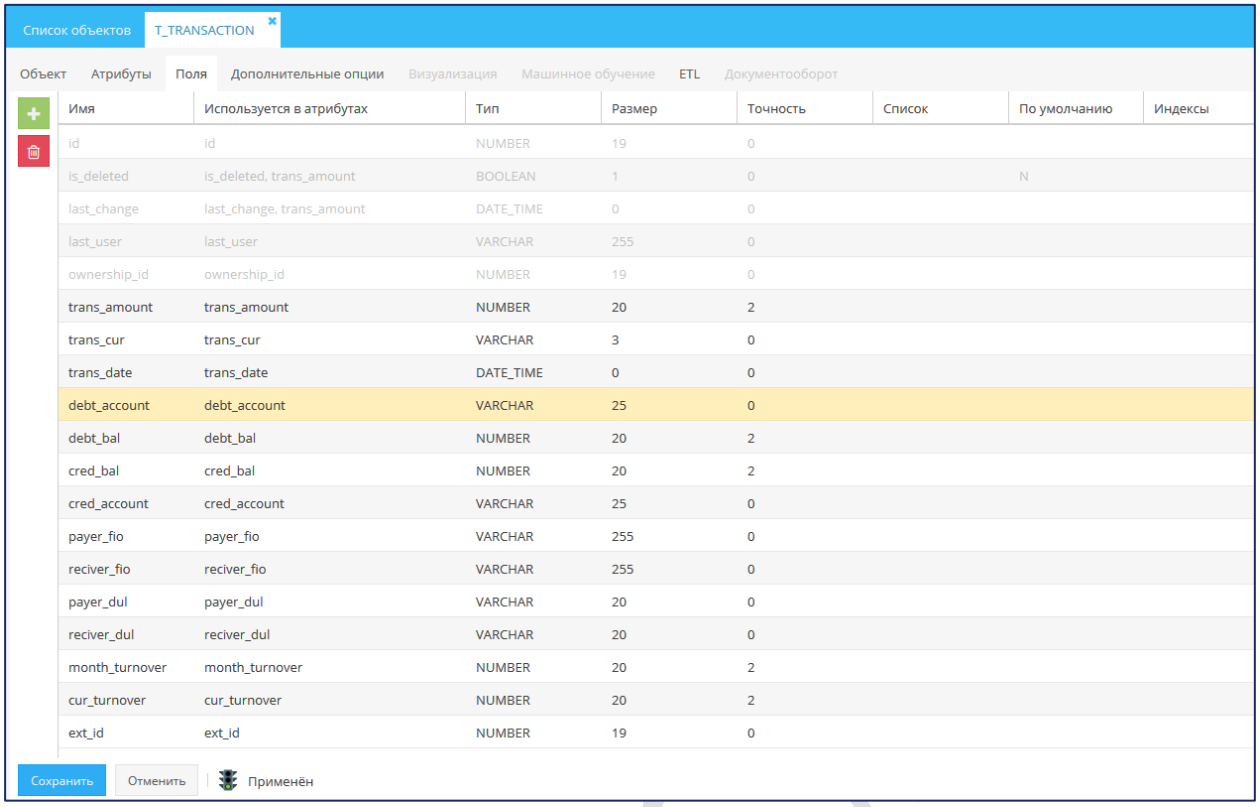


Рисунок 44 – Просмотр описания полей таблицы объекта

6.2.4 Подтверждение конфигурации объекта (создание таблицы в БД)

Подтверждение конфигурации объекта необходимо для того, чтобы все изменения, внесенные в объект, вступили в силу, а Jet Detective начала использовать именно эту конфигурацию объекта в работе.

Подтверждение конфигурации объекта доступно только для объектов в статусе «Новый, готов к применению» или «Изменён, готов к применению».

Для подтверждения конфигурации:

1) Откройте вкладку **Список объектов** (см. раздел 6.2.2).

1) Нажмите кнопку Применить изменения  .

2) Нажмите кнопку **Да** в появившемся запросе.

Если объект был в статусе «Новый, готов к применению», то по завершении процесса применения объекта будет создана таблица объекта в БД.

Если объект был в статусе «Изменён, готов к применению», то по завершении процесса применения изменений объекта, все внесенные изменения будут внесены в объект и таблицу БД.

6.2.5 Редактирование конфигурации объекта

Чтобы изменить конфигурацию объекта:

1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.2.2).

2) На вкладках экранной формы внесите изменения в конфигурацию объекта.

3) Нажмите кнопку **Сохранить**.

6.2.6 Управление табличным представлением и формой объектов

Настройки отображения табличных представлений и форм объектов могут сохраняться в профиле пользователя (см. раздел 4.5.1).

Чтобы изменить табличное представление конкретного объекта:

1) Откройте форму просмотра экземпляра объекта (см. раздел 5.4.2) или откройте форму создания экземпляра объекта (см. раздел 5.4.3).

2) Нажмите на кнопку **Настроить**  .

3) В открывшемся модальном окне с помощью флагов отметьте те колонки, которые должны быть в табличном представлении объекта. Перетаскивая строки в таблице, установите тот порядок атрибутов, в котором они должны отображаться в табличном представлении.

4) Нажмите кнопку **Применить**.

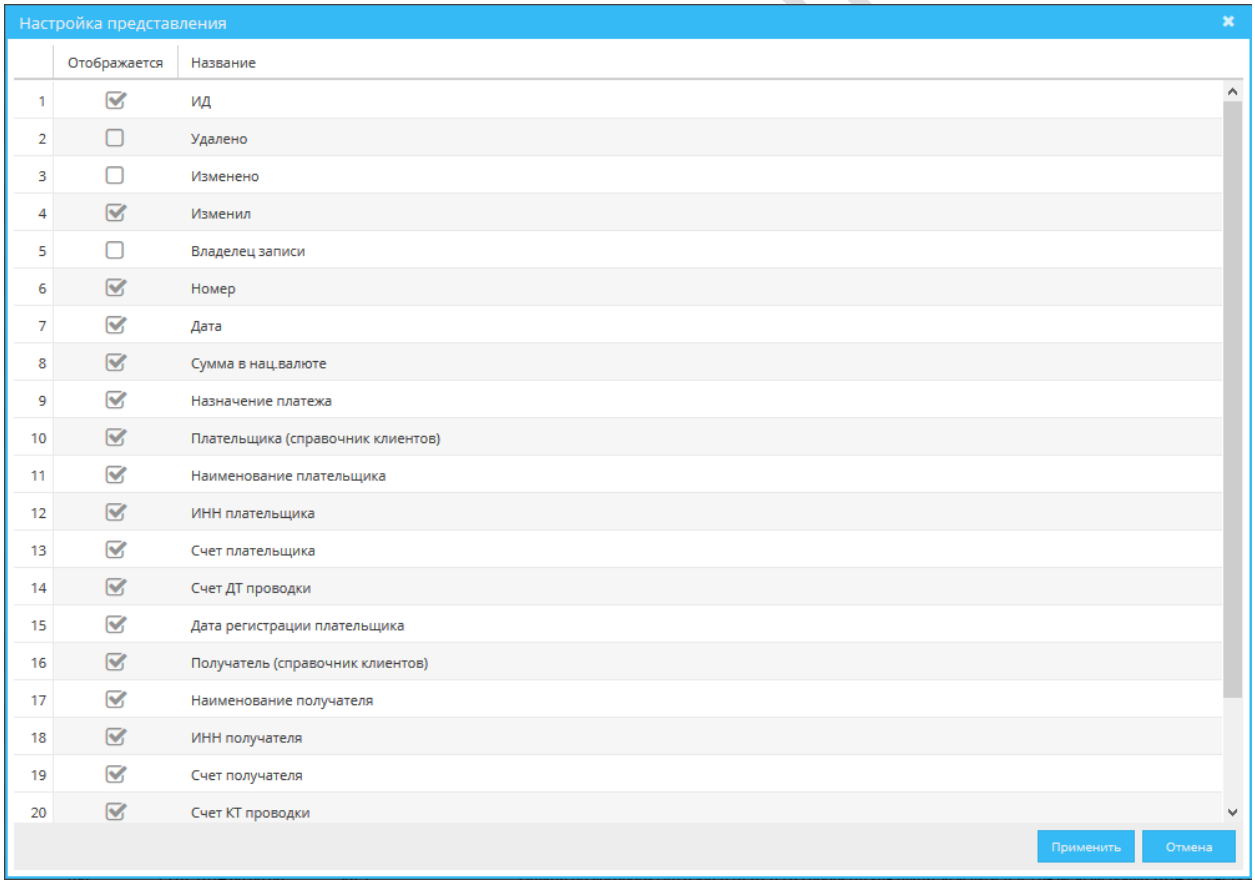


Рисунок 45 – Форма настройки табличного представления объекта

Чтобы изменить отображение полей на форме объекта:

1) Откройте форму просмотра экземпляра объекта (см. раздел 5.4.2) или откройте форму создания экземпляра объекта (см. раздел 5.4.3).

2) Нажмите на кнопку **Настроить**  .

3) В открывшемся модальном окне (Рисунок 45) с помощью флагов отметьте те атрибуты, которые должны быть на форме объекта. Перетаскивая строки в таблице, установите тот порядок атрибутов, в котором они должны отображаться на форме объекта.

4) Нажмите кнопку **Применить**.

6.3 ОБОГАЩЕНИЕ ДАННЫХ

6.3.1 Общие сведения

Для создания полноценного объекта в процессе загрузки данные проходят отдельный процесс, который служит для обогащения данных дополнительной информацией. При сохранении результатов обогащения в событие может быть сохранены только те параметры, которые заданы у события в настройках объекта в **Фабрике данных** (см. раздел 6.2).

Все параметры, полученные в процессе обогащения, но которых нет в метаданных объекта, будут исключены.

Возможны следующие типы обогащения:

- данными связанных справочников;
- данными пользовательского запроса;
- вычисляемыми данными.

Эти типы обогащения используются для выстраивания необходимой процедуры обогащения для каждого типа события.

Для управления процессом обогащения используется системные справочники:

- **ENRICHMENT_EXTERNAL_ACTION_TYPE** (Типы действий для процесса обогащения событий). В этом справочнике перечислены все доступные типы обогащения, которые могут использоваться для составления процесса обогащения. Подробнее о составе справочника см. в разделе 6.3.2.
- **ENRICHMENT_EXTERNAL_ACTION** (Действия процесса обогащения события). В этом справочнике происходит настройка самого процесса обогащения. Для каждого типа события прописывается индивидуальный процесс обогащения. Подробнее о настройке процесса обогащения см. в разделе 6.3.3.

Оба справочника являются стандартными объектами **Фабрики данных** и подчиняются правилам настройки, описанным в разделе 6.2.

6.3.2 Типы действий для процесса обогащения событий

Справочник **ENRICHMENT_EXTERNAL_ACTION_TYPE** имеет следующие доступные типы действий:

- **PERSIST** – Сохранить событие в базу данных (обязательный шаг);
- **OWNERSHIP_ID –** Задать объекту владение (обязательный шаг);
- **REF_ENRICH –** Обогатить ссылочные атрибуты;
- **CUSTOM_QUERY** – Выполнить SQL-запрос. Параметры подставляются через символ «?» (вопросительный знак). Возвращаемое значение должно иметь алиас в соответствии с именем поля;

- **SPEL_EVAL**- Выполнить выражение SPeL. Параметры подставляются через «#имя параметра»;
- **ROUTING –** Клонирует событие, завершая выполнение шагов обогащения первого экземпляра (target_topic зачищается).

Примечание. Изменение значений справочника ENRICHMENT_EXTERNAL_ACTION_TYPE (за исключением описания действий), а именно: добавление новых действий, удаление системных действий, изменение метаданных справочника, может привести к некорректной работе сервиса обогащения.

6.3.3 Настройка обогащения

Все описанные выше типы обогащения (см. раздел 6.3.2) и сохранения могут выполнятся как последовательно друг за другом, так и параллельно. Порядок выполнения определяется параметром «приоритет», который пользователь задает в справочнике **ENRICHMENT_EXTERNAL_ACTION**.

Задачи выполняются в порядке приоритета, при этом задачи с одинаковым приоритетом будут выполняться параллельно.

Чтобы настроить процесс обогащения события:

1) Откройте справочник **ENRICHMENT_EXTERNAL_ACTION –** Действия процесса обогащения события (см. раздел 5.4.2);
2) Добавьте в справочник шаг обогащения (см. раздел 5.4.3).
3) Заполните поля формы согласно логике, описанной в таблице:

ТАБЛ. 1 – Описание полей справочника действий процесса обогащения события

Поле	Обязательность	Описание
Тип действия (action_type_id)	Да	Ссылка на справочник действий для процесса обогащения **ENRICHMENT_EXTERNAL_ACTION_TYPE**
Описание (description)	Нет	Текстовое поле, для подробного описания шага обогащения
Имя объекта (event_name)	Да	Текстовое поле, где необходимо указать имя объекта (поле **Имя** на карточке объекта), для которого будет работать добавляемая строка обогащения
Выражение (expression)	Да, для типов действий **CUSTOM_QUERY** или **SPEL_EVAL** или **OWNERSHIP_ID**	Текстовое поле, где описывается либо SQL-запрос, либо SPeL-выражение. Используется только для типов действий **CUSTOM_QUERY** или **SPEL_EVAL** или **OWNERSHIP_ID.** ▪ **CUSTOM_QUERY:** Параметры, заданные в поле **params** задаются в запросе через "?" (знак вопроса). Параметры подставляются в запрос в том порядке, в котором они заданы в поле **params.** Возвращаемые значения должны иметь алиас, совпадающий с значениями, указанными в поле**result_fields** ▪ **SPEL_EVAL:** Параметры, заданные в поле **params,** задаются в запросе через "**#имя атрибута**". Выражение пишется без знаков равенства вначале строки.

Поле	Обязательность	Описание
		Пример: *#ref_attr*#sql_field (произведение двух атрибутов)* ▪ **OWNERSHIP_ID** – Параметры, заданные в поле **params.** Задаются в запросе через "?" (знак вопроса). *Примечание*. Выражения с типом **CUSTOM_QUERY** должны ОБЯЗАТЕЛЬНО заканчиваться знаком ";" (точка с запятой), если используется база данных Oracle
Параметры (params)	Да, для типов действий **CUSTOM_QUERY** или **SPEL_EVAL** или **OWNERSHIP_ID**	Текстовое поле, где задаются параметры, которые используются в запросах. Параметром могут выступать: ▪ атрибуты объекта **Фабрики данных**; ▪ атрибуты справочников, связанных с объектом **Фабрики данных** (задаются как «*имя ref-атрибута.имя атриубута справочника*»); ▪ константы Используются только для типов действий **CUSTOM_QUERY**, **SPEL_EVAL** и **OWNERSHIP_ID**. Параметры указываются без пробелов с разделителем "," (запятая)
Приоритет (priority)	Да	Приоритет начинается с 1. Приоритет 1 является наивысшим и выполняется первым. Действия выполняются в порядке следования номеров приоритета. При этом действия с одинаковым приоритетом будут выполняться параллельно
Имя полей (result_fields)	Да, для типов действий **CUSTOM_QUERY** или **SPEL_EVAL** или **OWNERSHIP_ID**	Текстовое поле, где указываются имена атрибутов события, в которые необходимо записать результат запроса/выражения. Атрибуты указываются без пробелов с разделителем "," (запятая). Для типа действия **OWNERSHIP_ID** должно быть указано поле **ownership_id.** Для изменения метаданных события в **Имени поля** (result_fields) можно использовать следующие значения (для sql нужно экранировать алиасы ""): ▪ ***metadata.break*** – прервать выполнение действий с событием и удалить его из списка обрабатываемых событий; ▪ ***metadata.topic*** – задать target_topic (можно указать несколько топиков через ','); ▪ ***metadata.name*** – изменить имя объекта, которому принадлежит событие. Создается новое событие со своими шагами обогащения. ▪ ***metadata.date*** – изменить даты события (event_date)

4) Повторяйте действия пунктов 2 и 3 до тех пор, пока не добавите все необходимые шаги обогащения события.

6.4 МОДЕЛИ ДОКУМЕНТООБОРОТА

Модель документооборота – это последовательность доступных для объекта переходов между статусами, где для каждого перехода можно задать набор выполняемых действий и логику определения ответственного лица для объекта после перехода.

6.4.1 Просмотр модели документооборота

Чтобы просмотреть настроенную модель документооборота:

1) Выберите пункт меню **Настройки** – **Объектная модель** – **Модели документооборота**.

В рабочей области отобразится одна или несколько вкладок:

- **Список моделей** (Рисунок 46);
- вкладки модели документооборота, открытые в этой сессии.

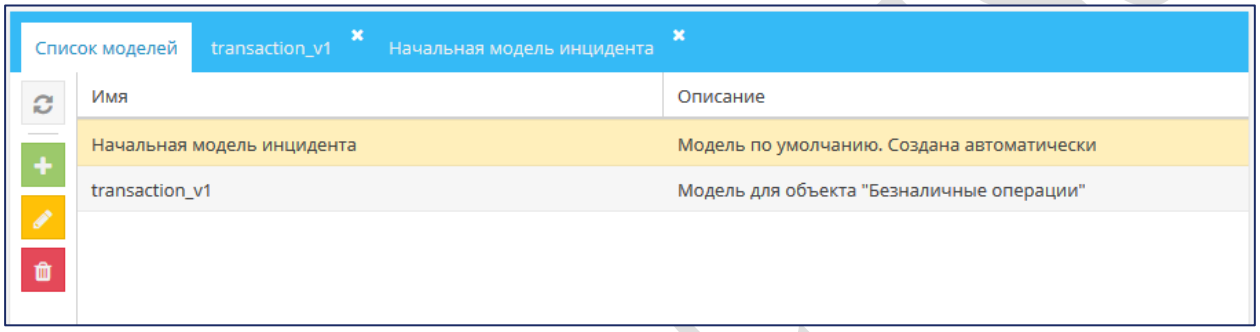


Рисунок 46 – Список моделей документооборота

2) На вкладке **Список моделей** дважды щёлкните по строке модели.

Экранная форма модели документооборота откроется на вкладке с наименование этой модели (Рисунок 47).

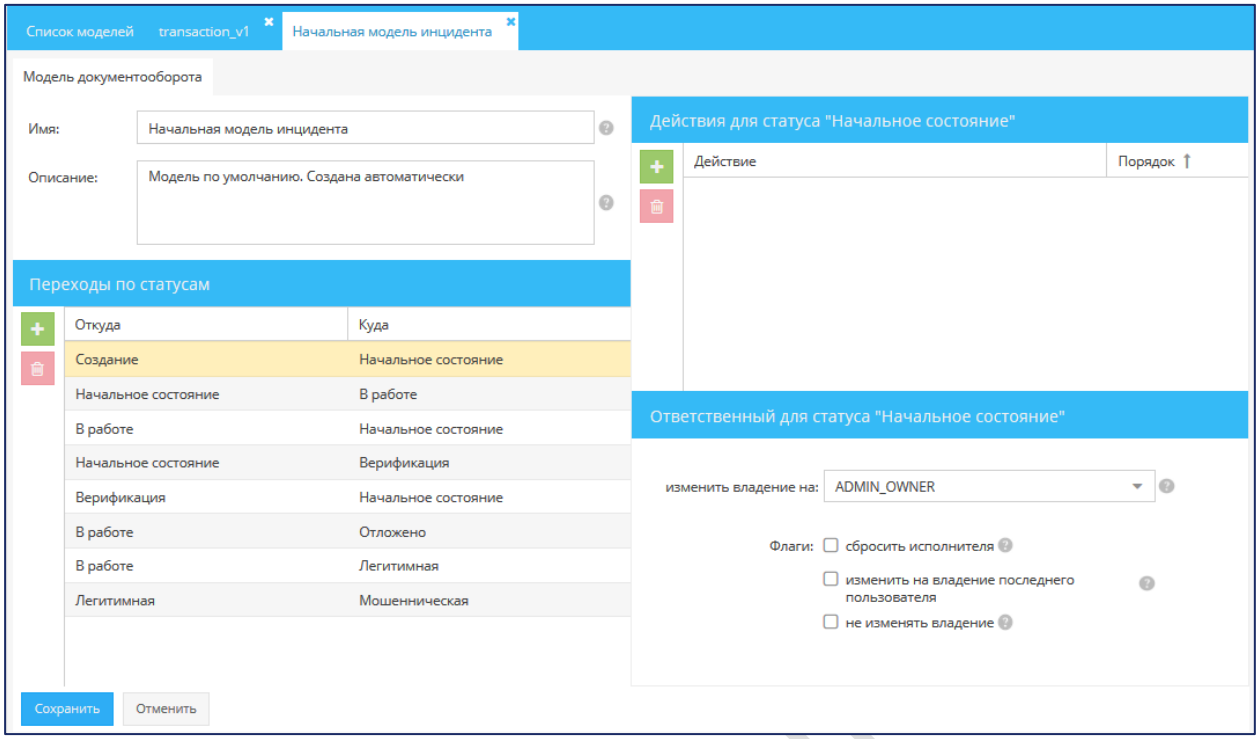


Рисунок 47 – Форма модели документооборота

6.4.2 Создание модели документооборота

Чтобы создать новую модель документооборота:

1) В **Списке моделей** (Рисунок 46) нажмите кнопку **Добавить**  .

Откроется модальное окно **Новая модель** (Рисунок 48).

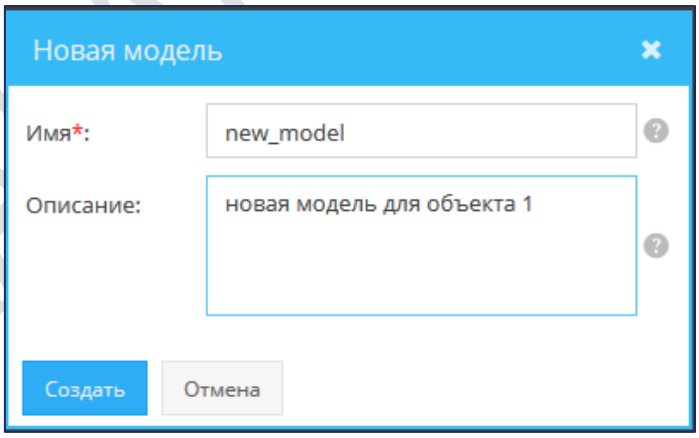


Рисунок 48 – Добавление новой модели документооборота

2) Заполните поля (Таблица 17).

Таблица 17 – Описание полей окна **Новая модель**

Поле	Описание
Имя	Системное имя модели. Уникальное значение. Допустимы только латинские буквы, цифры и символ «_»
Описание	Описание модели документооборота

3) Нажмите кнопку **Создать**.

Модель создана. Она откроется в новой вкладке для настройки (Рисунок 47).

6.4.3 Настройка модели документооборота

Чтобы настроить модель:

1) Откройте экранную форму модели документооборота (см. раздел 6.4.1).

Форма разделена на четыре части:

- **Общая информация** – имя и описание модели, заданные при создании.
- **Переходы по статусам** – набор доступных переходов по статусам.
- **Действия** – отображает набор действий, которые выполняются при смене статуса на выбранном переходе. Зависит от выбранного перехода в разделе **Переход по статусам.**
- **Ответственный** – настройка логики определения ответственного за объект, который назначается при смене статуса на выбранном переходе. Зависит от выбранного перехода в разделе **Переход по статусам.**

2) Заполните таблицу переходов по статусам.

Первая строка любой модели всегда задает переход из начального статуса объекта.

При этом:

- **Создание** – значение по умолчанию в столбце **Откуда**;
- статус в столбце **Куда** соответствует первому статусу объекта, к которому будет привязана модель.

Чтобы задать значение начального статуса в первой сроке таблицы **Переходы по статусам**:

а) В столбце **Куда** дважды щелкните по ячейке.

Отобразится раскрывающийся список с доступными значениями статусов.

б) Выберите статус.

Список доступных статусов можно пополнить – он находится в пользовательских справочниках (меню **Пользовательские объекты** – **Справочники**, справочник **Все доступные статусы объектов**).

Добавьте следующий переход:

а) Нажмите кнопку **Добавить**  .

б) В новой строке заполните значения **Откуда** и **Куда**.

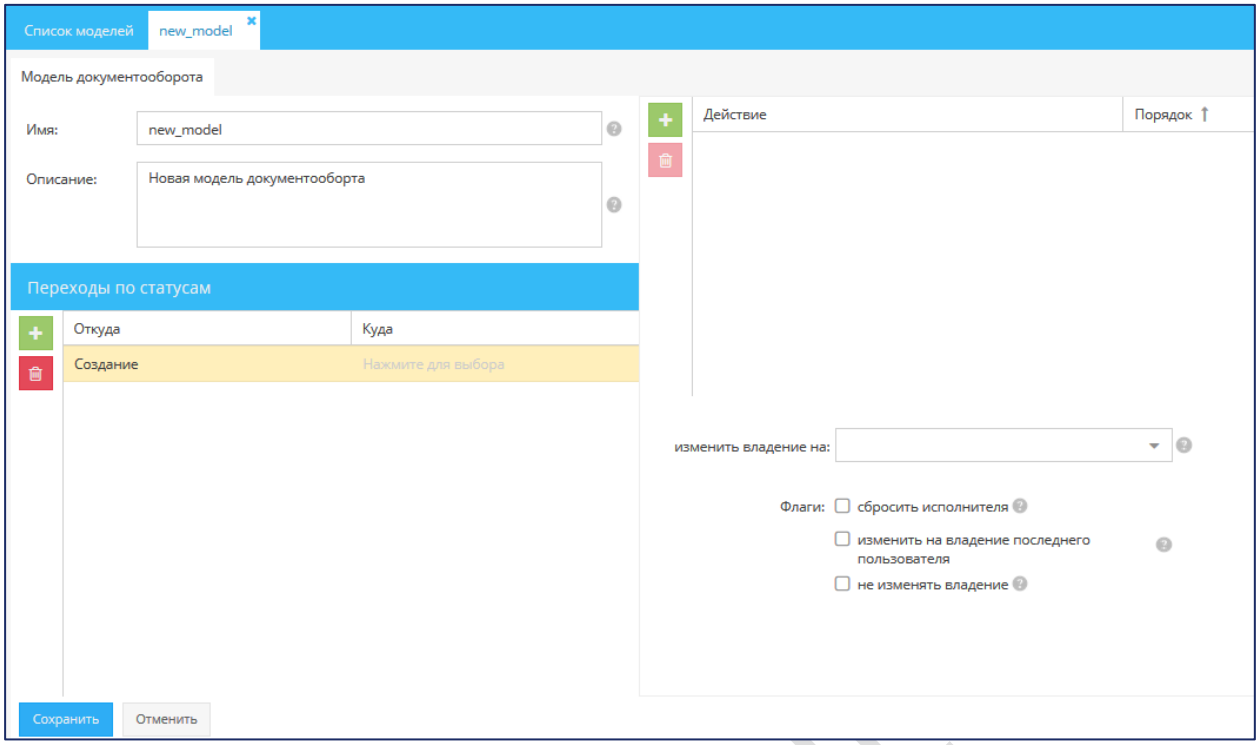


Рисунок 49 – Форма настройки модели документооборота

3) Для каждого перехода в таблице **Переходы по статусам** в разделе **Действия** выберите действия, которые Jet Detective должна выполнить при переходе. Для этого:

   а) Выберите строку в таблице **Переходы по статусам**.

   б) В разделе **Действия** добавьте действие, для выбранного перехода – с помощью кнопки **Добавить**  .

   в) В появившейся строке выберите действие в раскрывающемся списке.

Список доступных действий соответствует справочнику действий (см. раздел 6.9.2).

   г) При необходимости измените прядок выполнения действий в столбце **Порядок**.

Действия выполняются в порядке от меньшего к большему. Действия с одинаковым номером порядка выполняются в произвольном порядке в рамках своей очереди.

4) Для каждого перехода в таблице **Переходы по статусам** в разделе **Ответственный** выберите логику определения ответственного за объект при выполнении перехода (см. рисунок 50). Для этого:

   а) Выберите значение в раскрывающемся списке **Поменять владение на**.

К выбранному владению будут присваиваться объекты при выполнении перехода в статус, указанный в столбце **Куда**. Описание владений приведено в разделе 6.5.4).

   б) Установите флажки:

   - **отменить назначенного исполнителя** – если этот флаг установлен, то для объекта будет сбрасываться ответственный**.**
   - **поменять на владение последнего пользователя** – если этот флаг установлен, то объекту будет присвоено владение пользователя, который выполнял предыдущий переход.

Этот флаг полезен, если при переходе необходимо вернуть объект в работу прошлому ответственному.

- **не изменять владение** – если этот флаг установлен, то для объекта при переходе не изменится владение.

5) Нажмите кнопку **Сохранить.**

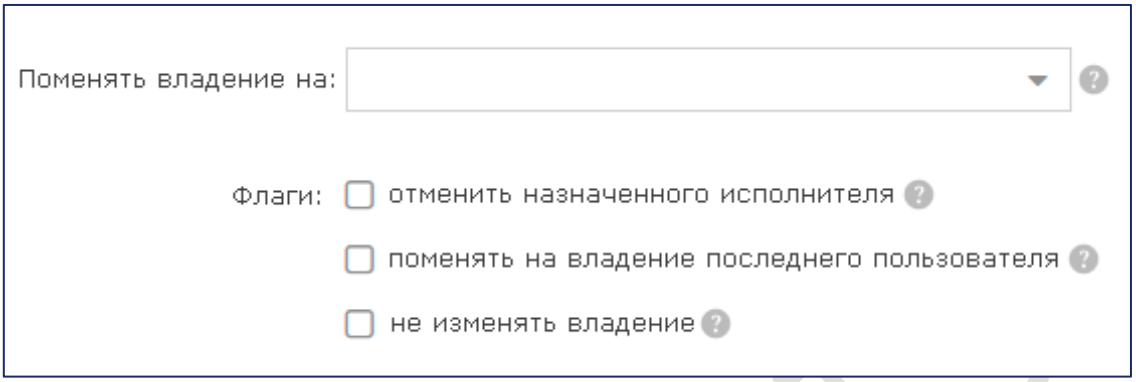


Рисунок 50 – Настройка логики определения ответственного при переходе

6.5 МОДЕЛЬ РАСПРЕДЕЛЕНИЯ ПРАВ ДОСТУПА

6.5.1 Механизмы управления доступом

Модель распределения прав доступа определяет механизм управления правами доступа пользователя к функциям, объектам и хранимым данным.

В Jet Detective реализованы два механизма: разрешения (см. раздел 6.5.2) и владения (см. раздел 6.5.4).

Набор прав доступа каждого пользователя определяется установленными для него разрешениями в рамках владений, к которым он прикреплен (Рисунок 51).

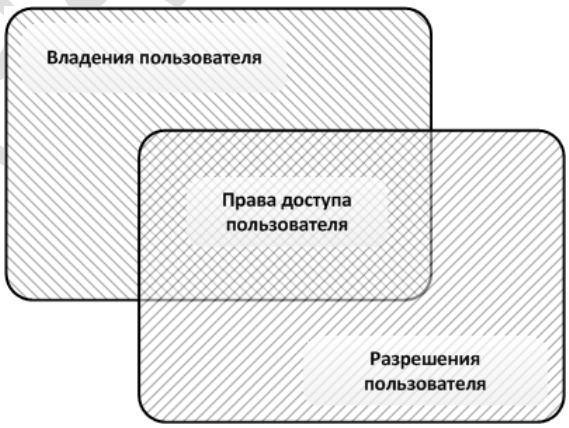


Рисунок 51 – Права доступа пользователя определяются совокупностью владений и разрешений

6.5.2 Разрешения

Разрешения – это механизм управления доступом пользователей к элементам интерфейса, программным сервисам и объектам. Соответственно, существует три типа разрешений:

- интерфейс пользователя – разрешение на доступ к определенному элементу интерфейса;
- сервис – разрешение на доступ к определенному программному сервису, реализующему действия в Jet Detective;
- объект – разрешение на действия с экземплярами определенного объекта: создание, чтение, редактирование или удаление экземпляров этого объекта.

Все возможные в Jet Detective разрешения представлены в виде *дерева разрешений* (Рисунок 52). Такое представление позволяет группировать разрешения и выстраивать понятную и удобную для работы иерархию.

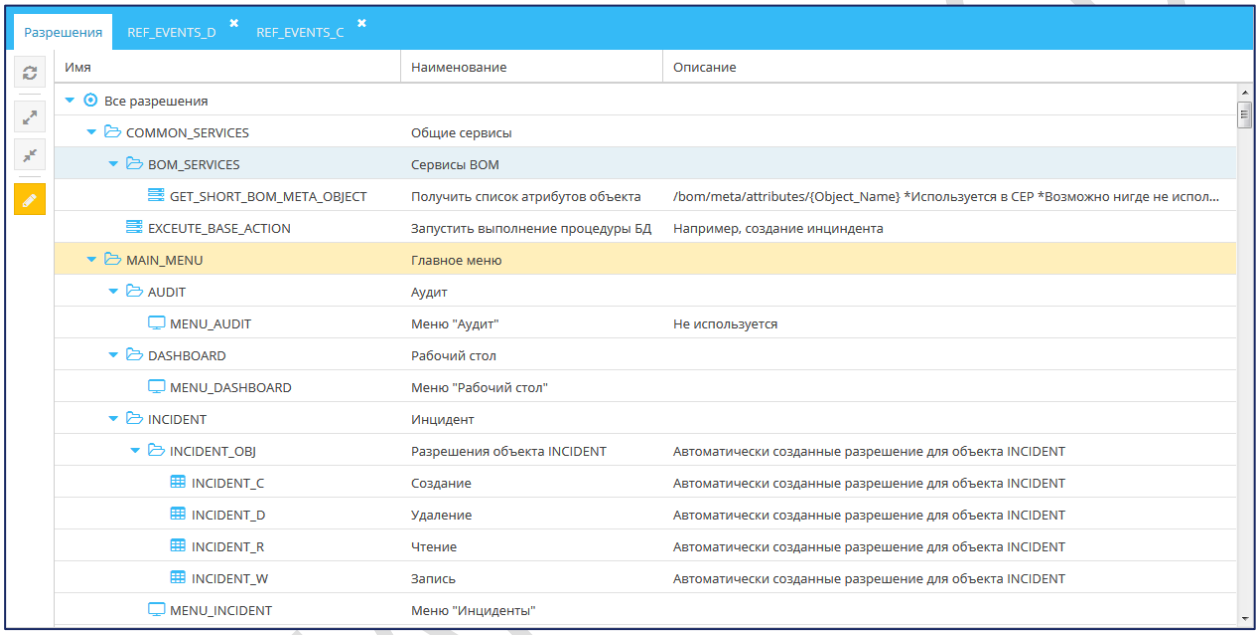


Рисунок 52 – Пример дерева разрешений

С точки зрения доступа, элемент интерфейса пользователя и связанный с ним программный сервис отделены друг от друга и требуют отдельных разрешений. Зачастую следует устанавливать оба эти разрешения. Например, нажатие кнопки в пользовательском интерфейсе приводит к вызову соответствующего программного сервиса. Иными словами, пользователю для выполнения такой операции в Jet Detective необходимы разрешения и на кнопку, и на сервис. Автоматизированному агенту (программной сущности) для выполнения этой же операции достаточно получить только разрешение на сервис, так как общепринятые правила информационной безопасности предписывают в явном виде лишать информационных агентов доступа к элементам интерфейса пользователя.

Администратор Jet Detective может перемещать разрешения по дереву разрешений, формируя вид дерева, наиболее удобный для управления правами доступа.

При создании конфигурации нового объекта в дерево разрешений автоматически добавляются четыре узла с разрешениями:

- <имя объекта>_C – на создание экземпляров объекта;
- <имя объекта>_D – на удаление экземпляров объекта;
- <имя объекта>_R – на чтение экземпляров объекта;

- <имя объекта>_W – на редактирование данных в экземплярах объекта.

Администратор Jet Detective определяет набор разрешений для каждого пользователя. Существуют следующие инструменты для формирования набора разрешений:

- назначение пользователю одной или нескольких ролей (см. раздел 6.5.3.1);
- установка для пользователя одного или нескольких индивидуальных разрешений (см. раздел 6.5.3.2);
- установка запрета на одно или несколько разрешений (см. раздел 6.5.3.3).

6.5.3 Инструменты для формирования наборов разрешений

6.5.3.1 Роли

Роли – это инструмент для формирования наборов разрешений на основе дерева разрешений. Использование ролей является основным способом установки разрешений для пользователей.

Ролью в широком смысле называется выделенная совокупность рабочих действий пользователя, которая в контексте управления доступом представляет собой набор разрешений, необходимых для выполнения этих действий.

В Jet Detective реализована возможность построения иерархии – *дерева ролей* – и реализован механизм передачи прав доступа вверх по иерархии. Узлу дерева ролей автоматически передаются все разрешения, которые установлены на уровнях дочерних узлов.

Администратор Jet Detective может выполнять все операции с деревом ролей:

- добавлять и удалять роли;
- перемещать роли по дереву и тем самым формировать иерархию, наиболее удобную для управления правами доступа;
- устанавливать для ролей наборы разрешений и запретов.

6.5.3.2 Индивидуальные разрешения

Установка индивидуальных разрешений – это инструмент для увеличения набора прав доступа пользователя путем прямой установки для него какого-либо разрешения. Например, разрешение может быть дано в дополнение к уже назначенным ролям.

Индивидуальные разрешения устанавливаются администратором Jet Detective при настройке прав доступа пользователя.

6.5.3.3 Запреты

Запреты – это инструмент для уменьшения набора прав доступа роли или пользователя путем установки прямого запрета на то или иное разрешение.

Запрет может использоваться как при настройке разрешений для роли, так и при настройке разрешений для конкретного пользователя. В первом случае установка запрета позволяет отменить какое-либо разрешение, полученное от дочерних узлов в дереве ролей, во втором – отменить разрешение, полученное от назначенной пользователю роли.

Администратор Jet Detective устанавливает запреты при настройке ролей и при настройке прав доступа пользователя.

6.5.4 Владения

6.5.4.1 Области владения и схемы владения пользователей

Владения – это механизм управления правами доступа пользователей к конкретным записям в таблицах объектов: создание, чтение, редактирование или удаление записей в таблицах объектов, относящиеся к тому или иному владению.

«Владение» или «владение данными» на логическом уровне определяет некоторое множество экземпляров объектов Jet Detective. На уровне хранения данных таблицы всех объектов имеют поле для хранения *идентификатора владения*, который и определяет соответствие экземпляра объекта тому или иному владению.

При настройке прав доступа пользователя администратор определяет *схему владения пользователя* – те владения, к данным которых пользователь получит доступ при наличии достаточных разрешений.

В Jet Detective реализована возможность построения иерархии – *дерева владений*. Узел дерева владений определяет владение не только данными, относящимися непосредственно к этому узлу, но и данными всех дочерних узлов. Таким образом, узел образует *область владения* (Рисунок 53). Родительский узел, находящийся наверху иерархии в области владения, называется *корневым узлом* области владения.

Древовидная иерархия хорошо проецируется на организационную структуру. Построение дерева владений по подобию организационной структуры в значительной степени облегчает настройку и понимание схем владения отдельных пользователей. Первичное построение дерева владений выполняется на этапе внедрения. Администратор Jet Detective может добавлять владения в дерево.

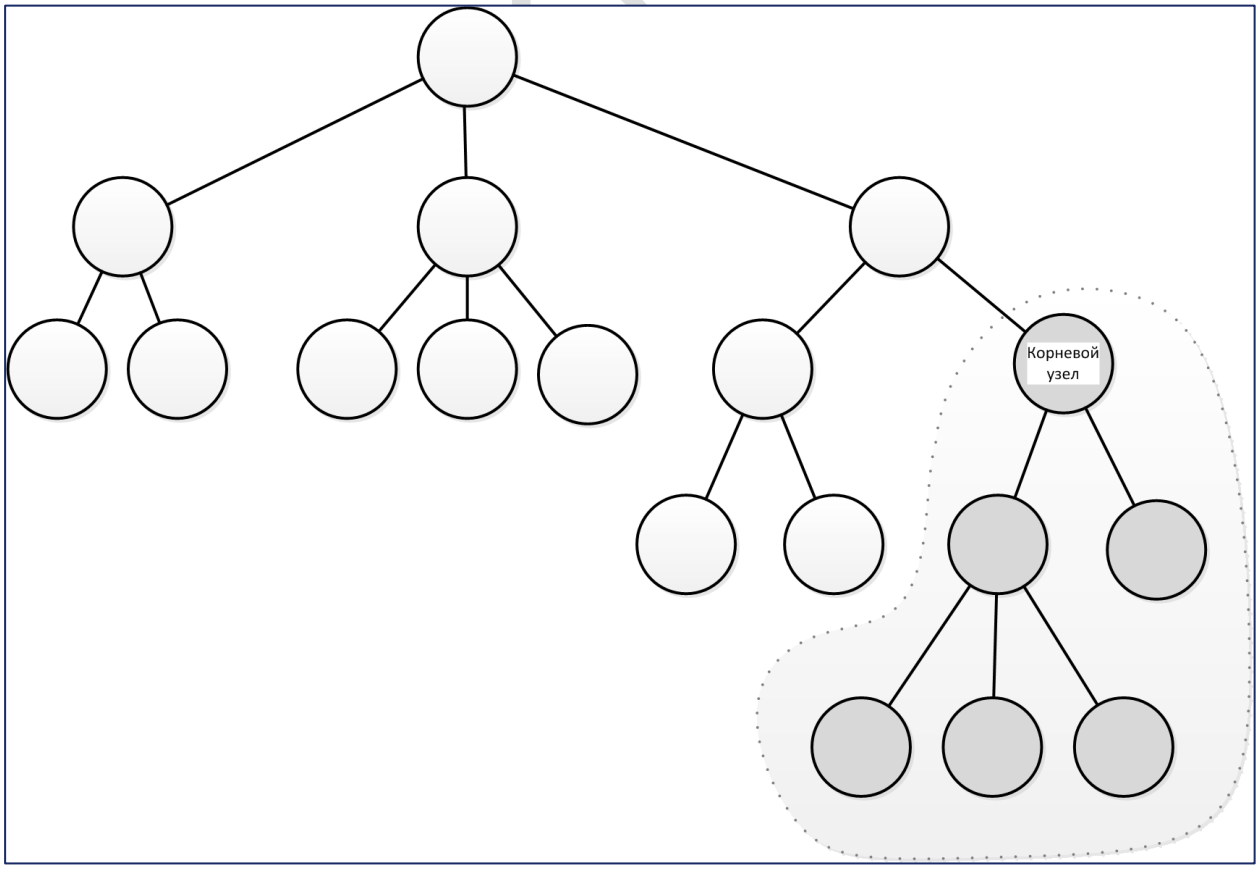


Рисунок 53 – В дереве владений узел и его дочерние узлы образуют область владения

Схему владения пользователя образуют составляющие двух типов:

- область владения по умолчанию (см. раздел 6.5.4.2);
- области дополнительных владений (см. раздел 6.5.4.3).

Например, если на рисунке 54 область владения по умолчанию образована корневым узлом **А**, то области, образованные корневыми узлами **Б** и **В**, являются областями дополнительных владений.

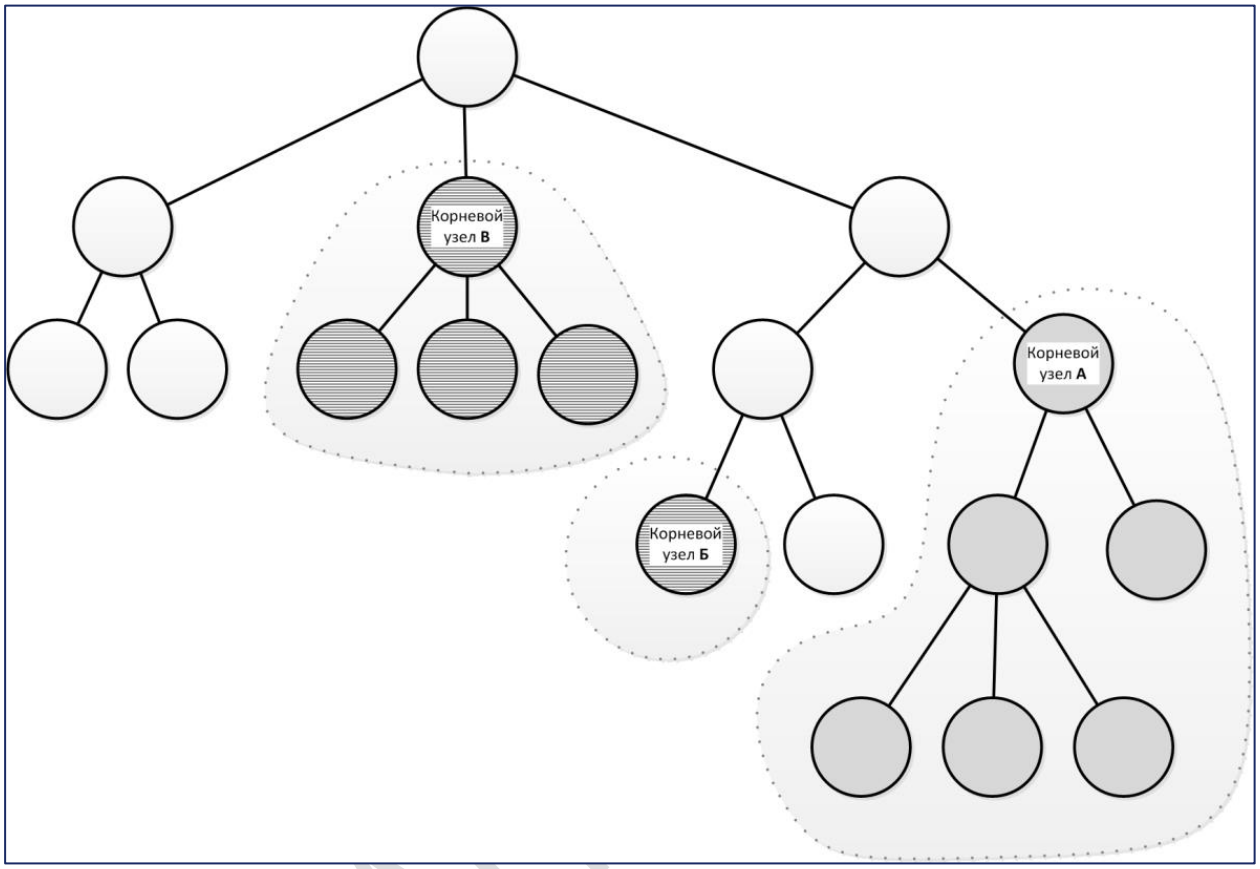


Рисунок 54 – Схему владения пользователя образуют область владения по умолчанию и области дополнительных владений

Администратор Jet Detective может прикрепить пользователя к одному или нескольким владениям и тем самым определить для него основное и дополнительные владения. Существуют инструменты гибкой настройки областей владения. Из любой области владения можно исключить:

- дочерние узлы (например, на рисунке 55 из области владения исключены дочерние узлы корневого узла **А**);
- узел вместе с дочерними узлами (например, на 56 из области владения исключен корневой узел **А**).

Всем пользователям администратор настраивает доступ к каждой области владения, входящей в схему владения этого пользователя, и устанавливает права:

- на чтение записей в таблицах объектов;
- редактирование записей в таблицах объектов;
- удаление записей из таблиц объектов.

В зоне пересечения двух областей владения применяются права доступа той области, корневой узел которой располагается ниже по иерархии.

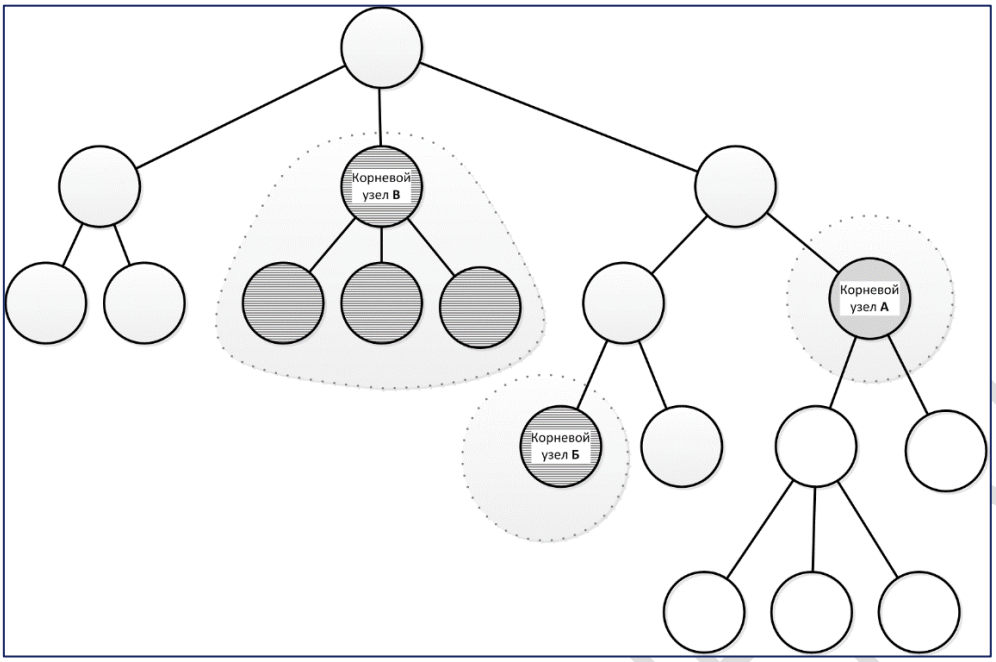


Рисунок 55 – Из любой области владения можно исключить все дочерние владения

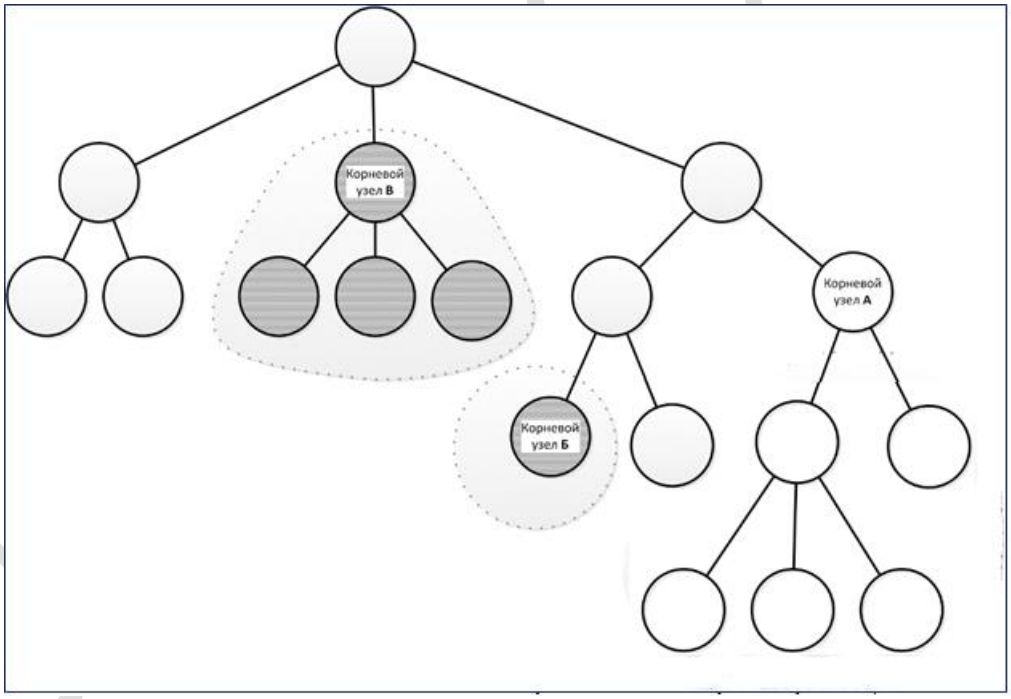


Рисунок 56 – Из любой области владения можно исключить корневой узел

6.5.4.2 Владение по умолчанию

Каждого пользователя прикрепляют к одному из узлов дерева владений – *владению по умолчанию*. Это означает, что в схему владения пользователя включается целая область владения, которая состоит из корневого узла области владения по умолчанию и всех его дочерних узлов (см. рисунок 53).

Если дерево владений построено по подобию организационной структуры, то дочерние узлы в области владения являются владениями по умолчанию для подчиненных пользователей. Таким образом, вышестоящий пользователь получает (при наличии достаточных разрешений) доступ к данным подчиненных пользователей.

В разделе 6.5.4.1 было отмечено, что каждая запись в таблице любого объекта маркируется идентификатором владения. При этом:

- запись, созданная в результате добавления пользователем экземпляра объекта через интерфейс пользователя, маркируется идентификатором владения по умолчанию, к которому прикреплен этот пользователь;
- запись, созданная в результате поступления данных из внешней системы, также маркируется идентификатором определенного владения. Правило, по которому выбирается владение для маркировки записи, задается при настройке алгоритма ETL-процесса. Этот алгоритм используется для загрузки данных и зависит от их источника и содержимого.

При внесении изменений в запись объекта идентификатор владения этой записи не меняется, независимо от того, к какому владению по умолчанию прикреплен пользователь, вносящий изменения.

В каждый момент времени пользователь прикреплен только к одному владению по умолчанию. Прикрепление к другому владению автоматически отключает пользователя от предыдущего владения по умолчанию.

6.5.4.3 Дополнительные владения

Для расширения схемы владения пользователя используются *дополнительные владения*. Пользователя можно прикрепить к любому количеству дополнительных владений. Подключение к дополнительному владению также означает включение в схему владения пользователя целой области владения, состоящей из корневого узла области дополнительного владения и всех его дочерних узлов (см. рисунок 54).

Дополнительные владения могут потребоваться, например, в следующих случаях:

- необходимо исключить распространение прав доступа к данным некоторых дочерних узлов области владения по умолчанию;
- пользователь должен помочь коллегам из других подразделений. В этом случае пользователю предоставляется доступ к другим областям владения, которые не пересекаются с его областью владения по умолчанию;
- пользователь должен на время заместить вышестоящего сотрудника. В этом случае пользователю предоставляется доступ к более объемной области владения, которая включает в себя его собственную область владения по умолчанию или пересекается с ней.

6.6 НАСТРОЙКА МЕХАНИЗМОВ УПРАВЛЕНИЯ ДОСТУПОМ

6.6.1 Общие сведения

К настройке механизмов управления доступом относится построение дерева разрешений и дерева владений.

На этапе внедрения администратор Jet Detective выполняет первичное построение:

- дерева разрешений (см. раздел 6.6.2).

Примечание. Изначально в Jet Detective уже присутствует дерево разрешений, которое охватывает все функции Jet Detective.

- дерева владений (см. раздел 6.6.3).
- дерева ролей (см. раздел 6.6.4).

В экранных формах дерева разрешений и ролей (вкладка **Разрешения**) отображаются следующие кнопки с пиктограммами:

- <разрешение> или <запрет> – флажок установлен явно. Это означает, что при назначении какой-либо роли пользователь получит разрешение или запрет;
- <разрешение> или <запрет> – флажок не установлен. Это означает, что при назначении какой-либо роли пользователь не получит разрешение или не получит запрет;
- или <набор разрешений> – флажок установлен явно. Это означает, что при назначении какой-либо роли пользователь получит все разрешения этого набора;
- или <набор разрешений> – флажок установлен условно. Это означает, что разрешения установлены или не во всех дочерних узлах, или ни в одном узле.

На вкладке **Права владения** экранной формы пользователя (см. раздел 6.7.5.1) отображаются следующие кнопки с пиктограммами:

- – флажок установлен явно. Это означает, что права владения предоставлены;
- – флажок установлен условно. Это означает, что пользователю предоставлены права владения, расположенные ниже по иерархии дерева владений;
- – флажок не установлен. Это означает, что права владения не предоставлены.

6.6.2 Дерево разрешений

6.6.2.1 Просмотр дерева разрешений, свойств его узлов и листьев

Общие сведения о дереве разрешений приведены в разделе 6.5.2.

Чтобы посмотреть дерево разрешений:

1) Выберите пункт меню **Настройки** – **Доступ** – **Разрешения**.

В рабочей области отобразится одна или несколько вкладок:

- дерева разрешений (Рисунок 57);
- узлов дерева, открытых в этой сессии.

Существует четыре типа узлов дерева разрешений, исключая корневой:

- Пользовательский интерфейс;
- Сервис;
- Объект;
- Папка.

Папка – это вспомогательный внутренний узел для организации в дереве разрешений иерархической структуры. Позволяет распределять узлы с разрешениями по уровням иерархии.

Остальные разрешения всегда отображаются листьями дерева.

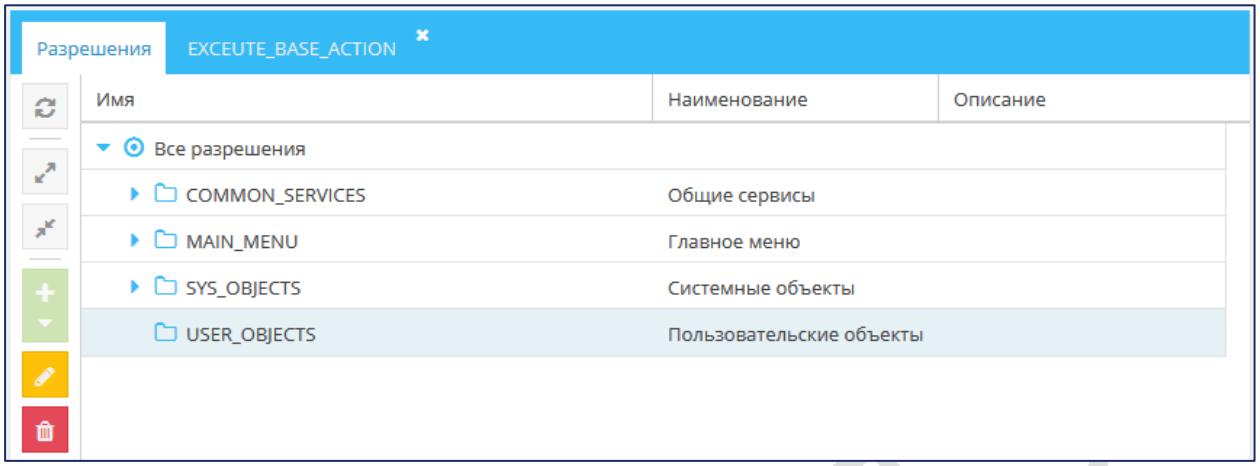


Рисунок 57 – Пример дерева разрешений, развернутого на один уровень

2) Разверните дерево (см. раздел 4.4.5) и дважды щёлкните по строке узла.

Экранная форма узла откроется на отдельной вкладке (Рисунок 58).

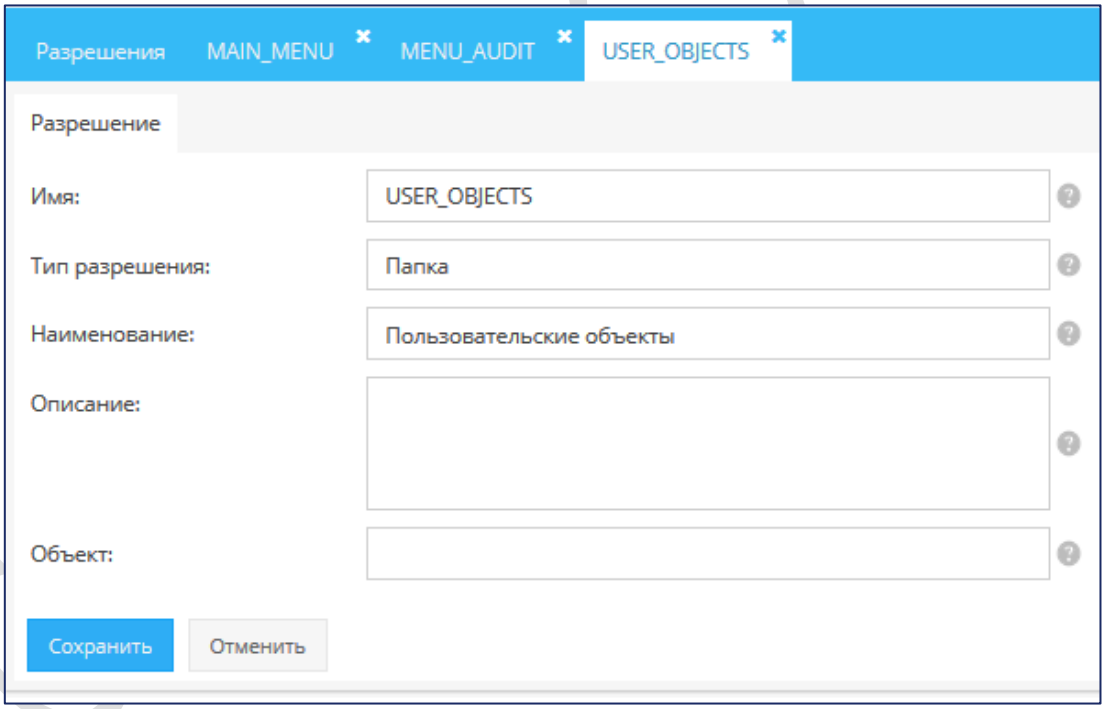


Рисунок 58 – Вкладка с экранной формой узла USER_OBJECTS

Атрибуты узла описаны в таблице 18.

Таблица 18 – Атрибуты узла дерева разрешений

Атрибут	Описание
Имя	Системное имя узла (далее – *имя узла*)
Тип разрешения	Тип узла

Атрибут	Описание
Наименование	Название узла
Описание	Описание (например, назначение узла)
Объект	Для разрешений с типом **Объект**: имя объекта, для управления доступом к которому используется это разрешение

3) Чтобы посмотреть атрибуты разрешения:

- перейдите на вкладку **Разрешения**;
- дважды щёлкните по строке разрешения (Рисунок 59).

Экранная форма выбранной записи откроется на отдельной вкладке (Рисунок 60).

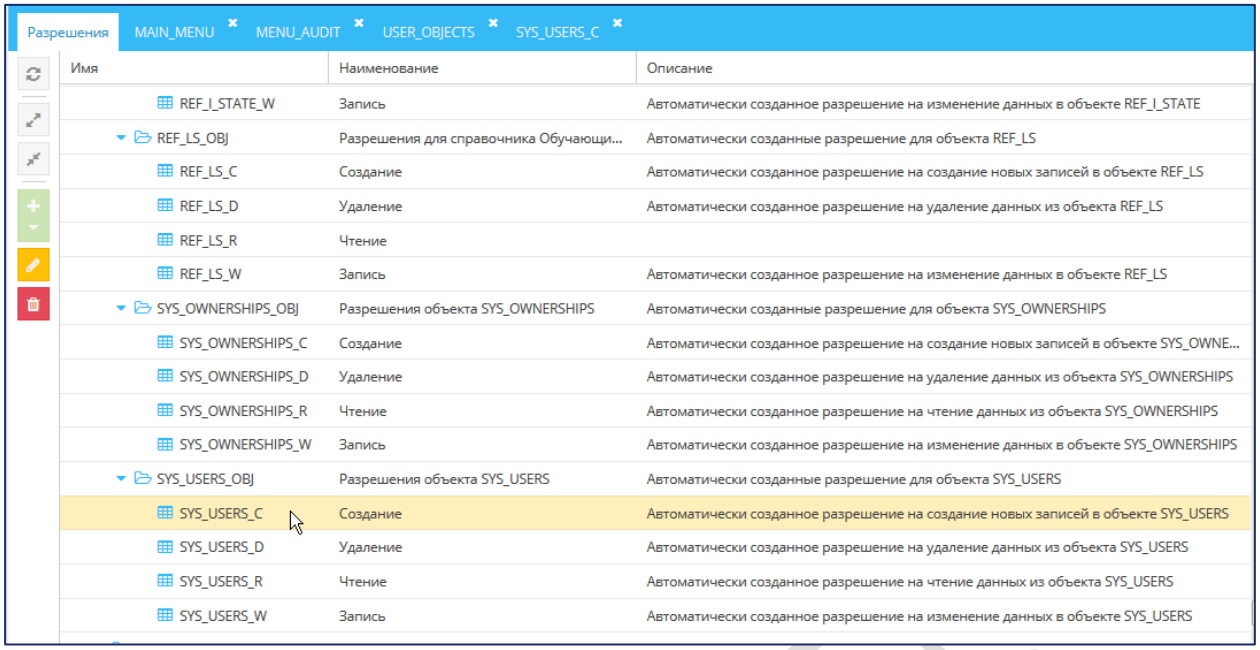


Рисунок 59 – Выбор разрешения SYS_USERS_C

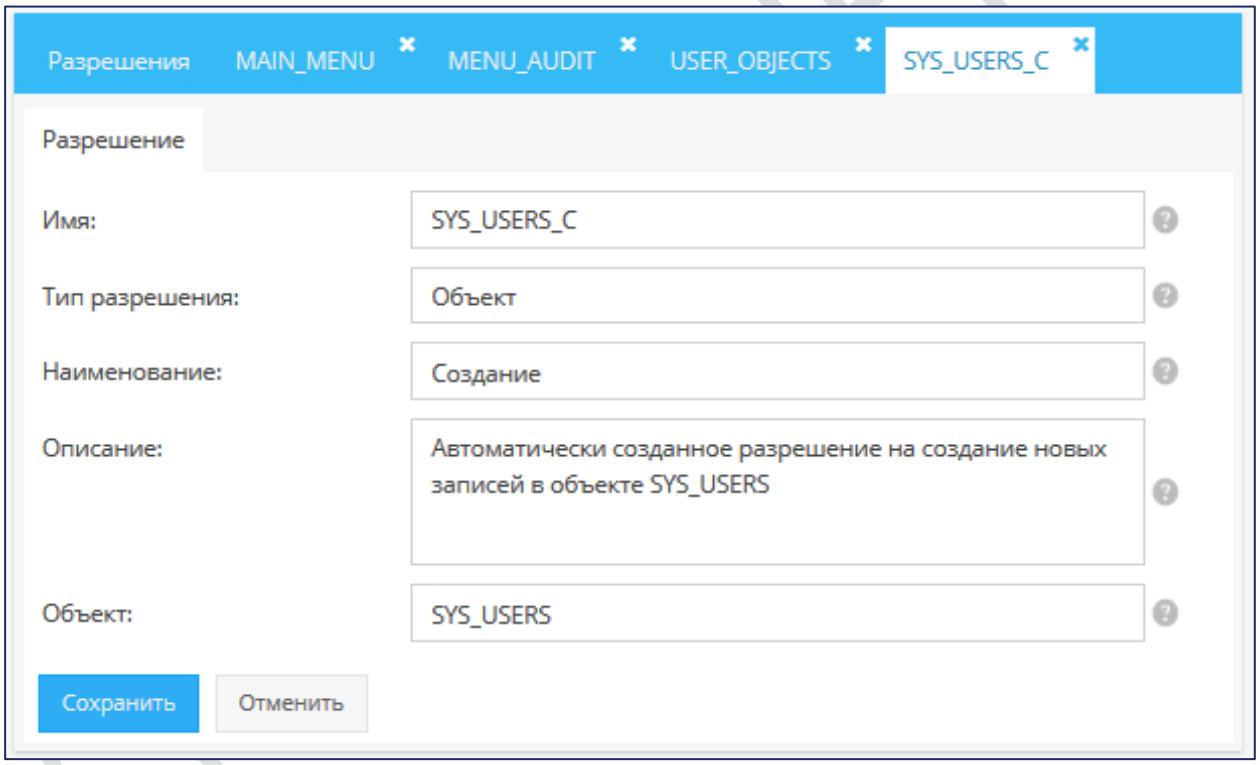


Рисунок 60 – Экранная форма разрешения SYS_USERS_C

6.6.2.2 Редактирование разрешений и свойств узла в дереве разрешений

Можно отредактировать наименование и описание узла. Для этого:

1) Откройте экранные формы разрешения и узла дерева разрешений (см. раздел 6.6.2.1, Рисунок 58, Рисунок 60).
2) Измените наименование и описание узла.
3) Нажмите кнопку **Сохранить**.

6.6.2.3 Перемещение узла между папками дерева разрешений

Администратор может перемещать по дереву разрешений как узлы, так и папки. Если перемещается папка, то вместе с ней перемещаются все входящие в нее папки и разрешения.

Чтобы переместить узел из одной папки в другую:

1) Выберите пункт меню **Настройки** – **Разрешения**.
2) Найдите в дереве узел – папку или узел с разрешением (работа с иерархическими списками описана в разделе 4.4.5).
3) Найдите в дереве папку, куда следует переместить узел.
4) С помощью мыши перетащите узел в эту папку.

Перемещение узла не влияет на наборы прав доступа пользователей.

6.6.2.4 Добавление узла и разрешения в дерево разрешений

Примечание. Изначально в Jet Detective уже присутствует дерево разрешений, которое охватывает все функции Jet Detective. Разрешения типа **Объект** создаются автоматически во время создания объектов. Администратор может перестроить дерево разрешений по своему усмотрению.

Чтобы добавить узел в дерево разрешений:

1) Выберите пункт меню **Настройки** – **Разрешения**.
2) Выберите в дереве папку, в которую следует добавить узел (работа с иерархическими списками описана в разделе 4.4.5).
3) Нажмите кнопку **Добавить**  и в раскрывшемся меню выберите тип создаваемого узла.
4) В открывшемся окне укажите имя и наименование узла (Рисунок 61).

Примечание. Имена разрешений для сервисов и элементов интерфейса также указываются на программном уровне в свойствах сервисов и элементов интерфейса.

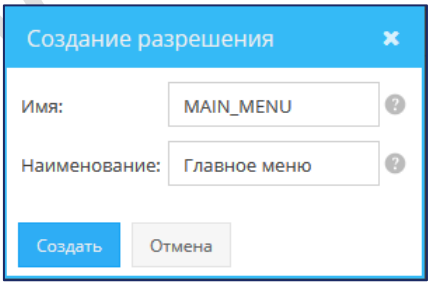


Рисунок 61 – Создание разрешения

5) Нажмите кнопку **Добавить**.

Узел добавится в дерево разрешений. Экранная форма узла откроется на отдельной вкладке.

6) Введите текст в поле **Описание** (Рисунок 58).
7) Нажмите кнопку **Сохранить**.

6.6.2.5 Удаление узла из дерева разрешений

Чтобы удалить узел из дерева разрешений:

1) Откройте экранную форму дерева разрешений (см. раздел 6.6.2.1).
2) Выберите узел (см. раздел 4.4.5).
3) Нажмите кнопку **Удалить**  .

   Примечание. При удалении папки будут также удалены все входящие в нее папки и узлы с разрешениями.

4) Нажмите кнопку **Да** в появившемся запросе.

6.6.3 Дерево владений

6.6.3.1 Просмотр дерева владений и его свойств

Общие сведения о дереве владений приведены в разделе 6.5.4.1.

Чтобы посмотреть дерево владений:

1) Выберите пункт меню **Настройки** – **Доступ** – **Владения**.

В рабочей области отобразится одна или несколько вкладок:

- **Владения** – дерево владений (Рисунок 62);
- узлов дерева, открытых в этой сессии.

Все узлы в дереве владений однотипны и дальше называются просто владениями.

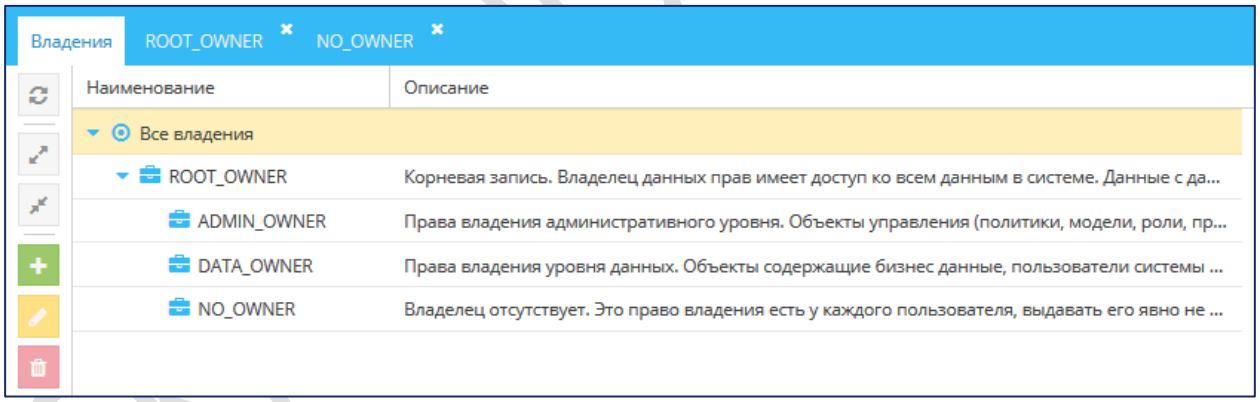


Рисунок 62 – Пример дерева владений

2) Разверните дерево (см. раздел 4.4.5) и дважды щёлкните по строке узла.

Экранная форма владения откроется на отдельной вкладке (Рисунок 63).

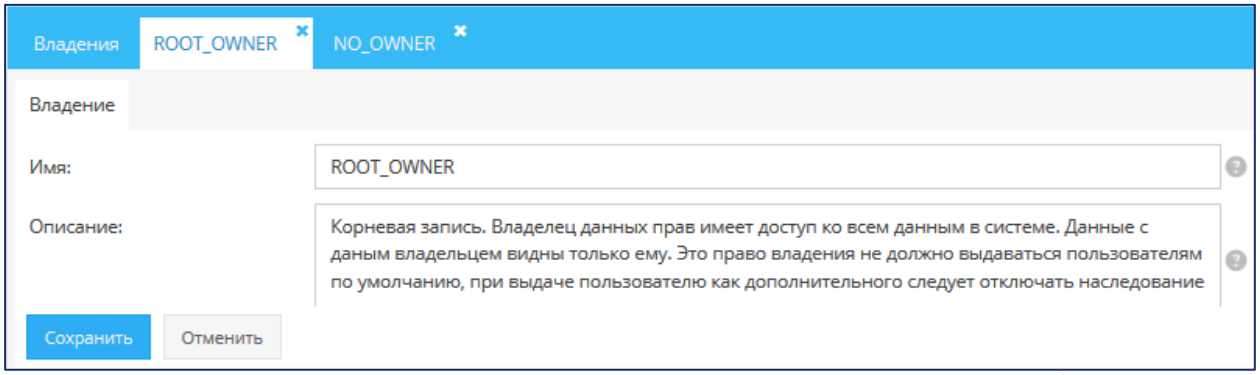


Рисунок 63 – Вкладка с экранной формой узла ROOT_OWNER

Атрибуты записи владения описаны в таблице 19.

Таблица 19 – Атрибуты записи владения

Атрибут	Описание
Имя	Системное имя владения (далее – *имя владения*)
Описание	Описание владения

3) Чтобы посмотреть атрибуты записи владения:

- перейдите на вкладку **Владения**;
- дважды щёлкните по строке владения (Рисунок 64).

Экранная форма выбранной записи откроется на отдельной вкладке (Рисунок 65).

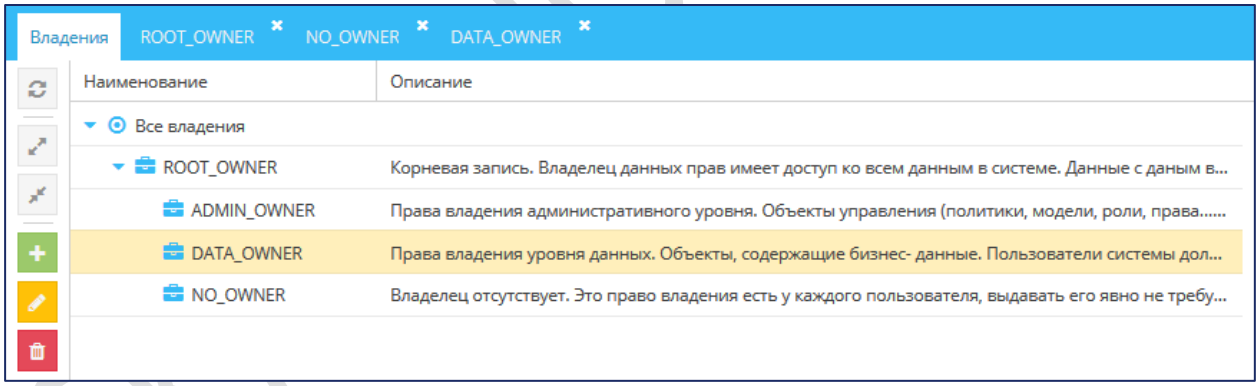


Рисунок 64 – Выбор владения DATA_OWNER

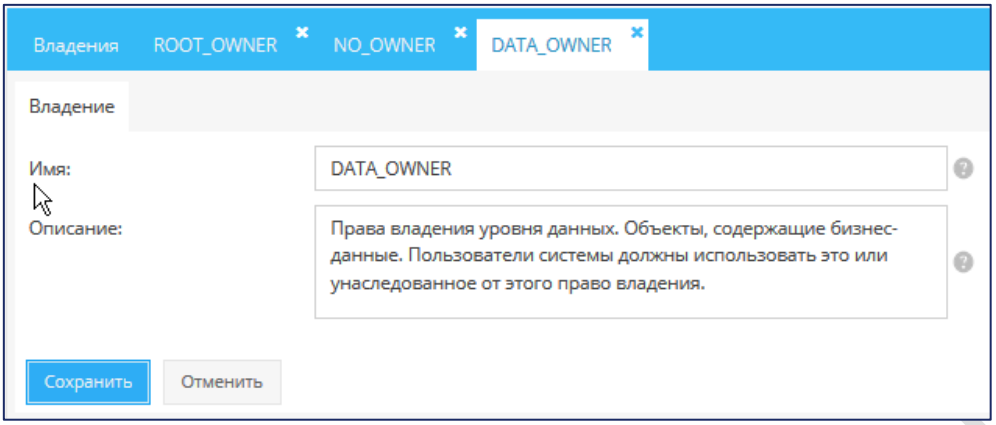


Рисунок 65 – Экранная форма владения DATA_OWNER

6.6.3.2 Редактирование атрибутов записи владения

Можно отредактировать описание владения. Для этого:

1) Откройте экранную форму узла владения и форму владения (см. раздел 6.6.3.1, Рисунок 63 и Рисунок 65).
2) Измените текст в поле **Описание** (Таблица 19).
3) Нажмите кнопку **Сохранить**.

6.6.3.3 Добавление владения

Администратор Jet Detective может добавлять владения в дерево владений.

Предварительно рекомендуется внимательно ознакомиться с общими сведениями о владениях (см. раздел 6.5.4).

Чтобы добавить владение в дерево владений:

1) Перейдите к просмотру дерева владений (см. раздел 6.6.3.1).
2) Выберите в дереве родительский узел для создаваемого владения.
3) Нажмите кнопку **Добавить** .
4) В открывшемся окне укажите имя владения.
5) Нажмите кнопку **ОК**.

Владение добавится в дерево владений. Экранная форма владения откроется на отдельной вкладке.

6) Введите текст в поле **Описание**.
7) Нажмите кнопку **Сохранить**.

6.6.3.4 Удаление владения из дерева владений

Чтобы удалить владение из дерева:

1) Откройте экранную форму дерева владений (см. раздел 6.6.3.1).
2) Выберите владение (см. раздел 4.4.5).

3) Нажмите кнопку **Удалить**  .

*Примечание***.** При удалении владения из дерева будут также удалены все дочерние узлы.

4) Нажмите кнопку **Да** в появившемся запросе.

Примечание. Владение можно удалить только при условии, если это владение не используется в объектах (см. раздел 6.5.4) и не назначено пользователям (см. раздел 6.7.5).

6.6.4 Дерево ролей

6.6.4.1 Просмотр дерева ролей и роли

Общие сведения о дереве ролей см. в разделе 6.5.3.1.

Чтобы посмотреть дерево ролей:

1) Выберите пункт меню **Настройки** – **Доступ** – **Роли**.

В рабочей области отобразится одна или несколько вкладок:

- **Роли** – дерево ролей (Рисунок 66);
- узлов дерева, открытых в этой сессии.

Все узлы в дереве ролей однотипны и дальше называются просто ролями.

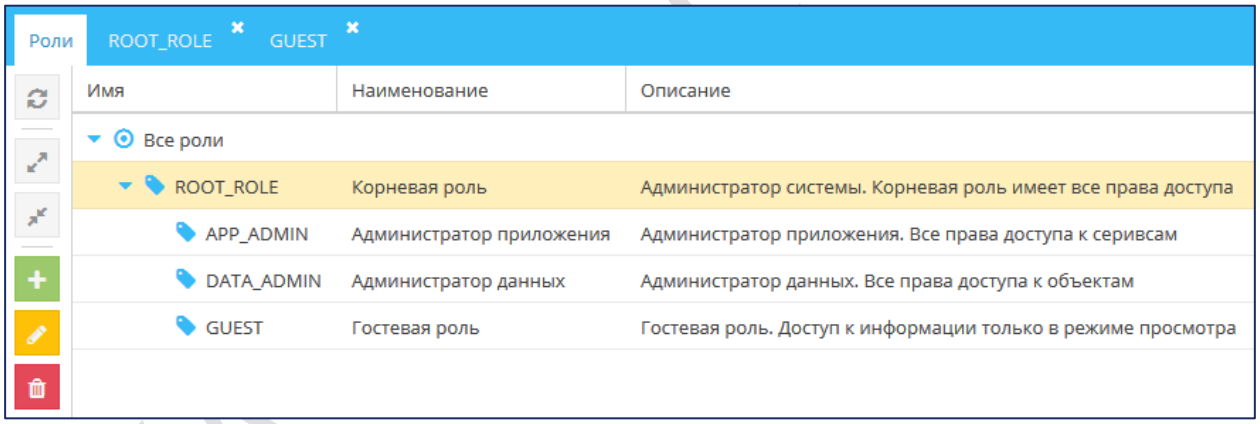


Рисунок 66 – Пример дерева ролей

2) Дважды щёлкните по строке роли.

Экранная форма роли откроется на отдельной вкладке. В свою очередь, сама форма тоже имеет вкладки:

- **Роль** – содержит сведения об атрибутах роли (см. Рисунок 67, Таблица 20);
- **Разрешения** – содержит дерево разрешений и инструменты установки разрешений и запретов для роли (см. раздел 6.6.4.5).

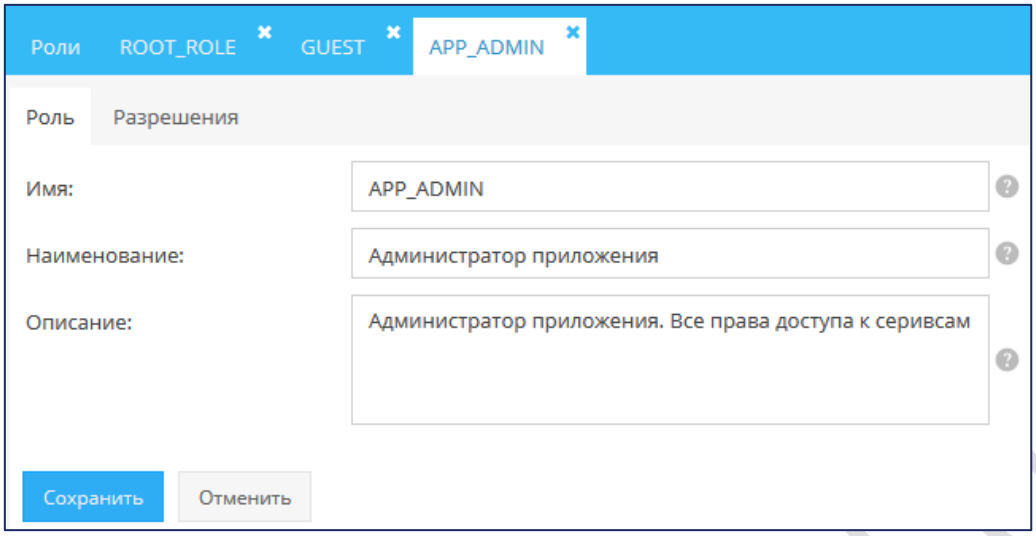


Рисунок 67 – Вкладка **Роль.** Пример для APP_ADMIN

Таблица 20 – Атрибуты роли

Атрибут	Описание
Имя	Системное имя роли (далее – *имя роли*)
Наименование	Название роли
Описание	Описание роли

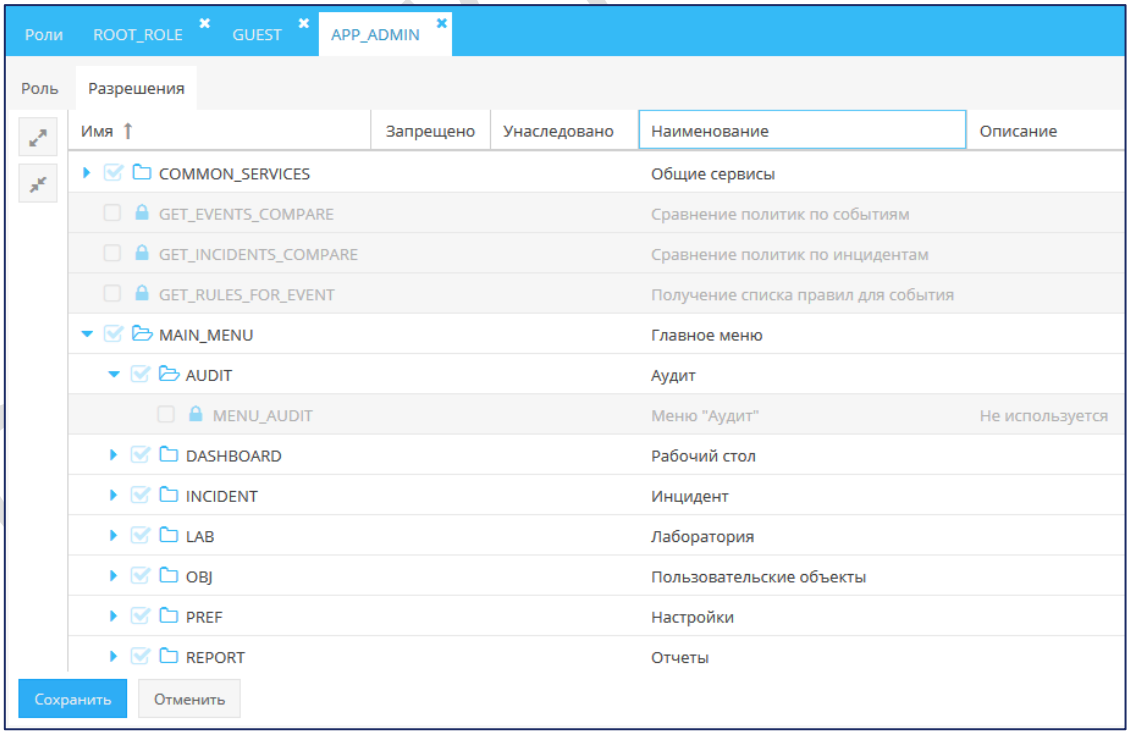


Рисунок 68 – Вкладка **Разрешения**. Пример для APP_ADMIN

6.6.4.2 Редактирование роли

Можно отредактировать наименование и описание роли. Для этого:

1) Откройте экранную форму роли (см. раздел 6.6.4.1, Рисунок 67, Рисунок 68)
2) Измените наименование и описание роли.
3) Нажмите кнопку **Сохранить**.

6.6.4.3 Перемещение роли в дереве ролей

Чтобы переместить роль:

1) Выберите пункт меню **Настройки** – **Доступ** – **Роли**.
2) Найдите роль, которую следует переместить (работа с иерархическими списками описана в разделе 4.4.5).
3) Найдите роль, которая должна стать для перемещаемой роли родительской.

   Примечание. Так как каждой роли автоматически передаются все разрешения, которые установлены на уровнях дочерних ролей, то перемещение роли влияет на наборы прав доступа пользователей. Перемещение роли следует выполнять с особой осторожностью.

4) С помощью мыши перетащите роль на название новой родительской роли.

Наборы прав доступа пользователей изменятся в соответствии с изменившейся иерархией ролей.

6.6.4.4 Добавление роли

Чтобы добавить роль в дерево ролей:

1) Выберите пункт меню **Настройки** – **Доступ** – **Роли**.
2) Выберите роль, которая должна стать для создаваемой роли родительской (работа с иерархическими списками описана в разделе 4.4.5).
3) Нажмите кнопку **Добавить**  .
4) В открывшемся окне укажите имя и наименование роли (Рисунок 69).
5) Нажмите кнопку **Создать**.

Роль добавится в дерево ролей, а её экранная форма откроется на отдельной вкладке. Экранная форма состоит из двух вкладок:

- **Роль** – содержит сведения о свойствах роли;
- **Разрешения** – содержит дерево разрешений и инструменты установки разрешений и запретов для роли.

6) Заполните поля на вкладках **Роль** и **Разрешения** (разрешения и запреты для роли описаны в разделе 6.6.4.5).
7) Нажмите кнопку **Сохранить**.

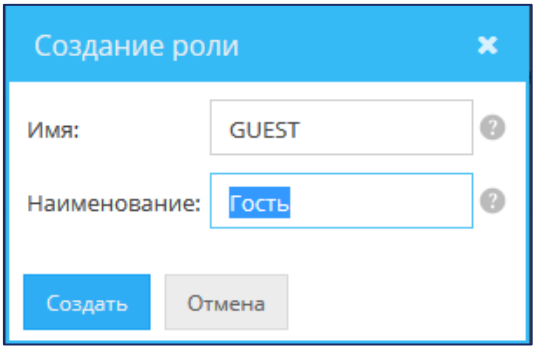


Рисунок 69 – Создание роли

6.6.4.5 *Установка разрешений и запретов для роли*

Для каждой роли можно настроить набор разрешений и запретов. Общие сведения о разрешениях см. в разделе 6.5.2. Общие сведения о запретах см. в разделе 6.5.3.3.

Установка разрешений и запретов выполняется на вкладке **Разрешения** экранной формы роли (Рисунок 70, Таблица 21).

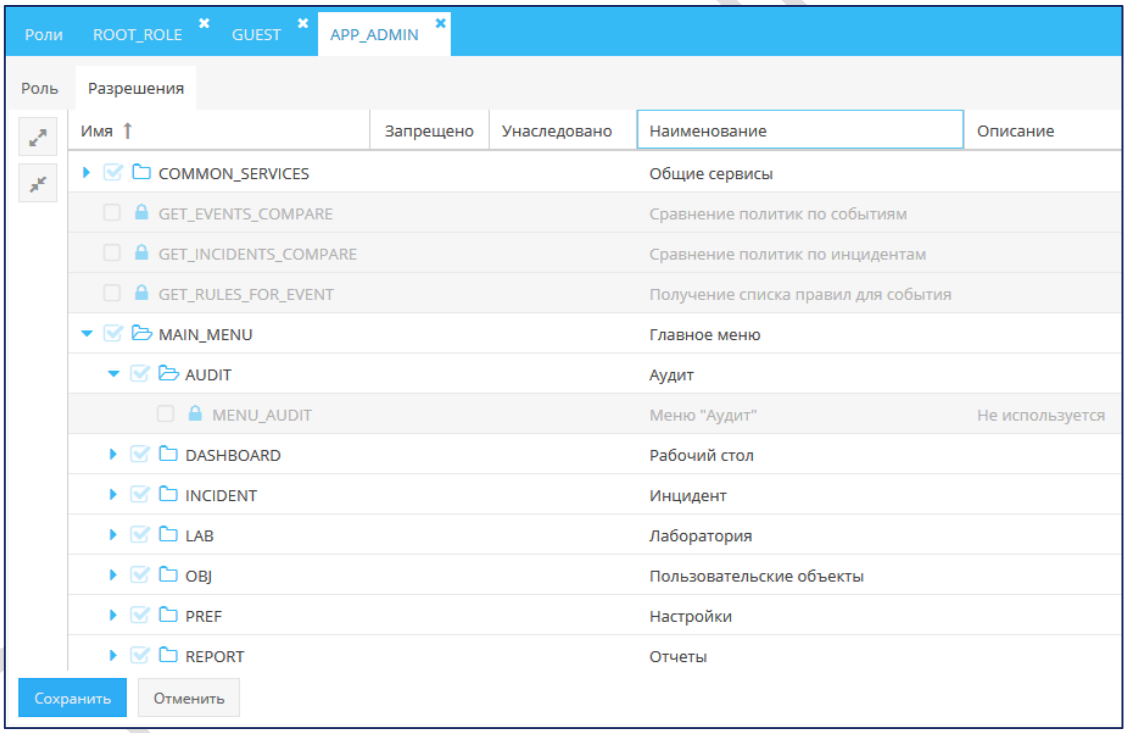


Рисунок 70 – Экранная форма роли. Пример вкладки **Разрешения**

Таблица 21 – Описание столбцов на вкладке **Разрешения**

Столбец	Описание
Имя	Имя узла в дереве разрешений. В целом, в столбце отображается дерево разрешений
Запрещено	Инструмент для установки запрета
Унаследовано	Перечень дочерних ролей, от которых автоматически получены разрешения и запреты
Наименование	Название узла

Столбец	Описание
Описание	Описание, например Назначение узла

На вкладке **Разрешения** отображается дерево разрешений. У каждого узла дерева имеется поле для установки флажка. Возможные варианты флажков описаны в разделе общих сведений (6.6.1).

Чтобы установить разрешения и запреты для роли:

1) Перейдите на вкладку **Разрешения** (см. рисунок 70).
2) Чтобы установить какое-либо разрешение, установите явный флажок в соответствующем узле дерева.
3) Чтобы в одно действие установить разрешения во всех дочерних узлах какой-либо папки, установите явный флажок для узла этой папки.

   Примечание. При установке разрешений следует учитывать, что эти разрешения будут автоматически переданы родительской роли.

4) Чтобы установить запрет на какое-либо разрешение, установите флажок в столбце **Запрещено** (в строке узла с этим разрешением).

   Примечание. Запрет можно установить только для явно установленного разрешения. Узлы с такими разрешениями имеют индикацию и флажок в столбце **Запрещено** (Рисунок 71).

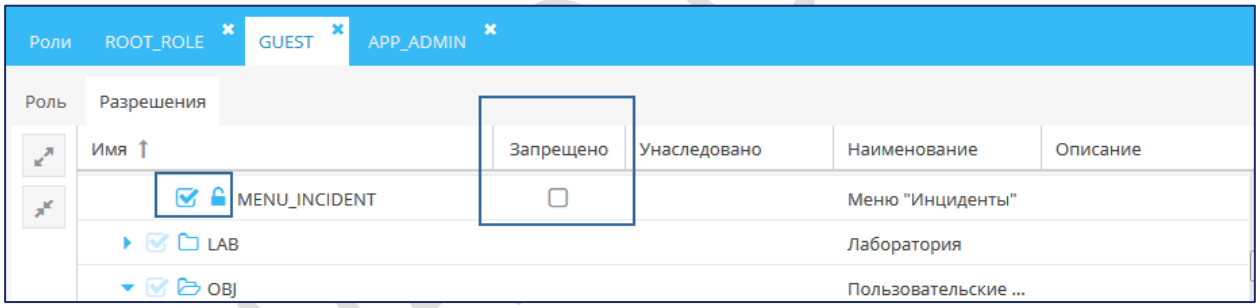


Рисунок 71 – Поле для установки запрета

5) Нажмите кнопку **Сохранить**.

Наборы прав доступа пользователей изменятся в соответствии с изменившимся набором разрешений роли.

6.6.4.6 Удаление роли

*Примечание***.** Так как каждой роли автоматически передаются все разрешения, которые установлены на уровнях дочерних ролей, то удаление роли влияет на наборы прав доступа пользователей. При удалении роли из дерева ролей будут удалены и все её дочерние роли. Это также отразится на наборах прав доступа пользователей, которым ранее были назначены удаленные роли.

Чтобы удалить роль из дерева:

1) Перейдите к просмотру дерева ролей (см. раздел 6.6.4.1).
2) Выберите в дереве роль (см. раздел 4.4.5).

3) Нажмите кнопку **Удалить**  .

4) Нажмите кнопку **Да** в появившемся запросе.

Роль удалится из дерева вместе со всеми ее дочерними ролями. Наборы прав доступа пользователей будут изменены в соответствии с изменившейся иерархией ролей.

6.7 УПРАВЛЕНИЕ УЧЁТНЫМИ ЗАПИСЯМИ

6.7.1 Просмотр списка пользователей и учётной записи пользователя

Чтобы посмотреть информацию:

1) Выберите пункт меню Настройки – Доступ – Пользователи.

В рабочей области отобразится одна или несколько вкладок (Рисунок 72):

- списка пользователей
- учётных записей пользователей, открытых в этой сессии.

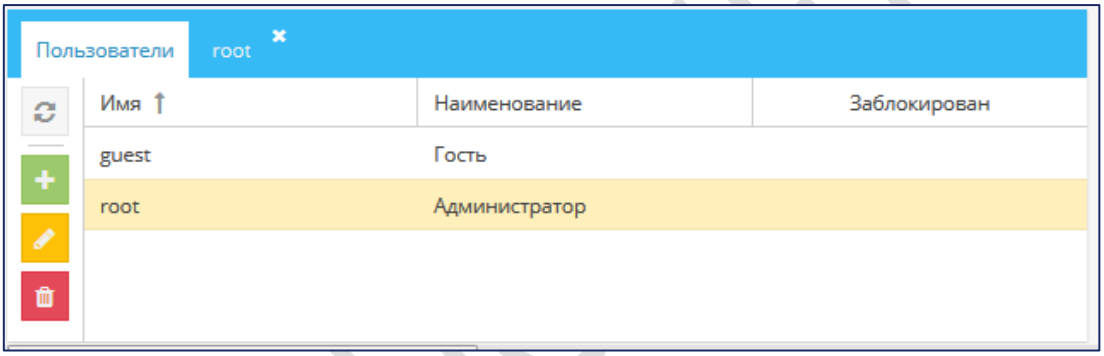


Рисунок 72 – Список пользователей

2) На вкладке со списком пользователей дважды щёлкните по строке с учётной записью пользователя.

Экранная форма учётной записи откроется на отдельной вкладке (Рисунок 73). Сведения о пользователе и его правах доступа размещены на нескольких вкладках формы. Краткое описание этих вкладок приведено в таблице 22.

Таблица 22 – Краткое описание вкладок на экранной форме учётной записи пользователя

Вкладка	Описание
Пользователь	Общие сведения о пользователе
Роли	Дерево ролей и инструменты для назначения пользователю ролей
Разрешения	Дерево разрешений и инструменты установки для пользователя индивидуальных разрешений и запретов
Права владения	Дерево владений и инструменты для прикрепления пользователя к дополнительным владениям, настройки областей владения и прав доступа пользователя в каждой области владения

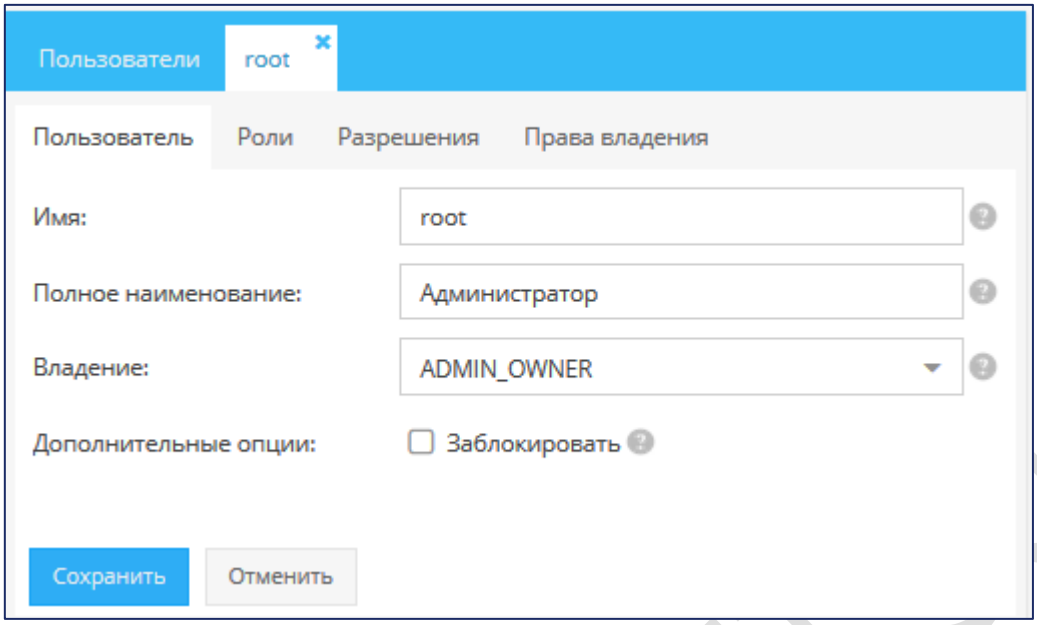


Рисунок 73 – Экранная форма учётной записи. Вкладка **Пользователь**

6.7.2 Создание учётной записи пользователя

Чтобы добавить учётную запись пользователя:

1) Выберите пункт меню Настройки – Доступ – Пользователи.
2) На вкладке **Пользователи** (Рисунок 72) нажмите кнопку **Добавить** .
3) В открывшемся окне **Создание пользователя** (Рисунок 74) заполните поля (Таблица 23).

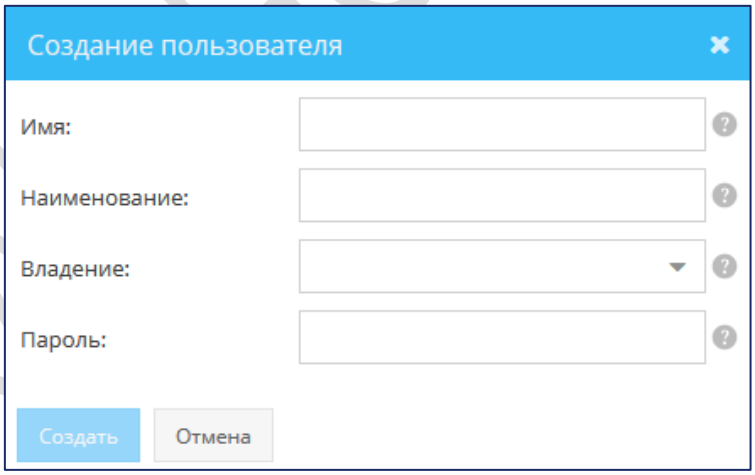


Рисунок 74 – Создание учётной записи пользователя

Таблица 23 – Описание полей вкладки **Пользователь**

Элемент интерфейса	Описание
Поле **Имя**	Регистрационное имя пользователя
Поле **Полное наименование**	Фамилия, имя, отчество пользователя или другое название учётной записи пользователя

Элемент интерфейса	Описание
Поле **Владение**	Владение по умолчанию, к которому прикреплен пользователь
Флажок **Заблокировать**	Если флажок установлен, то учётная запись пользователя заблокирована

Когда будет заполнено поле **Пароль**, добавится ещё одно поле для повторного ввода пароля (Рисунок 75).

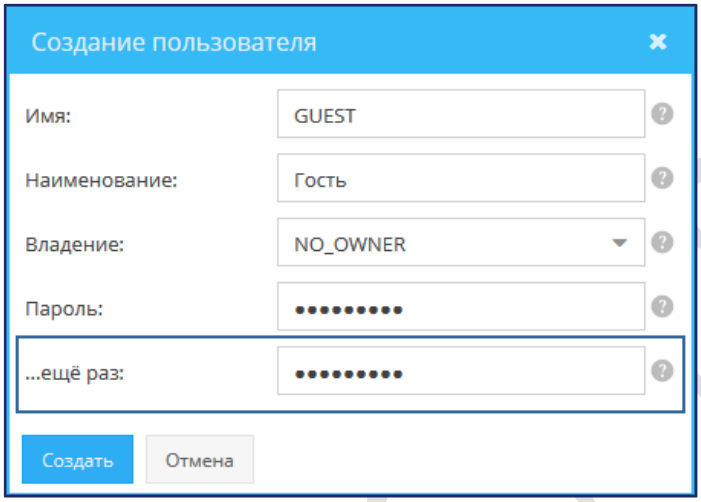


Рисунок 75 – Поле для повторного ввода пароля. Пример новой учётной записи

4) Введите пароль повторно.

5) Нажмите кнопку **Создать**.

Экранная форма учётной записи будет открыта на отдельной вкладке (Рисунок 76).

6) Нажмите кнопку **Сохранить**.

7) Настройте права доступа пользователя на вкладках **Роли**, **Разрешения**, **Права владения** (см. разделы 6.7.3 – 6.7.5).

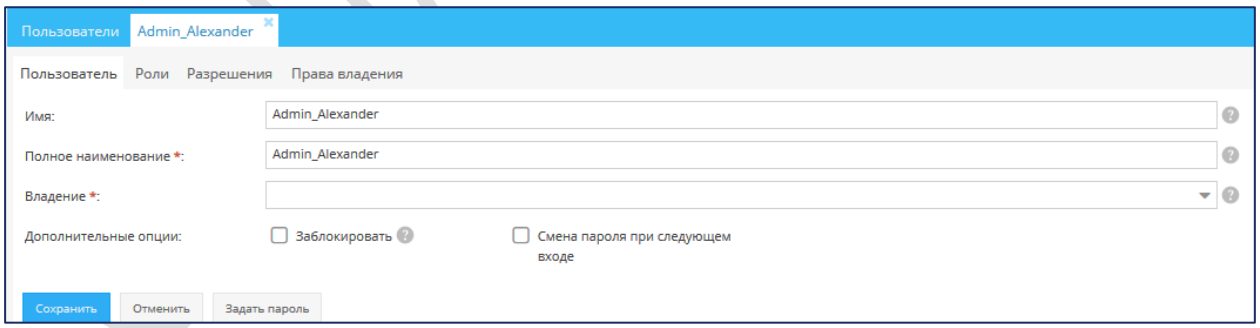


Рисунок 76 – Экранная форма учетной записи пользователя

6.7.3 Порядок настройки прав доступа пользователя

Настройка прав доступа выполняется в следующем порядке:

1) Формирование набора разрешений пользователя:

- назначение пользователю одной роли или нескольких ролей (см. раздел 6.7.4.1);

- если необходимо:
- добавьте в дерево ролей недостающих ролей (см. раздел 6.6.4.4) и установите для них разрешения и запреты (см. раздел 6.6.4.5).
- установите для пользователя индивидуальные разрешения и запреты (см. раздел 6.7.4.2);

2) Формирование схемы владения пользователя:

- настройка области владения по умолчанию и прав доступа пользователя в области владения по умолчанию (см. раздел 6.7.5.1);
- если необходимо:
- добавьте в дерево владений недостающие владения (см. раздел 6.6.3.3);
- прикрепите пользователя к дополнительным владениям;
- настройте области дополнительных владений и права доступа пользователя в каждой области дополнительных владений (см. раздел 6.7.5.1);
- смените владения по умолчанию (см. раздел 6.7.5.2).

6.7.4 Формирование набора разрешений пользователя

6.7.4.1 Назначение ролей пользователю

Использование ролей является основным способом установки разрешений для пользователей. Общие сведения о ролях см. в разделе 6.5.3.1.

Назначение ролей выполняется на вкладке **Роли** экранной формы учётной записи пользователя (Рисунок 77).

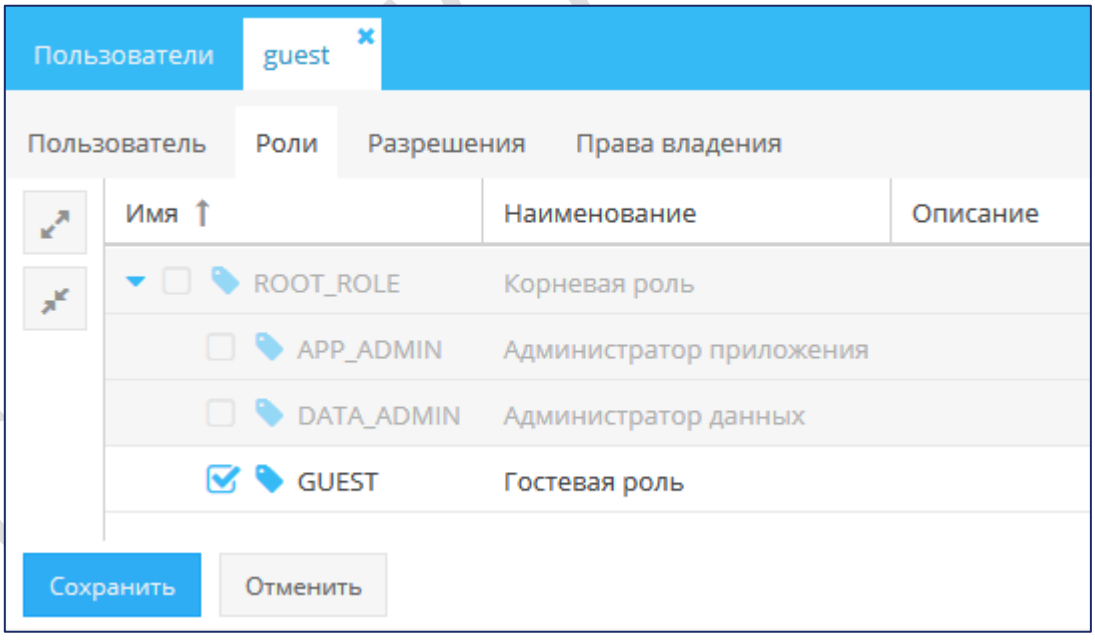


Рисунок 77 – Экранная форма учётной записи пользователя. Вкладка **Роли**

На вкладке отображается дерево ролей, в котором каждый узел снабжен полем для установки флажка.

Чтобы назначить пользователю одну или несколько ролей:

1) Откройте экранную форму учётной записи пользователя (см. раздел 6.7.1).

2) Перейдите на вкладку **Роли** (Рисунок 77).

3) В дереве ролей установите флажок рядом с названием одной роли или нескольких ролей.

4) Нажмите кнопку **Сохранить**.

Пользователь получит доступ к данным из своей схемы владения в соответствии с установленным набором разрешений.

5) Скорректируйте набор разрешений пользователя – установите для него индивидуальные разрешения и запреты (см. раздел 6.7.4.2).

6.7.4.2 Установка разрешений и запретов для пользователя

Администратор может установить для пользователя индивидуальные разрешения и запреты и тем самым скорректировать набор разрешений, которые определяет назначенная роль.

Общие сведения об индивидуальных разрешениях приведены в разделе 6.5.3.2, общие сведения о запретах – в разделе 6.5.3.3.

Установка индивидуальных разрешений и запретов выполняется на вкладке **Разрешения** экранной формы учётной записи пользователя (Рисунок 78).

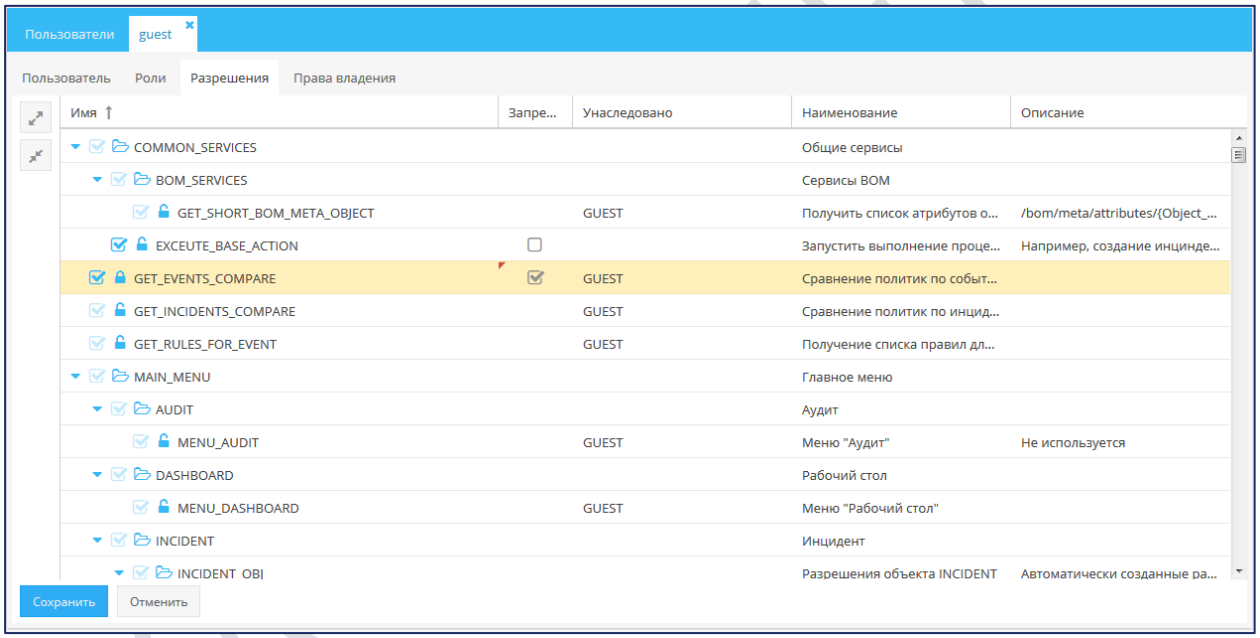


Рисунок 78 – Экранная форма учётной записи пользователя. Вкладка **Разрешения**

Чтобы установить индивидуальные разрешения и запреты:

1) Откройте экранную форму учётной записи пользователя (см. раздел 6.7.1).

2) Перейдите на вкладку **Разрешения** (Рисунок 78).

3) Чтобы установить одно индивидуальное разрешение, установите явный флажок в соответствующем узле дерева (см. раздел 6.6.1).

4) Чтобы установить индивидуальные разрешения сразу во всех дочерних узлах какой-либо папки, установите явный флажок в узле с этой папкой.

5) Чтобы установить запрет на какое-либо разрешение, установите флажок в столбце **Запрещено** – в строке узла с этим разрешением.

Примечание. Запрет можно установить только для явно установленного разрешения. Узлы с такими разрешениями имеют индикацию и поле флажка в столбце **Запрещено.**

6) Нажмите кнопку **Сохранить**.

Пользователь получит доступ к данным из своей схемы владения в соответствии со своим набором разрешений.

6.7.5 Формирование схемы владения пользователя

6.7.5.1 Настройка областей владения пользователя и настройка прав доступа пользователя в областях владения

Общие сведения о владениях приведены в разделе 6.5.4. Сведения о том, к какому владению по умолчанию прикреплен пользователь, приведены на вкладке **Права владения** экранной формы учётной записи пользователя.

Для каждого пользователя следует настроить права доступа в области владения по умолчанию. Можно также предварительно настроить саму область владения по умолчанию, исключив из нее дочерние узлы или корневой узел.

Если необходимо расширить схему владения пользователя, следует прикрепить его к одному или нескольким дополнительным владениям, а затем настроить области дополнительных владений и настроить права доступа пользователя в каждой области дополнительных владений.

Настройка областей владения пользователя и настройка прав доступа пользователя в областях владения выполняются на вкладке **Права владения** (Рисунок 79, Таблица 24).

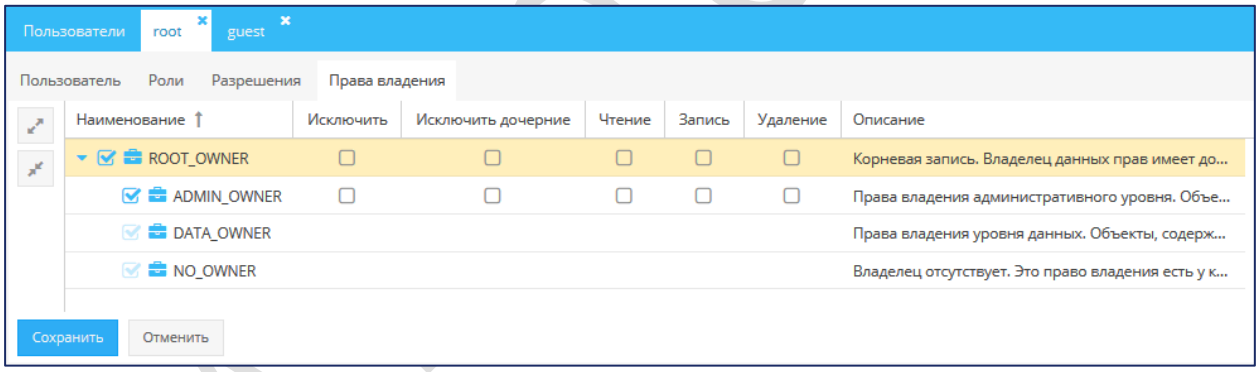


Рисунок 79 – Экранная формы учётной записи пользователя. Вкладка **Права владения**

Таблица 24 – Описание столбцов на вкладке **Права владения**

Столбец	Описание
Наименование	Имя узла в дереве владений. В целом, в столбце отображается дерево владений
Исключить	Инструмент для настройки области владения: исключить из области владения корневой узел
Исключить дочерние	Инструмент для настройки области владения: исключить из области владения все дочерние узлы
Чтение	Инструмент для настройки прав доступа: дать права на чтение записей в таблицах объектов согласно настройке области владения
Запись	Инструмент для настройки прав доступа: дать права на редактирование записей в таблицах объектов согласно настройке области владения

Столбец	Описание
Удаление	Инструмент для настройки прав доступа: дать права на удаление записей в таблицах объектов согласно настройке области владения
Описание	Описание владения

На вкладке **Права владения** отображается дерево владений, в котором каждый узел снабжен полем для установки флажка (см. раздел 6.6.1).

Чтобы настроить области владения пользователя и его права доступа в областях владения:

1) В экранной форме учётной записи пользователя перейдите на вкладку **Права владения.**
2) Прикрепите пользователя к дополнительному владению – в дереве владений установите флажок рядом с названием владения.

   Примечание. Следует также отметить флажком область владения по умолчанию, если в дальнейшем нужно настроить права доступа пользователя в этой области.

3) Настройте области владения, включенные в схему владения пользователя, – установите флажки в столбце **Исключить** или **Исключить дочерние** (см. таблицу 24).
4) Настройте права доступа пользователя в той или иной области владения – установите флажки в столбцах **Чтение**, **Запись**, **Удаление**.
5) Нажмите кнопку **Сохранить**.

Пользователь получит доступ к данным из своей схемы владения в соответствии со своим набором разрешений.

6.7.5.2 Смена владения по умолчанию

Первое прикрепление пользователя к владению по умолчанию выполняется в процессе создания учётной записи пользователя. В каждый момент времени пользователь прикреплен только к одному владению по умолчанию, но его можно поменять.

Чтобы сменить для пользователя владение по умолчанию:

1) Откройте экранную форму учётной записи пользователя (см. раздел 6.7.1).
2) На вкладке **Пользователь**, в поле **Владение**, укажите другое владение по умолчанию – выберите значение в раскрывающемся списке (Рисунок 80).
3) Нажмите кнопку **Сохранить**.

   Примечание. При создании экземпляров объектов от имени этого пользователя соответствующие записи в таблицах объектов будут маркироваться идентификатором актуального владения по умолчанию. Записи, созданные в прошлом, останутся маркированными идентификаторами тех владений, которые были владением по умолчанию на момент создания записи.

4) Настройте права доступа пользователя в области владения по умолчанию. Предварительно можно настроить саму область владения по умолчанию – исключить из нее дочерние узлы или корневой узел (см. раздел 6.7.5.1).

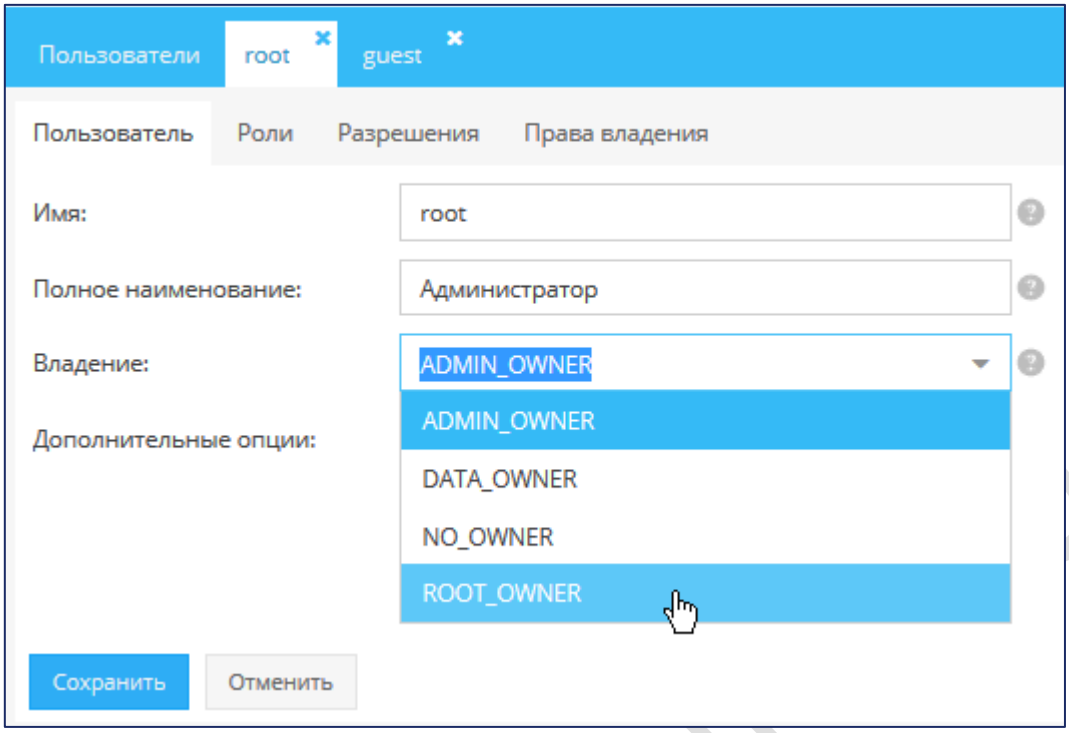


Рисунок 80 – Смена владения по умолчанию

6.7.6 Редактирование учётной записи пользователя

Чтобы отредактировать учётную запись пользователя:

1) Выберите пункт меню Настройки – Доступ – Пользователи.
2) На вкладке со списком пользователей дважды щёлкните по строке учётной записи.
3) Внесите изменения в поля на всех вкладках экранной формы.
4) Нажмите кнопку **Сохранить**.

6.7.7 Блокировка и разблокировка учётной записи пользователя

Администратор может заблокировать учётную запись пользователя. Такой пользователь теряет доступ к Jet Detective до тех пор, пока администратор не разблокирует его.

Чтобы заблокировать:

1) Откройте экранную форму учётной записи пользователя (см. раздел 6.7.1).
2) На вкладке **Пользователь** установите флажок **Заблокировать**.
3) Нажмите кнопку **Сохранить**.

Чтобы разблокировать:

1) На вкладке **Пользователь** снимите флажок **Заблокировать**.
2) Нажмите кнопку **Сохранить**.

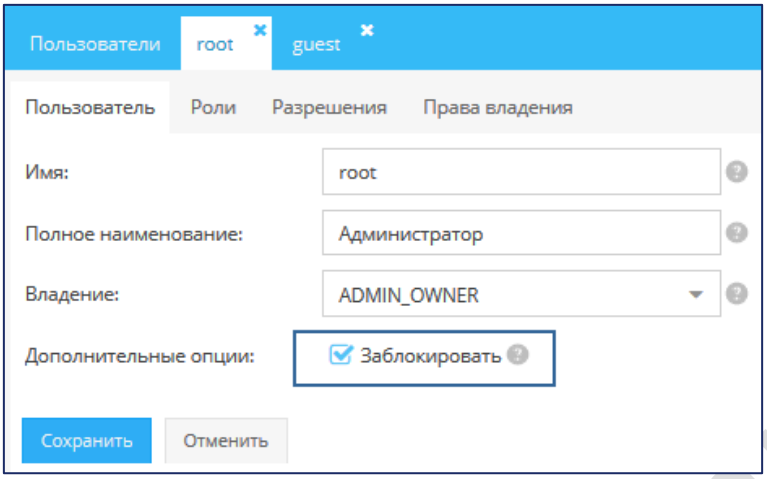


Рисунок 81 – Блокировка учётной записи пользователя

6.7.8 Управление паролем учётной записи пользователя

Чтобы задать новый пароль для учетной записи пользователя:

1) Откройте экранную форму учётной записи пользователя (см. раздел 6.7.1).
2) На вкладке **Пользователь** нажмите кнопку **Задать пароль** (для доступа к этой кнопке у пользователя должно быть выдано отдельное разрешение).
3) В открывшемся модальном окне (Рисунок 82) введите новый пароль для учетной записи пользователя.

Появится дополнительное поле для повторного ввода (Рисунок 83).

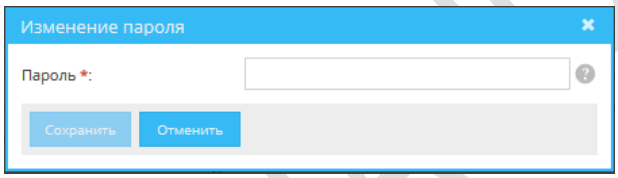


Рисунок 82 – Модальное окно для изменения пароля учетной записи пользователя

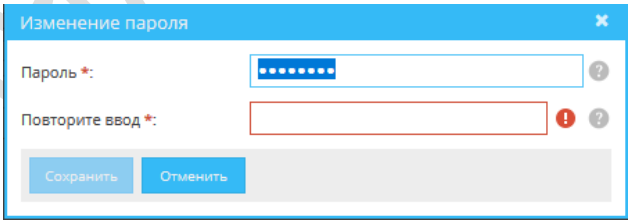


Рисунок 83 – Повторный ввод пароля

4) Повторите указанный пароль.
5) Нажмите кнопку **Сохранить.**

Чтобы при следующей авторизации в системе была инициирована смена пароля у учетной записи:

1) Откройте экранную форму учётной записи пользователя (см. раздел 6.7.1).
2) На вкладке Пользователь установите флаг Смена пароля при следующем входе.
3) Нажмите кнопку **Сохранить.**

При следующей авторизации выбранного пользователя система автоматически запросит смену пароля. Когда пароль будет изменен, флаг **Смена пароля при следующем входе** будет автоматически снята с учетной записи.

6.7.9 Удаление учётной записи пользователя

Чтобы удалить учётную запись пользователя:

1) Выберите пункт меню Настройки – Доступ – Пользователи.
2) На вкладке со списком пользователей выберите учётную запись пользователя.
3) Нажмите кнопку **Удалить**  (Рисунок 84).
4) Нажмите кнопку **Да** в появившемся запросе.

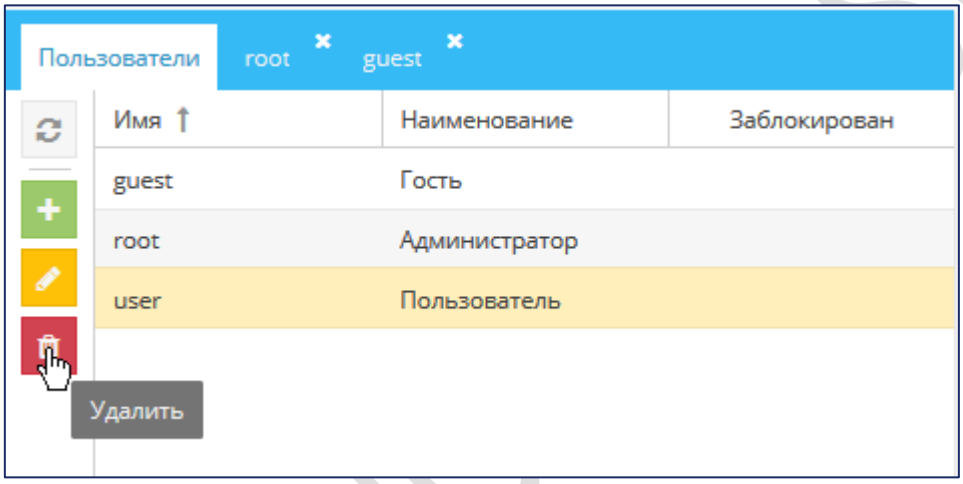


Рисунок 84 – Переход к режиму удаления учётной записи пользователя

6.8 ОТЧЕТЫ

6.8.1 Общие сведения

В Jet Detective реализована возможность создавать различные отчеты по заранее загруженным шаблонам. Отчеты можно высылать на e-mail, выкладывать в настроенную сетевую папку или выгружать локально. Также можно настраивать формирование и рассылку/публикацию отчетов по расписанию.

6.8.2 Шаблоны отчетов

Шаблон отчета – это сущность, которая хранит параметры шаблона отчета, созданного в формате rtrp, а также входные параметры отчета и их характеристики.

6.8.2.1 Просмотр и редактирование шаблона отчета

Чтобы просмотреть шаблон отчетов:

1) Выберите пункт меню Настройки – **Отчеты** – **Шаблоны отчетов**.

В рабочей области отобразится одна или несколько вкладок:

- **Шаблоны отчетов** (Рисунок 85);

- экранных форм шаблонов отчетов, открытых в этой сессии.

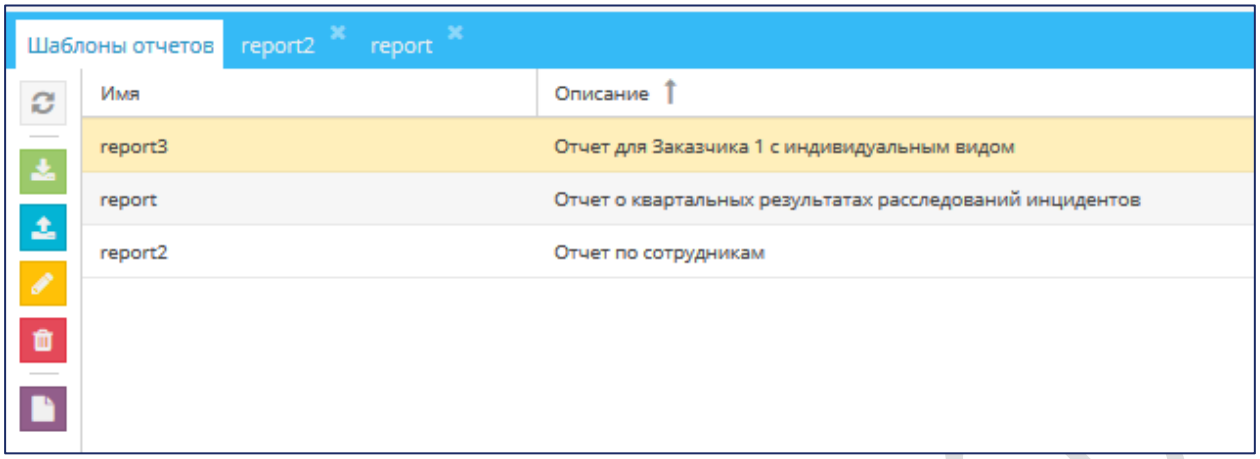


Рисунок 85 – Список шаблонов отчетов, загруженных в Jet Detective

2) На вкладке с перечнем **Шаблонов отчетов** дважды щёлкните по строке записи шаблона отчета. Экранная форма шаблона отчета отобразится на отдельной вкладке (Рисунок 86).

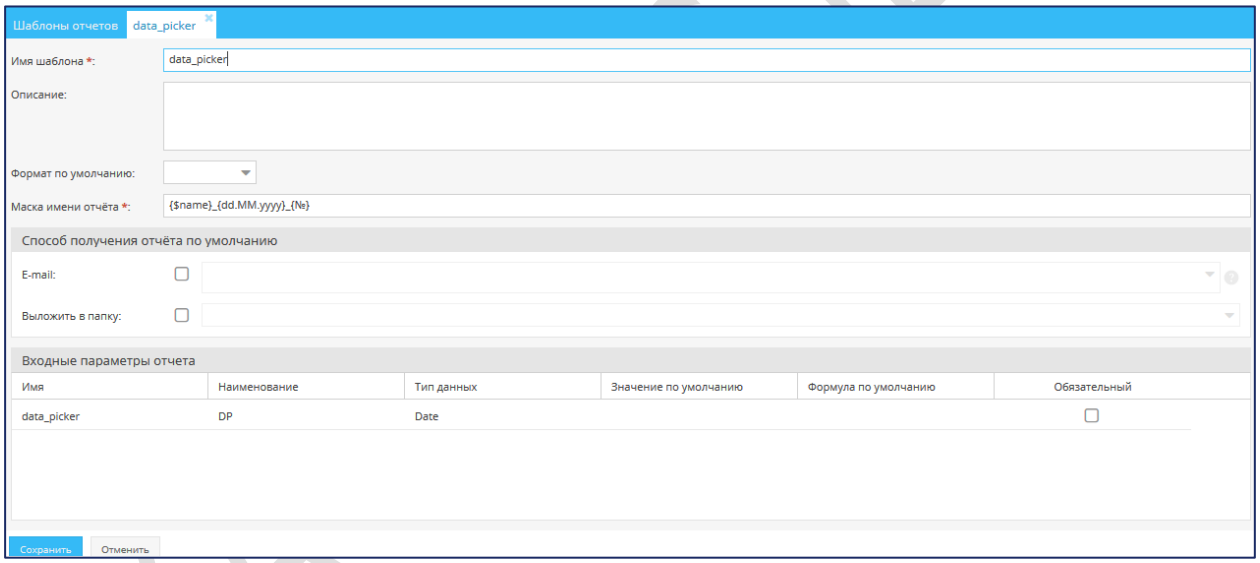


Рисунок 86 – Экранная форма шаблона отчета

3) Внесите изменения в поля экранной формы и выберите входные параметры (см. таблицу 25).

Таблица 25 – Элементы формы шаблона отчета

№	Поле	Описание
1.	Поле **Имя шаблона**	Имя шаблона отчета. При загрузке шаблона отчета заполняется именем, указанным в файле загружаемого шаблона (формат rtrp), или именем загружаемого файла, если в шаблоне имя не задано. Поле доступно для редактирования
2.	Поле **Описание**	Текстовое поле для подробного описания шаблона. При загрузке шаблона поле пустое. Доступно для редактирования

№	Поле	Описание
3.	Поле **Формат по умолчанию**	Формат отчета, который будет использоваться по умолчанию, если при формировании не будет указано другое. Раскрывающийся список. Возможен выбор только одного значения. Доступные значения: ▪ PDF ▪ CSV ▪ XLS ▪ RTF ▪ DOCX
4.	Поле **Маска имени отчета**	Поле позволяет задать маску имени, для отчетов, которые будут формироваться. В маске доступно использование следующих составляющий: ▪ **Константа** – любые буквы (латиница, кириллица), проблемы. нижнее подчеркивание ▪ **Дата/время формирования** – экранированное фигурными скобками одно из значений: ▪ dd.MM.yyyy HH:mm:ss ▪ dd.MM.yyyy ▪ dd.MM.yy ▪ yyyy ▪ **Входные параметры отчета** – экранированное фигурными скобками имя входного параметра. Позволяет использовать значения входных параметров в имени. Также можно указывать, какое количество символов необходимо вывести из значения указанного параметра: ▪ для вывода первых X символов значения параметра необходимо указать (X) после открывающей скобкой { ▪ для вывода последний X символов значения параметра необходимо указать (X) перед закрывающей скобкой } ▪ (X) – только положительное число **Пример:** {(3)pan} – вернет первые три символа значения параметра pan, без указания имени параметра. *Примечание:* 1) Если сумма указанных для вывода символов (X) больше, чем общее количество символов в значении параметра, то выводится все значение параметра без искажений. 2) Если у параметра задано выводить часть символов и с начала, и конца значения И сумма количества символов (X) меньше, чем общее количество символов в значении параметра, то между выводимыми частями значения добавляется знак "_". ▪ **Порядковый номер** – экранированное фигурными скобками знак № ▪ **Имя шаблона отчета** – экранированное фигурными скобками слово «$name» **Пример маски имени:** *Отчет_1001_{dd.MM.yyyy} {incident_id}_{№}*
5.	Блок **Способ получения отчета по умолчанию**	Блок отвечает за то, какие действия необходимо выполнить с отчетом по умолчанию, если иного не будет указано при его формировании. **e-mail:** Если **флаг установлен**, то становится доступным поле выбора электронного адреса.

№	Поле	Описание
		Выберите адрес в раскрывающемся списке e-mail) или укажите в поле произвольный адрес e-mail. Если указан произвольный адрес после него необходимо поставить «,» (запятую), чтобы адрес добавится в список. Если **флаг снят**, то адрес рассылки по умолчанию не используется. **Выложить в папку:** Если **флаг установлен**, то становится доступным раскрывающийся список справочника директорий. Возможен выбор одного значения. В справочнике директорий может быть указана динамическая директория. Имя директории может формироваться из тех же составляющих, что используются в поле **Маска имени отчета.** Если **флаг установлен**, то поле не может быть пустым. Если **флаг не установлен** директория по умолчанию не используется при формировании отчета.
6.	Табличный список **Входные параметры отчета**	Таблица параметров, которые необходимо подать на вход отчета для его построения. Таблица с входными параметрами не доступна для редактирования
6.1.	Столбец **Тип данных**	Тип данных, который используется во входном параметре. *Примечание. Для корректного формирования отчетов, входные параметры должны быть только следующих типов: Number, Date, String, Boolean*
6.2.	Столбец **Значение по умолчанию**	Значение, которое будет подставлено в параметр по умолчанию при формировании отчёта, если не будет указано другое значение
6.3.	Столбец **Формула по умолчанию**	Формула, которая будет использована в параметре по умолчанию при формировании отчёта, если не будет указано другое значение
6.4.	Столбец **Обязательный**	Флаг, который указывает на обязательность передачи параметра при формировании отчёта

4) Нажмите кнопку **Сохранить**.

6.8.2.2 Загрузка шаблона отчета

Чтобы загрузить шаблон отчета в Jet Detective:

1) Откройте список **Шаблоны отчетов** (см. раздел 6.8.2.1).

2) Нажмите кнопку **Загрузить**  .

Откроется модальное окно выбора файла для загрузки (Рисунок 87).

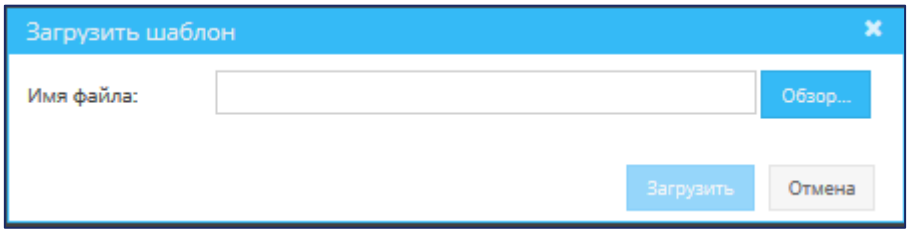


Рисунок 87– Окно выбора файла для загрузке шаблона отчета

3) Нажмите кнопку **Обзор** и выберите файл шаблона отчета.

4) Нажмите кнопку **Загрузить.**

Модальное окно для выбора файла закроется, в списке шаблонов отчета появится новая запись с загруженным шаблоном.

6.8.2.3 Выгрузка шаблона отчета

Чтобы выгрузить шаблон отчета из Jet Detective:

1) Откройте список **Шаблоны отчетов** (см. раздел 6.8.2.1).

3) Выберите запись в списке.

4) Нажмите кнопку **Выгрузить**  **.**

Выгрузка файла будет выполнена согласно настройкам браузера, в котором работает авторизованный пользователь.

6.8.2.4 Удаление шаблона отчета

Чтобы удалить шаблон:

1) Откройте список **Шаблоны отчетов** (см. раздел 6.8.2.1).

5) Выберите запись в списке.

6) Нажмите кнопку **Удалить**  **.**

> *Примечание*. Удалить можно только те шаблоны, по которым нет ни одного запрошенного отчета (см. раздел 6.8.3) и не создана задача на расписание (см. раздел 6.8.4).

6.8.2.5 Формирование отчета по шаблону

Чтобы сформировать отчет по шаблону:

1) Откройте список **Шаблоны отчетов** (см. раздел 6.8.2.1).

2) Выберите запись в списке.

3) Нажмите кнопку **Сформировать** 

Откроется форма для задания параметров формирования отчета (Рисунок 88).

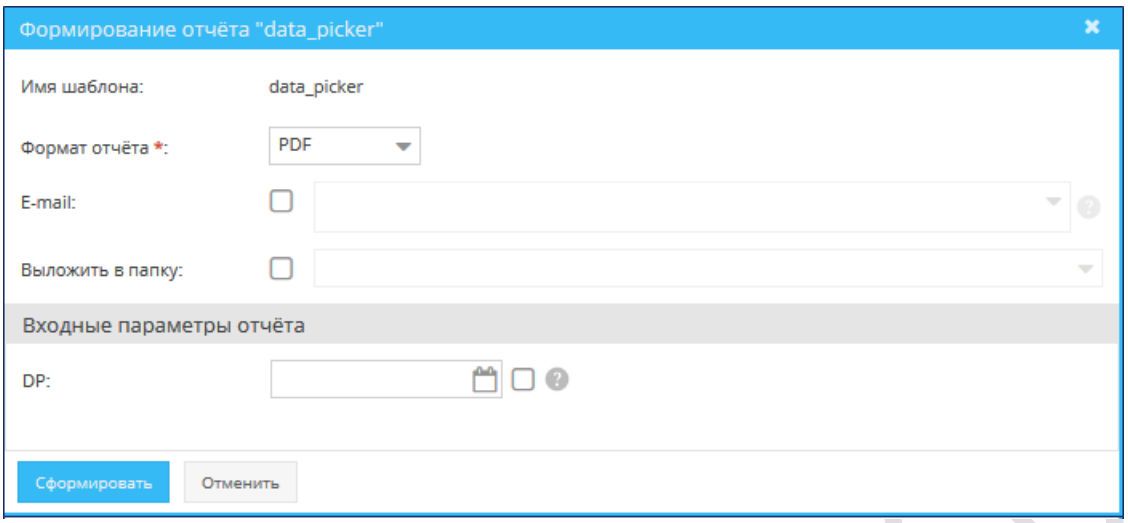


Рисунок 88 – Форма для задания параметров формирования отчета

4) Заполните поля формы (Таблица 26).

Таблица 26 – Элементы формы формирования отчета по шаблону

Элемент интерфейса	Описание элемента и его применения
Поле **Имя**	Поле недоступно для редактирования. Содержит имя шаблона, по которому будет сформирован отчет
Поле **Формат отчета**	Выберите в раскрывающемся списке формат, в котором будет сформирован отчет. Доступные значения: ▪ PDF (выбрано по умолчанию); ▪ CSV; ▪ XLS; ▪ RTF; ▪ DOCX Если у выбранного шаблона отчета заполнено поле **Формат по умолчанию** (см. раздел 6.8.2.1), то указанный в шаблоне формат подставится автоматически
Флаг **e-mail**	Если у выбранного шаблона отчета заполнено поле **e-mail** в блоке **Способы получения по умолчанию**, то указанные в шаблоне адреса подставятся автоматически. Скорректируйте список адресов, если требуется. Корректировка списка выполняется так же, как при редактировании шаблона отчета (см. раздел 6.8.2.1).
Флаг **выложить в папку**	Если у выбранного шаблона отчета заполнено поле **Выложить в папку** в блоке **Способы получения по умолчанию** (см. раздел 6.8.2.1), то указанные в шаблоне директории подставятся автоматически. Скорректируйте список директорий, если требуется. Корректировка списка выполняется так же, как при редактировании шаблона отчета (см. раздел 6.8.2.1).

Элемент интерфейса	Описание элемента и его применения
Табличный список **Входные параметры**	В этом блоке отображаются все входные параметры, которые можно подать на вход шаблона отчета. Если в шаблоне отчета заданы **Значение по умолчанию** или **Формула по умолчанию** для параметра, то для этих параметров значения подставятся автоматически. Заполните входные параметры отчета. Если требуется, измените значения параметров, которые заполнены автоматически. Для параметров с типом данных **Дата** доступно два способа заполнения: ▪ Указание конкретной даты – выберите значение в календаре. ▪ Указание формулы даты – поставьте рядом с параметром флаг **Формула** и введите формулу используя следующий формат: **=ФУНКЦИЯ()[+/-NT][+/-NT][+/-NT]…,** где: a) **ФУНКЦИЯ()** – одна из следующих функций: ▪ **NOW()** – сейчас, т. е. дата и время формирования отчета; ▪ **TODAY()** – сегодня, т. е. день формирования отчёта (время 00:00:00); ▪ **YESTERDAY()** – вчера, т. е. предыдущий день относительно дня формирования отчёта (время 00:00:00); b) **[]** – опциональное дополнение к функции; c) **+/-** – добавление или уменьшение времени в функции; d) **N** – число временных единиц, добавляемых к функции; e) **T** – временная единица, которая может быть одной из перечисленных ниже: ▪ **y** – год, ▪ **M** – месяц, ▪ **d** – день, ▪ **h** – час, ▪ **m** – минута, ▪ **s** – секунда. Пример корректной формулы: **=NOW()-1y+3d-1h**

5) Нажмите кнопку **Сформировать.**

После этого:

- Модальное окно с параметрами формирования закроется.
- Будет создана запись в запрошенных отчетах (см. раздел 6.8.3).
- Когда формирование отчета завершится, выполнятся действия согласно флагам, установленным при указании параметров формирования (отправка отчета на e-mail или размещение в папке).

6.8.3 Запрошенные отчеты

Любой сформированный по шаблону отчет фиксируется в разделе **Запрошенные отчеты**.

В этом разделе отображаются:

- дата формирования отчета;
- шаблон, по которому сформировался отчёт;
- выходные параметры отчета;
- статус формирования

Любой отчет, запрошенный ранее, можно загрузить локально, отправить на e-mail или выложить в папку.

6.8.3.1 Просмотр запрошенного отчета

Чтобы посмотреть отчет:

1) Выберите пункт меню Настройки – **Отчеты** – **Запрошенные отчеты**.

В рабочей области отобразится одна или несколько вкладок:

- **Запрошенные отчеты** (Рисунок 89);
- экранных форм запрошенных отчетов, открытых в этой сессии.

Статусы запрошенных отчетов описаны в таблице 28.

2) На вкладке **Запрошенные отчеты** дважды щёлкните по строке записи отчета.

Экранная форма запрошенного отчета отобразится на отдельной вкладке (Рисунок 90). Все поля формы недоступны для редактирования. Описание элементов формы приведено в таблице 27.

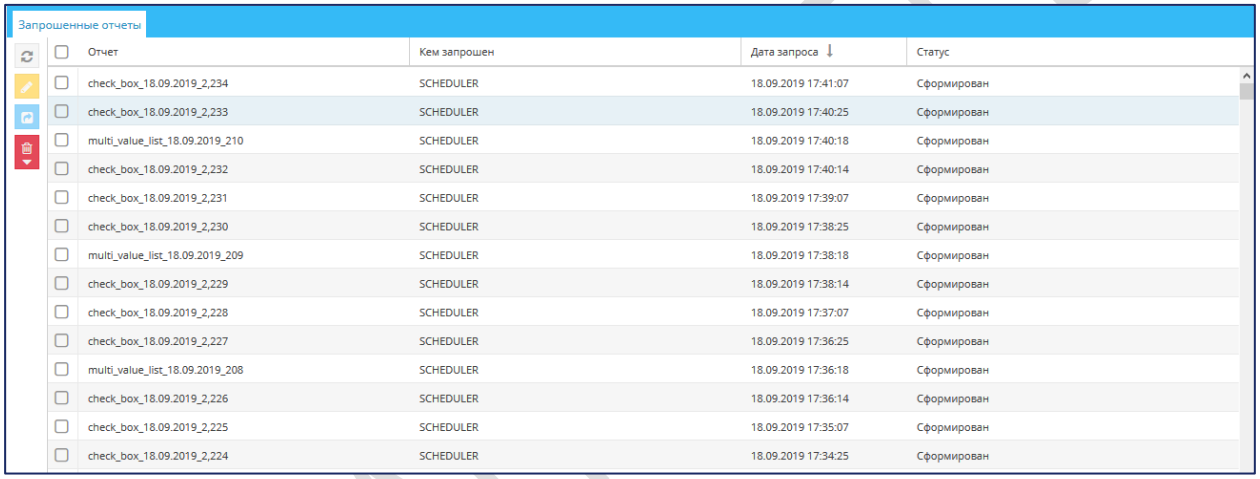


Рисунок 89 – Список запрошенных отчетов

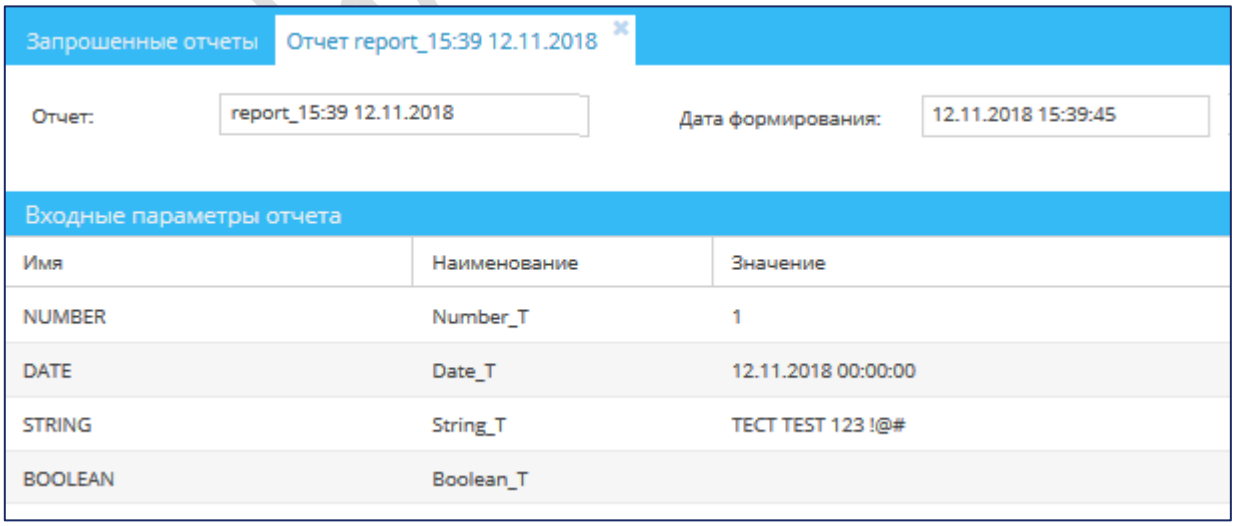


Рисунок 90 – Форма запрошенного отчета

Таблица 27 – Описание элементов формы запрошенного отчета

Элемент интерфейса	Описание
Поле **Отчет**	Имя запрошенного отчета – состоит из имени шаблона отчета, по которому был сформирован отчет, и даты формирования
Поле **Дата формирования**	Дата и время, когда был запрошен отчет
Табличный список **Входные параметры отчета**	Входные параметры отчета и значения этих параметров, с которыми был сформирован отчет

Таблица 28 – Статусы запрошенного отчета

Статус	Описание
Сформирован	Отчет сформирован
Формируется	Выполняется формирование отчета
Ошибка	Не удалось сформировать отчет

6.8.3.2 Получение запрошенного отчета

Чтобы получить запрошенный отчет:

1) Откройте список **Запрошенные отчеты** (см. раздел 6.8.3.1).
2) Установите флажки для одной или нескольких записей списка.
3) Нажмите кнопку **Получить**  .

Откроется модальное окно **Получить выбранные отчёты** (Рисунок 91).

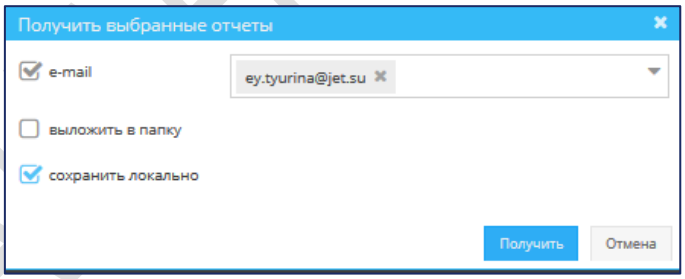


Рисунок 91 – Окно **Получить выбранные отчёты**

4) Укажите параметры получения отчета. Их описание приведено в таблице 29.

Таблица 29 – Параметры получения запрошенного отчета

Параметр	Описание
e-mail	Логика работы Jet Detective при указании этого параметра такая же, как при формировании отчета по шаблону (см. раздел 6.8.2.5)
выложить в папку	Логика работы Jet Detective при указании этого параметра такая же, как при формировании отчета по шаблону (см. раздел 6.8.2.5)

Параметр	Описание
сохранить локально	Если указан этот параметр, то выбранные отчеты сохранятся локально на компьютере авторизованного пользователя. При сохранении отчёта учитываются параметры сохранения для браузера, в котором работает пользователь

5) Нажмите кнопку **Получить.**

6.8.3.3 Удаление запрошенных отчетов

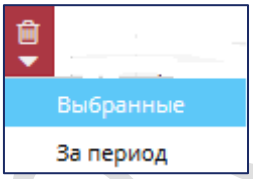
Чтобы удалить запрошенные отчеты:

1) Откройте список **Запрошенные отчеты** (см. раздел 6.8.3.1).
2) Существует два способа удаление:
   - Удаление выбранных записей списка запрошенных отчетов:

   а) Выберите записи в списке запрошенных отчетов

   б) Нажмите кнопку **Удалить**.

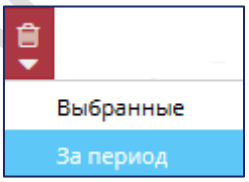
   в) Выберите пункт **Выбранные**:



   - Удаление запрошенных отчетов за период:

   а) Нажмите кнопку **Удалить**.

   б) Выберите пункт **За период**:



   в) В открывшемся модальном окне (Рисунок 92) укажите период для удаления и выберите шаблон, по которому необходимо удалить запрошенные отчеты.

Если шаблон не указан, то удалятся всее запрошенные отчеты за указанный период.

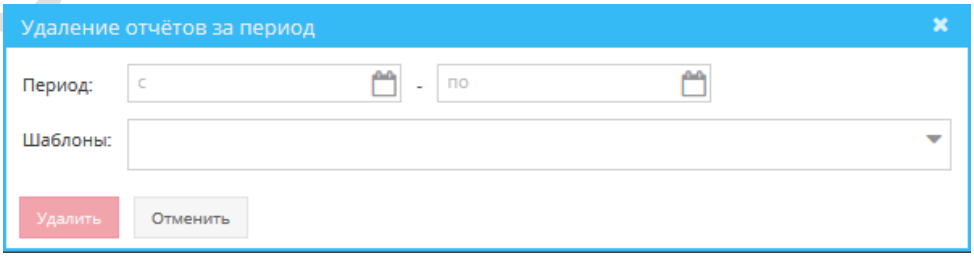


Рисунок 92 – Модальное окно удаления запрошенных отчетов за период

   г) Нажмите **Удалить**

6.8.4 Расписание отчетов

Для регулярного формирования отчетов по заданным параметрам в Jet Detective реализован механизм создания расписания. Этот механизм позволяет выбрать шаблон отчета, задать периодичность формирования, способ получения отчета и значения входных параметров отчета. Задание на расписание выполняется с указанной периодичностью. Все сформированные по расписанию отчеты сохраняются в **Запрошенных отчетах** (см. раздел 6.8.3).

6.8.4.1 Просмотр расписания

Чтобы просмотреть расписание формирования отчетов:

1) Выберите пункт меню Настройки – **Отчеты** – **Расписание**.

В рабочей области отобразится одна или несколько вкладок:

- **Расписание** (Рисунок 93);
- экранных форм расписаний формирований отчетов, открытых в этой сессии.

В списке расписаний в столбце **Состояние** отображается статус каждой записи. Описание значения каждого состояния приведено в 30.

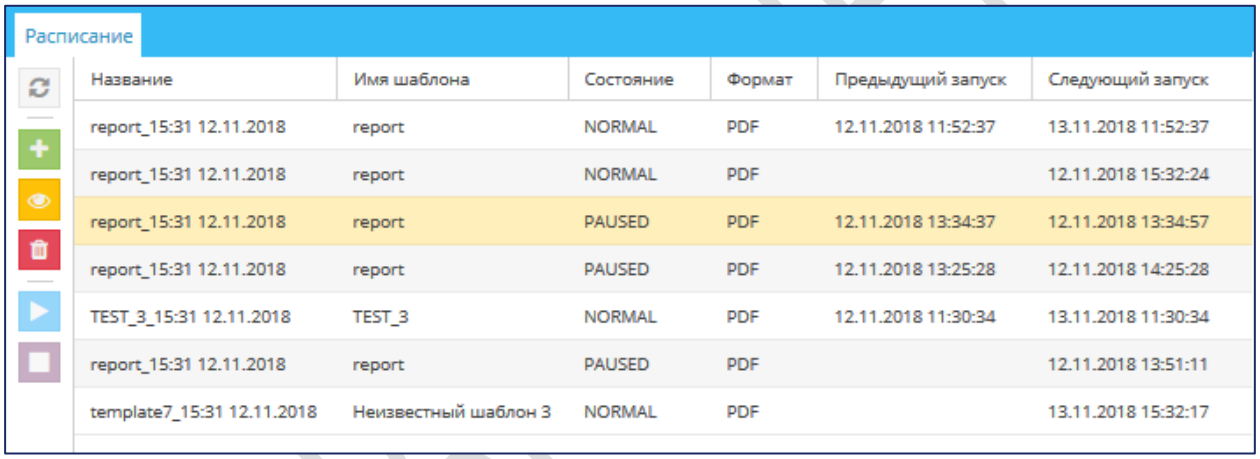


Рисунок 93 – Список расписаний формирования отчетов

Таблица 30 – Статусы расписаний формирования отчетов

Статус	Описание
NORMAL	Расписание действует и по нему формируются отчеты
PAUSED	Формирование отчетов по расписанию приостановлено
ERROR	В процессе работы расписания отчетов произошла ошибка. Необходимо повторно запустить формирование отчетов по расписанию (см. описание в разделе 6.8.4.5)
BLOCKED	Формирование отчета по расписанию невозможно, т. к. перегружен сервис построения отчетов. Когда сервис освободится для выполнения задания по расписанию, статус поменяется автоматически

2) На вкладке с перечнем **Расписаний** дважды щёлкните по строке записи.

Экранная форма расписания формирования отчета отобразится на отдельной вкладке (Рисунок 94). Описание элементов формы расписания приведено в таблице 31.

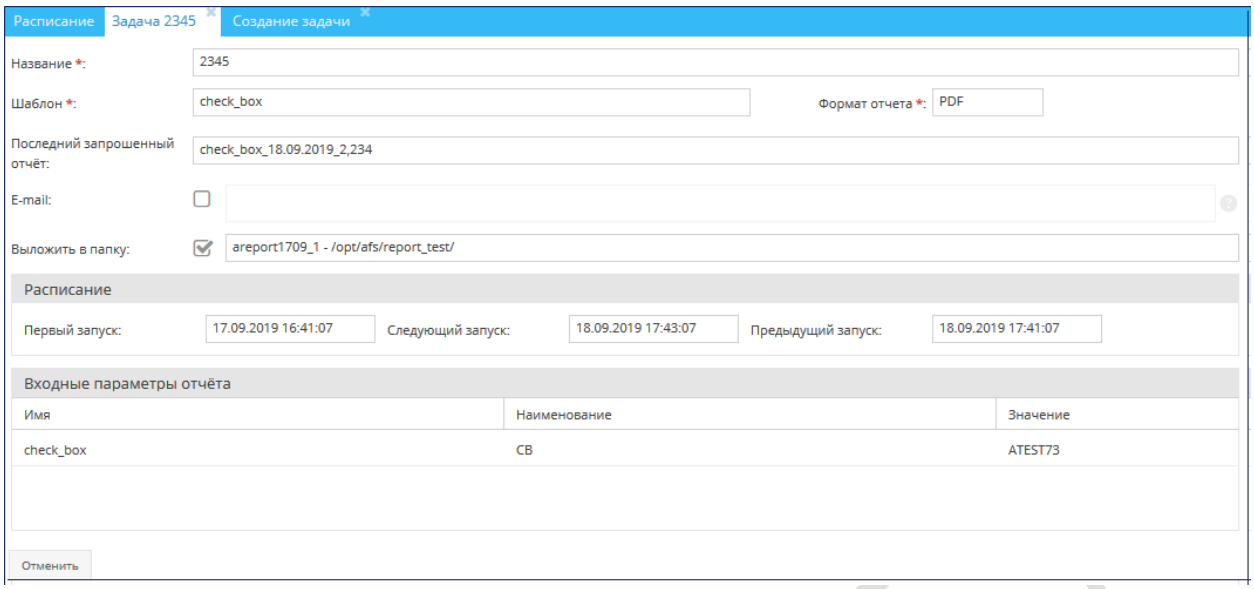


Рисунок 94 – Форма расписания формирования отчета

Таблица 31 – Элементы формы расписания для формирования отчетов

Элемент интерфейса	Описание
Поле **Название**	Наименование создаваемого расписания для формирования отчета
Поле **Шаблон**	Имя используемого шаблона отчета (см. раздел 6.8.2)
Поле **Последний запрошенный отчет**	Имя последнего запрошенного отчета по этому расписанию
Поле **Формат отчета**	Формат, в котором формируется отчет
Флаг **e-mail** и поле рядом	Адреса e-mail для рассылки сформированного отчета
Флаг **выложить в папку**	Директория, куда публикуются сформированные отчеты
Группа полей **Расписание**	**Первый запуск** – дата и время первого формирования отчета по расписанию. **Предыдущий запуск** – дата и время предыдущего формирования отчета. **Следующий запуск** – дата и время, когда в следующий раз отчет будет сформирован по расписанию, если расписание будет запущено в этот момент (статус NORMAL)
Табличный список **Входные параметры отчета**	Входные параметры отчета и их значения, с которыми выполняется формирование отчета по расписанию

6.8.4.2 Создание и запуск расписания

Чтобы создать расписание формирования отчетов:

1) Откройте список **Расписание** (см. раздел 6.8.4.1).

2) Нажмите кнопку **Добавить**  .

Откроется новая вкладка с формой для создания нового расписания формирования отчета (Рисунок 95).

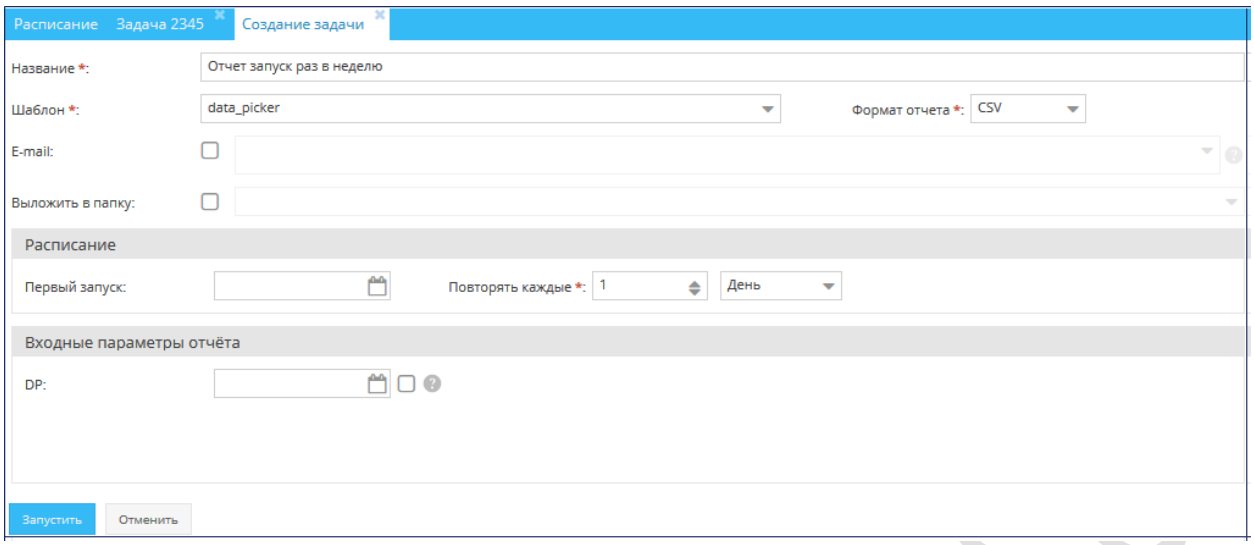


Рисунок 95 – Форма создания расписания формирования отчета

3) Заполните поля формы. Описание элементов формы приведено в таблице 32.

Таблица 32 – Элементы формы создания расписания формирования отчета

Элемент интерфейса	Описание элемента и его применения
Поле **Название**	Укажите имя создаваемого расписания
Поле **Шаблон**	Выберите в раскрывающемся списке шаблон, на основе которого будет формироваться отчет
Поле **Формат отчета**	Заполните аналогично заполнению одноименного поля при формировании отчета по шаблону (см. раздел 6.8.2.5)
Флаг **e-mail**	Логика работы Jet Detective при установке флага такая же, как при формировании отчета по шаблону (см. раздел 6.8.2.5)
Флаг **выложить в папку**	Логика работы Jet Detective при установке флага такая же, как при формировании отчета по шаблону (см. раздел 6.8.2.5)
Группа полей **Расписание**	Группа полей, в котором указаны поля параметров, отвечающих за регулярность формирования отчета по заданному расписанию. Укажите: ▪ **Первый запуск** – дату и время первого запуска формирования отчета по расписанию. Параметр не обязательный. *Примечание.* Дата **Первый запуск** не может быть меньше даты сохранения расписания. Если дата не указана, то в первый раз формирование отчета начнется сразу после сохранения расписания, а дата заполнится автоматически. ▪ **Повторять каждый** – интервал и единица измерения интервала повторения формирования отчета (начиная с даты первого запуска)
Группа полей **Входные параметры отчета**	Заполните поля, аналогично полям входных параметров при формировании отчета по шаблону (см. раздел 6.8.2.5). В доступных формулах для параметров с типом **Дата** добавлены две новые функции: ▪ **PREV_FIRE()** – время последнего срабатывание расписания (параметр **Предыдущий запуск**); ▪ **NEXT_FIRE()** –– время следующего срабатывания расписания (параметр **Следующий запуск**)

4) Нажмите кнопку **Запустить.**

В таблицу расписаний добавиться новая запись. Формирование отчета будет выполняться согласно настроенному расписанию.

6.8.4.3 Копирование расписания

Чтобы скопировать расписание формирования отчетов:

6) Откройте список **Расписание** (см. раздел 6.8.4.1).

7) Выберите запись в списке.

8) Нажмите кнопку **Копировать**  .

Откроется вкладка с формой создания нового расписания формирования отчета (Рисунок 95). Поля формы заполнены теми же значениями, что указаны для копируемой записи, но при этом поля группы **Расписание** будут пустыми.

9) Заполните поля формы (см. раздел 6.8.4.2).

10) Нажмите кнопку **Запустить**.

6.8.4.4 Удаление расписания

Чтобы удалить расписание формирования отчетов:

1) Откройте список **Расписание** (см. раздел 6.8.4.1).

2) Выберите одну запись в списке.

3) Нажмите кнопку **Удалить**  .

6.8.4.5 Перезапуск формирования отчета по расписанию

Для перезапуска формирования отчета:

1) Откройте список **Расписание** (см. раздел 6.8.4.1).

2) Выберите запись в списке.

3) Нажмите кнопку Продолжить выполнение задачи  .

6.8.4.6 Остановка формирования отчета по расписанию

Для остановки формирования отчета:

1) Откройте список **Расписание** (см. раздел 6.8.4.1).

2) Выберите одну запись в списке.

3) Нажмите кнопку **Остановить задачу**  .

6.9 СЛУЖЕБНЫЕ СПРАВОЧНИКИ

6.9.1 Серверы обработки

Сервер обработки – справочник серверов, которые используются для выполнения политик выявления.

6.9.1.1 ПРОСМОТР СЕРВЕРОВ ОБРАБОТКИ

Чтобы посмотреть запись в справочнике серверов обработки:

1) Выберите пункт меню Настройки – **Прочее** – **Серверы обработки**.

В рабочей области отобразится одна или несколько вкладок:

- **Серверы обработки** – перечень серверов обработки (Рисунок 96);
- экранных форм серверов обработки, открытых в этой сессии.

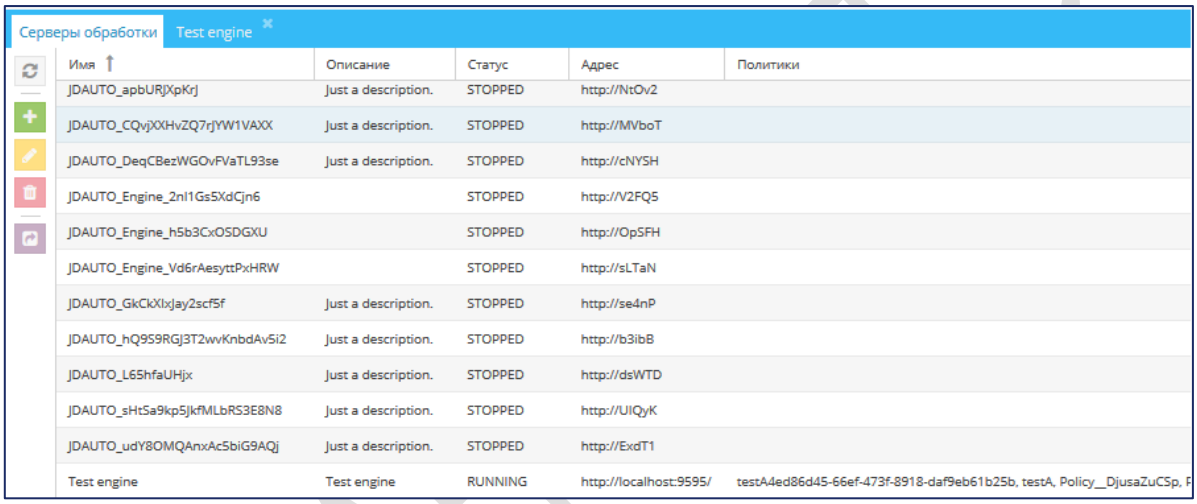


Рисунок 96 – Вкладка с перечнем серверов обработки

В перечне серверов обработки (Рисунок 96) в столбце **Статус** отображается состояние каждой записи. Описание значения каждого статуса описано в таблице 33.

Таблица 33 – Возможные статусы сервера обработки

Статус	Описание
RUNNING	Сервер запущен и работает
STORED	Сервер остановлен

2) На вкладке с перечнем дважды щёлкните по строке записи сервера обработки.

Экранная форма сервера обработки откроется на отдельной вкладке (Рисунок 97).

Форма содержит поля **Имя**, **Описании** и **Адрес** и список политик, связанных с сервером обработки. Связь политики и сервера обработки устанавливается при создании и настройке политики выявления (см. раздел 7.1.3.2).

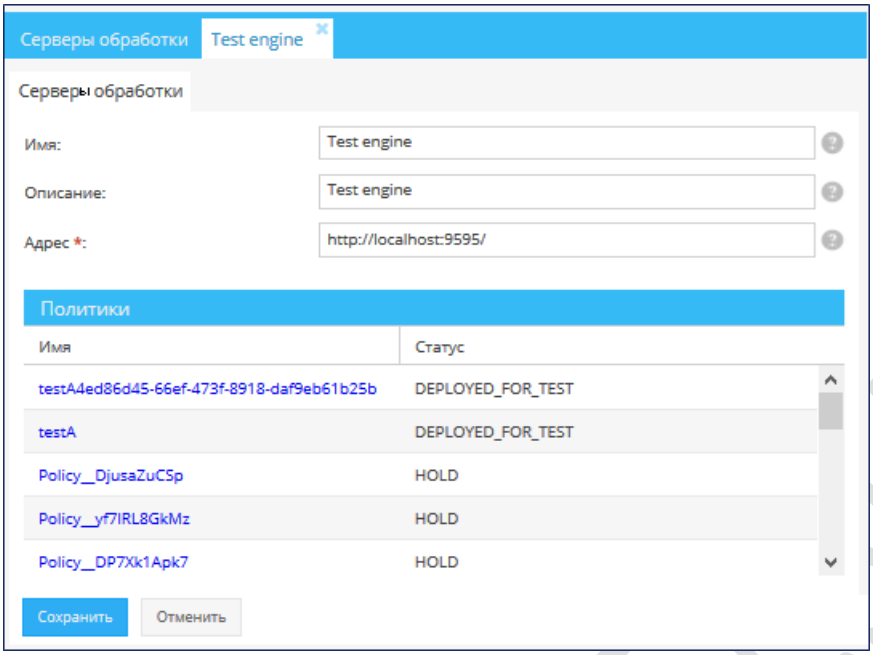


Рисунок 97 – Вкладка с экранной формой сервера обработки

6.9.1.2 Добавление сервера обработки

Чтобы добавить серверы обработки:

1) Откройте справочник **Сервера обработки** (см. раздел 6.9.1.1).
2) Нажмите кнопку **Добавить**  (Рисунок 96).

Откроется вкладка **Создание сервера обработки** (Рисунок 98).

3) Заполните поля вкладки.
   - **Имя** – уникальное имя для сервера обработки;
   - **Описание** – текстовое описание;
   - **Адрес** – путь к серверу.
4) Нажмите кнопку **Сохранить**.

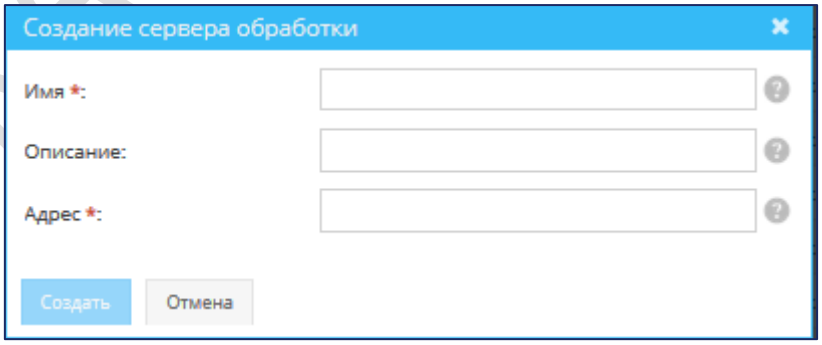


Рисунок 98 – Вкладка **Создание сервера обработки**

6.9.1.3 Редактирование сервера обработки

Чтобы отредактировать запись в справочнике:

1) Откройте справочник **Серверы обработки** (см. раздел 6.9.1.1).
2) Дважды щёлкните по строке записи сервера обработки.

Откроется вкладка выбранной записи (Рисунок 97).

3) Внесите изменения в поля вкладки.
4) Нажмите кнопку **Сохранить**.

6.9.1.4 Удаление сервера обработки

Чтобы удалить запись из справочника:

1) Откройте справочник **Серверы обработки** (см. раздел 6.9.1.1).
2) Выберите запись на вкладке **Серверы обработки**.
3) Нажмите кнопку **Удалить** .
4) Нажмите кнопку **Да** в появившемся запросе.

6.9.1.5 Массовый перенос политик с одного сервера обработки на другой

Для массового переноса политик с сервера обработки:

1) Откройте справочник **Сервера обработки** (см. раздел 6.9.1.1).
2) Выберите запись на вкладке **Серверы обработки**.
3) Нажмите кнопку Перенести связанные политики .

Откроется окно (Рисунок 99) для выбора нового сервера обработки.

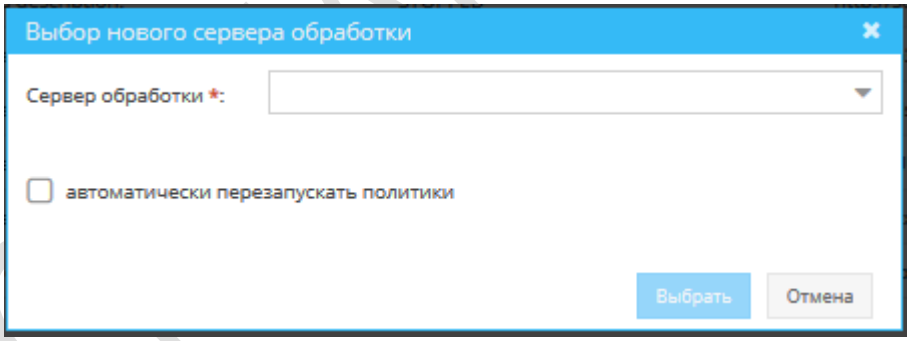


Рисунок 99 – Окно для выбора нового сервера обработки

4) В поле **Сервер обработки** выберите сервер, куда нужно перенести связанные с выбранным сервером политики.
5) Установите флаг **автоматически перезапускать политики**, чтобы после смены сервера обработки все политики, которые находились в статусе DEPLOYED и HOLD (см. подробное описание статусов политик в разделе 7.1.3.1) были перезапущены автоматически.
6) Нажмите кнопку **Выбрать.**

После этого Jet Detective выполнит следующие действия:

- Поиск всех политик, связанных с сервером обработки, в любом статусе, кроме DEPLOYED_FOR_TEST.
- Приостановление политик:
- если найдены политики в статусе DEPLOYED, то установка статуса этих политик – HOLD;
- если не найдены политики в статусе DEPLOYED, то пропуск этого шага.
- Для найденных политик – замена значения параметра **Сервер обработки** значением, выбранным в модальном окне.
- Автоматический перезапуск политик:
- если установлен флаг **автоматически перезапускать политики**, то запуск политик в статусе HOLD.

  Примечание. Перезапускаются только те политики, которые до переноса на другой сервер обработки были в статусе DEPLOYED и в HOLD, т. е. те, которые были запущены или приостановлены вследствие остановки сервера.

- если флаг **автоматически перезапустить политики** не установлен, то завершение процесса.
- Для каждой политики:
- если запуск выполнен успешно, то замена статуса политики HOLD статусом DEPLOYED.
- если запуск по каким-либо причинам не выполнен, то статус политики остаётся прежним – HOLD.

6.9.2 Действия

Действие – справочник доступных действий, которые может выполнить Jet Detective. Действия используются в настройке политик выявления аномалий, моделях документооборота, в правилах выявления или на рабочем столе оператора.

В Jet Detective предусмотрен ряд стандартных действий, но можно добавлять другие действия. Для этого используются Groovy-скрипты.

6.9.2.1 Просмотр действий

Чтобы посмотреть запись в справочнике действий:

1) Выберите пункт меню Настройки – **Прочее** – **Действия**.

В рабочей области отобразится одна или несколько вкладок:

- **Действия** – перечень действий (Рисунок 100);
- экранных форм действий, открытых в этой сессии.

2) На вкладке с перечнем дважды щёлкните по строке записи действия.

Экранная форма действия откроется на отдельной вкладке (Рисунок 101).

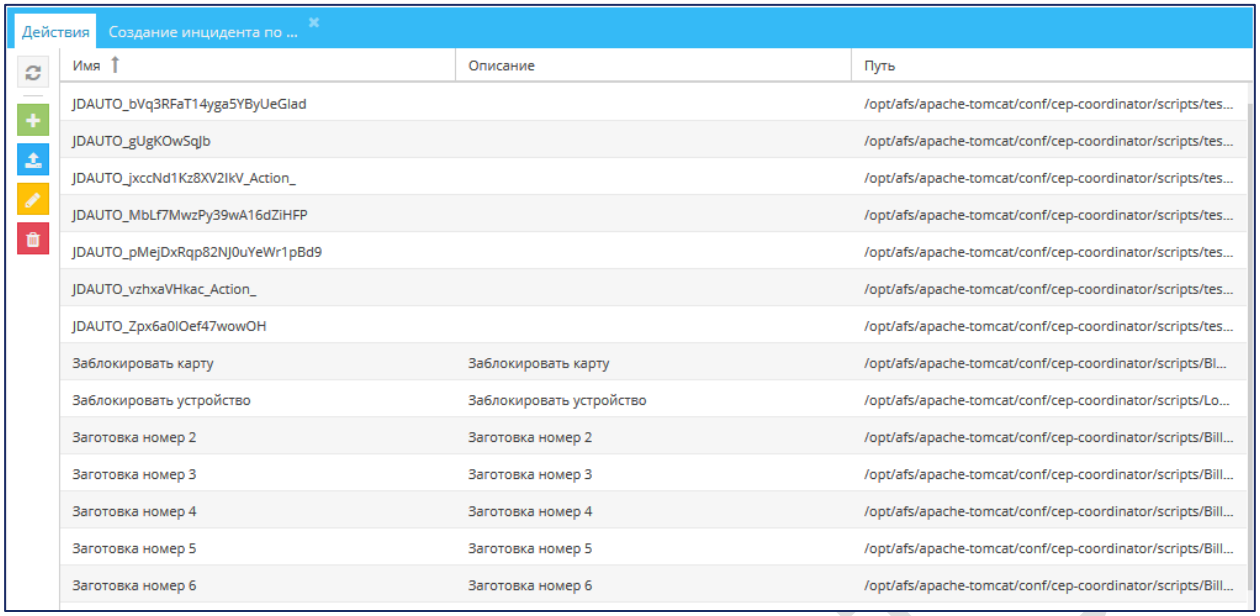


Рисунок 100 – Вкладка с перечнем действий

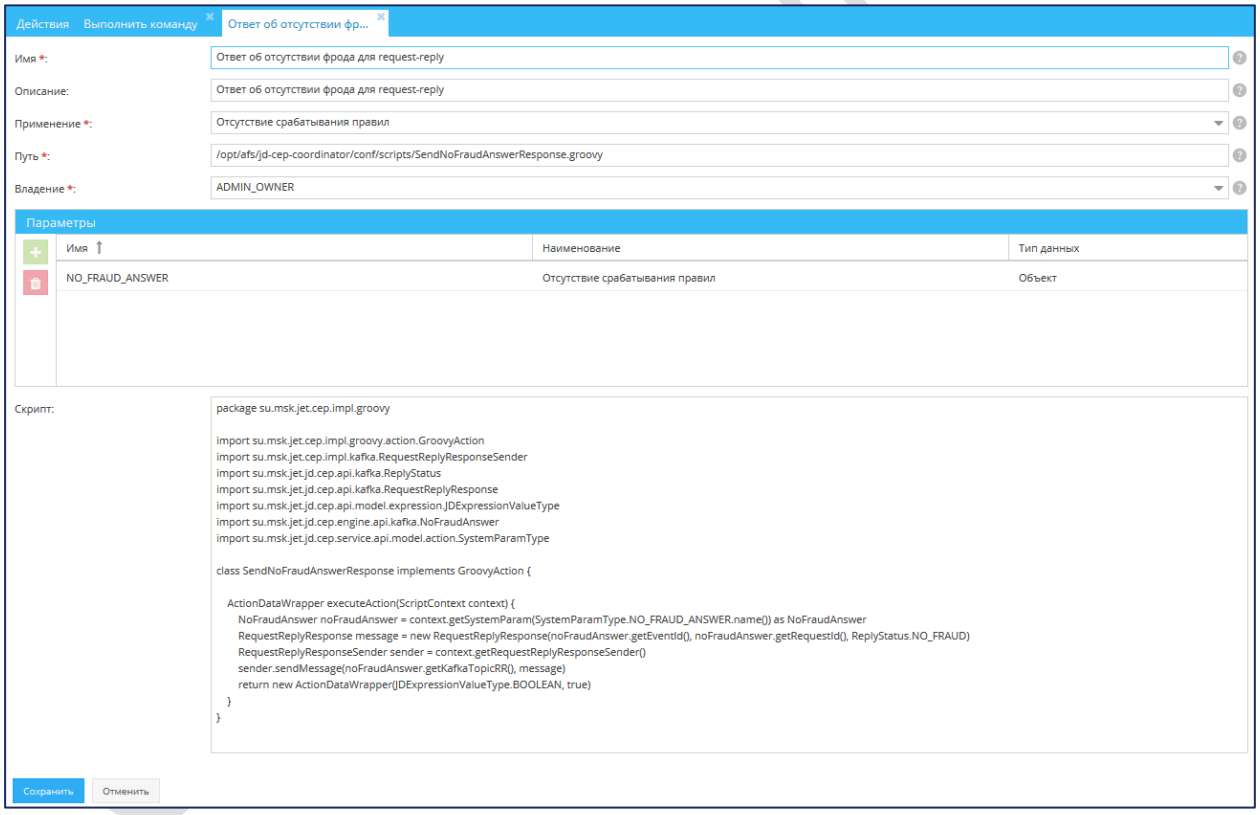


Рисунок 101 – Вкладка с экранной формой действия

6.9.2.2 Добавление действия

Чтобы добавить в систему действие, которое уже размещено на сервере:

1) Откройте справочник **Действия** (см. раздел 6.9.2.1).

2) Нажмите кнопку **Добавить**  (Рисунок 100).

Откроется вкладка **Создание действия** (Рисунок 102).

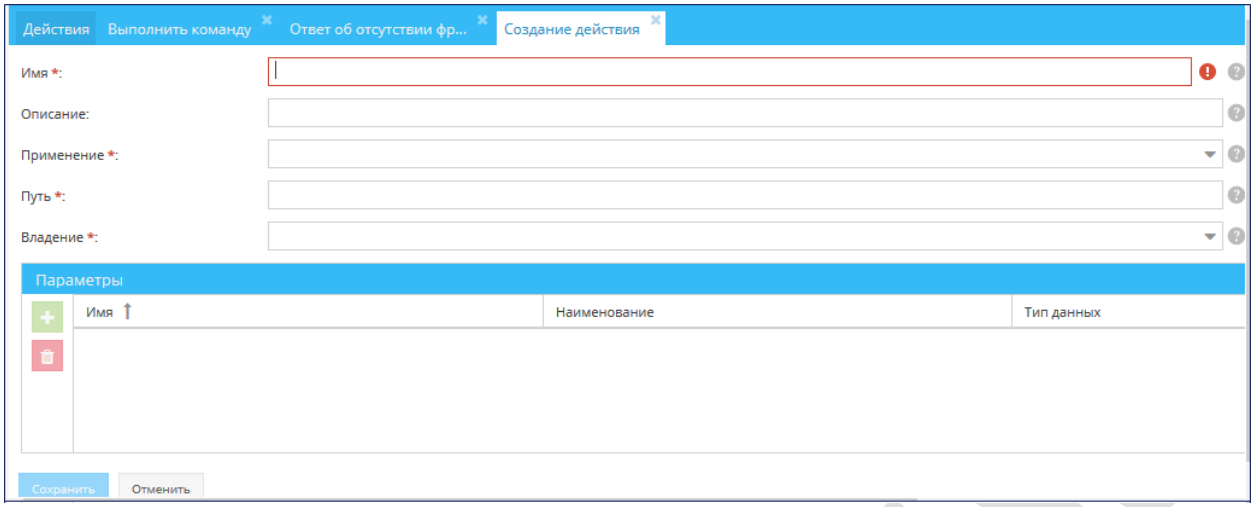


Рисунок 102 – Форма **Создание действия**

3) Заполните поля вкладки.

- **Имя** – уникальное имя для действия.
- **Описание** – текстовое описание.
- **Применение** – тот функционал где будет использоваться действие. Список отображает справочник **Лейблы действий** в **Фабрике данных** (см. раздел 6.2). В раскрывающемся списке доступны следующие значения:
- Модели документооборота;
- Отсутствие срабатывания правил;
- Правила;
- Рабочий стол оператора;
- Срабатывание строки матрицы.
- **Путь** – путь до Groovy-скрипта, выполняющего действие. Это уникальный путь для каждого действия в системе.
- **Владение** – владение, к которому будет относиться действие.
- **Параметры** – таблица с входными параметрами действия. Если в поле **Применение** у выбранного значение указаны входные параметры по умолчанию, то они отобразятся в таблице **Параметры**. Добавьте требуемые входные параметры для выполнения действия.

  Примечание: для системных действий добавление и изменение входных параметров недоступно.
- **Имя –** Текстовое поле. Для ввода доступны только латинские буквы, цифры и "_". Это уникальное значение в рамках одного действия.
- **Наименование –** Текстовое поле. Показывает, как параметр будет отображаться пользователю в форме ввода данных.
- **Тип данных** – раскрывающийся список с типами данных:
- **Текст,**
- **Число,**

- **Дата и время,**
- **Логический**
- **Объект.**

4) Нажмите кнопку **Сохранить**.

6.9.2.3 *Загрузка действия*

Чтобы загрузить groovy-скрипт с локального компьютера пользователя:

1) Откройте справочник **Действия** (см. раздел 6.9.2.1).

2) Нажмите кнопку **Загрузить**  (Рисунок 100).

   Откроется форма загрузки действия (Рисунок 103).

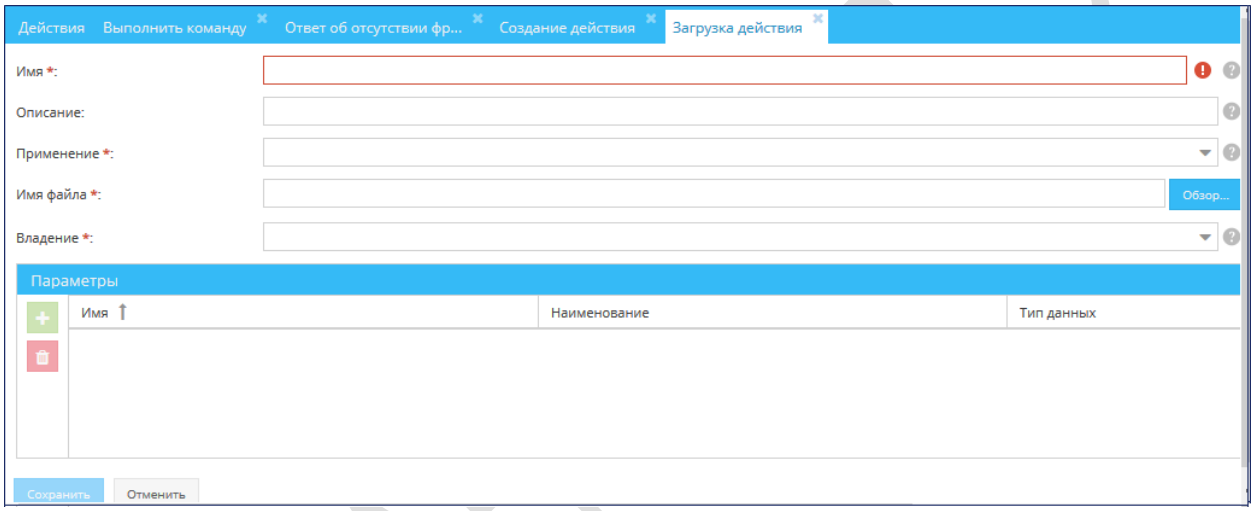


Рисунок 103 – Форма **Загрузки действия**

3) Заполните поля формы, так же как на форме создания действия (см. раздел 6.9.2.2). В параметре **Имя файла** выберите файл для загрузки. Расширение файла должно быть *.groovy*

4) Нажмите **Сохранить**

6.9.2.4 *Редактирование действия*

Чтобы отредактировать запись в справочнике действий:

1) Откройте справочник **Действия** (см. раздел 6.9.2.1).

2) Дважды щёлкните по строке записи.

Откроется вкладка выбранной записи (см. Рисунок 101).).

3) Внесите изменения в поля вкладки. Для редактирования также доступен текст самого запроса. Внесенные изменения будут сохранены в файле действия на сервере, с которым связано это действие.

4) Нажмите кнопку **Сохранить**.

6.9.2.5 Удаление действия

Чтобы удалить запись из справочника:

1) Откройте справочник **Действия** (см. раздел 6.9.2.1).
2) Выберите запись на вкладке **Действия**.
3) Нажмите кнопку **Удалить**  .
4) Нажмите кнопку **Да** в появившемся запросе.

6.9.3 Переменные

Переменная – служебная сущность, которая позволяет хранить переменное значение и централизованно его изменять.

Переменные используются в правилах выявления аномалий (см. раздел 7.1). Если изменить значение переменной в справочнике, то автоматически это значение поменяется во всех правилах, где используется переменная. Изменить значения можно как вручную, так и посредством созданного действия (см. раздел 6.9.2.1).

6.9.3.1 Просмотр переменной

Чтобы посмотреть запись в справочнике переменных:

1) Выберите пункт меню Настройки – **Прочее** – **Переменные**.

В рабочей области отобразится одна или несколько вкладок:

- списка переменных (Рисунок 104);
- экранных форм переменных, открытых в этой сессии.

2) На вкладке со списком дважды щёлкните по строке переменной.

Экранная форма откроется на отдельной вкладке (Рисунок 105).

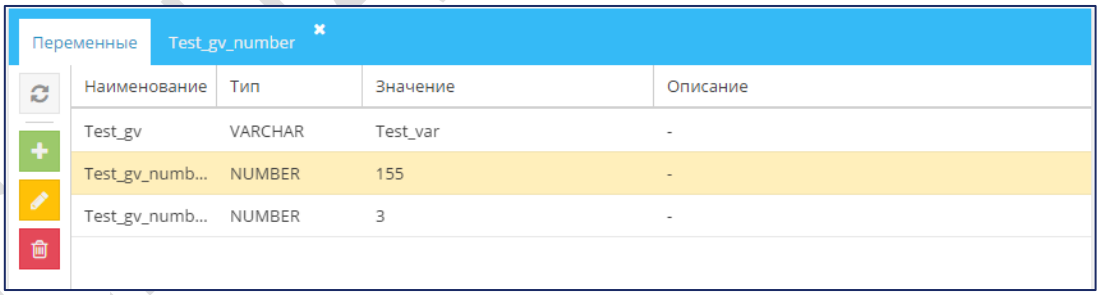


Рисунок 104 – Вкладка со списком переменных

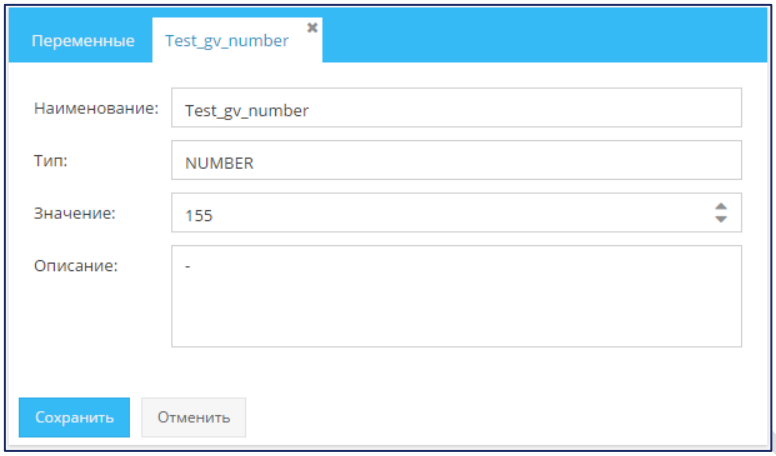


Рисунок 105 – Вкладка с экранной формой переменной

6.9.3.2 *Добавление переменной*

Чтобы добавить переменную:

1) Откройте справочник **Переменные** (см. раздел 6.9.3.1).
2) Нажмите кнопку **Добавить** (см. Рисунок 104).

Откроется вкладка **Создание переменной** (Рисунок 106).

3) Заполните поля вкладки.
4) Нажмите кнопку **Сохранить**.

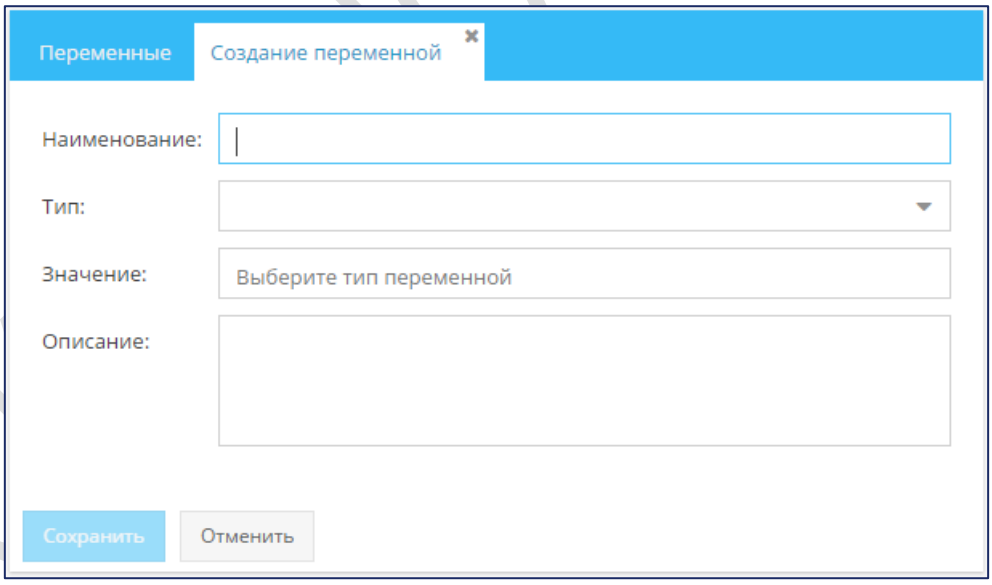


Рисунок 106 – Вкладка **Создание переменной**

6.9.3.3 *Редактирование переменной*

Чтобы отредактировать запись в справочнике переменных:

1) Откройте справочник **Переменные** (см. раздел 6.9.3.1).
2) Дважды щёлкните по строке переменной.

Откроется вкладка выбранной записи (см. Рисунок 105).

3) Внесите изменения в поля вкладки.

4) Нажмите кнопку **Сохранить**.

6.9.3.4 Удаление переменной

Чтобы удалить запись из справочника:

1) Откройте справочник **Переменные** (см. раздел 6.9.3.1).

2) Выберите запись на вкладке **Переменные** (см. Рисунок 104).

3) Нажмите кнопку **Удалить**  .

4) Нажмите кнопку **Да** в появившемся запросе.

6.9.4 Объекты поиска

Объект поиска – это служебная сущность, которая определяет, какие атрибуты объекта используются в поиске по спискам. Списки, для которых которых выполняется поиск, являются объектами **Фабрики данных** (см. раздел 6.2).

Объект поиска позволяет настроить сложную логику поиска по списку: по нескольким полям списка одновременно; использование не только точных совпадений, но и логических выражений и нечеткого поиска.

Настроенные **Объекты поиска** используются при настройке правил выявления аномалий (см. раздел 7.1.2).

6.9.4.1 Просмотр объекта поиска

Чтобы посмотреть запись в справочнике объектов поиска:

1) Выберите пункт меню Настройки – **Прочее** – **Объекты поиска**.

В рабочей области отобразится одна или несколько вкладок:

- перечень объектов поиска (Рисунок 107);
- экранных форм объектов поиска, открытых в этой сессии.

2) На вкладке с перечнем дважды щёлкните по строке записи объекта поиска.

Экранная форма объекта поиска откроется на отдельной вкладке (Рисунок 108).

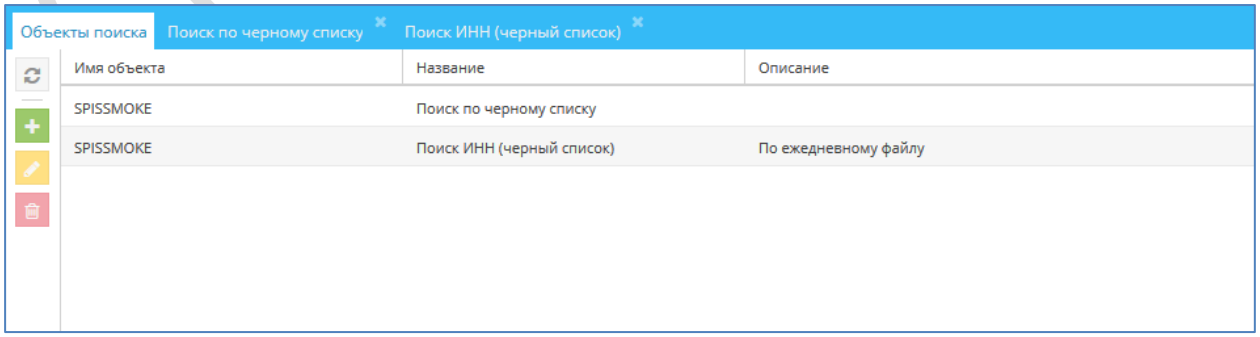


Рисунок 107 – Вкладка с перечнем объектов поиска

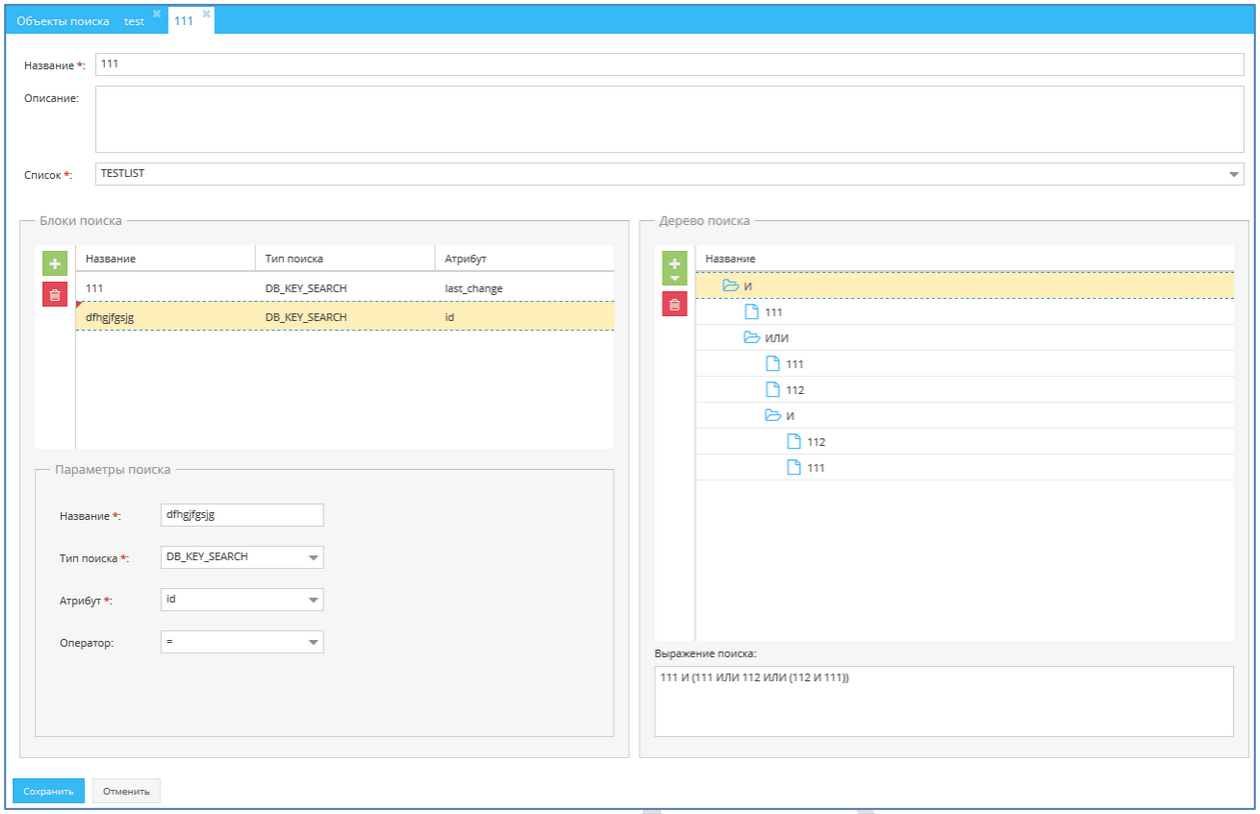


Рисунок 108 – Вкладка с экранной формой объекта поиска

6.9.4.2 Добавление объекта поиска

Чтобы добавить объект поиска:

1) Откройте справочник **Объекты поиска** (см. раздел 6.9.4.1).

2) Нажмите кнопку **Добавить** (Рисунок 107)

Откроется вкладка **Создание объекта поиска** (Рисунок 109).

3) Заполните поля вкладки.

- **Название** – текстовое поле для имени объекта поиска. Это имя будет отображаться при настройке правил выявления.
- **Описание** – текстовое поле для подробного описания объекта поиска.
- **Список**– раскрывающийся список объектов **Фабрики данных** (см. раздел 6.2) с типом **Список**, которые находятся в статусе «Применен» или были применены ранее.
- **Блоки поиска** – в этом разделе настраиваются параметры, которые будут участвовать в поиске по списку, выбранному в параметре **Список.**

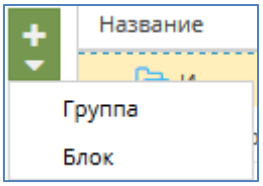
  С помощью кнопок **Добавить** и **Удалить** в таблице блоков сформируйте набор параметров проверки. При добавлении строки таблицы блока параметры строки настраиваются в разделе **Параметры поиска**.

- **Параметры поиска** – раздел отражает параметры строки, выбранной в таблице блоков. Для каждой строки таблицы блоков заполните параметры.
- **Название** – текстовое поле для указания имени блока поиска. Значение этого поля будет отображаться в дочерних ветвях дерева условий, если будет выбран этот объект поиска.

- **Тип поиска** – раскрывающийся список с доступными значениями (выбор одного значения):
- **DB_REGEXP_SEARCH** – поиск с использованием ранее настроенного регулярного выражения;
- **DB_KEY_SEARCH** – поиск по полному совпадению (по умолчанию);
- **DB_FUZZY_SEARCH** – полнотекстовый поиск. Используются встроенные механизмы поиска с расчетом расстояния Левенштейна.
- **Атрибут** – раскрывающийся список с атрибутами объекта, выбранного в параметре **Список.** По выбранному атрибуту будет проводиться настроенный поиск.
- **Дистанция** – параметр виден только в том случае, если в параметре **Тип поиска** выбрано значение **DB_FUZZY_SEARCH.** В поле указывается максимально допустимое количество операций вставки одного символа, удаления одного символа и замены одного символа другим – необходимых для превращения одной строки в другую (расстояние Левенштейна).
- **Оператор** – параметр виден только в том случае, если в параметре **Тип поиска** выбрано значение **DB_KEY_SEARCH** или **DB_FUZZY_SEARCH**. Раскрывающийся список с доступными значениями (выбор одного значения):
- = (по умолчанию)
- **>**
- **<**
- **=>**
- **=<**
- !=
- **Регулярное выражение** – параметр виден только в том случае, если в параметре **Тип поиска** выбрано значение **DB_REGEXP_SEARCH.** Раскрывающийся список с регулярными выражениями (см. раздел 6.9.5), у которых задана динамическая составляющая (есть переменная ${SEARCH_VALUE}).
- **Дерево поиска** – выстраивает взаимосвязь блоков поиска. В построении дерева доступны блоки поиска, из таблицы блоков и логические операторы **И** и **ИЛИ**.

  С помощью кнопок **Добавить** и **Удалить** составьте дерево поиска с использованием добавленных блоков.

  При нажатии на кнопку **Добавить** открывается раскрывающийся список с выбором элемента, который требуется добавить в дерево: **Блок** или **Группа:**



  Элемент дерева добавляется дочерним к тому, который выбран в дереве. Элемент редактируется непосредственно в дереве. Двойным нажатием на строку откройте раскрывающийся список элемента дерева:

- элемент **Блок**: список блоков, добавленных в таблице блоков;
- элемент **Группа**: **И** (по умолчанию) и **ИЛИ.**

4) Нажмите кнопку **Сохранить**.

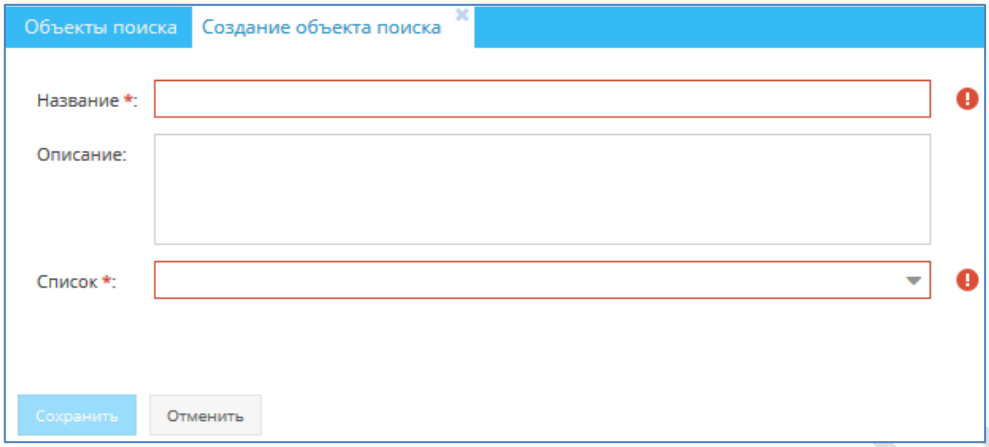


Рисунок 109 – Вкладка **Создание объекта поиска**

6.9.4.3 Редактирование объекта поиска

Чтобы отредактировать запись в справочнике объектов поиска:

1) Откройте справочник **Объекты поиска** (см. раздел 6.9.4.1).
2) Дважды щёлкните по строке записи объекта поиска.

Откроется вкладка выбранной записи (Рисунок 108).

3) Внесите изменения в поля вкладки.
4) Нажмите кнопку **Сохранить**.

6.9.4.4 Удаление объекта поиска

Чтобы удалить запись из справочника:

1) Откройте справочник **Объекты поиска** (см. раздел 6.9.4.1).
2) Выберите запись на вкладке **Объекты поиска**.
3) Нажмите кнопку **Удалить** .
4) Нажмите кнопку **Да** в появившемся запросе.

6.9.5 Регулярные выражения

Регулярное выражение – это служебная сущность для составления шаблонов поиска и шаблонов манипуляций с подстрокой. Для составления выражений используется структура регулярных выражений POSIX.

6.9.5.1 Просмотр регулярного выражения

Чтобы посмотреть запись в справочнике регулярных выражений:

1) Выберите пункт меню Настройки – **Прочее** – **Регулярные выражения**.

В рабочей области отобразится одна или несколько вкладок:

- перечень регулярных выражений (Рисунок 110);

- экранных форм регулярных выражений, открытых в этой сессии.

2) На вкладке с перечнем дважды щёлкните по строке записи регулярного выражения.

Экранная форма регулярного выражения откроется на отдельной вкладке (Рисунок 111).

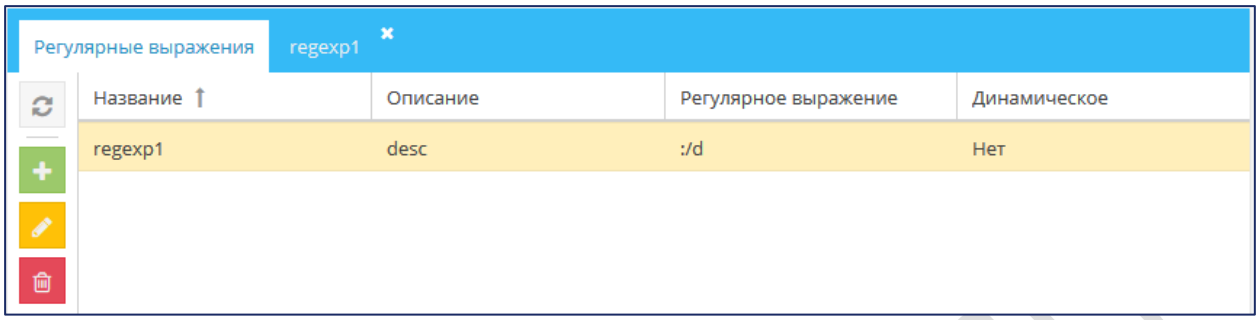


Рисунок 110 – Вкладка с перечнем регулярных выражений

Рисунок 111 – Вкладка с экранной формой регулярного выражения

6.9.5.2 Добавление регулярного выражения

Чтобы добавить регулярное выражение:

1) Откройте справочник **Регулярные выражения** (см. раздел 6.9.5.1).

2) Нажмите кнопку **Добавить** (Рисунок 110).

Откроется вкладка **Создание регулярного выражения** (Рисунок 112).

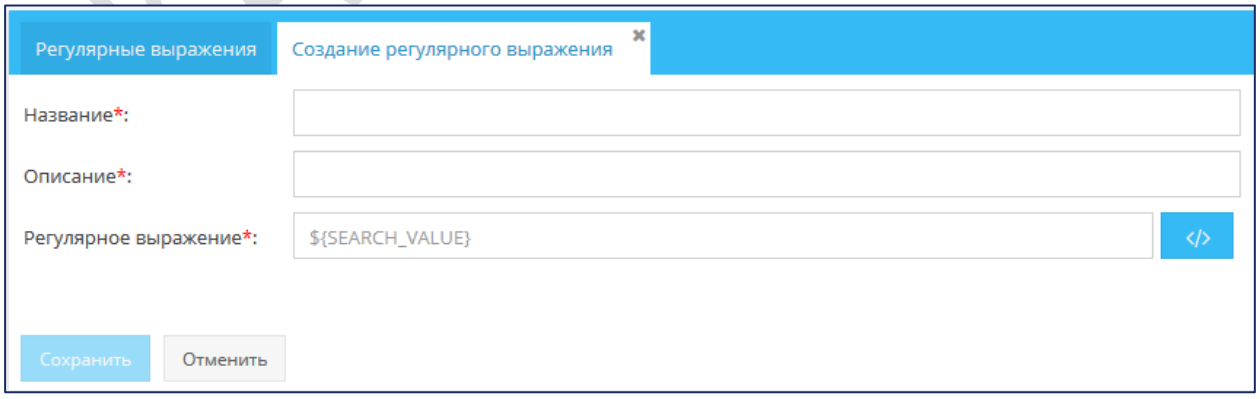


Рисунок 112 – Вкладка **Создание регулярного выражения**

3) Заполните поля вкладки.

- **Название** – уникальное имя для регулярного выражения;
- **Описание** – текстовое описание;
- **Регулярное выражение** – выражение, описанное с помощью структуры регулярных выражений POSIX.

  С помощью кнопки **Добавить динамическую часть выражения**  в регулярное выражение можно добавить переменную часть. При дальнейшем использовании регулярного выражения в правилах выявления аномалий можно указать, какой параметр объекта будет использоваться в качестве этой переменной части.

4) Нажмите кнопку **Сохранить**.

6.9.5.3 Редактирование регулярного выражения

Чтобы отредактировать запись в справочнике регулярных выражений:

1) Откройте справочник **Регулярные выражения** (см. раздел 6.9.5.1).
2) Дважды щёлкните по строке записи регулярного выражения.

Откроется вкладка выбранной записи (Рисунок 110).

3) Внесите изменения в поля вкладки.
4) Нажмите кнопку **Сохранить**.

6.9.5.4 Удаление регулярного выражения

Чтобы удалить запись из справочника:

1) Откройте справочник **Регулярные выражения** (см. раздел 6.9.5.1).
2) Выберите запись на вкладке **Регулярные выражения**.
3) Нажмите кнопку **Удалить**  .
4) Нажмите кнопку **Да** в появившемся запросе.

6.9.6 Справочник e-mail

Служебный справочник, в котором хранятся адреса e-mail. Справочник может быть использован при формировании отчетов.

6.9.6.1 Просмотр адресов e-mail

Чтобы посмотреть запись в справочнике e-mail:

1) Выберите пункт меню Настройки – **Прочее** – **Справочник e-mail**.

В рабочей области отобразится одна или несколько вкладок:

- **Справочник e-mail** – перечень записей адресов e-mail (Рисунок 113);
- экранных форм записей адресов e-mail, открытых в этой сессии.

2) На вкладке с перечнем дважды щёлкните по строке записи адреса e-mail.

Экранная форма записи адреса e-mail откроется на отдельной вкладке (Рисунок 114).

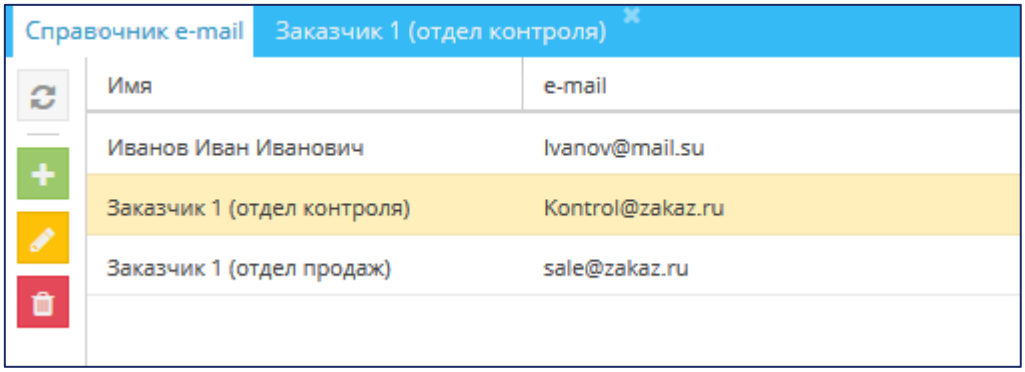


Рисунок 113 – Список записей адресов e-mail

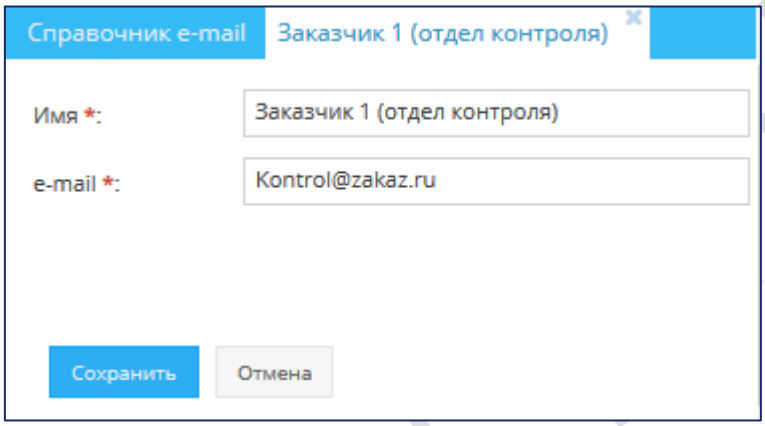


Рисунок 114 – Экранная форма записи адреса e-mail

6.9.6.2 Добавление адреса e-mail

Чтобы добавить запись адреса электронной почты:

1) Откройте **Справочник e-mail** (см. раздел 6.9.6.1).

2) Нажмите кнопку **Добавить** (Рисунок 113).

Откроется вкладка **Создание адреса** (Рисунок 115).

3) Заполните поля вкладки.

- **Имя** – введите текстовое описание адреса e-mail.
- **e-mail** – введите адрес электронной почты.

4) Нажмите кнопку **Сохранить**

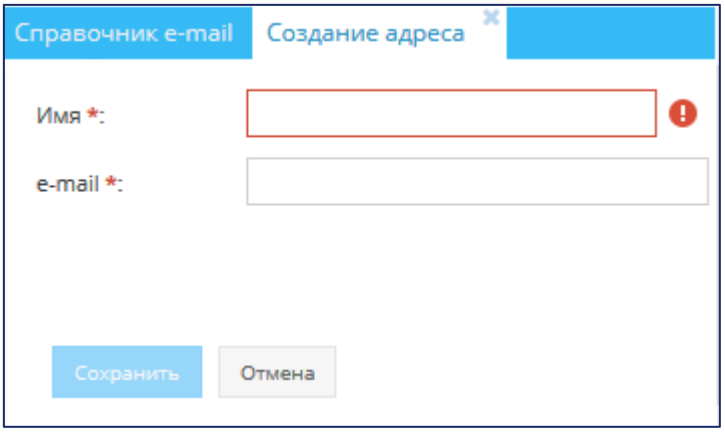


Рисунок 115 – Форма создания адреса e-mail

6.9.6.3 Редактирование адресов e-mail

Чтобы отредактировать запись адреса электронной почты:

1) Откройте **Справочник e-mail** (см. раздел 6.9.6.1).
2) Дважды щёлкните по строке записи адреса e-mail.

Откроется вкладка выбранной записи

3) Внесите изменения в поля вкладки.
4) Нажмите кнопку **Сохранить**.

6.9.6.4 Удаление адресов e-mail

Чтобы удалить запись адреса электронной почты:

1) Откройте **Справочник e-mail** (см. раздел 6.9.6.1).
2) Выберите запись в списке адресов e-mail.
3) Нажмите кнопку **Удалить** .

6.9.7 Справочник директорий

Справочник директорий – это служебный справочник, в котором хранятся адреса директорий. Он используется при формировании отчетов.

6.9.7.1 Просмотр директорий

Чтобы посмотреть запись в справочнике директорий:

1) Выберите пункт меню Настройки – **Прочее** – **Справочник директорий**.

В рабочей области отобразится одна или несколько вкладок:

- **Справочник директорий** – перечень записей директорий (Рисунок 116);
- экранных форм записей директорий, открытых в этой сессии.

2) На вкладке с перечнем дважды щёлкните по строке записи директории.

Экранная форма записи директории откроется на отдельной вкладке (Рисунок 117).

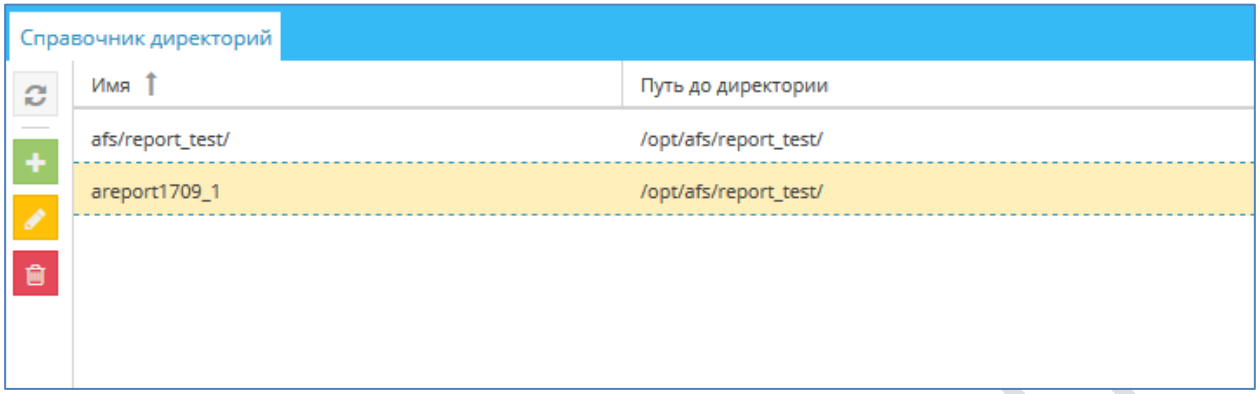


Рисунок 116 – Список записей директорий

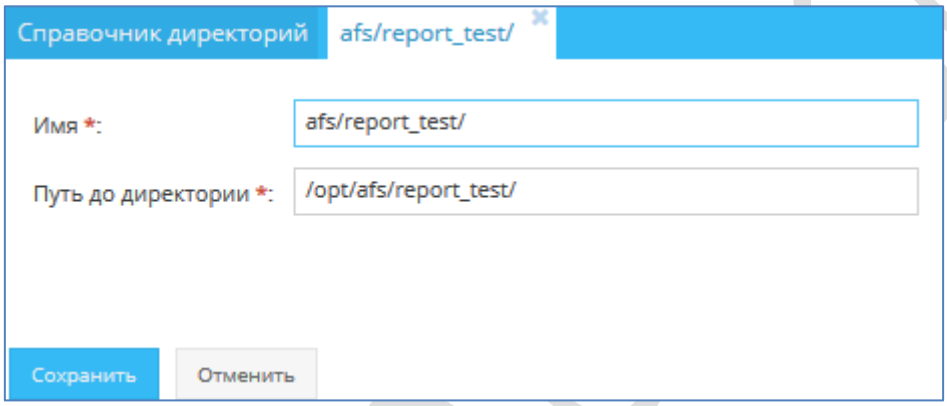


Рисунок 117 – Экранная форма записи директории

6.9.7.2 Добавление директории

Чтобы добавить запись директории:

1) Откройте **Справочник директорий** (см. раздел 6.9.7.1).

2) Нажмите кнопку **Добавить**  (Рисунок 116).

Откроется вкладка **Создание директории** (Рисунок 118).

3) Заполните поля вкладки.

- **Имя** – введите текстовое описание директории.
- **Путь до директории** – введите пусть до директории.

4) Нажмите кнопку **Сохранить**

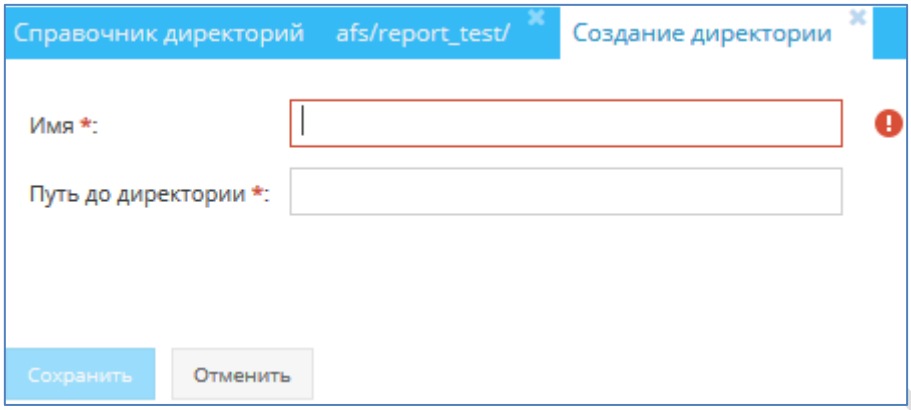


Рисунок 118 – Форма создания директории

6.9.7.3 Редактирование записи директории

Чтобы отредактировать запись:

1) Откройте **Справочник директорий** (см. раздел 6.9.7.1).
2) Дважды щёлкните по строке записи директории.

Откроется вкладка выбранной записи (Рисунок 117).

3) Внесите изменения в поля вкладки.
4) Нажмите кнопку **Сохранить**.

6.9.7.4 Удаление записи директории

Чтобы удалить запись:

1) Откройте **Справочник директорий** (см. раздел 6.9.7.1).
2) Выберите запись в списке директории
3) Нажмите кнопку **Удалить** .

6.9.8 Конфигурация сервисов

Для управления настройками сервисов, входящих в состав Jet Detective, реализованы функции конфигурирования сервисов.

> *Примечание.* После добавления, изменения или удаления конфигурации сервиса администратор Jet Detective должен перезапустить сервис вручную, чтобы внесенные изменения вступили в силу.

6.9.8.1 Просмотр конфигурации сервисов

Чтобы посмотреть запись в справочнике конфигурации сервисов:

4) Выберите пункт меню Настройки – **Прочее** – **Конфигурация сервисов**.

В рабочей области отобразится одна или несколько вкладок:

- **Конфигурация сервисов** – перечень записей конфигураций сервисов (Рисунок 119);

- экранных форм записей конфигураций сервисов, открытых в этой сессии.

5) На вкладке с перечнем дважды щёлкните по строке записи конфигурации сервиса.

Экранная форма записи откроется на отдельной вкладке (Рисунок 120).

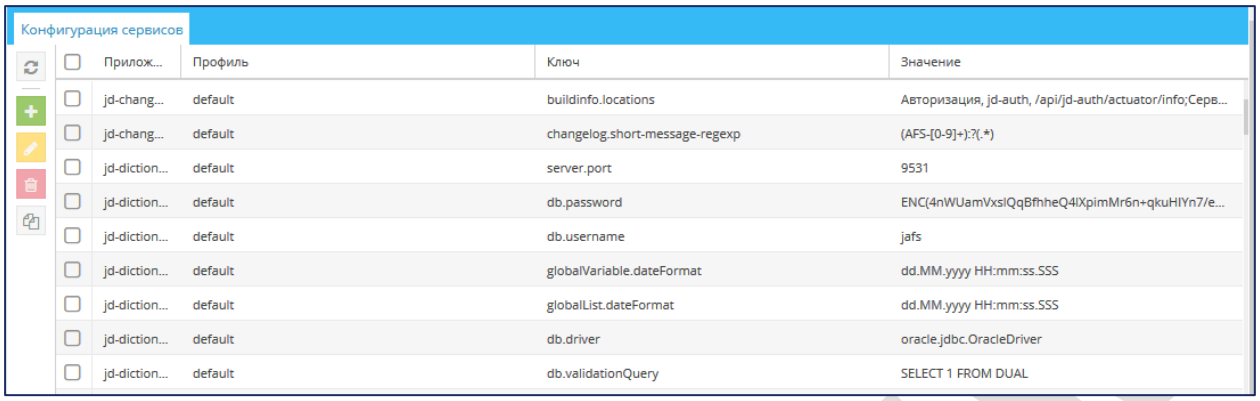


Рисунок 119 – Список записей конфигураций сервисов

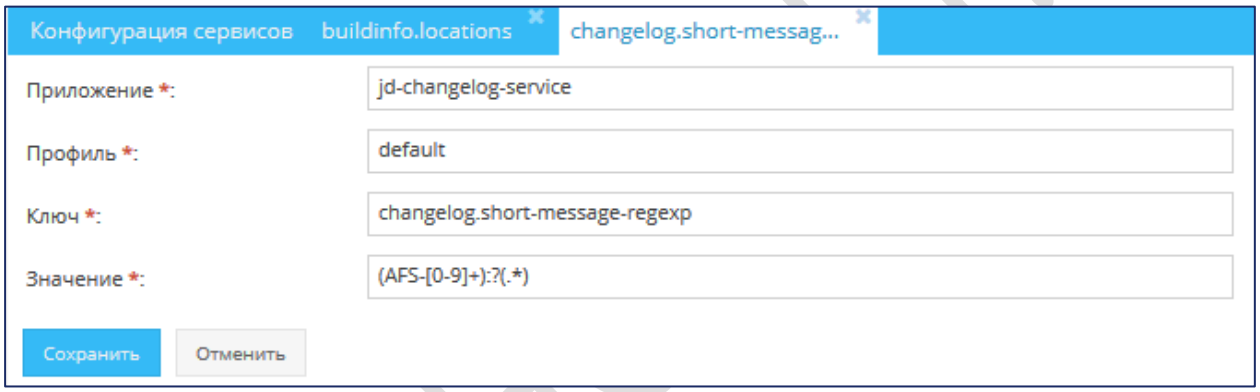


Рисунок 120 – Экранная форма записи конфигурации сервиса

6.9.8.2 Добавление конфигурации сервисов

Чтобы добавить запись конфигурации сервиса:

1) Откройте список **Конфигурация сервисов** (см. раздел 6.9.8.1).

2) Нажмите кнопку **Добавить** (Рисунок 119).

Откроется вкладка **Создание конфигурации** (Рисунок 121).

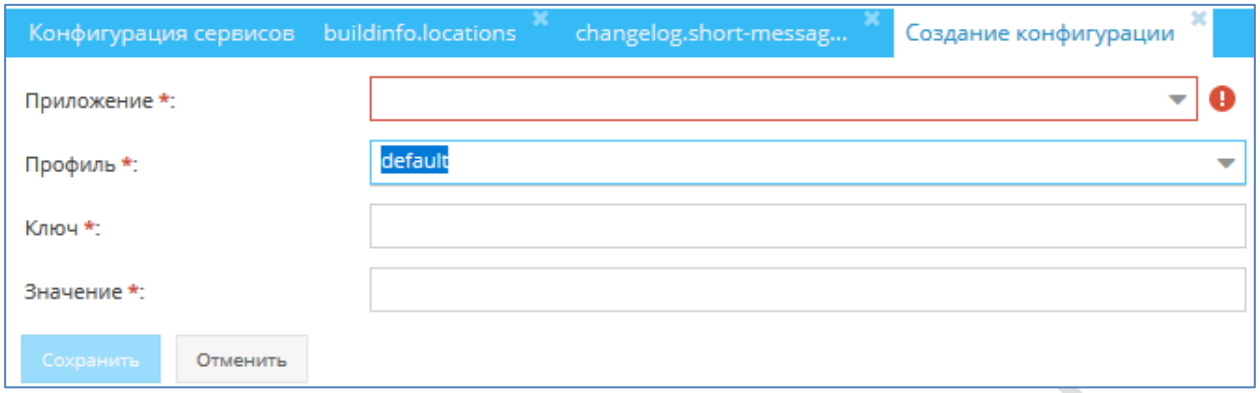


Рисунок 121 – Экранная форма создания записи конфигурации сервиса

3) Заполните все поля вкладки.

- **Приложение** – выберите в раскрывающемся списке сервис, для которого будет создана конфигурация. Если конфигурация будет использоваться несколькими сервисами одновременно, то выберите значение all.
- **Профиль** – этот параметр доступен для всех приложений кроме all и frontend. Позволяет создавать разные настройки для одинаковых приложений, которые находятся на разных узлах. Выберите значение профиля приложения. Значение по умолчанию: default. Для выбора доступны только те профили, которые уже созданы для приложения. Создание нового профиля описано в разделе 6.9.8.3.
- **Ключ** – укажите ключ для настройки сервиса. Для всех записей одного приложения значения поля **Ключ** должны быть уникальными, т. е. не может быть создано больше одной записи с одинаковым ключом для одного приложения.

  Допустимые символы поля:

  - латинские буквы в верхнем и нижнем регистре;
  - цифры;
  - символы "." (точка), "-" (минус), "_" (нижнее подчеркивание).
- **Значение** – укажите значение для настройки сервиса.

4) Нажмите кнопку **Сохранить**

6.9.8.3 Создание профиля конфигурации сервисов

Чтобы создать новый профиль конфигураций приложения:

1) Нажмите кнопку **Копировать** в списке конфигураций сервисов (см.раздел 6.9.8.1).
2) В появившемся модальном окне (Рисунок 122) заполните поля:
   - **Приложение** – выберите приложение, из которого необходимо скопировать все настройки в новый профиль. В списке недоступны приложения all и frontend;
   - **Профиль** – выберите профиль приложения, который необходимо скопировать;
   - **Имя нового профиля** – укажите имя для создаваемого профиля
3) Нажмите **Сохранить**.

После сохранения берутся все настройки выбранного приложения с указанными профилем, копируются и имя профиля меняется на указанное имя.

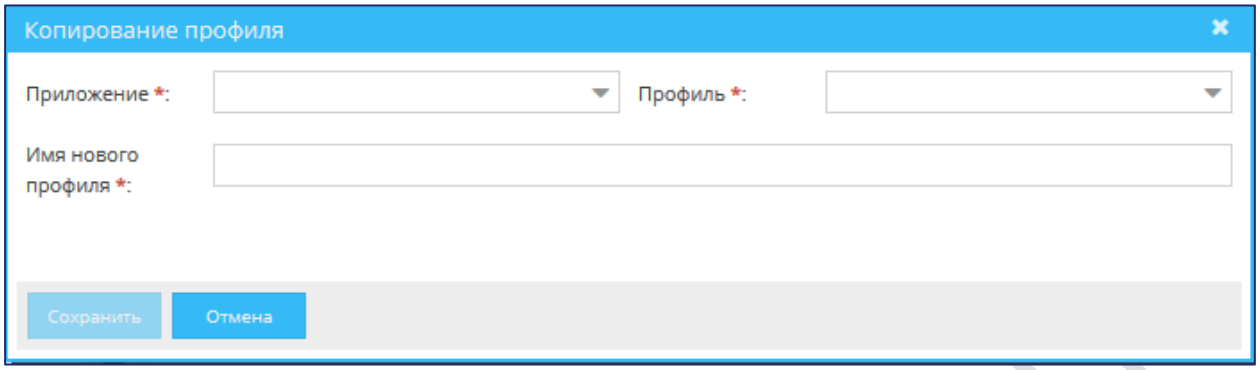


Рисунок 122 – Модальное окно для копирования профиля конфигурации сервисов

6.9.8.4 Редактирование конфигурации сервисов

Чтобы отредактировать запись конфигурации сервиса:

1) Откройте список **Конфигурация сервисов** (см. раздел 6.9.8.1).
2) Дважды щёлкните по строке записи конфигурации сервиса.

Откроется вкладка выбранной записи (Рисунок 120).

3) Внесите изменения в поле **Значение**.
4) Нажмите кнопку **Сохранить**.

6.9.8.5 Удаление конфигурации сервисов

Чтобы удалить запись конфигурации сервиса:

1) Откройте список **Конфигурация сервисов** (см. раздел 6.9.8.1).
2) Выберите запись в списке конфигураций сервисов.
3) Нажмите кнопку **Удалить** .

6.9.9 Архивация

В Jet Detective предусмотрен механизм архивации объектов с типом **Событие**. Создание отдельного механизма связано с тем, что объекты этого типа являются основным объектом анализа и в перспективе могут иметь очень большие объемы данных.

Все объекты с типом **Событие**, которые поступают в систему, сохраняются в отдельную БД, где существует архив. Таким образом, в тот момент, когда ресурсы рабочей БД будут исчерпаны, лишние данные оттуда можно будет удалить. При этом вся информация этих объектов сохранится в архивной БД.

Сервис архивации может находиться в двух статусах:

- **Запущен** – все объекты с типом Событие, при поступлении в Jet Detective сохраняются и в рабочую БД, и в архивную. При этом в архивную БД сохраняется полностью обогащенный слепок события.

- **Остановлен** – поступающие в Jet Detective события сохраняются только в рабочую БД.

Управление процессом архивации находится в меню ***Прочее – Архивация.***

Форма управления процессом архивации показана на рисунке 123.

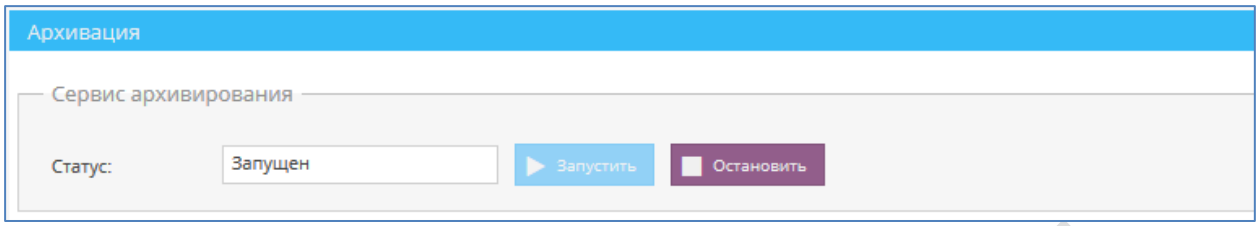


Рисунок 123 – Форма управления процессом архивации

В электронной форме отображается статус архивации, актуальный на данный момент.

Кнопка **Остановить** используется для остановки процесса архивации.

Кнопка **Запустить** используется для запуска процесса архивации.

6.9.10 Управление стилями таблиц объектов

В Jet Detective реализован механизм управления стилями таблиц, который позволяет динамически изменять фон строк, ячеек и шрифта в таблицах объектов **Фабрики данных** (см. раздел 6.2) – в зависимости от значений определенного атрибута. Например, с помощью этого механизма можно выделить строки таблицы, где в определенном столбце указано значение «fraud».

В качестве объекта хранения стилей используется объект **Фабрики данных** (см. раздел 6.2) – **STYLES.**

> *Примечание.* Для корректной работы механизма динамического изменения стилей таблиц не рекомендуется вносить изменения в объект **STYLES**.

6.9.10.1 Просмотр стилей

Чтобы посмотреть запись в справочнике стилей:

1) Выберите пункт меню **Настройки** – **Прочее** – **Стили**.

В рабочей области отобразится одна или несколько вкладок:

- **Стили** – перечень действий (Рисунок 124);
- экранных форм стилей, открытых в этой сессии.

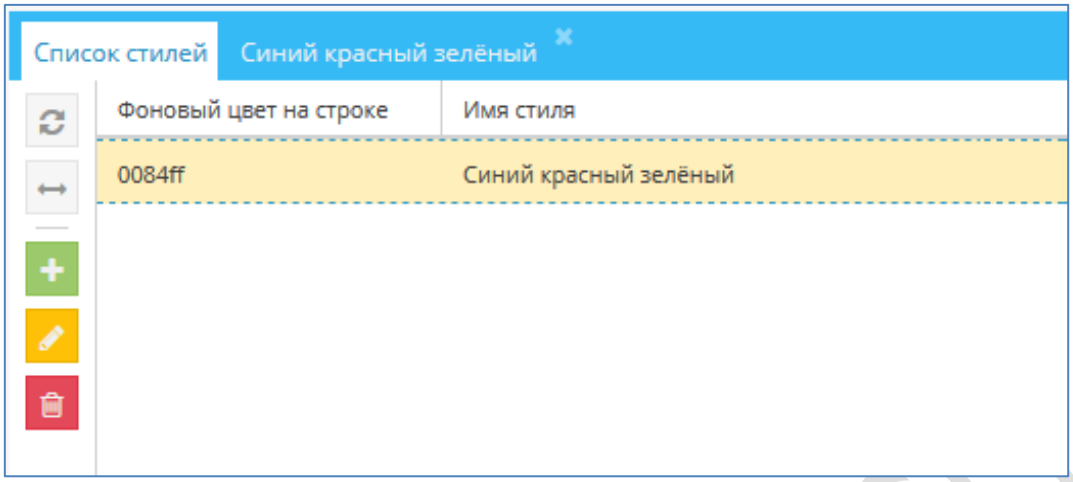


Рисунок 124 – Вкладка с перечнем стилей

2) На вкладке с перечнем дважды щёлкните по строке записи стиля.

Экранная форма стиля откроется на отдельной вкладке (Рисунок 125).

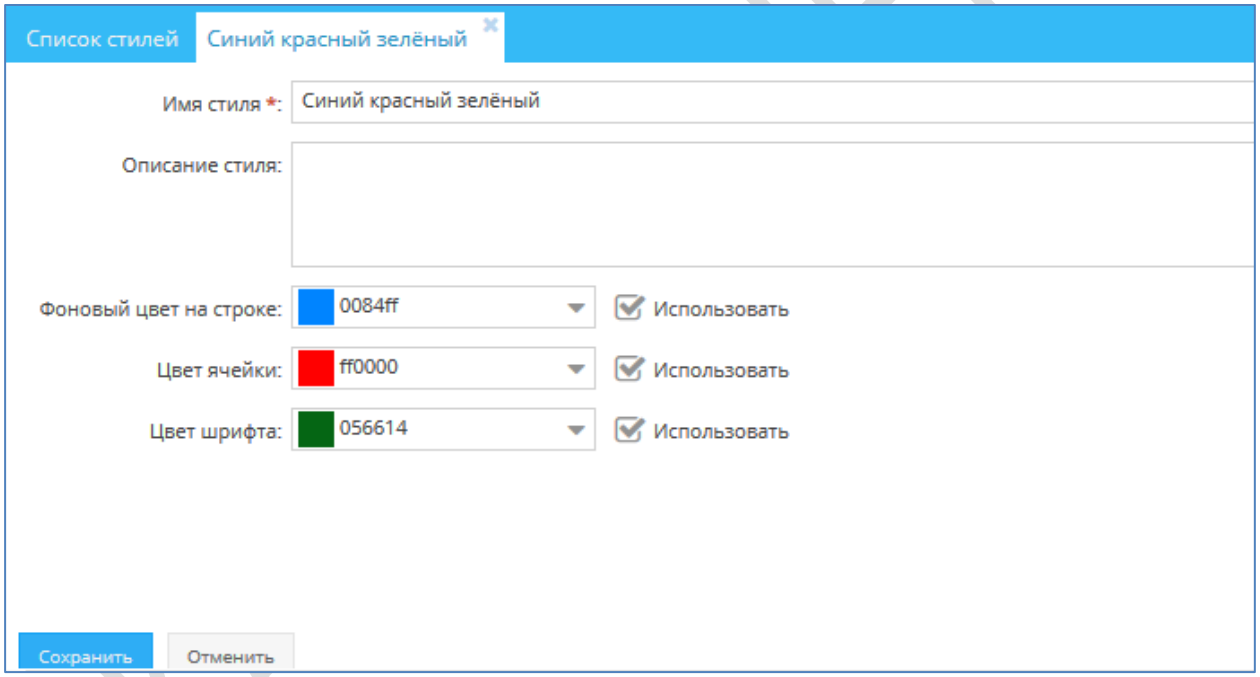


Рисунок 125 – Вкладка с экранной формой стиля

6.9.10.2 Создание стиля

Чтобы добавить стиль:

1) Откройте справочник **Стилей** (см. раздел 6.9.10.1).

2) Нажмите кнопку **Добавить**  (Рисунок 124).

Откроется вкладка **Создание действия** (Рисунок 126).

3) Заполните поля вкладки.

- **Имя** – наименование стиля;

- **Описание** – текстовое описание;
- **Фоновый цвет строки** – раскрывающаяся палитра (Рисунок 127) для выбора цвета фона, который будет применяться к строке, с определенным значением. Палитра становится доступна для выбора цвета при установленным флаге **Использовать;**
- **Цвет ячейки** – раскрывающаяся палитра (Рисунок 127) для выбора цвета, который будет применяться к ячейки, значение которой влияет на выбор стиля в строке. Палитра становится доступна для выбора цвета при установленным флаге **Использовать;**
- **Цвет шрифта –** раскрывающаяся палитра (Рисунок 127) для выбора цвета, который будет применяться к шрифту строки, с определенным значением. Палитра становится доступна для выбора цвета при установленным флаге **Использовать.**

4) Нажмите кнопку **Сохранить**.

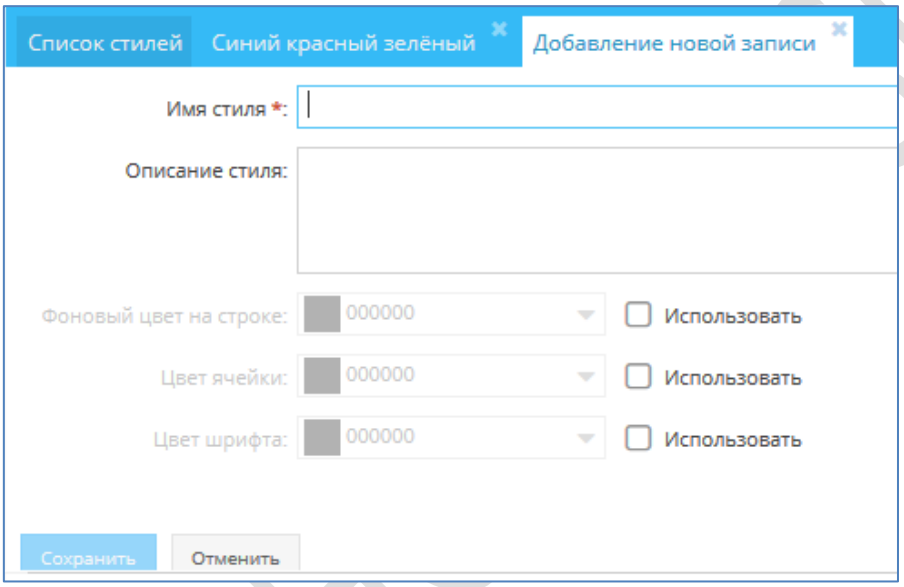


Рисунок 126 – Форма **Создание стиля**

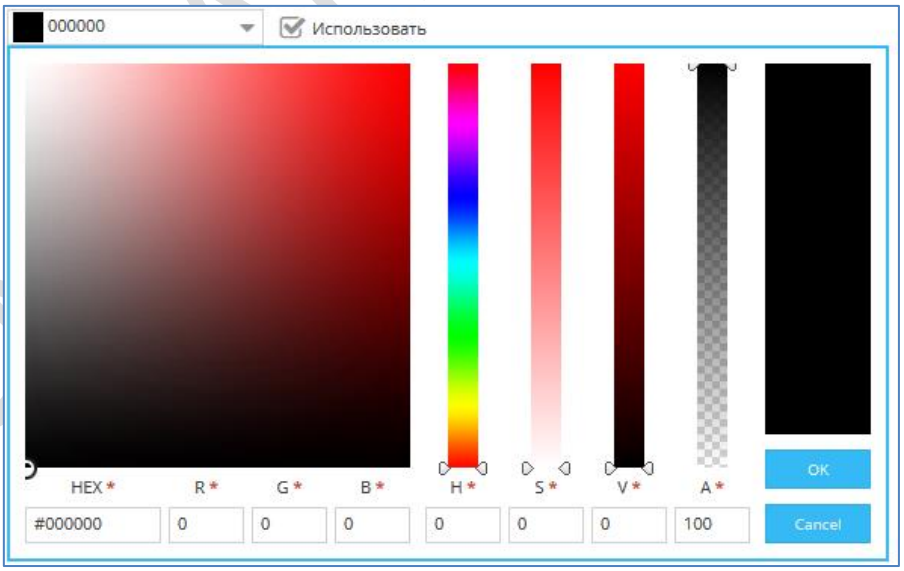


Рисунок 127 – Палитра для выбора цвета

6.9.10.3 Редактирование стиля

Чтобы отредактировать стиль:

1) Откройте справочник **Стилей** (см. раздел 6.9.10.1).
2) Дважды щёлкните по строке записи действия.

Откроется вкладка выбранной записи (см рисунок 125).

3) Внесите изменения в поля вкладки
4) Нажмите кнопку **Сохранить**.

6.9.10.4 Удаление стиля

Чтобы удалить стиль:

1) Откройте справочник **Стилей** (см. раздел 6.9.10.1).
2) Выберите запись в списке стилей.
3) Нажмите кнопку **Удалить**  **.**
4) Нажмите кнопку **Да** в появившемся запросе.

6.9.10.5 Использование стиля

Для использования стилей объект **Фабрики данных** (см. раздел 6.2) должен иметь связь со справочником стилей через справочник значений, от которых должен зависеть стиль (Рисунок 128).

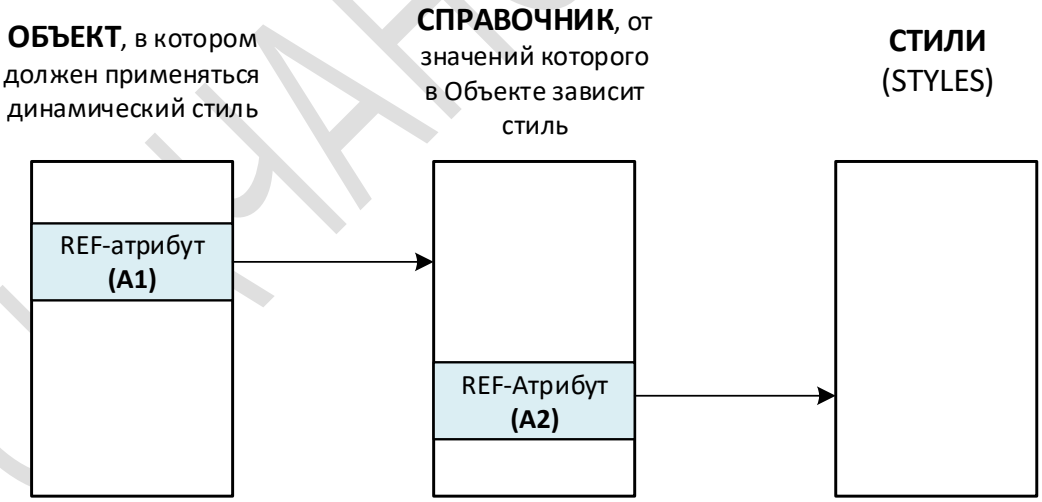


Рисунок 128 – Иллюстрация связи объекта со справочником стилей

Пример настройки стиля:

ОБЪЕКТ – объект **Фабрики данных** (см. раздел 6.2), в таблице которого должны быть применен стиль строкю

A1 – атрибут в **ОБЪЕКТЕ**, от значения которого должен зависеть цвет строки.

СПРАВОЧНИК – справочник, на который ссылается атрибут **A1.**

A2 – атрибут **СПРАВОЧНИКА**, который ссылается на справочник **СТИЛИ**.

1) Атрибут **A1**, значения которого будут влиять на стиль строк, должен быть ссылкой на **СПРАВОЧНИК** – REF-атрибутом.
2) Атрибут **A1**, значения которого будут влиять на стиль строк, должен быть ссылкой на **СПРАВОЧНИК** – REF-атрибутом.
3) **СПРАВОЧНИК** должен иметь ссылку на справочник **СТИЛИ**: **REF**-атрибут **A2**.
4) В параметре **Атрибуты для ссылочного представления СПРАВОЧНИКА**, должен присутствовать атрибут **A2.**
5) В **СПРАВОЧНИКЕ** (в меню **Пользовательские объекты – Справочники**) для записей, которые должны влиять на цвет строк связанного **ОБЪЕКТА**, в поле атрибута **A2**, нужно выбрать стиль в справочнике **СТИЛИ.**

6.10 МОНИТОРИНГ ПРОЦЕССОВ ETL

6.10.1 Общие сведения

В Jet Detective реализовано следующие виды ETL-активностей:

- Преобразование (трансформация);
- Задание.

Преобразование – это связанные между собой задачи – шаги преобразования. Данные, поступающие на вход процесса преобразования, пошагово обрабатываются: фильтруются, сортируются, агрегируются, объединяются, обогащаются. На выходе процесса появляются изменённые данные, которые можно сохранить в виде следующих объектов:

- события;
- справочники;
- списки.

Задание – это рабочий процесс, состоящий из нескольких преобразований. Задание предназначено для запуска и координации хода выполнения трансформаций; обработки исключений; условных ветвлений, которые задают порядок выполнения.

Преобразования и задания создаются, а затем регистрируются. После этого они отображаются в Jet Detective в виде древовидного списка (Рисунок 129).

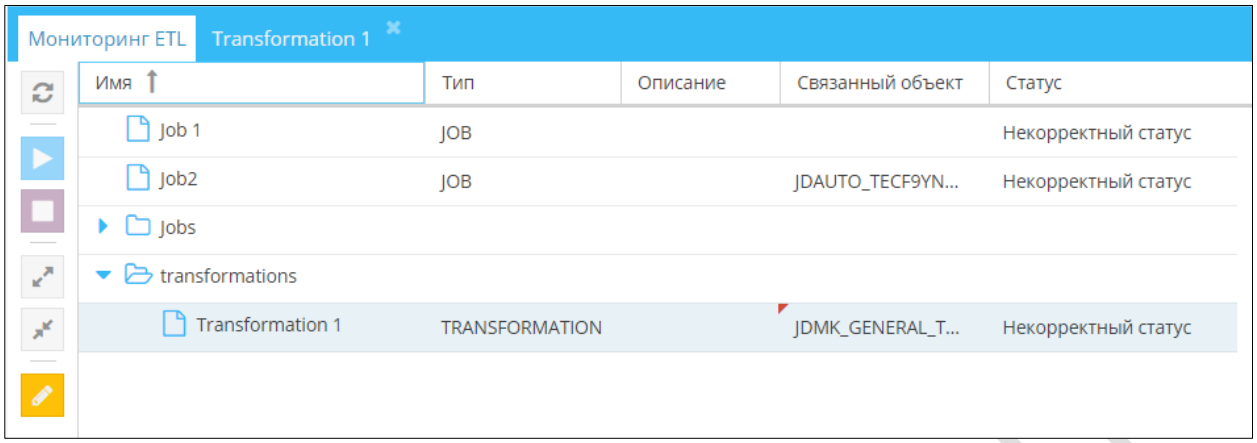


Рисунок 129 – Общий вид рабочей области ETL-процессов

Пользователь может выполнять следующие операции:

- просматривать и настраивать отдельные параметры ETL-процесса (см. раздел 6.10.3.1);
- отслеживать состояние ETL-процесса (см. раздел 6.10.3.2);
- просматривать историю запусков ETL-процесса с типом «Трансформация» (см. раздел 6.10.3.3);
- запускать и останавливать ETL-процесс (см. разделы 6.10.5, 6.10.6).

6.10.2 Просмотр списка ETL-процессов

Чтобы посмотреть список ETL-процессов, выберите пункт меню **Настройки** – **Объектная модель** – **Мониторинг ETL**.

В рабочей области отображается одна или несколько вкладок:

- список ETL-процессов (Рисунок 129);
- экранных форм ETL-процессов, открытых в этой сессии.

6.10.3 Просмотр ETL-процесса

Чтобы посмотреть ETL-процесс:

1) Выберите пункт меню **Настройки** – **Объектная модель** – **Мониторинг ETL**.
2) На вкладке со списком дважды щёлкните по строке с записью ETL-процесса.

Экранная форма ETL-процесса откроется на отдельной вкладке (Рисунок 130). Краткое описание вкладок экранной формы приведено в таблице 34.

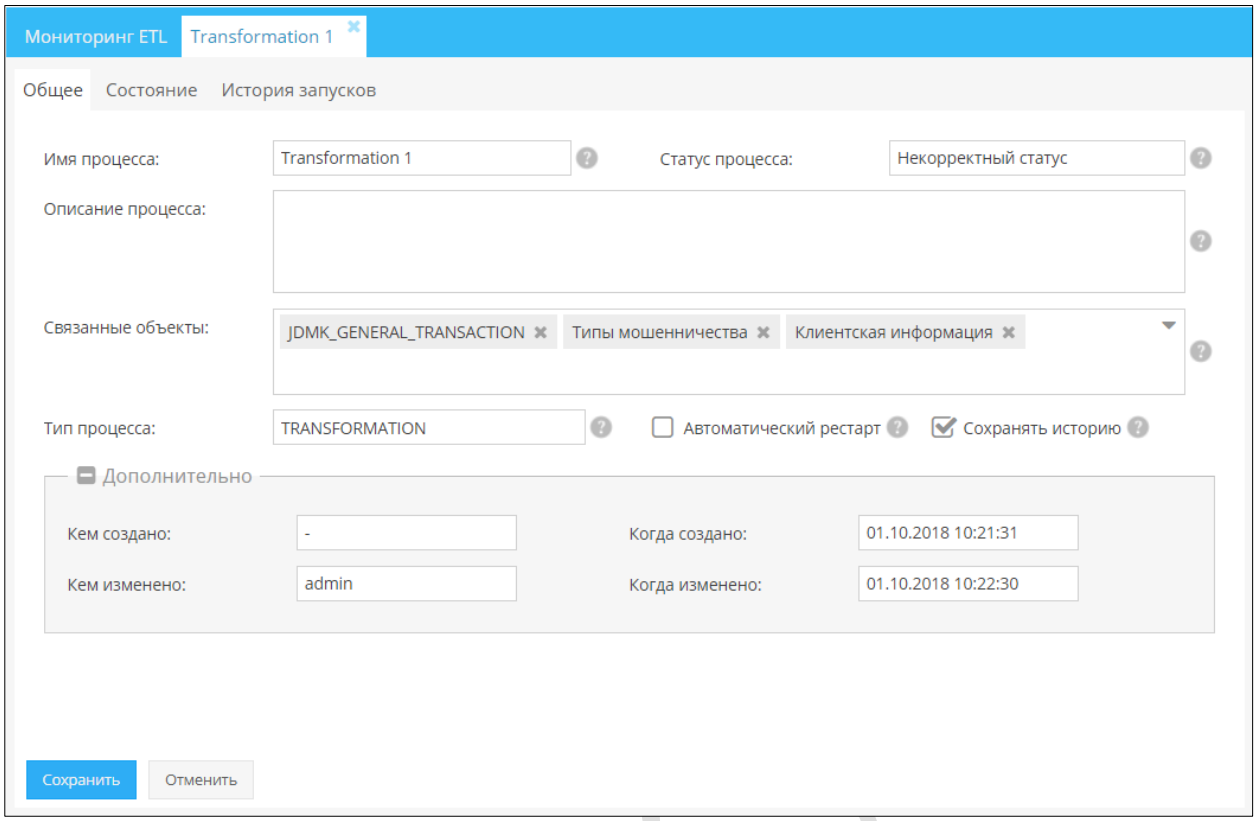


Рисунок 130 – Вкладка с общей информацией ETL-процесса

Таблица 34 – Краткое описание вкладок экранной формы ETL-процесса

Вкладка	Описание
Общее	Общие сведения об ETL-процессе (см. раздел 6.10.3.1)
Состояние	Сведения о состоянии ETL-процесса (см. раздел 6.10.3.2)
История запусков	Сведения об истории запусков ETL-процессов с типом «трансформация» (см. раздел 6.10.3.3)

6.10.3.1 Просмотр общей информации и настройка ETL-процесса

Чтобы просмотреть общую информацию и настроить ETL-процесс:

1) Откройте форму ETL-процесса (см. раздел 6.10.3)

Экранная форма ETL-процесса откроется на вкладке **Общее** (см. рисунок 129).

Описание полей вкладки приведено в таблице 35. Статусы ETL-процесса – в таблице 36.

Таблица 35 – Описание полей вкладки **Общее**

Элемент	Возможность редактирования	Описание
Имя процесса	Нет	Имя процесса
Статус процесса	Нет	Статус процесса
Описание процесса	Да	Текстовое поле для описания процесса

Элемент	Возможность редактирования	Описание
Связанные объекты	Да	Список объектов Jet Detective, которые созданы и применены в **Фабрике данных** (см. раздел 6.2). Поле доступно для изменения и поддерживает множественный выбор. *Примечание.* ETL-процесс, связанный с объектами, не обязательно выполняет действия с этими объектами. Объекты ассоциируются с ETL-процессом на логическом уровне для повышения информативности
Тип процесса	Нет	Возможные значения: ▪ **JOB** – задание, ▪ **TRANSFORMATION** – преобразование (трансформация)
Флаг **Автоматический рестарт**	Да	Если **флаг установлен**, то после аварийной остановки сервиса Jet Detective, отвечающего за выполнение ETL-процессов, и последующего восстановления его работоспособности, ETL-процесс будет запущен автоматически. Автоматически выполняется пять попыток перезапуска процесса. Если **флаг снят**, то автоматический перезапуск ETL-процессов не выполняется. По умолчанию флаг отключен
Флаг **Сохранять историю**	Да	Если **флаг установлен**, то история запусков ETL-процессов будет сохраняться в базе данных Jet Detective. Историю запусков ETL-процессов можно посмотреть на вкладке **История** (см. раздел 6.10.3.3). Если **флаг снят**, то история запусков ETL-процессов сохраняться не будет. По умолчанию флаг отключен
Кем создано	Нет	Регистрационное имя пользователя
Когда создано	Нет	Время создания ETL-процесса
Кем изменено	Нет	Регистрационное имя пользователя, внёсшего изменение в ETL-процесс
Когда изменено	Нет	Время изменения ETL-процесса

Таблица 36 – Статусы ETL-процесса

Код	Название	Описание
FINISHED	Выполнение завершено	Статус предназначен для ETL-процесса типа JOB
RUNNING	Запущенная	Процесс выполняется
PAUSED	Приостановленная	Процесс приостановлен
PREPARING_EXECUTING	Подготовка к выполнению	Статус обозначает, что выполняются подготовительные действия перед выполнением ETL-процесса
INITIALIZING	Инициализация	Процесс создан
WAITING	Ожидание	Статус предназначен для ETL-процесса типа TRANSFORMATION, и обозначает, что выполнение ETL-процесса завершено
FINISHED_WITH_ERRORS	Завершена с ошибкой	Статус обозначает, что во время выполнения ETL-процесса произошла ошибка. Процесс не выполнен
HALTING	Сбой	Статус обозначает, что во время выполнения ETL-процесса произошёл сбой. В отличие от статуса FINISHED_WITH_ERRORS, ETL-процесс выполнил часть действий
INCORRECT_STATUS	Некорректный статус	Статус обозначает, что поступил не известный статус

Код	Название	Описание
READY	Готова к выполнению	ETL-процесс готов к запуску. Описание запуска ETL-процесса приведено в разделе 6.10.5
STOPPED	Остановлена	ETL-процесс остановлен. Описание остановки ETL-процесса приведено в разделе 6.10.6

6.10.3.2 Просмотр состояния ETL-процесса

Чтобы просмотреть состояние ETL-процесса:

1) Откройте форму ETL-процесса (см. раздел 6.10.3)
1) Перейдите на вкладку **Состояние**.

Описание элементов вкладки приведено в таблцие 37. Все параметры на этой вкладке недоступны для редактирования.

Таблица 37 – Описание элементов вкладки **Состояние**

Элемент	Описание
Поле **Имя процесса**	Имя процесса
Поле **Статус процесса**	Статус процесса Возможные значения статуса ETL-процесса приведены в таблице 37
Кнопка **Обновить**	Обновление информации в полях **Статус процесса**, **Шаги процесса** и **Информация о процессе**
Флаг **Автообновление**	Если **флаг установлен**, то поля **Статус процесса**, **Шаги процесса** и **Информация о процессе** обновляются в автоматическом режиме каждые 10 секунд. Положение флага не запоминается и действует только пока открыта эта вкладка. Если **флаг снят**, то обновление **Статуса процесса**, **Шагов процесса** и **Информации о процессе** в автоматическом режиме не выполняется
Поле **Графическое представление ETL-процесса**	Графическое представление ETL-процесса
Табличный список **Шаги процесса**	Параметры шагов процесса. Описание столбцов табличной формы приведено в таблице 38
Поле **Информации о процессе**	Информация из системного журнала ETL-процесса

Таблица 38 – Описание столбцов табличной формы шагов процесса

Столбец	Описание
Шаг	Имя шага ETL-процесса
CopyNr	Номер копии шага
Read	Количество считанных строк входящего потока
Written	Количество записанных строк исходящего потока
Input	Количество считанных строк из файла или базы данных
Output	Количество записанных строк в файл или базу данных
Rejected	Количество отклонённых строк

Столбец	Описание
Errors	Количество возникших ошибок
Active	Статус шага: running, finished, stopped
Time	Время выполнения шага (в секундах)
Update	Количество изменённых строк
Speed	Скорость обработки строк (строк в секунду)
pn/in/out	▪ **pn** – приоритет шага (10 – наивысший, 1 – самый низкий). ▪ **in** – количество строк во входящем потоке. ▪ **out** – количество строк в исходящем потоке

6.10.3.3 Просмотр истории запусков ETL-процесса

Чтобы просмотреть историю запусков ETL-процесса с типом «трансформация»:

1) Откройте форму ETL-процесса (см. раздел 6.10.3).
2) Перейдите на вкладку **История запусков** (Рисунок 131).
3) Выберите запись в таблице истории запусков. Описание столбцов таблицы приведено в таблице 39.

В таблице **Детализация выполнения трансформации** будет представлена подробная информация работы ETL-процесса выбранного запуска. Описание столбцов таблицы приведено в таблице 39 в разделе 6.10.3.2.

4) Нажмите кнопку  для получения информации из системного журнала выбранного запуска ETL-процесса.

В модальном окне откроется форма системного журнала (Рисунок 132).

5) Нажмите кнопку  в форме системного журнала для копирования информации в буфер обмена.

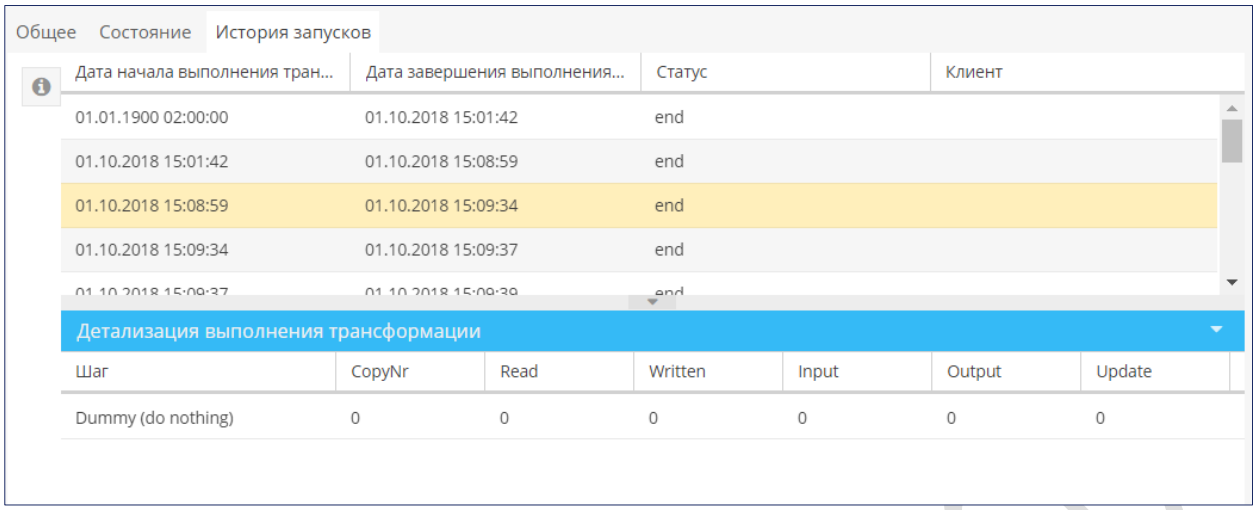


Рисунок 131 – Вкладка **История запусков** ETL-процесса

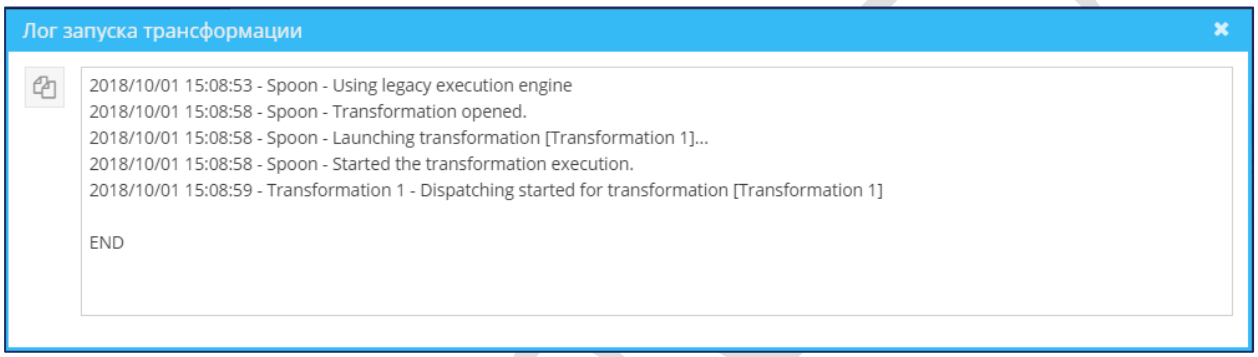


Рисунок 132 – Системный журнал запуска трансформации

Таблица 39 – Описание столбцов истории запусков

Столбец	Описание
Дата начала выполнения трансформации	Время начала выполнения трансформации
Дата завершения выполнения трансформации	Время завершения выполнения трансформации
Статус	Статус выполнения трансформации
Клиент	Возможные значения: Carte, Spoon

6.10.4 Редактирование ETL-процесса

Чтобы отредактировать ETL-процесс:

1) Откройте форму ETL-процесса (см. раздел 6.10.3).
2) Внесите корректировки в параметры процесса (Таблица 40), которые доступны для редактирования согласно табдице 35.
3) Нажмите кнопку **Сохранить**.

Таблица 40 – Параметры ETL-процесса

Параметр	Описание
Описание	Текстовое поле для описания процесса

Параметр	Описание
Связанные объекты	Раскрывающийся список с объектами Jet Detective, которые созданы и применены в **Фабрике данных** (см. раздел 6.2). Также в этом поле можно указать какие объекты наполняются выбранным процессом
Флаг **Автоматический рестарт**	Если **флаг установлен**: если выполнение процесса было прервано, то Jet Detective выполняет 5 попыток его перезапуска. в случае неудачи перезапуска процесс меняет статус на «Ошибка рестарта». Если **флаг снят**, то в случае если выполнение процесса было прервано, то автоматического перезапуска не выполняется
Флаг **Сохранить историю**	Если **флаг установлен**, то в историю сохраняется информация обо всех запусках процесса. Если **флаг снят**, то история запусков не сохраняется

6.10.5 Запуск ETL-процесса

Чтобы запустить ETL-процесс:

1) Выберите пункт меню **Настройки** – **Объектная модель** – **Мониторинг ETL**.
2) На вкладке со списком процессов выберите запись ETL-процесса.
3) Нажмите кнопку **Запустить**  .

Выбранный ETL-процесс запустится. Статус процесса поменяется на RUNNING или PREPARING_EXECUTING.

Примечание. Кнопка **Запустить** доступна при условии, что статус выбранного ETL-процесса не равен RUNNING или PREPARING_EXECUTING.

6.10.6 Остановка ETL-процесса

Чтобы остановить ETL-процесс:

1) Выберите пункт меню **Настройки** – **Объектная модель** – **Мониторинг ETL**.
1) На вкладке со списком процессов выберите запись запущенного ETL-процесса.
2) Нажмите кнопку **Остановить**  .

Выбранный ETL-процесс остановится. Статус процесса поменяется на READY.

Примечание. Кнопка **Остановить** доступна при условии, что статус выбранного ETL-процесса не равен INITIALIZING, READY или STOPPED.

7 НАСТРОЙКА МЕХАНИЗМОВ ВЫЯВЛЕНИЯ АНОМАЛИЙ

7.1 ПРАВИЛА И ПОЛИТИКИ ВЫЯВЛЕНИЯ АНОМАЛИЙ

7.1.1 Общие сведения

Средствами Jet Detective автоматически выполняется кросс-канальный анализ входящего потока данных, целью которого является выявление аномалий. Анализ проводится в соответствии со специальными правилами и политиками выявления аномалий (далее – правила выявления и политики выявления). К задачам аналитика[1] относится настройка этих правил (см. раздел 7.1.2) и политик (см. раздел 7.1.3).

Политика выявления – это набор *правил* для выявления определенного вида аномалии. Правила в политике могут относиться к разным событиям, что обеспечивает кросс-канальный анализ потоков, не связанных между собой событий, и позволяет выявлять цепочки событий.

Можно настраивать правила выявления следующих видов:

- простое правило;
- агрегативное правило.

Простые и *агрегативные правила* являются экспертными правилами. Они используются для выявления известных аномалий и представляют собой набор проверяемых условий. Экспертные правила составляются в отношении определенного объекта с типом **Событие**. При анализе правило применяется к экземпляру события. По результатам проверки описанных в правиле условий правило возвращает логическое значение ИСТИНА или ЛОЖЬ. Правило, вернувшее логическое значение ИСТИНА, называется *сработавшим*.

В политике выявления настраивают *матрицу срабатывания*. Для каждой строки матрицы определяют набор правил выявления, которые входят в политику, и определяют порядок срабатывания этих правил. Политика считается сработавшей, если в результате применения правил сработала хотя бы одна строка матрицы срабатывания или был достигнут пороговый скоринговый балл. Для каждой строки матрицы определяют автоматические действия (см. раздел 6.9.2), которые должны быть выполнены, например:

- создать инцидент;
- информировать пользователей;
- сформировать ответ во внешнюю информационную систему-источник событий;
- выполнить программный сценарий и т. д.

[1] Требования к уровню подготовки пользователей приведены в разделе 1.3.

7.1.2 Настройка правил выявления

7.1.2.1 Просмотр списка групп правил, создание группы, редактирование свойств группы

В Jet Detective правила выявления распределяют по группам. Правило соотносят с той или иной группой один раз в момент создания.

Группа правил – это объединение правил для удобства дальнейшей работы с ними.

Чтобы посмотреть список групп правил:

1) Выберите пункт меню **Лаборатория – Инструменты анализа – Правила**.

В рабочей области отобразится одна или несколько вкладок:

- список групп правил (Рисунок 133);
- правил выявления, открытых в этой сессии.

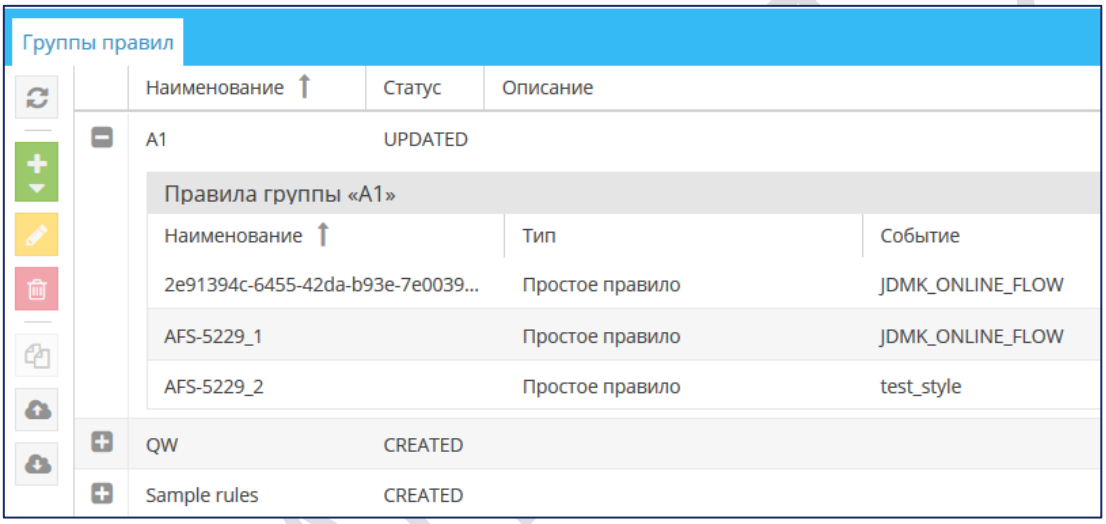


Рисунок 133 – Вкладка со списком групп правил

2) Чтобы раскрыть список правил выявления, входящих в группу, нажмите кнопку (находится слева от названия группы).
3) Чтобы скрыть список правил выявления, входящих в группу, нажмите кнопку .

Чтобы создать группу правил:

1) На вкладке со списком нажмите кнопку **Добавить** и в раскрывшемся меню выберите пункт **Группа правил** (Рисунок 134).

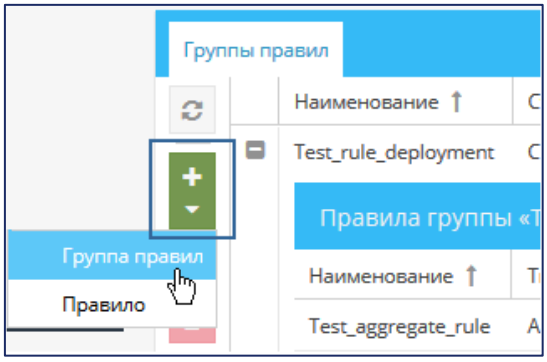


Рисунок 134 – Переход к режиму создания группы правил

3) В открывшемся окне укажите наименование и описание группы (Рисунок 135).
4) Нажмите кнопку **Сохранить**.

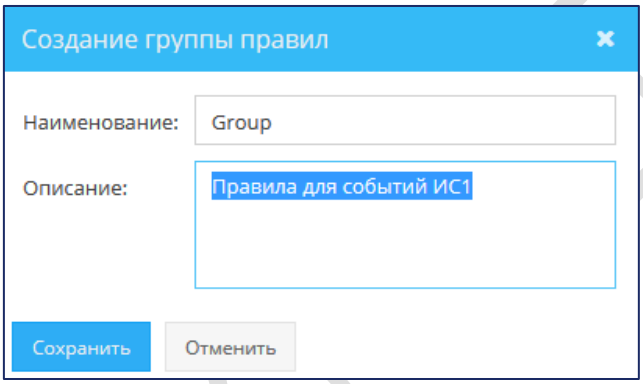


Рисунок 135 – Создание группы правил

Чтобы отредактировать свойства группы правил:

1) На вкладке со списком выберите группу правил (см. рисунок 133).
2) Дважды щёлкните по строке группы.
3) В открывшемся окне внесите изменения в свойства группы (см. рисунок 135).
4) Нажмите кнопку **Сохранить**.

7.1.2.2 Просмотр правила

Чтобы посмотреть правило выявления:

1) Перейдите к просмотру списка групп правил (см. раздел 7.1.2.1).
2) Разверните список входящих в группу правил.
3) Дважды щёлкните по выбранной строке правила.

Экранная форма правила откроется на отдельной вкладке.

На рисунках ниже представлены экранные формы правил разных типов.

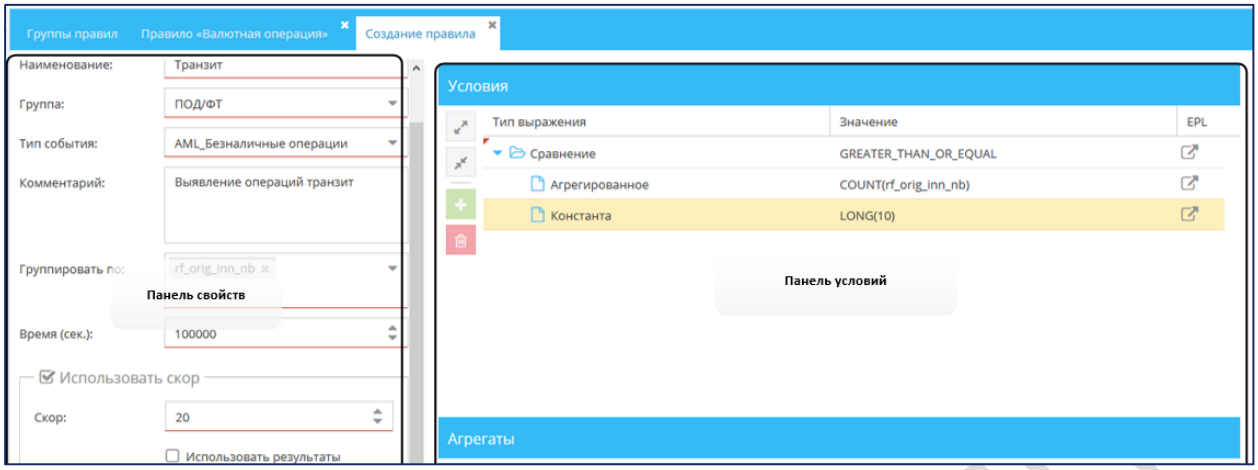


Рисунок 136 – Экранная форма агрегативного правила выявления

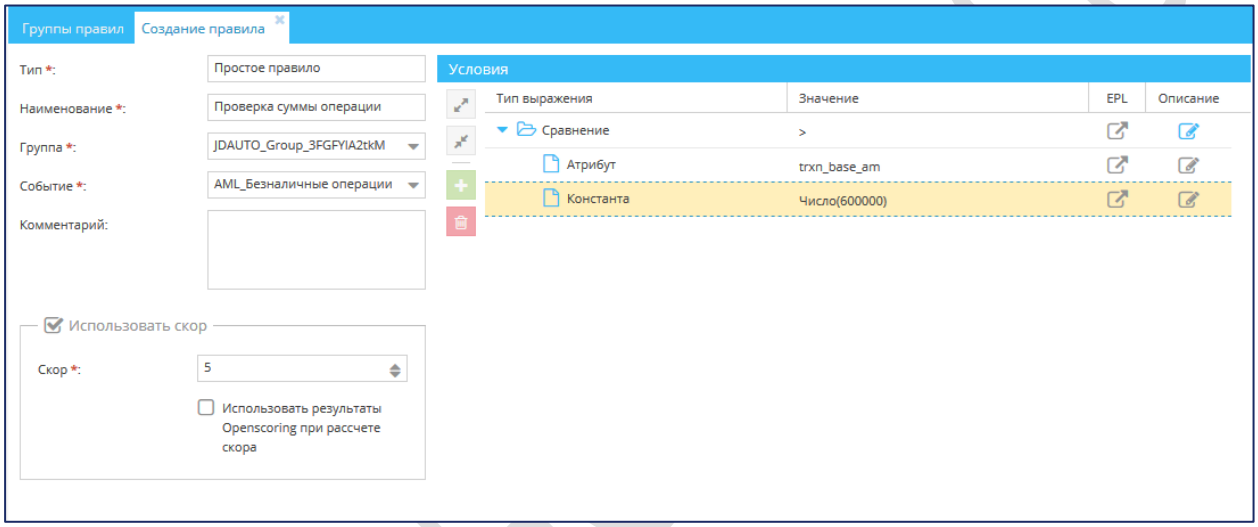


Рисунок 137 – Экранная форма простого правила выявления

Для экранных форм всех типов правил имеется *панель* свойств правил выявления. Отображается в левой части экранной формы (Рисунок 136,Рисунок 137).

В таблице 41 описаны свойства, которые имеются у всех типов правил выявления.

Специфические свойства каждого типа правил описаны ниже в разделах 7.1.2.5, 7.1.2.6.

Таблица 41 – Поля правила выявления

Поле	Описание
Тип	Тип правила выявления. Задается один раз при создании правила. Изменить тип правила нельзя
Наименование	Уникальное название правила (в пределах всех созданных правил выявления)
Группа	Группа правил, в которую входит правило выявления
Тип события	Тип событий, для анализа которых составляется правило (тип события соответствует тому или иному объекту Jet Detective). В раскрывающемся списке доступны только объекты с типом **Событие**. При этом список ограничен объектами, которые имеют статус «Применен», «Изменен, готов к применению», «Изменен, не готов к применению»

Поле	Описание
Комментарий	Текстовое описание правила
Флаг **Добавлять события агрегата**	Флаг доступен только в агрегативном правиле. Если флаг снят, то события, приведшие к срабатыванию условий блога **Агрегат** (тип выражения **Агрегат online,** см.раздел 7.1.2.4.8), не учитываются при выполнении действия создания инцидента (**Создание инцидента по сработавшей строке матрицы срабатывания**). В инцидент добавляется только событие-инициатор проверки. Если флаг установлен, то события, приведшие к срабатыванию условий блога **Агрегат** (тип выражения **Агрегат online,** см.раздел 7.1.2.4.8), учитываются при выполнении действия создания инцидента (**Создание инцидента по сработавшей строке матрицы срабатывания**). В инцидент добавляются все эти события
Флаг **Удалять события из окна после срабатывания правила**	Флаг доступен только в агрегативном правиле. Если флаг снят, то после срабатывания правила на каком-либо экземпляре события (событие-инициатор), все события, совпадающие с событием-инициатором по параметру **«Группировать по»,** остаются в памяти и участвуют при анализе последующих событий, поступающих на проверку. Если флаг установлен, то после срабатывания правила на каком-либо экземпляре события (событие-инициатор), все события, совпадающие с событием-инициатором проверки по параметру «**Группировать по**» (включая само событие -инициатор), удаляются из памяти и дальше контроль по этой группировке в рамках рассматриваемого правила начинается заново
Флаг **Использовать скор**	При установке флага открывается дополнительные параметры для настройке
Флаг **Параллельное исполнение выражений**	Флаг доступен всегда. Если флаг снят, параллельное исполнение выражений не применяется. Если флаг установлен и типы выражений правила соответствуют установленному списку, то исполнение выражений при обращении во внешние сервисы выполняется параллельно. Если установлены приоритеты у частей условия, то при исполнении учитывается номер приоритета. Установка приоритета доступна через редактор выражения после того, как проставлен флаг **Параллельное исполнение выражений**
Скор	Числовое значение от 0 до 100. Установленное значение балла присваивается событию, если правило сработало (вернуло значение ИСТИНА)
Использовать результаты Openscoring при расчете скора	Установленный флаг учитывается только в том случае, если в правиле используются экземпляры группы **Внешний вызов**. Если используется внешний вызов, который возвращает балл скоринга, то этот балл будет учитываться для события, если внешний вызов вернет значение ИСТИНА.

В правой части экранной формы простого или агрегативного правила располагается *панель условий*.

Панель условий **простого правила** состоит из раздела:

- **Условие** – в этом разделе отображается дерево условий (Рисунок 136), по которому будут проверяться данные входящего потока при их анализе.

Панель условий **агрегативного правила** состоит из двух разделов (Рисунок 137):

- **Условия** – в этом разделе составляют условия, которые будут использоваться как фильтр для отбора экземпляров событий, данные которых следует агрегировать;
- **Агрегаты** – в этом разделе настраивают функции агрегации данных и составляют условия, выполнение которых проверяется по отношению к агрегированным данным.

Можно настроить ширину панели условий. Для этого:

1) Подведите указатель мыши к границе панели так, чтобы он принял вид двусторонней стрелки.

2) Перетащите границу панели влево или вправо.

7.1.2.3 Создание правила

Существует два способа создания правила выявления:

- с нуля – в этом случае вручную указывают свойства правила и вручную добавляют в правило все условия;
- на базе существующего правила выявления той же группы – в этом случае имеющиеся свойства и условия берутся за основу. Базовые значения затем можно изменить.

Чтобы создать правило выявления с нуля:

1) Перейдите к просмотру списка групп правил (см. раздел 7.1.2.1).
2) Нажмите кнопку **Добавить**  и в раскрывшемся меню выберите пункт **Правило**.
3) В открывшемся окне (Рисунок 138) заполните поля **Тип** и **Тип события** (Таблица 41).

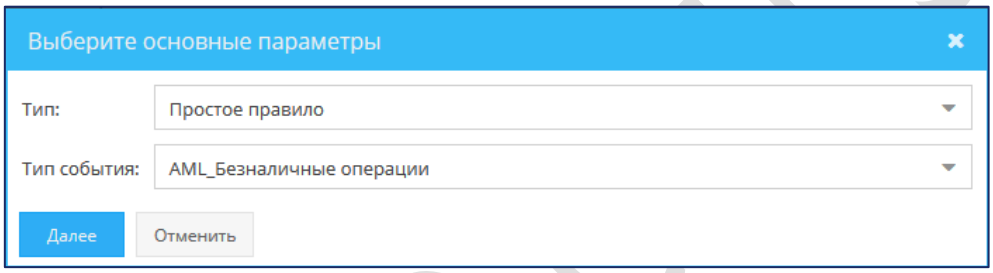


Рисунок 138 – Экранная форма окна создания правила выявления

4) Нажмите кнопку **Далее**.

Экранная форма правила откроется на отдельной вкладке (Рисунок 137 и Рисунок 138).

Примечание. По умолчанию поле **Группа** будет заполнено названием той группы, которая была выбрана в списке групп при создании правила.

5) Настройте правило выявления (см. разделы 7.1.2.5 и 7.1.2.6).
6) Нажмите кнопку **Сохранить**.

Примечания:

а) Простое правило можно сохранить только после добавления хотя бы одного условия.

б) Агрегативное правило можно сохранить только после добавления хотя бы одного условия в разделах **Условия** и **Агрегаты** на панели условий.

Чтобы создать правило выявления на базе существующего правила той же группы:

1) Перейдите к просмотру списка групп правил (см. раздел 7.1.2.1).
2) Выберите исходное правило выявления.
3) Нажмите кнопку **Копировать**  .
4) Нажмите кнопку **Да** в появившемся запросе.

В список правил, входящих в группу, добавится строка с новым правилом. Наименование правила сгенерируется автоматически. Остальные свойства правила, а также условия, скопируются из исходного правила.

5) Дважды щёлкните по строке созданного правила.

Экранная форма правила выявления откроется на отдельной вкладке.

6) Настройте правило (см. разделы 7.1.2.5 и 7.1.2.6).

7) Нажмите кнопку **Сохранить**.

7.1.2.4 Типы выражений и формирования условий

Правило представляет собой набор условий, которые при анализе применяются к данным экземпляра объекта – к конкретному событию. Раздел представляет собой условие в виде дерева, которое формируется с помощью логических групп AND(И) и OR(ИЛИ). По результатам проверки условий и с учетом соединяющих их логических операторов, правило возвращает логическое значение ИСТИНА или ЛОЖЬ.

В агрегативном правиле к условию добавляется еще и агрегация анализируемых данных (см. раздел 7.1.2.6). Логика настройки и формирования условий и агрегации одинакова.

7.1.2.4.1 Описание строк дерева условий

Для удобства в дереве условий на уровне строк можно добавлять комментарии. Добавление описания на узлы выявления правил доступно в редакторе выражения.

1) Двойным щелчком по строке/узлу правила откройте редактор выражения (Рисунок 139).

2) Заполните описание для выбранной строки дерева условий (Рисунок 140).

3) Нажмите кнопку **Применить** для сохранения изменений.

В дереве условий должно отобразиться описание.

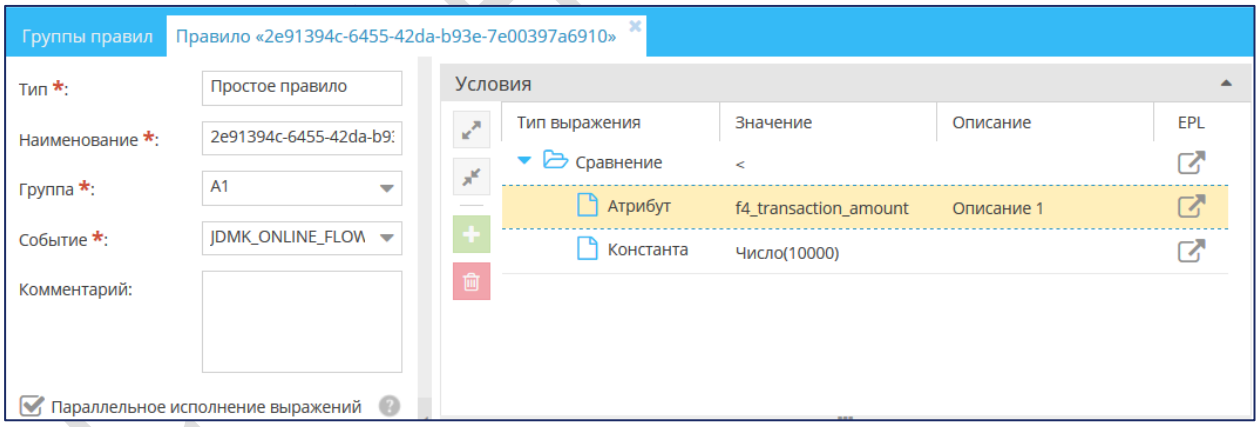


Рисунок 139 – Экранная форма простого правила выявления

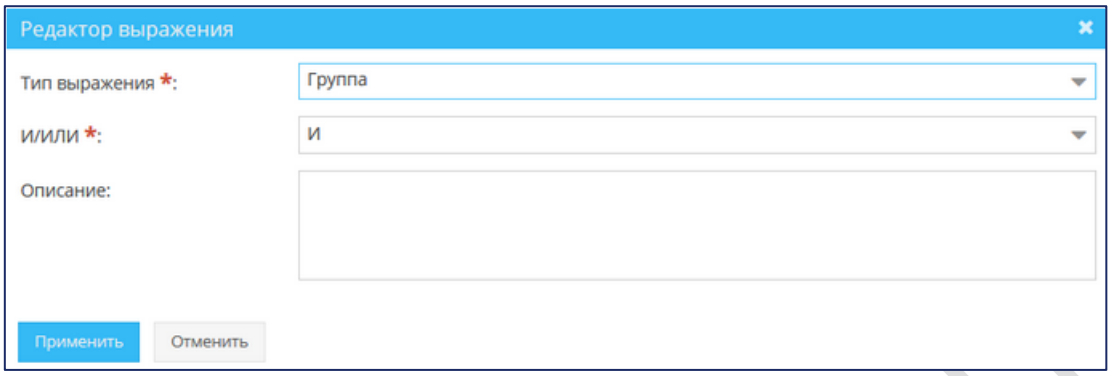


Рисунок 140 – Модальное окно редактора выражений

7.1.2.4.2 Настройка раздела Условия

Ниже описана логика настройки условий на примере раздела **Условия.**

При первоначальном создании правила в разделе **Условия** по умолчанию добавлена первая строка (Рисунок 141) с типом выражения **Атрибут**.

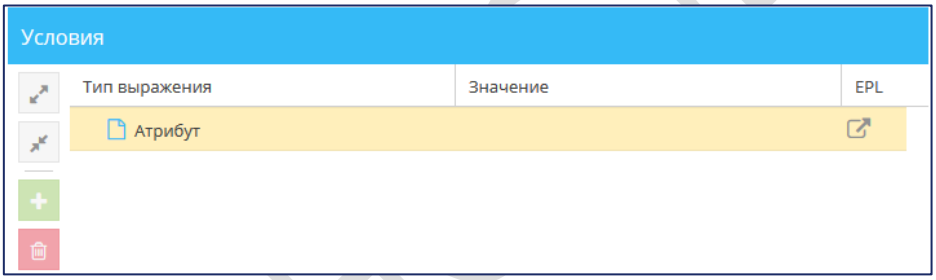


Рисунок 141 – Первоначальный вид раздела **Условие**

Логика формирования условия правила:

- Условия правила представляют собой логическое дерево условий, которое состоит из узлов – тип выражения **Группировка.**
- На ветвях этих узлов должны быть выражения, которые возвращают значение ИСТИНА/ЛОЖЬ или еще один узел.
- Внутри ветвей используются выражения, возвращающие значения.

  Для удобства настройки выражения объединены в группы (Таблица 42).

Таблица 42 – Таблица групп типов выражений

Группа типов выражений	Описание
Группировка	Выражения, которые являются узлами дерева условий
Условия	Выражения, которые по результатам своей работы возвращают значения ИСТИНА или ЛОЖЬ. Эти условия оперируют выражениями из групп типов **Выражения**, **Регулярное выражение**
Выражения	Выражения, которые по результатам своей работы возвращают значение. Эти значения не могут быть показателем срабатывания правила. Эти значения используются в выражениях групп **Условие** и **Регулярные выражения**

Группа типов выражений	Описание
Внешние вызовы	Выражения, которые позволяют использовать результаты работы внешних алгоритмов проверки. Результат работы этих выражений: ИСТИНА или ЛОЖЬ.
Регулярные выражения	Выражения, которые могут возвращать как результат значения ИСТИНА или ЛОЖЬ, так и другое значение. Все зависит от того, что указано в используемом регулярном выражении (см. раздел 6.9.5)
Агрегаты	Выражения, которые по результатам своей работы возвращают значение рассчитанного агрегата

7.1.2.4.3 Типы выражений Группировка

К выражениям **Группировка** относится тип выражения **Группа.**

Модальное окно для настройки типа выражения **Группа** приведено ниже (Рисунок 142).

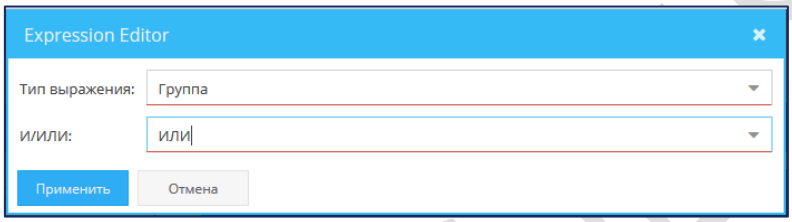


Рисунок 142 – Форма настройки выражения типа **Группа**

Для типа выражения **Группа** необходимо выбрать только вид группировки: **И** или **ИЛИ**.

При выборе типа выражения **Группа** к созданному узлу в дереве условий автоматически добавляется две дочерние ветви (см. рисунок 143).

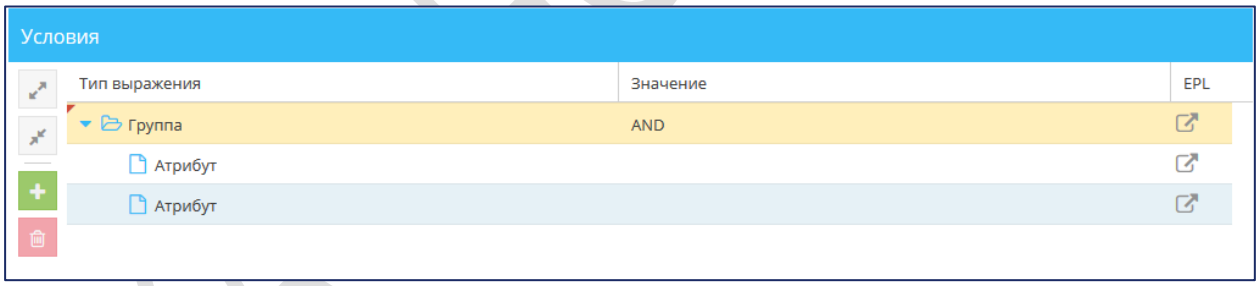


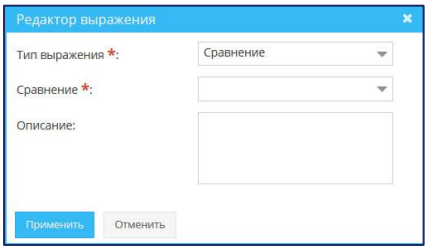
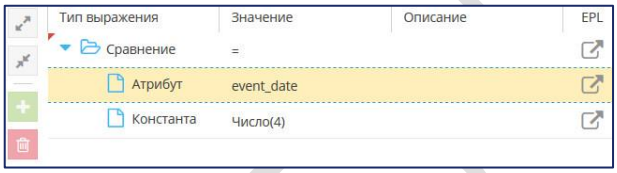
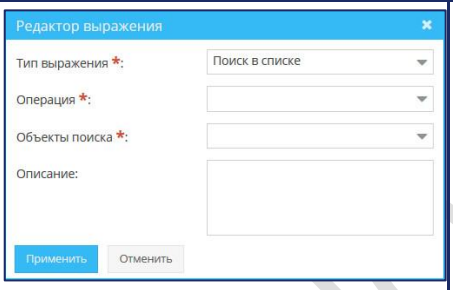
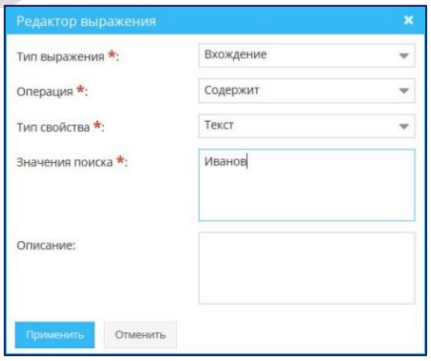
Рисунок 143 – Вид дерева условий при добавлении узла **Группа**

В этих ветвях должны быть выражения, которые возвращают значение ИСТИНА/ЛОЖЬ или еще один узел. Если узл должен иметь больше двух ветвей, то для добавления дополнительных ветвей необходимо выделить в дереве нужный узел и нажать **Добавить выражение**  **.**

7.1.2.4.4 Типы выражений Условие

Выражения группы **Условие** возвращают значения ИСТИНА или ЛОЖЬ. Список выражений, относящихся к группе **Условие,** и их параметры приведены в таблице 43, справочные сведения об операциях сравнения – в таблице 44, справочные сведения о функциях поиска по строковым данным – в таблице 45.

Таблица 43 – Список типов выражений, относящихся к группе **Условие**

Тип выражения	Вид модального окна	Описание выражения и его применения
Сравнение		Выражения с типом **Сравнение** позволяют проводить простые математические сравнения. Возможные операции сравнений описаны в таблице 44. Выберите одну из операций и нажмите **Применить.** После этого в дерево условий автоматически добавятся две дочерние ветви, связанные с созданным условием. Если выбрано значение **Пусто** или **Не пусто**, то дочерняя ветвь будет одна.  Это левая и правая часть операции сравнения. В приведенном примере описано выражение: *Event_date=06.05.2002*
Поиск в списке		Выражения с типом **Поиск в списке** позволяют выполнять поиск атрибута в созданном объекте поиска (см. раздел 6.9.4). Необходимо указать параметры выражения: 1) **Операция**: ▪ Содержит; ▪ Исключено. 2) **Объекты поиска** – раскрывающийся список. После того как параметры выражения указаны, нажмите **Применить.** После этого в дерево условий автоматически добавятся дочерние ветви, связанные с созданным выражением. Количество дочерних ветвей равно количеству записей в таблице блоков выбранного **Объекта поиска** (см. раздел 6.9.4). Каждая дочерняя ветвь имеет подпись равную значению **Наименование** соответствующей строки таблицы блоков **Объекта поиска**.  Каждой дочерней ветви необходимо указать значение, которое будет искаться в заданном объекте поиска
Вхождение		Выражения с типом **Вхождение** позволяют выполнять поиск точного совпадения с заданными значениями. Возможные операции описаны в таблице 44. Необходимо указать параметры выражения. 1) **Операция** ▪ Содержит; ▪ Исключено. 2) **Тип свойства** – раскрывающийся список с перечнем типов свойств для значений поиска.

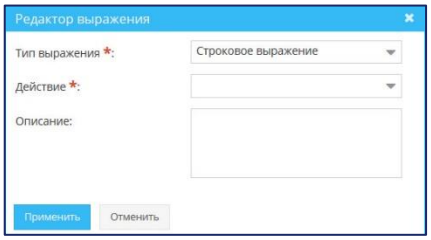
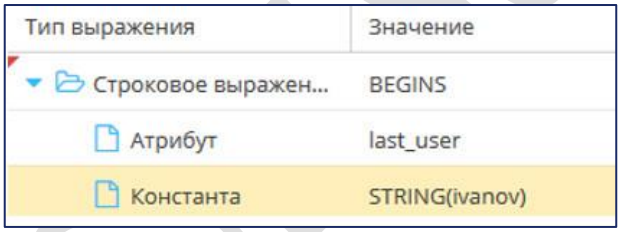
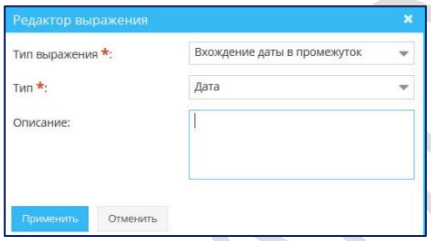
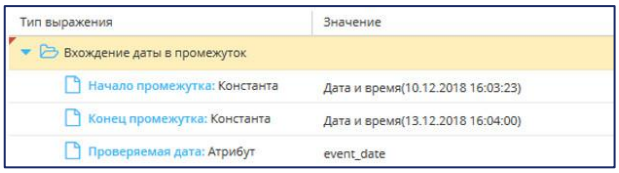
Тип выражения	Вид модального окна	Описание выражения и его применения
		3) **Значения поиска** – текстовое поле, где перечисляются значения для поиска через разделитель «,» (запятая). После того как параметры выражения указаны, нажмите **Применить.** После этого в дерево условий автоматически добавится одна дочерняя ветвь, связанная с созданным выражением. В этой ветви необходимо указать значение, которое будет проверяться на вхождение
Строковое выражение		Выражения с типом **Строковое выражение** позволяют сравнивать строковые значения. Возможные функции поиска строковых данных описаны в таблице 45. Выберите одну из функций и нажмите **Применить.** После этого в дерево условий автоматически добавятся две дочерние ветви, связанные с созданным условием.  Это левая и правая часть операции сравнения. В приведенном примере описано выражение: *last_user* начинается с *«Ivanov»*
Вхождение даты в промежуток		Выражения с типом **Вхождение даты в промежуток** позволяют проверить, попадает ли дата/время в указанный диапазон. Возможные значение параметра **Тип: Дата** и **Время.** Выберите одно из значений параметра **Тип** и нажмите **Применить.** После этого в дерево условий автоматически добавятся три дочерние ветви, связанные с созданным условием.  Во всех трех ветвях необходимо указать значение, которое будет возвращать дату/время. Значения в ветвях **Начало промежутка** и **Конец промежутка** не входят в проверяемый промежуток. В приведенном примере написано выражение: *10.12.2018 16:03:23 < event_date < 13.12.2018 16:04:00*

Таблица 44 – Справочные сведения об операциях сравнения

Операция	Описание	Типы данных, для которых применима операция	Пример
СРАВНЕНИЕ ЗНАЧЕНИЯ АТРИБУТА СОБЫТИЯ СО ЗНАЧЕНИЕМ ДРУГОГО АТРИБУТА СОБЫТИЯ, КОНСТАНТОЙ ИЛИ ЗНАЧЕНИЕМ ГЛОБАЛЬНОЙ ПЕРЕМЕННОЙ			
<=	Меньше или равно	Строковый, числовой, дата-время	event_attr <=10

Операция	Описание	Типы данных, для которых применима операция	Пример
<	Меньше	Строковый, числовой, дата-время	event_attr < 10
=	Равно	Строковый, числовой, дата-время, логический	event_attr = 10
!=	Не равно	Строковый, числовой, дата-время, логический	event_attr!=10
>	Больше	Строковый, числовой, дата-время	event_attr > 10
>=	Больше или равно	Строковый, числовой, дата-время	event_attr >=10
Сравнение значения атрибута события со значениями из списка			
Содержит (IN)	Значение атрибута события входит в список	Строковый, числовой	event_attr IN enum_list
Исключено (NOT_IN)	Значение атрибута не входит в список	Строковый, числовой	event_attr NOT_IN enum_list
Сравнение значения атрибута события с «пустым значением»			
Пусто (IS_NULL)	Значение атрибута «пустое значение»	Строковый, числовой, дата-время, логический	event_attr IS_NULL
Не пусто (IS_NOT_NULL)	Значение атрибута не «пустое значение»	Строковый, числовой, дата-время, логический	event_attr IS_NOT_NULL

Таблица 45 – Справочные сведения о функциях поиска по строковым данным

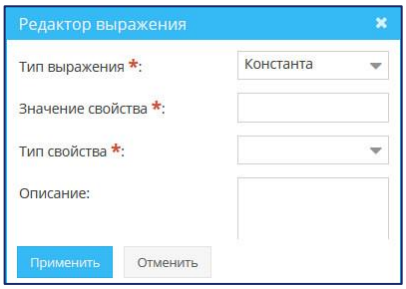
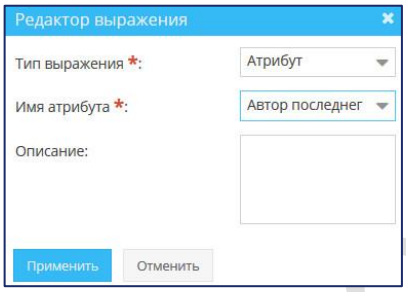
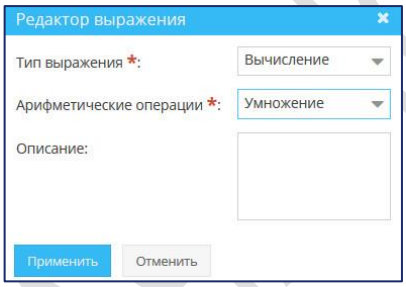
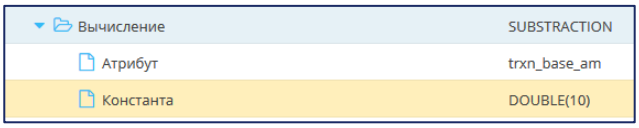
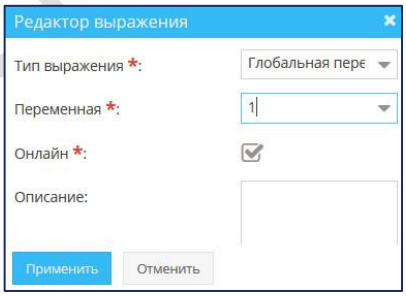
Функция	Описание	Тип данных, для которого применима функция	Пример
Содержит	Возвращает логическое значение ИСТИНА, если в любом месте строки значения первой дочерней ветки найдена подстрока, указанная во второй дочерней ветви	Строковый	event_attr INSTR 'перевод'
Заканчивается на	Возвращает логическое значение ИСТИНА, если строка значения первой дочерней ветви заканчивается подстрокой, указанной во второй дочерней ветви	Строковый	event_attr ENDS 'перевод'
Начинается с	Возвращает логическое значение ИСТИНА, если строка значения первой дочерней ветви начинается с подстроки, указанной во второй дочерней ветви	Строковый	event_attr BEGINS 'перевод'

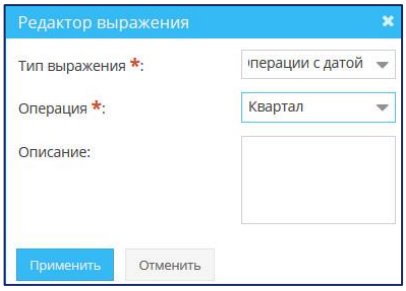
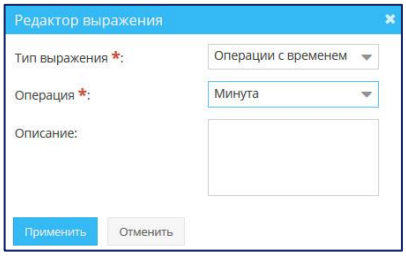
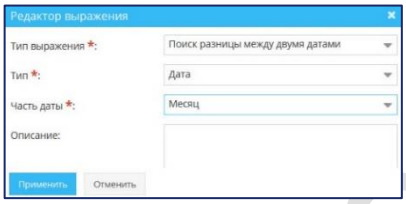
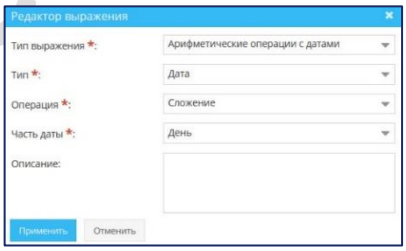
7.1.2.4.5 Типы выражений Выражения

Выражения группы **Выражения** по результатам своей работы возвращают значение.

Список выражений, относящихся к группе **Выражения**, и их параметры приведены в таблице 46, Справочные сведения о функциях преобразования данных в формате даты – в таблице 47, справочные сведения о функциях преобразования данных в формате время – в таблице 48.

Таблица 46 – Список типов выражений, относящихся к группе **Выражения**

Тип выражения	Вид модального окна	Описание выражения и его применения
Константа		Выражения с типом **Константа** позволяют использовать в составляемых выражениях значение константы. Необходимо указать **Значение свойства** и выбрать **Тип свойства**. Затем нажать **Применить.** После этого в дереве условий редактируемая строка примет значение константы. При этом связанные дочерние ветви не создаются
Атрибут		Выражения с типом **Атрибут** позволяют использовать в составляемых выражениях значение атрибута анализируемого события и объектов, связанных с ним с помощью REF-атрибутов. Необходимо выбрать атрибут в раскрывающемся списке и нажать **Применить.** После этого в дереве условий редактируемая строка примет значение атрибута. При этом связанные дочерние ветви не создаются
Вычисление		Выражения с типом **Вычисление** позволяют использовать математические преобразования при создании структуры условия. Необходимо выбрать **Арифметическую операцию** в списке и нажать **Применить.** После этого в дерево условий автоматически добавятся две дочерние ветви, связанные с созданным условием.  Это левая и правая часть арифметической операции. В приведенном примере описано выражение: *trxn_base_am – 10*
Глобальная переменная		Выражения с типом **Глобальная переменная** позволяют использовать значение переменной (см. раздел 6.9.3) в условиях. Необходимо выбрать **Переменную** в списке, установить флаг **online**, если требуется, и нажать **Применить.** После этого в дереве условий редактируемая строка примет значение глобальной переменной. При этом связанные дочерние ветви не создаются

Тип выражения	Вид модального окна	Описание выражения и его применения
Операции с датой		Выражения с типом **Операции с датой** возвращают значение, преобразованное из даты. Возможные операции описаны в таблице 47. Необходимо выбрать в списке **Операцию** и нажать **Применить.** После этого в дерево условий автоматически добавится одна дочерняя ветвь, связанная с созданным выражением. В этой ветви необходимо указать значение, которое будет проверяться на вхождение
Операции с временем		Выражения с типом **Операции с временем** возвращают значение, преобразованное из времени. Возможные операции описаны в таблице 48. Необходимо выбрать в списке **Операцию** и нажать **Применить.** После этого в дерево условий автоматически добавится одна дочерняя ветвь, связанная с созданным выражением. В этой ветви необходимо указать значение, которое будет проверяться на вхождение
Поиск разницы между двумя датами		Выражения с типом **Поиск разницы между датами** возвращают значение (число) разницы между выбранными даты/времени, выраженное в выбранной единице измерения. Для единицы измерения **Месяц** используется 30 дней, для определения **Года** 365 дней. Выражение возвращает целую часть полученного значения. ▪ Возможные значения параметра **Часть даты** описаны в 47. ▪ Возможные значения параметра **Тип: Дата** и **Время**. Необходимо выбрать в списке **Тип** и **Часть даты**, в которой будет представлено сравнение, и нажать **Применить.** После этого в дерево условий автоматически добавится две дочерние ветви, связанные с созданным выражением. В этих ветвях необходимо указать значения, которые будут возвращать даты/время для сравнения. *Пример:* Выбран **Тип** = **Дата** и **Часть даты** = **Месяц**, В первой дочерней ветви возвращается дата 15.02.2018, а на второй ветви – 16.03.2018 Выражение вернет значение 1. Выражение считает, что в любом месяце 30 дней. Получается 16 дней февраля (15.02.2018 также учитывается) и 15 дней марта, итого 31 день. 31/30 = 1,0333. Целая часть выражения 1
Арифметические операции с датами		Выражения с типом **Арифметические операции с датами** возвращает значение измененной даты/времени. ▪ Возможные значения параметра **Часть даты** описаны в таблице 47. ▪ Возможные значения параметра **Тип: Дата** и **Время.** ▪ Возможные значения параметра **Операция: Сложение** и **Вычитание**. Необходимо выбрать в списке **Тип, Операцию** и **Часть даты**, которая будет сравниваться и нажать **Применить.** После этого в дерево условий автоматически добавится две дочерние ветви, связанные с созданным выражением.

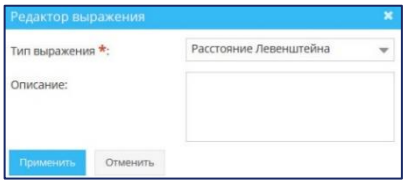
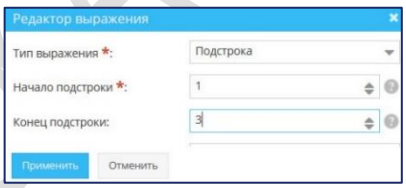
Тип выражения	Вид модального окна	Описание выражения и его применения
		В первой ветви необходимо указать значение, которое будет возвращать дату/время, с которой необходимо выполнить операцию. Во второй ветви необходимо указать значение, которое возвращает число. При выполнении арифметической операции выражение учитывает возможности календаря (количество дней в месяце, количество минут в часе и пр.). *Пример:* Выбраны ▪ **Тип** = **Дата** ▪ **Операция = Сложение** ▪ **Часть даты** = **День** В первой дочерней ветви возвращается дата 20.01.2018, а на второй ветви – значение 35. Выражение прибавит к 20.01.2018 35 дней и получит дату 19.02.2018
Расстояние Левенштейна		Выражения с типом **Расстояние Левенштейна** возвращает рассчитанное расстояние Левенштейна при сравнении двух строковых выражений. Расстояние Левенштейна — это минимальное количество операций вставки одного символа, удаления одного символа и замены одного символа другим, которые необходимы для превращения одной строки в другую. Для сравнения доступны только значения с типом данных Текст(VARCHAR). Строки в неизменном виде подаются на вход алгоритма, рассчитывающего расстояние Левенштейна. Алгоритм является регистронезависимым. Результат работы алгоритма – это целое число, отражающее количество операций, которые необходимо выполнить для того, чтобы одну строку превратить в другую. Чем число меньше, тем более похожи сравниваемые строки. Если одна или обе сравниваемые строки будут иметь значение NULL (пусто), то алгоритм вернет максимально возможное значение расстояния. Выберите выражение с типом **Расстояние Левенштейна** и нажмите **Применить.** После этого в дерево условий автоматически добавится две дочерние ветви, связанные с созданным выражением. В этих ветвях необходимо выбрать те выражения, которые будут возвращать строки для сравнения
Подстрока		Выражение с типом **Подстрока** возвращает подстроку. Начало подстроки и конец подстроки соответствуют порядковому номеру символов, между которыми будет проводиться поиск построки. Необходимо ввести **Начало подстроки, Конец подстроки** и нажать **Применить.** После этого в дерево условий автоматически добавится одна дочерняя ветвь, связанная с созданным выражением. В этой ветви необходимо указать значение, которое будет возвращать строки. *Пример:* Выбраны ▪ **Начало подстроки** = **1** ▪ **Конец подстроки = 3** ▪ Атрибут = last_user, сравнение с константой = ‘Iva’ Выражение получит все подстрки, которые содержат ‘Iva’ с 1-го по 3-й символ у атрибута last_user

Таблица 47 – Справочные сведения о функциях преобразования данных в формате даты

Функция	Описание	Тип данных, для которого применима функция	Операции с датой	Поиск разницы между двумя датами	Арифметические операции с датами
Год	Возвращает год из даты	Дата-время, дата	+	+	+
Квартал	Возвращает номер квартала даты	Дата-время, дата	+		
Месяц	Возвращает номер месяц из даты	Дата-время, дата	+	+	+
Неделя месяца (Неделя)	Возвращает номер недели в месяце	Дата-время, дата	+	+	+
Неделя года	Возвращает номер недели в году	Дата-время, дата	+		
День недели	Возвращает номер дня в неделе	Дата-время, дата	+		
День месяца (День)	Возвращает номер дня в месяце	Дата-время, дата	+	+	+
День года	Возвращает номер дня в году	Дата-время, дата	+		
Час	Возвращает час из даты	Дата-время	+	+	+
Минута	Возвращает минуты из даты	Дата-время	+	+	+
Секунда	Возвращает секунды из даты	Дата-время	+	+	+

Таблица 48 – Справочные сведения о функциях преобразования данных в формате время

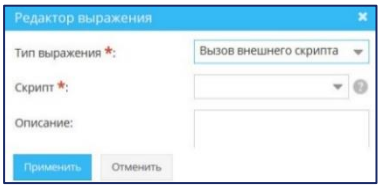
Функция	Описание	Тип данных, для которого применима функция
Час	Возвращает час из даты	Время
Минута	Возвращает минуты из даты	Время
Секунда	Возвращает секунды из даты	Время

7.1.2.4.6 Типы выражений Внешние вызовы

Выражения группы **Внешние вызовы** для работы используют внешние алгоритмы расчета и анализа. Результат работы внешнего вызова является значение ИСТИНА или ЛОЖЬ.

Список выражений, относящихся к группе **Внешние вызовы**, и их параметры приведены в таблице 49.

Таблица 49 – Список типов выражений, относящихся к группе **Внешние вызовы**

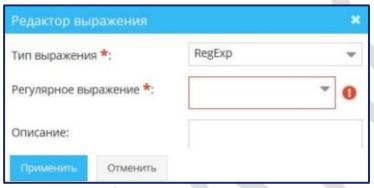
Тип выражения	Вид модального окна	Описание выражения и его применения
Вызов внешнего скрипта		Выражения с типом **Вызов внешнего скприта** позволяют использовать внешние алгоритмы анализа, которые добавляются в виде действий в справочник **Действий** (см. раздел 6.9.2). Необходимо выбрать действие в раскрывающемся списке и нажать **Применить**. После этого в дереве условий редактируемая строка примет значение выбранного действия. При этом связанные дочерние ветви не создаются

7.1.2.4.7 Типы выражений Регулярные выражения

Выражения группы **Регулярные выражения** могут возвращать как значение ИСТИНА или ЛОЖЬ, так и просто значение. Возвращаемое значение зависит от настроек регулярного выражения (см. раздел 6.9.5).

Список выражений, относящихся к группе **Регулярные выражения,** и их параметры приведены в таблице 50.

Таблица 50 – Список типов выражений, относящихся к группе **Регулярные выражения**

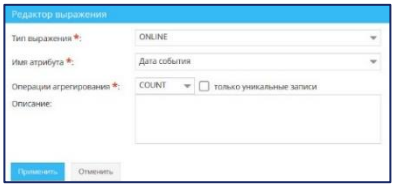
Тип выражения	Вид модального окна	Описание выражения и его применения
RegExp		Выражения с типом **RegExp** позволяют использовать настроенные регулярные выражения (см. раздел 6.9.5). Необходимо выбрать регулярное выражение в раскрывающемся списке и нажать **Применить**. После этого в дерево условий автоматически добавится одна дочерняя ветвь, связанная с созданным выражением. В этой ветви необходимо указать значение, которое будет использоваться в регулярном выражении

7.1.2.4.8 Типы выражений Агрегат

Выражения группы **Агрегат** возвращают значения рассчитанного агрегата.

Список выражений, относящихся к группе **Агрегат,** и их параметры приведены в таблице 51.

Таблица 51 – Список типов выражений, относящихся к группе **Агрегаты**

Тип выражения	Вид модального окна	Описание выражения и его применения
ONLINE (доступен только при настройке агрегативного правила в разделах **Условия** и **Агрегат**)		Выражения с типом **ONLINE (Агрегат)** позволяют задавать параметры агрегации отобранных событий. Результатом работы выражения является значение рассчитанного агрегата. Агрегация будет выполняться за промежуток времени, который указан в параметре **Время** и **Время в** – в панели свойств правила. Необходимо выбрать **Имя атрибута** и **Операции агрегирования**. Если выбран оператор COUNT, то появляется флаг «только уникальные записи».

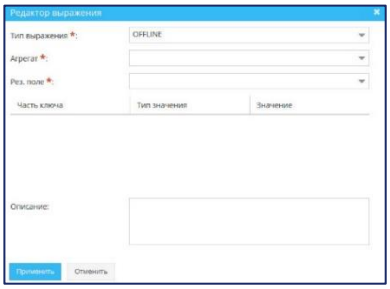
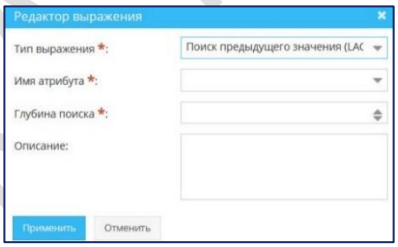
Тип выражения	Вид модального окна	Описание выражения и его применения
		Установите флаг, если для подсчета количества необходимо учитывать только записи с уникальными значениями, в атрибуте, выбранном в поле **Имя атрибута**. Нажмите **Применить.** После этого в дереве агрегации редактируемая строка примет значение выбранного действия. При этом связанные дочерние ветви не создаются
OFFLINE		Выражение типа **OFFLINE (Агрегат)** используется значение заранее рассчитанного агрегата (см. раздел 7.2) Для настройки этого типа выражения: 1) Выберите объект в раскрывающемся списке параметра **Агрегат.** В списке доступны объекты с типом **Агрегат**, для которых настроено управление агрегатом. 2) Выберите рассчитанное результирующее поле агрегата, которое будет использоваться в правиле. В списке доступны те результирующие поля, которые указаны в управлении агрегата в разделе **Функции агрегата** (см. раздел 7.2.3). 3) Заполните таблицу ключей агрегата. В таблице указано то количество ключей агрегата, которое задано в управлении этого агрегата в разделе **Ключи агрегата** (см. раздел 7.2.3). 4) Указажите, какие значения должны использоваться для ключей при поиске рассчитанных значений. 5) Для каждого ключа в таблице: ▪ Выберите **Тип значения**: ◆ Константа; ◆ Атрибут. ▪ Заполните значение ключа. ▪ Для типа значения **Константа** укажите значение. ▪ Для типа значения **Атрибут** выберите атрибут объекта, указанного в параметре **Событие** на Панели свойств правила. После этого в дереве агрегации редактируемая строка примет значение выбранного действия. При этом связанные дочерние ветви не создаются
Поиск предыдущего значения (LAG) (доступен только при настройке агрегативного правила в разделах **Условия** и **Агрегат**)		Выражение типа **Поиск предыдущего значения (LAG)** возвращает значение выбранного атрибута события из окна отслеживания, которое отстоит от события-инициатора проверки на заданное количество позиций. В окне отслеживания события выстраиваются по полю **event_date** в порядке от большего к меньшему значению. Для выражения с типом **Поиск предыдущего события (LAG)** событие-инициатор проверки – это событие с позицией 0. Следующее событие в окне отслеживания – событие с позицией 1 и дальше по очереди. Выберите в поле **Имя атрибута** в раскрывающемся списке атрибут, значение которого должно вернуть выражение. В поле **Глубина поиска** укажите позицию события, из которого необходимо получить данные относительно события-инициатора проверки. Нажмите кнопку **Применить**. Выражение работает только с теми событиями, которые попадают в окно отслеживания агрегативного правила. Никакие дочерние ветви при добавлении выражения этого типа не создаются

Таблица 52 – Справочные сведения об операциях агрегации

Операция	Описание	Тип данных, для которого применима операция
COUNT	Подсчитать количество	Строковый, числовой, дата-время, логический
AVG	Вычислить среднее значение	Числовой
SUM	Вычислить суммарное значение	Числовой
MAX	Найти максимальное значение	Числовой
MIN	Найти минимальное значение	числовой

7.1.2.5 НАСТРОЙКА ПРОСТОГО ПРАВИЛА

При настройке простого правила на панели свойств вручную указывают его свойства, кроме типа правила. Затем настраивают само условие простого правила.

Чтобы настроить условие в правиле выявления:

1) Дважды щелкните по первой строке условия, где по умолчанию задан тип выражения **Атрибут**.
2) Откроется модальное окно с выбором типа выражения и его характеристик. Выберите необходимый тип выражения и его характеристики (см. раздел 7.1.2.4).
3) Если требуется, повторяя действия пунктов 1 и 2 сформируйте дерево условий, используя доступные типы выражений.
4) Нажмите кнопку **Сохранить**.

7.1.2.6 НАСТРОЙКА АГРЕГАТИВНОГО ПРАВИЛА

Агрегативное правило представляет собой набор условий, которые в ходе анализа применяются к данным нескольких экземпляров одного объекта, а именно: нескольких событий одного вида.

При применении правила экземпляры событий предварительно подвергаются отбору (раздел **Условия**), а данные отобранных экземпляров группируются (список атрибутов в поле **Группировать по**) и агрегируются (раздел **Агрегат**) – см. рисунок 144.

Разделы **Условия** и **Агрегаты** настраиваются идентично разделу **Условия** простого правила (см. раздел 7.1.2.5).

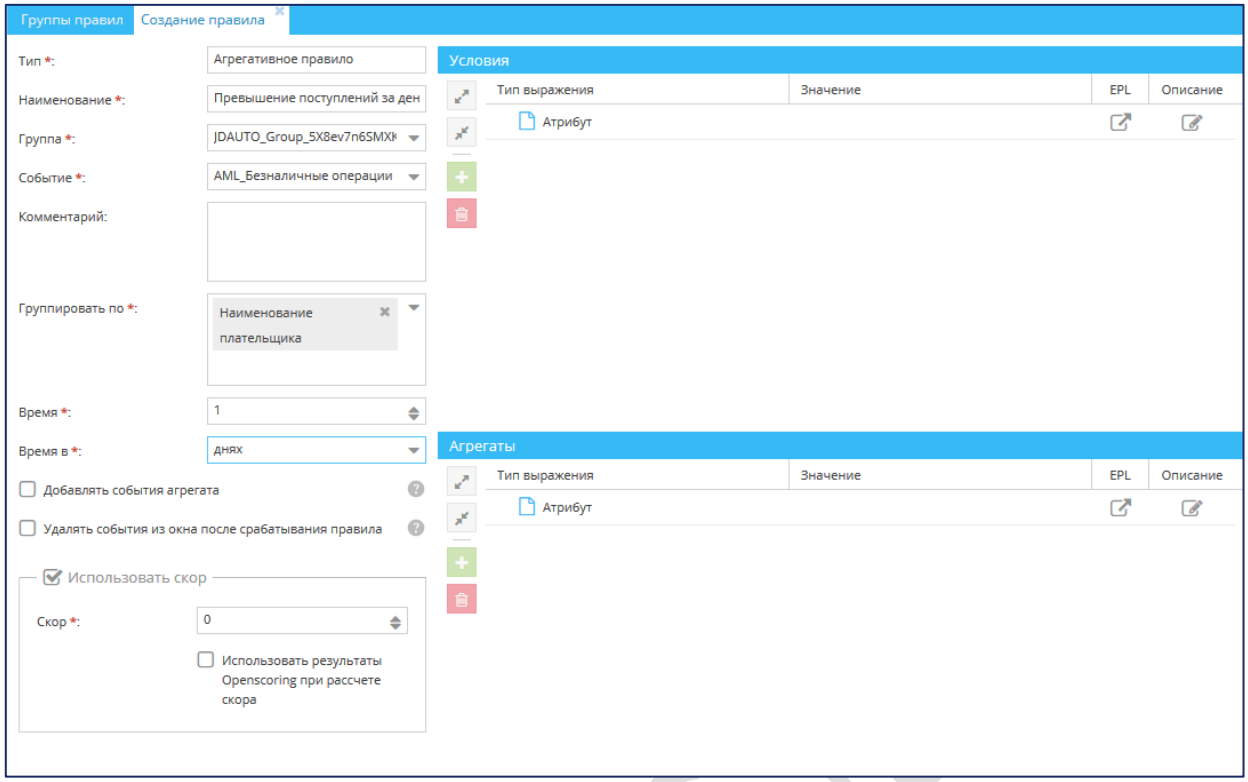


Рисунок 144 – Экранная форма агрегативного правила выявления

Условия, выполнение которых проверяется по отношению к агрегированным данным, соединяют с помощью логических операторов AND (И) или OR (ИЛИ). По результатам проверки условий и с учетом соединяющих их логических операторов, правило возвращает логическое значение ИСТИНА или ЛОЖЬ.

Общий порядок настройки агрегативного правила приведен в таблице 53.

Таблица 53 – Общий порядок настройки агрегативного правила

№	Шаг	Описание
1.	Настройка основных свойств правила	При создании агрегативного правила, на панели свойств вручную указывают его основные свойства, кроме типа и статуса правила
2.	Настройка интервала времени для отбора экземпляров событий	У каждого события имеется атрибут, в котором хранится время поступления события в Jet Detective (event_date). Для агрегативного правила настраивают продолжительность интервала, предшествующего поступлению анализируемого экземпляра события в Jet Detective. Правило каждый раз применяется по отношению к множеству событий, попадающих в такой интервал. Чтобы настроить интервал времени для отбора экземпляров событий, на панели свойств заполните поля **Время** и **Время в**
3.	Настройка условий, которые будут использоваться как фильтр для отбора экземпляров событий	Экземпляры событий, попавшие в настроенный интервал времени, проходят отбор на соответствие заданным условиям. Настройка этих условий выполняется на панели условий в разделе **Условия** так же, как настройка условий в простом правиле выявления (см. раздел 7.1.2.5)

№	Шаг	Описание
4.	Настройка группирования данных	Агрегативное правило имеет сходство с GROUP BY, применяемой в SQL. Для группирования следует указать один или несколько атрибутов события, аналогично тому, как это делается при использовании оператора GROUP BY. Настройка группирования действует для всех условий из раздела **Агрегаты** на панели условий. Чтобы настроить группирование данных, на панели свойств, в поле **Группировать по**, укажите один или несколько атрибутов события
5.	Настройка функций агрегации данных и составление условий, выполнение которых будет проверяться по отношению к агрегированным данным	Выполняется на панели условий в разделе **Агрегаты**

7.1.2.7 Редактирование правила

Чтобы отредактировать правило выявления:

1) Откройте экранную форму правила (см. раздел 7.1.2.2).
2) Внесите изменения в настройке правил.
3) Добавьте в правило одно или несколько условий или удалите условия из правила выявления (см. разделы 7.1.2.5 – 7.1.2.6, в зависимости от типа правила).
4) Нажмите кнопку **Сохранить**.

7.1.2.8 Удаление группы правил или правила

Примечания:

а) Группу правил можно удалить, если в ней нет ни одного правила выявления, которое используется в политиках выявления.

б) Правило выявления можно удалить, если оно не используется ни в одной политике выявления.

Чтобы удалить группу правил (правило выявления):

1) Откройте экранную форму списка групп правил (см. раздел 7.1.2.1).
2) Выберите группу в списке.
3) Нажмите кнопку **Удалить**  .
4) Нажмите кнопку **Да** в появившемся запросе на удаление.

Чтобы удалить правило выявления из какой-либо группы:

1) Выберите правило в списке группы.
2) Нажмите кнопку **Удалить**  .
3) Нажмите кнопку **Да** в появившемся запросе на удаление.

7.1.2.9 Импорт и экспорт правил

Чтобы экспортировать правила:

1) Перейдите к просмотру списка групп правил (см. раздел 7.1.2.1).

2) Нажмите кнопку **Экспортировать** 

3) В открывшемся модальном окне (Рисунок 145) с помощью флагов отметьте правила, которые нужно экспортировать.

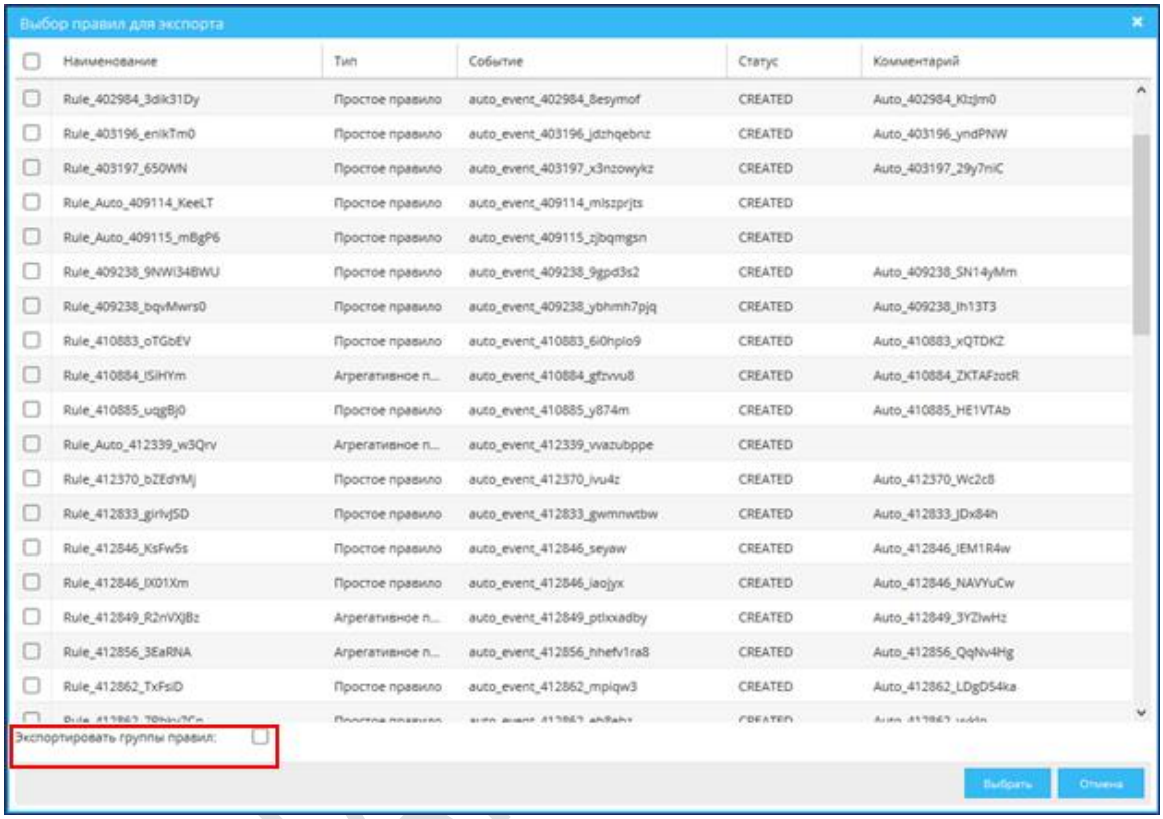


Рисунок 145 – Форма выбора правил для экспорта

4) Установите флаг **Экспортировать группы правил,** если при экспорте необходимо сохранить группы правил, к которым они привязаны.

5) Нажмите кнопку **Выбрать.**

Чтобы импортировать правила:

1) Перейдите к просмотру списка групп правил (см. раздел 7.1.2.1).

2) Нажмите кнопку **Импортировать**  .

3) В открывшемся модальном окне (Рисунок 146) выберите файл для загрузки.

В модальном окне отобразится список правил, которые будут импортированы (Рисунок 147).

Примечание: Расширение загружаемого файла должно быть .rls

4) Для каждого правила укажите группу правил, в которую каждое из правил должно загрузиться.

5) Нажмите кнопку **Импорт.**

Примечание: для корректного импорта правил необходимо, чтобы объекты и сущности, используемые в переносимом правиле, полностью совпадали с тем, как эти объекты и сущности настроены на стенде, с которого выполнен экспорт. В противном случае импорт правил невозможен.

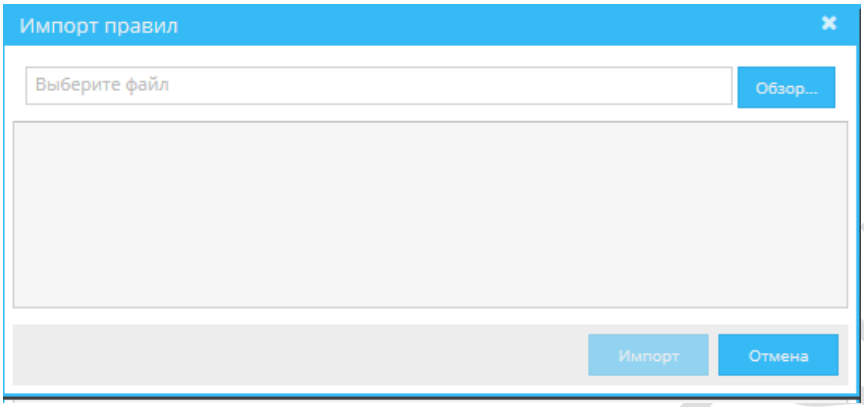


Рисунок 146 – Форма выбора файла для импорта правил

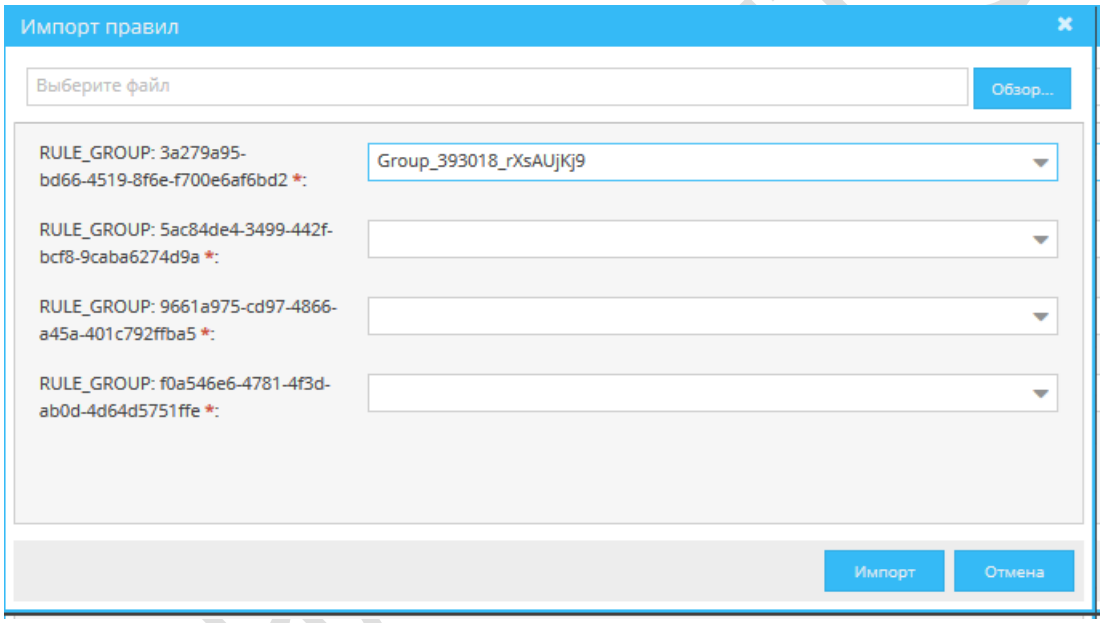


Рисунок 147 – Форма импорта правил. Список правил

7.1.3 Настройка политик выявления

7.1.3.1 Просмотр и редактирование политики

Если политика выявления не запущена на выполнение, её можно отредактировать. В противном случае следует предварительно остановить выполнение политики (см. раздел 7.1.3.4).

Чтобы посмотреть и отредактировать политику выявления:

1) Выберите пункт меню **Лаборатория – Инструменты анализа – Политики**.

2) В рабочей области отобразится одна или несколько вкладок:

- списка политик (Рисунок 148);
- экранных форм политик, открытых в этой сессии (Рисунок 149).

В списке политик выявления (Рисунок 148) в столбце **Статус** отображается состояние каждой записи. Описание значения каждого статуса описано в таблице 54.

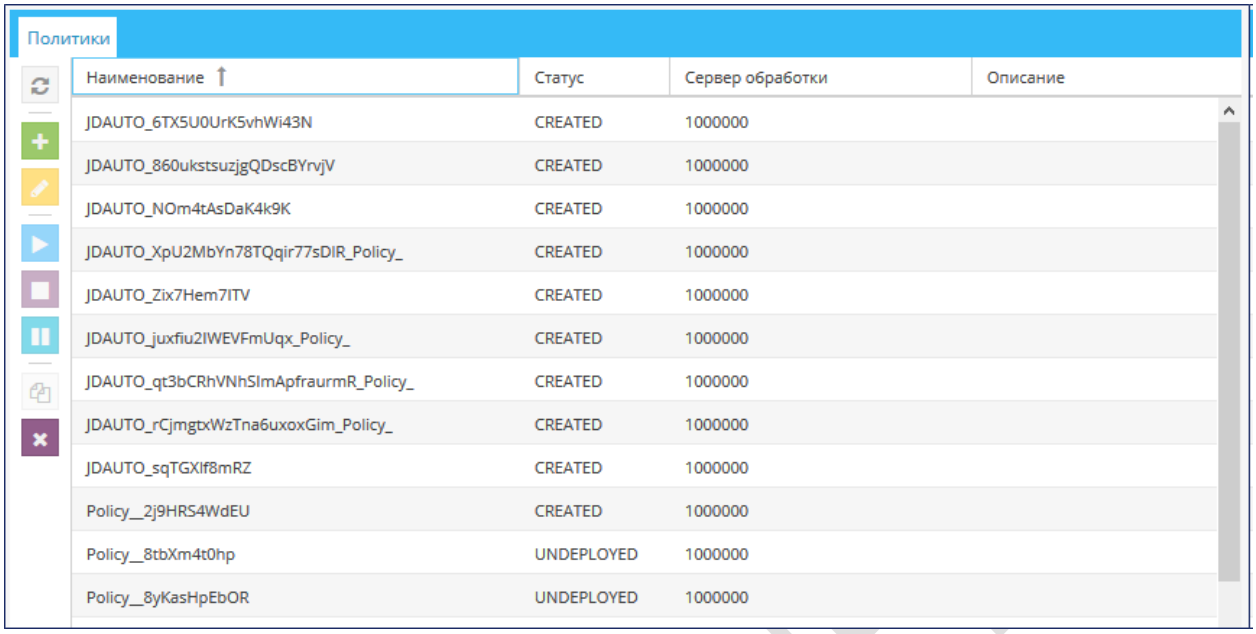


Рисунок 148 – Список политик выявления

Кнопка **Сбросить кеш** обновляет информацию о действиях, которые выполняются по результату работы политик. Кнопка необходима, если в действие, которое ранее уже было привязано к политике, вносились изменения.

Таблица 54 – Возможные значения статуса политик выявления

Статус	Описание	Доступные для редактирования параметры политики
CREATED	Политика создана и ни разу не была запущена	Редактирование полностью доступно
DEPLOING	Это промежуточный статус – ожидание ответа от сервера обработки. Статус устанавливается, если для политики была нажата кнопка **Запустить** или для объекта выполнения политики была нажата кнопка **Выполнить**, а сервер обработки еще не вернул ответ о том, что политика запущена	Редактирование полностью недоступно
DEPLOYED	Политика запущена. Сервер обработки сохранил слепок политики, актуальный на момент ее запуска и начала выполнения. Сервер отслеживает указанную в политике очередь, выполняет проверки и сохранение агрегативных расчетов	Редактирование полностью недоступно
UNDEPLOYED	Политика остановлена и проверки по ней не выполняются. Все результаты промежуточных расчетов (сохраненные агрегативные значения, результаты окна отслеживания срабатывания правил в строках матриц срабатывания) для неё удалены. После повторного перезапуска такой политики, расчет начнется заново	Редактирование полностью недоступно

Статус	Описание	Доступные для редактирования параметры политики
PAUSE	Политика приостановлена пользователем в интерфейсе. Этот статус идентичен статусу HOLD, но в статусе HOLD политика приостановлена в следствии сбоя, а в статусе PAUSE – пользователем. Промежуточные результаты расчетов по политике (агрегативные значения, результаты окна отслеживания срабатывания правил в строках матриц срабатывания) сохраняются и после перезапуска такой политики. Расчет начнется с учетом сохраненных значений	Доступно редактирование поля **Сервер обработки**
HOLD	Политика была запущена (статус DEPLOYED), но сервер обработки остановлен. Промежуточные результаты расчетов (агрегативные значения, результаты окна отслеживания срабатывания правил в строках матриц срабатывания) по такой политике сохраняются. После перезапуска политики в таком статусе расчет начнется с учетом сохраненных значений	Доступно редактирование поля **Сервер обработки**
DEPLOYED_FOR_TEST	Политика запущена в режиме испытания политик	Редактирование полностью недоступно

3) На вкладке со списком политик дважды щёлкните по строке политики.

Экранная форма политики откроется на отдельной вкладке (Рисунок 149). Форма содержит вкладки второго уровня: **Общие сведения** и **Матрица срабатывания**.

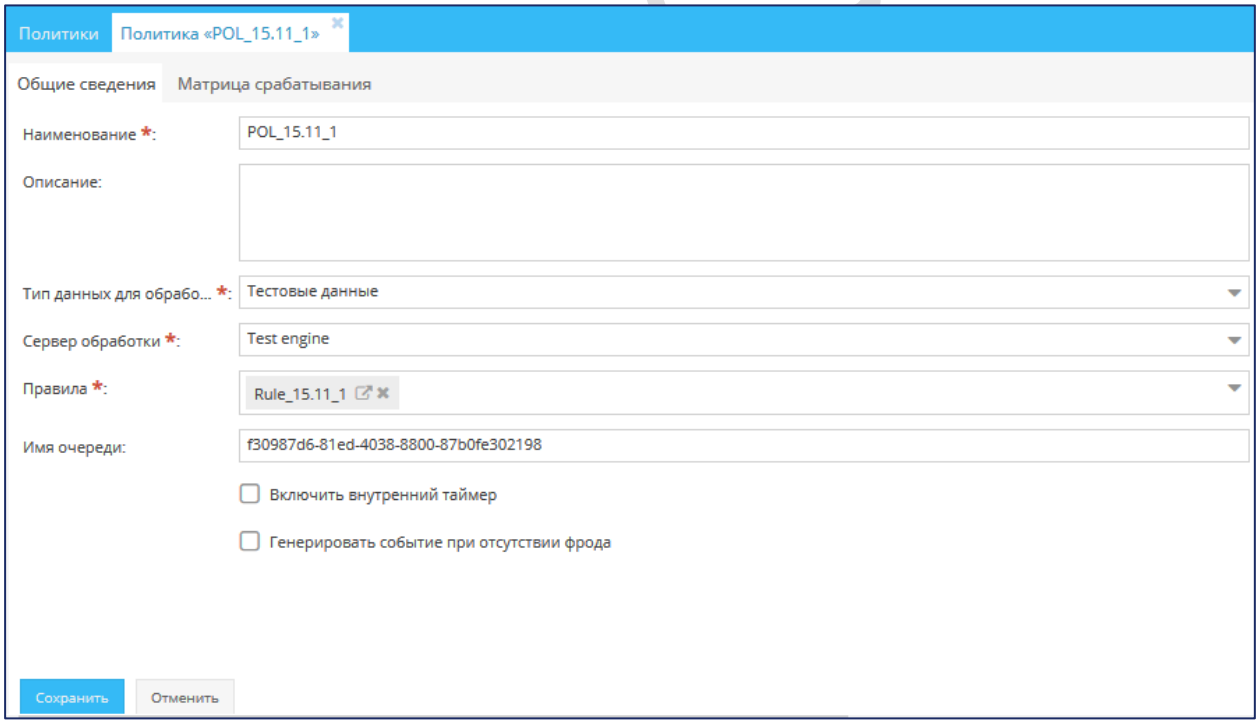
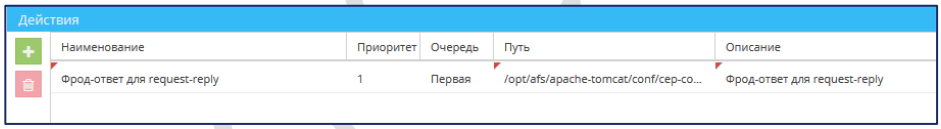


Рисунок 149 – Экранная форма политики выявления

Таблица 55 – Поля политики выявления

Поле	Описание
Наименование	Уникальное название политики
Описание	Описание политики

Поле	Описание
Тип данные	Выбор из двух значений: ▪ **Реальные данные** – политика будет анализировать реальные события, поступающие в Jet Detective. ▪ **Тестовые данные** – политика будет использоваться для тестирования и отладки
Сервер обработки	Выбор движка, который будет использовать политика при расчете, – в раскрывающемся списке серверов обработки (см. раздел 6.9.1)
Правила	Перечень правил выявления, включенных в политику. Выбор в раскрывающемся списке настроенных ранее правил (см. раздел 7.1.2)
Флаг **Включить внутренний таймер**	Если флаг снят, то для работы используется время события, которое пришло на анализ (event_date). Т. к. в топике шины события выстраиваются в хронологическом порядке по атрибуту event_date, то таким образом движок может корректно отслеживать временное окно для работы матриц срабатывания. Если флаг установлен, то для работы используется время сервера, на котором развернут экземпляр приложения. Такой режим работы используется для реализации одного ответа по событию от разных политик (см. раздел 7.1.3.5)
Флаг **Генерировать событие при отсутствии фрода**	При установке этого флага Jet Detective будет отсылать событие для внешней системы, если событие не попало под настроенные условия выявления. Откроется дополнительная область для настройки действий, которые должны выполняться, если для события не сработали настроенные правила выявления.  С помощью кнопок **Добавить** и **Удалить** сформируйте список необходимых действий, выбирая их в справочнике **Действий** (см. раздел 6.9.2)**.** Укажите приоритет каждого действия и очередь, в которой будет выполняться действие. Логика и правила заполнения этого раздела описана в разделе 7.1.3.4.

4) Чтобы посмотреть сведения о настройке строки матрицы срабатывания, перейдите на вкладку **Матрица срабатывания.**

На вкладке отображается список настроенных матриц срабатывания (РИС. 1).

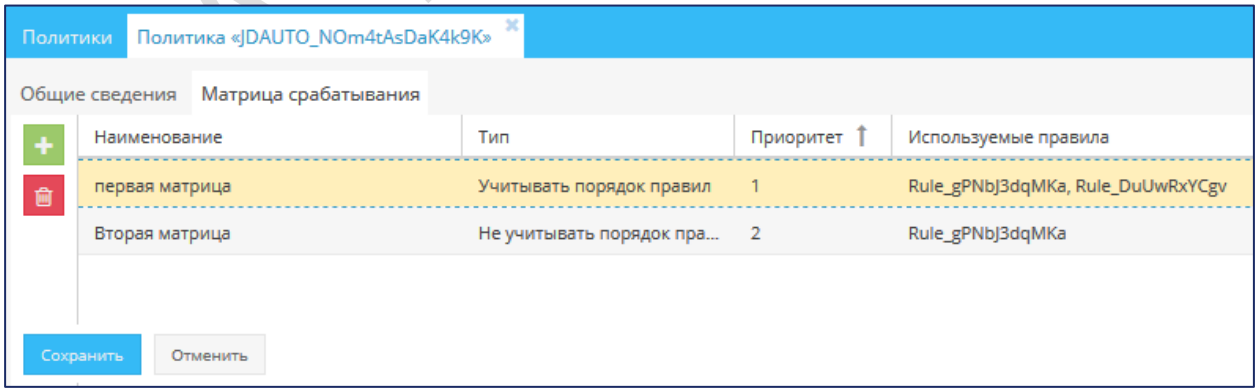


РИС. 1 – Список настроенных матриц срабатывания

5) Для просмотра параметров настройки матрицы срабатывания дважды щелкните по её строке.

Откроется окно **Строка матрицы срабатывания <наименование строки>** (РИС. 2). Окно состоит из двух вкладок:

- **Общие сведения** – содержит общие сведения о строке матрицы. В верхней части вкладки отображаются свойства строки (ТАБЛ. 2). раздел **Действия** содержит инструменты для настройки перечня автоматических действий, которые должны быть выполнены в случае срабатывания строки (см. раздел 6.9.2);
- **Связи правил** – содержит инструменты для настройки порядка срабатывания правил и настройки связей между событиями правил.

6) Внесите изменения в свойства политики.

7) Внесите изменения в матрицу срабатывания.

8) Нажмите кнопку **Сохранить**.

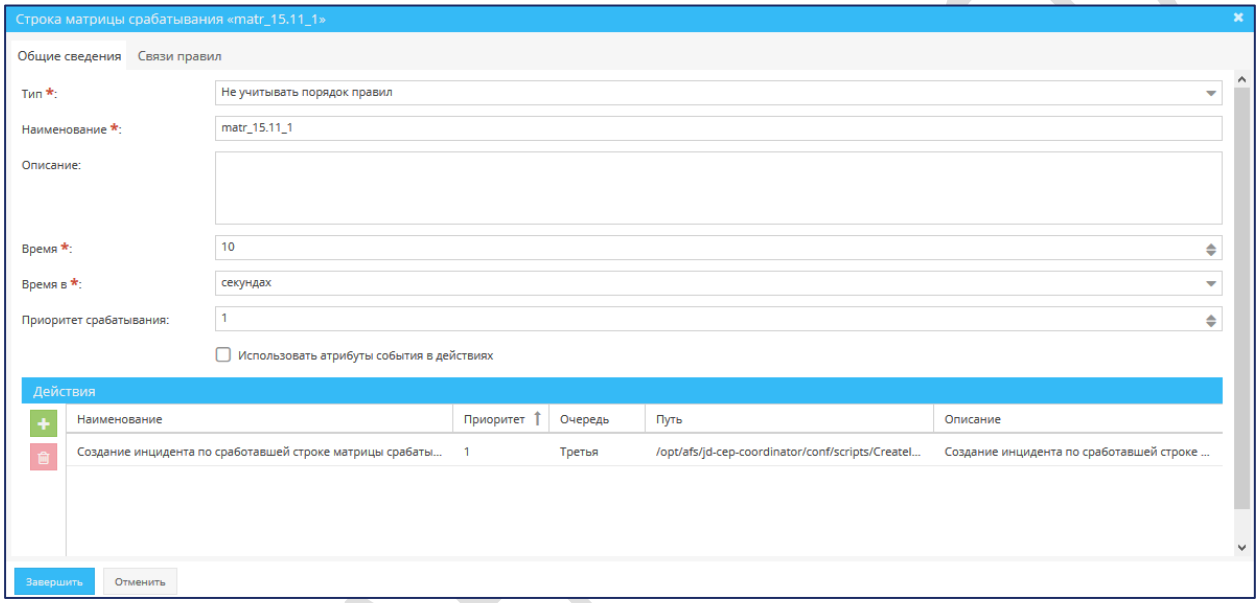


РИС. 2 – Окно **Строка матрицы срабатывания**

ТАБЛ. 2 – Поля строк в матрице срабатывания

Поле	Описание
Тип	Выбор из трех значений: ▪ Учитывать порядок правил ▪ Не учитывать порядок правил ▪ Использовать скоринг при обнаружении фрода
Граничный скор	Поле появляется, только если в параметре **Тип** выбрано значение **Использовать скоринг при обнаружении фрода**. Введите число от 1 до 9999
Наименование	Название строки
Описание	Описание строки
Время **Время в**	Укажите интервал времени и единицы измерения этого интервала (секунды, минуты, часы, дни). Указанный интервал – это тот промежуток времени, в течение которого матрица будет ожидать выполнение всех условий срабатывания с того момента, как появилось событие, которое вызвало срабатывание матрицы

Поле	Описание
Приоритет срабатывания	Укажите приоритет срабатывания матрицы. Если по одному событию сработало несколько матриц срабатывания одной политики, то сработавшей будет считаться матрица с наименьшим приоритетом. Если у сработавших строк одинаковый приоритет, то обе строки считаются сработавшими. Действия, заданные на сработавших матрицах, выполняются все (никакая дедубликация не выполняется)

7.1.3.2 Создание политики

Чтобы создать политику выявления:

1) Выберите пункт меню **Лаборатория – Инструменты анализа – Политики**.
2) На вкладке **Политики** нажмите кнопку **Добавить**  .

Экранная форма политики откроется на отдельной вкладке (Рисунок 149).

3) Укажите свойства политики (Таблица 55).
4) В поле **Правила** укажите все правила выявления, которые следует включить в политику – выберите их наименования в раскрывающемся списке.
5) Настройте действия, которые будут выполняться в случае срабатывания политики (см. раздел 7.1.3.4).
6) Настройте матрицу срабатывания.
7) Нажмите кнопку **Сохранить**.

Политика выявления начнет применяться к входящему потоку данных после её запуска (см. раздел 7.1.3.3).

7.1.3.3 Запуск политики

Политика выявления начнёт применяться к входящему потоку данных после её запуска.

Чтобы запустить политику выявления на выполнение:

1) Выберите пункт меню **Лаборатория – Инструмент анализа – Политики**.
2) Выберите в списке запись политики, которую необходимо запустить (статус записи должен быть CREATED или HOLD, или UNDEPLOYED).
3) На вкладке **Политики** нажмите кнопку **Запустить**  .
4) Значение статуса политики поменяется на DEPLOYED.

7.1.3.4 Выполнение действий по результату работы политики

Действия в политиках выявления используются в двух местах:

- Список действий, который указывается на строке матрицы, – это действия, которые должны выполниться при срабатывании строки матрицы;
- Список действий на политике (когда установлен флаг «Генерировать событие при отсутствии фрода») – действия, которые должны выполниться, если событие не попало ни под одно из условий строк матрицы срабатывания.

Форма настройки действий в двух этих списках одинаковая (Рисунок 150).

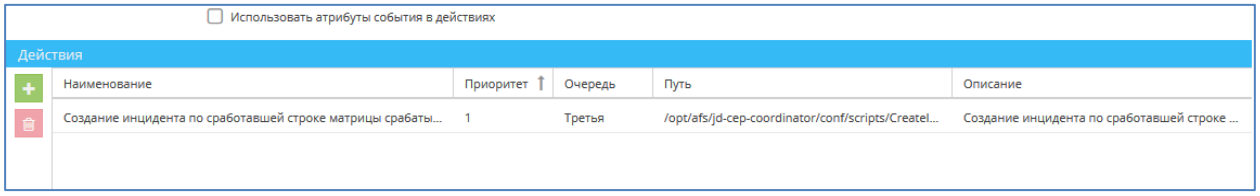


Рисунок 150 – Таблица настройки действий на политиках выполнения и на строках матриц срабатывания

Для настройки списка автоматически выполняемых системой действий:

1) В разделе **Действия** нажмите кнопку **Добавить** .

2) В добавившейся строке:

- Выберите действие в раскрывающемся списке в строке **Наименование**. Список доступных действий формируется в разделе **Действия (**см. раздел 6.9.2).
- Установите приоритет действия и очередь, в которой будет добавлено действие. Действия добавляются в очереди согласно указанному приоритету (значения приоритета от меньшего к большему).

Очереди имеют следующие различия по логике работы:

- **первая** и **вторая** очередь являются многопоточными. В них действия выполняются в несколько одновременных потоков.
- **третья** очередь является однопоточной. Эта очередь должна использоваться для действия **Создание инцидента по сработавшей строке матрицы срабатывания**.

Примечание:

- Отдельные очереди необходимы для того, чтобы действия, для которых критична скорость выполнения (например, действие ответа внешней системе), могли добавляться в одну очередь – отдельно от действий, выполнение которых может занять некоторое время (например, действие создания инцидента).
- Если действие по созданию инцидента будет использовать первую или вторую очередь, то может возникнуть ситуация, когда в силу многопоточности выполнения действий будет создан не один инцидент, а несколько (например, когда одно событие привело к срабатыванию двух строк матрицы с одинаковым приоритетом)

3) Установите флаг «Использовать атрибуты события в действиях», если в скриптах действий, выбранных в таблице **Действия,** необходимо использовать атрибуты события, которое привело к срабатыванию этого действия.

4) Сохранение списка действий происходит в момент сохранения всей политики.

При выполнении действие может возвращать значение true или false. Если по результатам своей работы действие возвращает значение false, то все последующие действия, которые стоят в той же очереди, выполняться не будут. При этом не будут выполняться только те действия, которые относятся к той же политике/строке матрицы и тому же событию, которые были связаны с действием, вернувшим false.

7.1.3.5 Настройка для одного ответа внешней системе от нескольких политик

Чтобы по одному событию во внешнюю систему уходил один ответ, основанный на решениях по нескольким политикам необходимо:

1) Во всех настроенных политиках, где анализируется нужный тип события, в действия на матрице срабатывания добавьте действие «Фрод ответ для другой политики». Это действие будет:

- дополнять параметры события атрибутом, который зафиксирует результат, что по событию было срабатывание политики;
- ставить событие в очередь, которую будет «слушать» верхнеуровневая политика, реализующая ответ внешней системе.

2) Во всех настроенных политиках, где анализируется нужный тип события, в действия при флаге **Генерировать ответ при отсутствии фрода** добавьте действие «Ответ об отсутствии фрода для другой политики». Это действие будет:

- дополнять параметры события атрибутом, который зафиксирует, что по событию не было срабатывание политики;
- ставить событие в очередь, которую будет «слушать» верхнеуровневая политика, реализующая ответ внешней системе.

3) Настройте правило выявления (см. раздел 7.1.2), которое анализирует нужный тип события, а внутри условия анализирует атрибуты, заполненные в пунктах 1 и 2, для получения необходимого результата для ответа.

4) Настройте вернеуровневую политику, которая формирует итоговый ответ по событию во внешнюю систему, со следующими обязательными настройками:

- Использование правила из пункта 3.
- Установка флаг «Включить внутренний таймер».
- В действиях матрицы срабатывания выбрано действие с ответом внешней системе.

7.1.3.6 Остановка политики

Администратор может прекратить применение политики к входящему потоку данных.

Для этого:

1) Выберите пункт меню **Лаборатория – Инструмент анализа – Политики**.
2) Выберите в списке запись политики, которую необходимо остановить (статус записи должен быть HOLD или DEPLOYED).
3) На вкладке **Политики** нажмите кнопку **Остановить**  .

Значение статуса политики поменяется на UNDEPLOYED.

7.1.3.7 Приостановка политики

Чтобы приостановить выполнение политики, но при этом не потерять состояние ее выполнения (промежуточные агрегативные расчеты, значения окон отслеживания в рамках матриц срабатывания):

1) Выберите пункт меню **Лаборатория – Инструмент анализа – Политики**.
2) Выберите в списке запись политики, которую необходимо остановить (статус записи должен быть DEPLOYED).

3) На вкладке **Политики** нажмите кнопку **Пауза**  .

4) Значение статуса политики поменяется на PAUSE.

7.2 РАСЧЕТ АГРЕГАТОВ

7.2.1 Общие сведения

В Jet Detective реализован **Модуль Агрегатов**, который позволяет рассчитывать агрегированные значения на больших объемах данных за большие промежутки времени, а также рассчитывать значение агрегата на базе анализа разных типов событий.

Модуль предоставляет инструмент настройки параметров расчета агрегатов для разных событий Jet Detective. При настройке параметров расчета задаются ключи связи между событиями и период времени анализа. Также задаются типы агрегата, которые необходимо рассчитывать (сумма, среднее, количество и т. пр.).

Модуль Агрегатов позволяет настроить расписания запусков расчета агрегатов – таким образом расчет может выполнятся в то время, когда нагрузка на Jet Detective минимальна.

Для управления параметрами расчетов агрегата в Jet Detective предусмотрен объект **Управление агрегатами**.

Результаты каждого расчета агрегата сохраняются в объекте **Фабрике данных** с типом **Агрегат** (см. раздел 6.2.1), который предварительно создан и связан с соответствующим **Управлением агрегата**. Результаты расчета, сохраненные в объекте **Агрегат**, используются в правилах выявления, если тип выражения равен «Агрегат OFFLINE».

7.2.2 Просмотр управления агрегатом

Чтобы посмотреть запись в справочнике управлений агрегатами:

1) Выберите пункт меню **Настройки** – **Прочее** – **Управление агрегатами**.

В рабочей области отобразится одна или несколько вкладок:

- перечень управлений агрегатами (Рисунок 151);
- экранных форм управлений агрегатами, открытых в этой сессии;
- перечень истории расчета (см. раздел 7.2.8), открытый в этой сессии.

В перечне управлений агрегата (Рисунок 151) в столбце **Статус** отображается статус каждой записи. Описание значения каждого статуса описано в таблице 56.

Таблица 56 – Возможные статусы записей справочника Управление агрегатами

Статус	Описание
READY	Управление агрегатом создано/изменено. Никакие вычисления по агрегату не ведутся. Управление агрегатом готово к запуску расчета
DEPLOYED	Управление агрегатом настроено и запущено для расчета. Т. е. по нему ведутся вычисления согласно настройкам и заданному режиму запуска. Переход в этот статус выполняется из статуса READY при нажатии кнопки **Запустить**
CALCULATION	Статус доступен только для управления агрегатом в режиме запуска **Расписание**. Устанавливается для управления агрегатом в тот момент, когда непосредственно выполняется расчет по агрегату. В этот статус может перейти только агрегат из статуса

Статус	Описание
	DEPLOYED. После завершения расчета управление агрегата возвращается в статус DEPLOYED

1) На вкладке с перечнем дважды щёлкните по строке записи управления агрегатами.

Экранная форма управления агрегатами отобразится на отдельной вкладке (Рисунок 152).

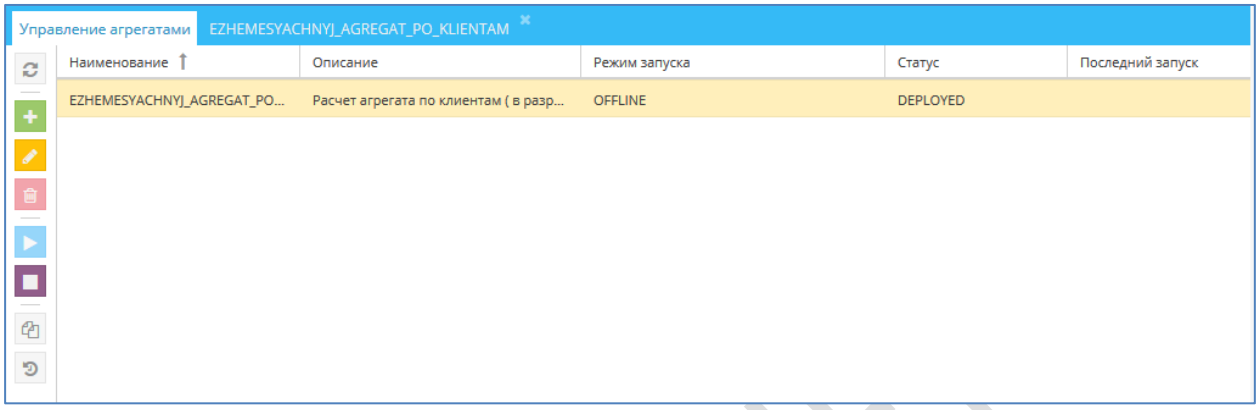


Рисунок 151 – Форма списка управлений агрегатами

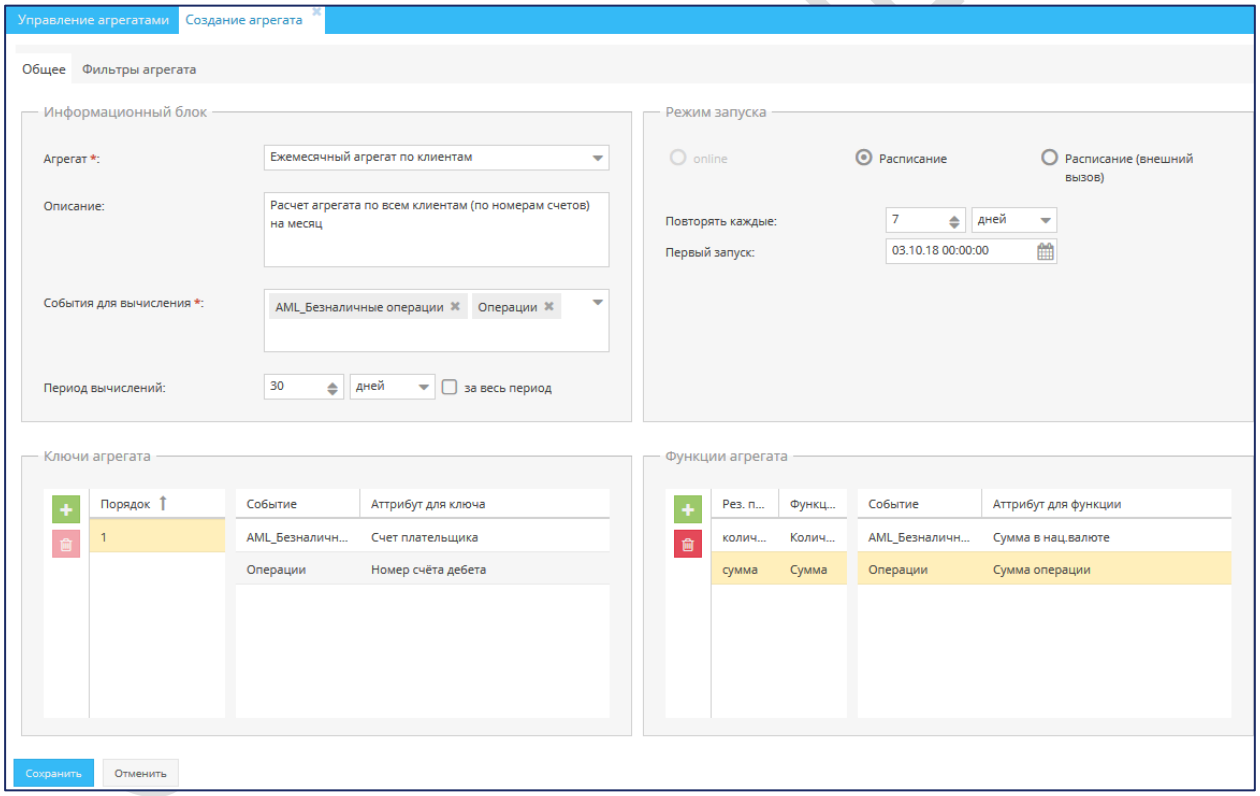


Рисунок 152 – Форма управления агрегатом

7.2.3 Добавление управления агрегатом

Чтобы добавить управление агрегатом:

1) Убедитесь, что в **Фабрике данных** создан объект с типом **Агрегат** (см. раздел 6.2.1), в который будут сохраняться результаты расчета.

2) Откройте справочник **Управление агрегатами** (см. раздел 7.2.2).

3) Нажмите кнопку **Добавить**  (Рисунок 151).

Откроется вкладка **Создание агрегата** (Рисунок 153).

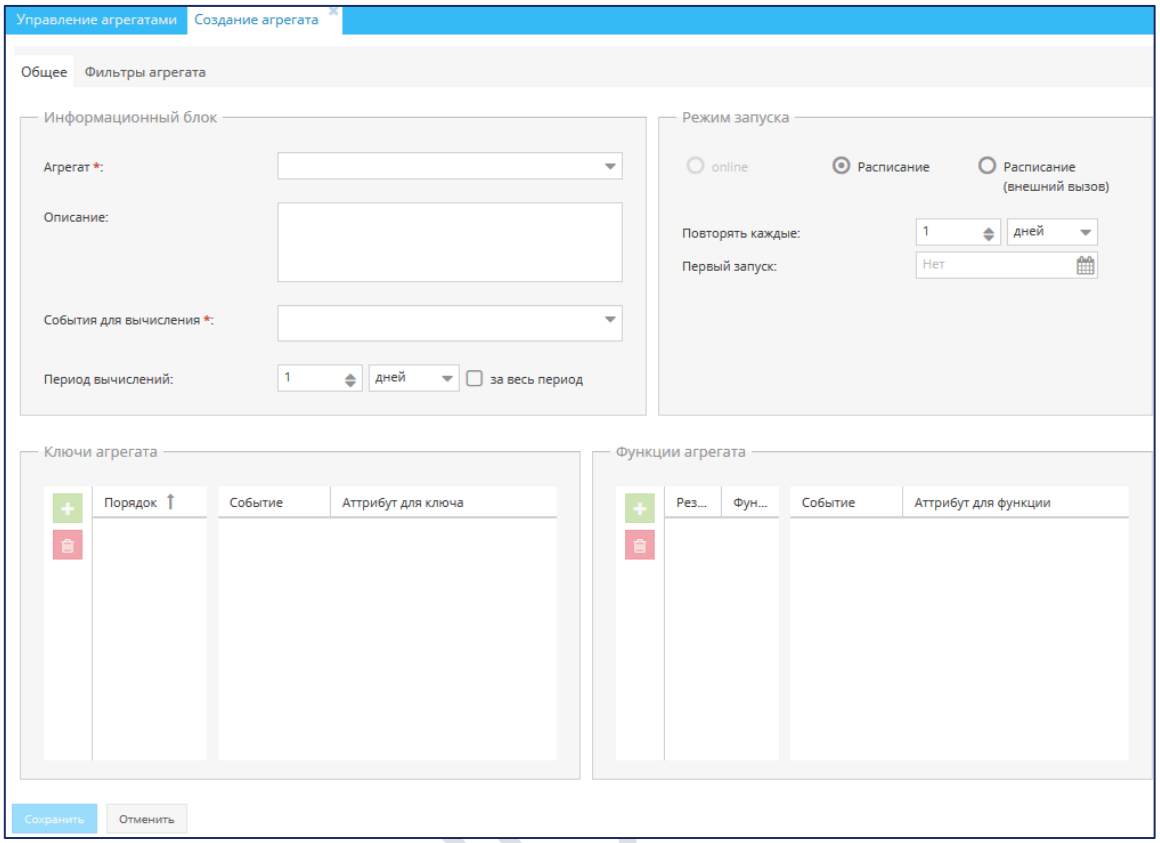


Рисунок 153 – Форма **Создание агрегата**

4) Заполните поля вкладки.

5) Вкладка **Создание агрегата** состоит из двух вкладок второго уровня: **Общее** и **Фильтры агрегата.**

Вкладка **Общее** состоит из четырех блоков:

- ***Информационный блок*** – содержит общую информацию об агрегате (Таблица 57): объект, в котором следует сохранять параметры расчёта; типы события, которые учитываются при расчете; период, за который проводится расчет.
- ***Режим запуска*** – содержит информацию о режиме запуска агрегата (Таблица 58).
- ***Ключи агрегата*** – содержит информацию о том, по каким атрибутам необходимо агрегировать данные событий, выбранных в параметре **События для вычисления** в блоке **Информационный блок** (Таблица 59).

Выбранные в этом блоке атрибуты объектов в момент расчета складываются в уникальный ключ в указанном порядке – для каждого типа событий. По этому ключу выполняется агрегирование данных при расчете агрегата и поиск данных при работе правил выявления.

С помощью кнопок **Добавить**  и **Удалить**  и указав значения атрибутов событий для каждого ключа, можно составить необходимый набор ключа для агрегата.

- ***Функции агрегата*** – содержит информацию о том, какие функции должен рассчитывать агрегат, в какие атрибуты объекта (параметр **Агрегат** блока **Информационный блок**) их необходимо сохранять и какие атрибуты событий (параметр **События для вычисления** блока **Информационный блок**) необходимо использовать при расчете этих значений (Таблица 60).

С помощью кнопок добавить  и удалить  можно составить необходимый набор функций, которые должен рассчитывать агрегат.

Таблица 57 – Описание элементов интерфейса **Информационного блока** вкладки **Общее** при создании управления агрегатом

Элемент интерфейса	Описание элемента интерфейса и его применения
Поле **Агрегат**	Раскрывающийся список с объектами с типом **Агрегат** из **Фабрики данных** Jet Detective. В списке отображаются только те объекты, которые хотя бы один раз применялись. Выберите один объект, в который будут сохраняться результаты расчета агрегата. С одним объектом типа **Агрегат** может быть связано только одно **Управление агрегатом**
Поле **Описание**	Текстовое поле для детального описания расчета агрегата
Поле **Событие для вычисления**	Раскрывающийся список с объектами типа **Событие** из **Фабрики данных** Jet Detective. В списке отображаются только те объекты, которые хотя бы один раз применялись. В этом параметре выберите те объекты, которые должны участвовать в процессе расчета агрегата. Доступен множественный выбор
Поля **Период вычисления**	Укажите период, за который будет рассчитываться агрегат, и единицу измерения этого периода (дни, часы, минуты, секунды)
Флаг **за весь период**	Если **флаг установлен**, то в расчет агрегата будут попадать все события без учета даты возникновения события. Если **флаг снят**, то события будут отбираться за период, указанный в параметре **Период вычисления**

Таблица 58 – Описание элементов интерфейса блока **Режим запуска** вкладки **Общее** при создании управления агрегатом

Элемент интерфейса	Описание элемента интерфейса и его применения
Переключатель **Online**	Переключатель всегда снят и недоступен для изменения
Переключатель **Расписание**	Если **переключатель установлен**, то доступны поля **Повторять каждый** и **Первый запуск** Если **переключатель снят**, то установлен переключатель **Расписание «Внешний вызов»**
Переключатель **Расписание «Внешний вызов»**	Если **переключатель установлен**, то Jet Detective ожидает, что объект, выбранный в параметре **Агрегат Информационного блока**, будет наполнятся с помощью внешнего вызова. В этом случае создание управления агрегатом необходимо для дальнейшего корректного использования загруженных значений агрегата при настройке и работе правил выявления. Если **переключатель снят**, то установлен переключатель **Расписание**
Поля **Повторять каждый**	Укажите периодичность, с которой будет запускаться расчет агрегата по расписанию, и единицу измерения этого периода (дни, часы, минуты, секунды)
Поле **Первый запуск**	Укажите дату и время, с которого должен начаться расчет. Нельзя выбрать дату и время меньше, чем момент сохранения управления агрегата. Если параметр **Первый запуск** оставить незаполненным, то расчет агрегата начнется в момент нажатия кнопки «Запустить»

Таблица 59 – Описание элементов интерфейса блока **Ключи агрегата** вкладки **Общее** при создании управления агрегатом

№	Элемент интерфейса	Описание элемента интерфейса и его применения
1.	Таблица **Порядок**	В таблице отображается порядковый номер добавленного ключа связи. Выберите строку с добавленным значением
2.	Таблица **Событие/Атрибут для ключа**	Если в таблице **Порядок** выбрано значение, то в таблице **Событие/Атрибут для ключа** автоматически отобразится соответствующий набор событий, которые выбраны в параметре **События для вычисления** в **Информационном блоке**
2.1.	Столбец **Событие**	Список событий – недоступен для редактирования. Отображает тот набор событий, которые выбраны в параметре **События для вычисления** в **Информационном блоке**
2.2.	Столбец **Атрибут для ключа**	Для каждого значения ключа должны быть заполнены все **Атрибуты для ключа** – для всех значений в столбце **Событие**. Применение: 1) Для каждого значения в столбце **События** выберите в раскрывающемся списке атрибут, который будет использоваться как часть ключа для агрегата. 2) Откройте раскрывающийся список двойным щелчком по строке в столбце **Атрибут для ключа** возле соответствующего события. Обратите внимание, что для одного значения ключа, атрибуты объектов должны совпадать по значениям. Например: если в качестве ключа используются номер счета и ИНН, то в первом ключе для всех событий должны быть выбраны атрибуты, которые содержат значение номера счета, а во второй ключе – атрибуты, которые содержат значение ИНН

Таблица 60 – Описание элементов интерфейса блока **Функции агрегата** вкладки **Общее** при создании управления агрегатом

№	Элемент интерфейса	Описание элемента интерфейса и его применения
1.	Таблица с функциями	Табличный список добавленных функций. Выберите строку с добавленным значением
1.1.	Столбец **Рез.поле**	Результирующие поле. Применение: 1) Откройте раскрывающийся список двойным щелчком по строке в столбце **Рез.поле** возле соответствующей функции. В раскрывающемся списке содержатся атрибуты объекта **Агрегат**, который выбран в **Информационном блоке**. 2) Для каждой функции выберите атрибут, в который будет сохраняться рассчитанное значение этой функции
1.2.	Столбец **Функция**	Применение: 1) Откройте раскрывающийся список двойным щелчком по строке в столбце **Функция**. 2) Выберите одну из следующих функций: ▪ **Сумма**; ▪ **Максимум**; ▪ **Минимум**; ▪ **Среднее**; ▪ **Количество**

№	Элемент интерфейса	Описание элемента интерфейса и его применения
2.	Таблица **Событие /Атрибут для функции**	Если в таблице функций выбрано значение, то в таблице **Событие /Атрибут для функции** автоматически отобразится соответствующий набор событий, которые выбраны в параметре **События для вычисления** в **Информационном блоке**
2.1.	Столбец **Событие**	Список событий – недоступен для редактирования. Отображает тот набор событий, которые выбраны в параметре **События для вычисления** в **Информационном блоке**
2.2.	Столбец **Атрибут для функции**	Для каждого значения функции должны быть заполнены все **Атрибуты для функции** – для всех значений в столбце **Событие.** Для каждого значения в столбце **События** выберите в раскрывающемся списке атрибут, который будет использоваться для расчета агрегата. Обратите внимание, что если выбрана функция **Количество**, то **Атрибут для функции** указывать не нужно – он автоматически заполнится значением «*»

6) Перейдите на вкладку **Фильтры агрегата** (Рисунок 154).

7) Если для расчета агрегата нужно использовать не все экземпляры событий, которые выбраны в параметре **События для вычисления** в **Информационном блоке**, а отбирать их по какой-то определённой логике, то настройте эту логику на вкладке **Фильтры агрегата** (Таблица 61).

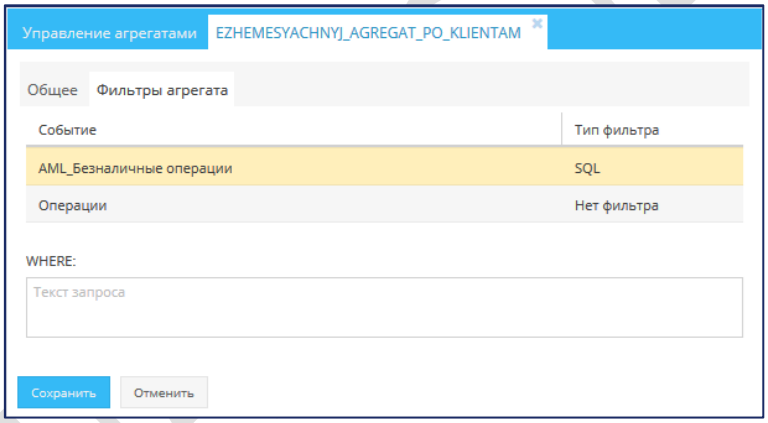


Рисунок 154 – Вид вкладки **Фильтры** агрегата на форме создания агрегата

Таблица 61– Описание элементов интерфейса вкладки **Фильтры агрегата** при создании управления агрегатом

№	Элемент интерфейса	Описание элемента интерфейса и его применения
1.	Таблица фильтров	Табличный список доступных фильтров экземпляров событий
1.1.	Столбец **Событие**	Список событий – недоступен для редактирования. Отображает тот набор событий, которые выбраны в параметре **События для вычисления** в **Информационном блоке**
1.2.	Столбец **Тип фильтра**	Применение: 1) Откройте раскрывающийся список двойным щелчком по строке в столбце **Тип фильтра**. 2) Поменяйте значение **Нет фильтра** на **SQL**
2.	Поле **WHERE:**	Это поле отображается, если в столбце **Тип фильтра** указано значение **SQL**. Введите условие фильтрации событий в виде SQL-запроса. *Примечание:* в запросах используются имена полей объектов, а не атрибутов

8) Нажмите кнопку **Сохранить**.

7.2.4 Редактирование управления агрегатом

Редактирование **Управления агрегатом** доступно только для записей в статусе READY (см. раздел 7.2.2).

Для этого:

1) Откройте управление агрегатом (см. раздел 7.2.2).
2) Внесите изменения в поля управления агрегатом (см. раздел 7.2.3).
3) Нажмите кнопку **Сохранить**.

> *Примечание*. раздел **Режим запуска** недоступен для изменений до тех пор, пока есть связанные с управлением агрегата слепки расчета.

7.2.5 Удаление управления агрегатом

Можно удалить управление агрегатом в статусе READY.

Для этого:

1) Откройте список управлений агрегатами (см. раздел 7.2.2).
2) Выберите строку объекта выполнения.
3) Нажмите кнопку **Удалить**  .
4) В появившемся модальном окне нажмите кнопку:

- **Да** – если хотите удалить управление агрегатом и все результаты расчета, которые были созданы при его выполнении в объекте **Агрегат**;
- **Нет** – если хотите удалить управление агрегатом, но сохранить все результаты расчета, которые были созданы при его выполнении в объекте **Агрегат**.

7.2.6 Запуск расчета агрегата

Чтобы расчет агрегата выполнялся по созданным настройкам в управлении агрегатом необходимо запустить этот расчета. Для этого:

1) Откройте список управлений агрегатами (см. раздел 7.2.2).
2) Выберите строку объекта выполнения.
3) Нажмите кнопку **Запустить**  – доступна только при выборе записи в статусе READY.

Агрегат будет расчитан в дату первого запуска.

Дата первого запуска – дата, начиная с которой отсчитывается период, указанный в параметре **Период вычислений.** Полученный диапазон служит фильтром для отбора событий, указанных в параметре **События для вычислений**.

События, которые будут участвовать в расчете агрегата, должны попадать в этот диапазон по дате возникновения этих событий в Jet Detective (атрибут **event_date**).

Дата первого запуска может быть определена после нажатия кнопки **Запустить**. Логика определения этой даты зависит от наличия уже рассчитанных слепков[2] в истории расчета и от наличия даты в настройке агрегата в параметре **Первый запуск**. При первом запуске может быть рассчитан один слепок или несколько.

Логика определения даты первого запуска заключается в следующем:

1) Если в **Истории расчетов** (см. раздел 7.2.8) есть записи (т. е. по выбранному управлению агрегатом уже выполнялись вычисления и хранятся рассчитанные значения), то Jet Detective проигнорирует дату, указанную в параметре **Первый запуск,** и проведет расчет всех недостающих слепков, начиная с последнего найденного. Расчет выполняется по той же логике, что и **Расчет за прошлые периоды см. раздел** 7.2.9), где:

   - Дата начала расчета – дата **Начала периода актуальности** ближайшего к текущей дате слепка.
   - Дата конца расчета – дата нажатия на кнопку **Запустить**.

В этом случае расчет начнется в момент нажатия кнопки **Запустить**.

2) Если в **Истории расчетов** (см. раздел 7.2.8) нет ни одной записи (т. е. нет рассчитанных значений, связанных с выбранным управлением агрегата), выполняется проверка на наличие даты в параметре **Первый запуск** блока **Режим запуска** (см. раздел 7.2.3):

   а) Если дата в параметре **Первый запуск** не указана, то датой запуска считается момент нажатия кнопки **Запустить.** В параметре **Первый запуск** будет указана эта дата.

   б) Если дата в параметре **Первый запуск** больше или равна дате нажатия кнопки **Запустить,** то расчет начнется в указанные дату и время.

   в) Если дата в параметре **Первый запуск** меньше даты нажатия кнопки **Запустить,** то расчет подчиняется правилам расчета за прошлые периоды и начнется в момент нажатия кнопки **Запустить.** При этом:

      - Дата начала расчета – дата в параметре **Первый запуск**;
      - Дата конца расчета – дата нажатия кнопки **Запустить**.

7.2.7 Остановка расчета агрегата

Чтобы остановить расчет агрегата:

1) Откройте список управлений агрегатами (см. раздел 7.2.2).
2) Выберите строку объекта выполнения.
3) Нажмите кнопку **Остановить**  . Кнопка доступна только при выборе записи в статусе DEPLOYED или CALCULATION.

7.2.8 Просмотр истории расчета

По результатам каждого расчета агрегата для управления агрегатом создается запись в истории расчета – слепок расчетов.

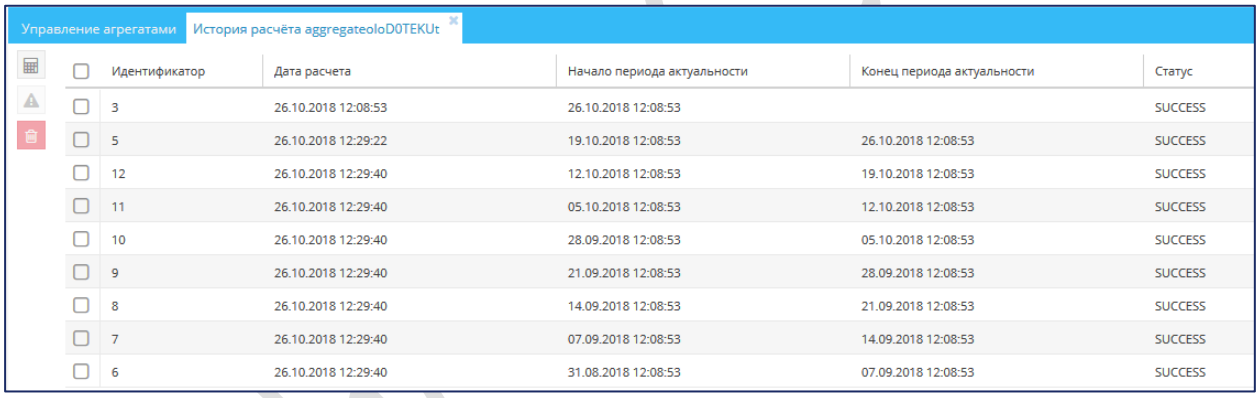
Каждая запись в истории расчета:

- имеет связь со всеми результатами расчета, которые были получены и сохранены в объекте, который указан в параметре **Агрегат** в **Информационном блоке** (атрибут **Идентификатор истории расчета**);
- имеет границы периода актуальности, которые не могут пересекаться для одного управления агрегатом.

Период актуальности слепка в истории расчета – это тот диапазон, в который рассчитанные значения, связанные со слепком, являются актуальными для использования в правилах выявления.

Чтобы посмотреть существующие слепки, связанные с управлением агрегатом:

1) Откройте список управлений агрегатами (см. раздел 7.2.2).
2) Выберите строку управления агрегатом.
3) Нажмите кнопку **История расчета** .
4) В рабочей области вкладки **Управления агрегатами** откроется новая вкладка с перечнем слепков расчета (Рисунок 155).



Идентификатор	Дата расчета	Начало периода актуальности	Конец периода актуальности	Статус
3	26.10.2018 12:08:53	26.10.2018 12:08:53		SUCCESS
5	26.10.2018 12:29:22	19.10.2018 12:08:53	26.10.2018 12:08:53	SUCCESS
12	26.10.2018 12:29:40	12.10.2018 12:08:53	19.10.2018 12:08:53	SUCCESS
11	26.10.2018 12:29:40	05.10.2018 12:08:53	12.10.2018 12:08:53	SUCCESS
10	26.10.2018 12:29:40	28.09.2018 12:08:53	05.10.2018 12:08:53	SUCCESS
9	26.10.2018 12:29:40	21.09.2018 12:08:53	28.09.2018 12:08:53	SUCCESS
8	26.10.2018 12:29:40	14.09.2018 12:08:53	21.09.2018 12:08:53	SUCCESS
7	26.10.2018 12:29:40	07.09.2018 12:08:53	14.09.2018 12:08:53	SUCCESS
6	26.10.2018 12:29:40	31.08.2018 12:08:53	07.09.2018 12:08:53	SUCCESS

Рисунок 155 – Перечень слепков расчета в **Истории расчета**

В **Истории расчета агрегата** (Рисунок 155) в столбце **Статус** отображается статус каждого слепка расчета. Описание значения каждого статуса приведено в таблице 62.

Таблица 62– Возможные статусы слепков **Истории расчета агрегата**

Статус	Описание
CALCULATING	Для выбранного слепка выполняются вычисления. В правилах выявления такой слепок не участвует, т. к. для него еще нет рассчитанных значений
SUCCESS	Вычисления для слепка завершены успешно. Результаты расчета сохранены в объекте, который указан в параметре **Агрегата** в **Информационном блоке.** Результаты связанные с этим слепком, участвуют в правилах выявления
ERROR	Вычисления результатов завершились ошибкой. В объекте, который указан в параметре **Агрегата** в **Информационном блоке**, нет значений, связанных с таким слепком. В правилах выявления слепки с таким статусом не учитываются

7.2.9 Расчет агрегата за прошедшие периоды

Чтобы получить рассчитанные значения агрегата, которые будут актуальны для событий с прошедшей датой возникновения:

1) Откройте список историй расчета (см. раздел 7.2.8).

2) Нажмите кнопку **Расчёт** 

Откроется модальное окно, для выбора диапазона расчета (Рисунок 156).

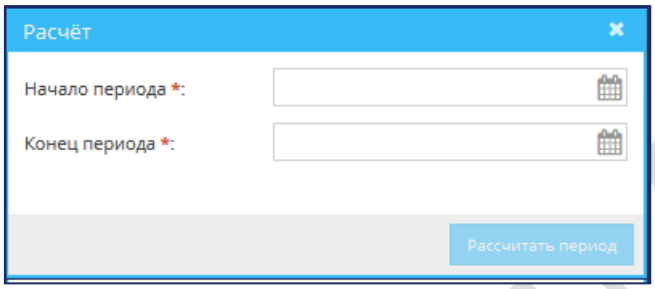


Рисунок 156 – Форма для выбора диапазона расчета слепков агрегата за прошлый период

3) Укажите начало и конец периода вычислений – заполните поля **Начало периода** и **Конец периода**.

4) Нажмите кнопку **Рассчитать период**.

Расчет начнется сразу после нажатия этой кнопки**.**

Расчет слепков за прошедший период Jet Detective выполняет исходя из указанных пользователем границ расчета и с учетом уже существующих слепков расчета.

Так как слепки не могут пересекаться по периодам актуальности, но при этом должны иметь одинаковую длину периода, то для выполнения этого условия Jet Detective скорректирует указанные пользователем даты расчета для прошедшего периода.

Сокращения, используемые в описании алгоритма расчета:

- **from** – дата начала периода расчета;
- **to** – дата окончания периода расчета;
- **ОД** – *опорная дата* – техническая величина, необходимая для процедуры калибровки дат и выполнения условия актуальности слепков;
- **P** – период актуальности слепков. Равен периоду запуска, указанному в блоке **Режима запуска** управления агрегатом.

Алгоритм расчета слепков за прошедший период:

1) Определяется **ОД** для калибровки периода расчета. Для этого проверяется наличие слепков в истории расчёта (без учёта статуса слепка):

- Нет – проверяется наличие даты в параметре **Первый запуск** (блок **Режим запуска** управления агрегатом):
  - Да – **ОД** равна дате в параметре **Первый запуск**;
  - Нет – **ОД** равна **from**.
- Есть – **ОД** равна дате **date_from** любого рассчитанного слепка.

2) Калибровка начала периода расчета, относительно существующих слепков.

Цель калибровки – сдвинуть дату **from** влево по временно́й шкале. Дата сдвигается до тех пор, пока между **from** и существующими слепками не будет помещаться целое число периодов актуальности.

- Если **ОД**=**from**, то калибровка не требуется.
- Если **ОД≠from**, то дата **from** сдвигается влево по временно́й шкале на недостающий промежуток времени до тех пор, пока количество периодов актуальности между новой датой и существующими слепками не будет равно целому числу.

3) Запускается процесс создания и расчета слепков агрегата – последовательно, начиная от даты ОД. При этом:
   а) Дата начала периода актуальности слепка = **ОД**.
   б) Дата окончания периода актуальности слепка = **ОД** + **P.**
   в) Каждый следующий слепок сдвигается вправо по временно́й шкале на **P** относительно предыдущего слепка:
      - Если в процессе расчета Jet Detective встречает уже рассчитанный слепок в статусе SUCCESS, то такой слепок пропускается и расчет идет дальше.
      - Если в процессе расчета Jet Detective встречает уже рассчитанный слепок в статусе ERROR, то такой слепок пересчитывается.

4) Процесс расчета завершается в тот момент, когда **Дата окончания периода актуальности** слепка будет больше даты **to**, заданной пользователем при указании периода (см. раздел 7.2.9). Слепок с такой датой будет последним рассчитанным в рамках процедуры расчета за прошедший период.

7.2.10 Пересчет отдельных слепков

Для пересчета отдельных слепков расчета агрегата в **Истории расчета**:

1) Откройте список историй расчета (см. раздел 7.2.8).
2) Выберите в списке один или несколько слепков в статусе ERROR.
3) Нажмите кнопку **Пересчёт** 

СПИСОК СОКРАЩЕНИЙ

ETL	Extract, Transform, Load – процессы обработки данных
БД	База данных
СУБД	Система управления базами данных

ГЛОССАРИЙ

Термин	Описание
Business Object Model (модель бизнес-объектов)	Совокупность сущностей Jet Detective, отображающая их атрибуты и связи
ETL-система	(от англ. Extract, Transform, Load) – система, предназначенная для организации процессов переноса данных из систем-источников в системы-потребители с выполнением промежуточных трансформаций данных
Агрегат	Данные, агрегируемые в Jet Detective на основе данных поступающих событий. Например, можно создать агрегат по платежам, в котором будут храниться максимальные, минимальные и средние значения платежей того или иного вида
Агрегация данных	Процесс вычисления обобщенных показателей массива данных: суммирование, вычисление среднего (максимального, минимального, медианного) значений и т. п. Является разновидностью обогащения данных
Аномалия	Выявленные в потоке данных нарушения, отклонения от обычного поведения; состояния, выходящих за пороговые значения; подозрительные или мошеннические действия
Владение	Множество объединённых экземпляров объектов. Используется для управления правами доступа пользователей к конкретным записям в таблицах объектов: создание, чтение, редактирование или удаление записей в таблицах объектов, относящиеся к тому или иному владению
Действие	Служебная сущность, которая позволяет хранить доступные действия, которые может выполнить Jet Detective
Задание	ETL-активность, которая представляет собой рабочий процесс, состоящий из нескольких преобразований. Задание предназначено для запуска и координации хода выполнения трансформаций, обработки исключений, условных ветвлений, которые задают порядок выполнения
Запрет	Разрешение, которое напрямую запрещено использовать. Указывается для роли или Пользователя. набора прав доступа роли или пользователя
Индивидуальное разрешение	Разрешение, которое не входит в набор прав доступа роли или владения. Используется для увеличения набора прав доступа пользователя путем прямой установки для него какого-либо разрешения
Инцидент	Информационная запись Jet Detective, обладающая следующими свойствами: связана с событиями, в которых были выявлены аномалии; отображает информацию о сработавших политиках и правилах выявления; отображает информацию о статусе расследования и результатах процесса выявления и расследования
Конфигурация объекта	Совокупность всех свойств объекта, таких как: ▪ атрибуты объекта; ▪ поля объекта; ▪ дополнительные опции объекта; ▪ модель документооборота
Модель документооборота	Последовательность доступных для объекта переходов между статусами, где для каждого перехода можно задать набор выполняемых действий и логику определения ответственного лица для объекта после перехода
Обогащение данных	Процесс дополнения данных новой информацией, которая делает данные более полезными для дальнейшего использования. В частности, обогащение выполняется за счет данных из нескольких источников
Объект Jet Detective	Взаимосвязанные бизнес-сущности, такие как «клиенты», «платежи», «устройства», «действия» и любые другие
Объект поиска	Служебная сущность, которая определяет, какие атрибуты объекта используются в поиске
Очистка данных	Процесс повышения качества данных с помощью выявления и устранения ошибок и несоответствия данных

Термин	Описание
Переменная	Служебная сущность, которая позволяет хранить переменное значение и централизованно его изменять
Политика выявления	Набор *правил* для выявления определенного вида аномалии. Правила в политике могут относиться к разным событиям, что обеспечивает кросс-канальный анализ потоков, не связанных между собой событий, и позволяет выявлять цепочки событий
Правило	Набор проверяемых условий, которые при анализе применяются к данным экземпляра объекта Jet Detective
Преобразование	ETL-активность, которая представляет собой связанные между собой задачи – шаги преобразования. Данные, поступающие на вход процесса преобразования, пошагово обрабатываются: фильтруются, сортируются, агрегируются, объединяются, обогащаются. На выходе процесса появляются изменённые данные, которые можно сохранить в виде таких объектов, как: ▪ события; ▪ справочники; ▪ списки;
Разрешение	Право, которое предоставляется пользователю для доступа к тем или иным элементам интерфейса Jet Detective, её программным сервисам и объектам
Регулярное выражение	Служебная сущность для составления шаблонов поиска и шаблонов манипуляций с подстрокой. Для составления выражений используется структура регулярных выражений POSIX
Роль	Выделенная совокупность рабочих действий пользователя, которая в контексте управления доступом представляет собой набор разрешений, необходимых для выполнения этих действий
Связывание данных	Процесс поиска и установки связей между сущностями. Является разновидностью обогащения данных
Сервер обработки	Служебная сущность, позволяющая хранить сведения о серверах Jet Detective,которые используются для выполнения политик выявления
Событие	Информационная запись в Jet Detective, отображающая свойства события определенного вида, например: платеж, перемещение материальных средств, действие сотрудника в прикладной программной системе и т. п. Информация о событии поступает в Jet Detective из систем-источников
Справочник	Информационная запись в Jet Detective, данные которой используются для обогащения данных поступающих событий. Примеры: справочник клиентов, справочник счетов, справочник сотрудников
Шаблон отчета	Сущность, которая хранит параметры шаблона отчета, созданного в формате rtrp, а также входные параметры отчета и их характеристики.