

ИНФОСИСТЕМЫ
ДЖЕТ



ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «JET DETECTIVE»



РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

2017

АННОТАЦИЯ

В руководстве приведены сведения о назначении и функциональных возможностях программного обеспечения **Jet Detective**, а также описаны операции, которые выполняют пользователи при работе с **Jet Detective** и его настройке.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ	6
1.1 ОБЛАСТЬ ПРИМЕНЕНИЯ	6
1.2 КРАТКОЕ ОПИСАНИЕ ВОЗМОЖНОСТЕЙ	6
1.3 УРОВЕНЬ ПОДГОТОВКИ ПОЛЬЗОВАТЕЛЕЙ	7
2. НАЗНАЧЕНИЕ JET DETECTIVE	8
3. СТРУКТУРА JET DETECTIVE	9
3.1 ПЕРЕЧЕНЬ ФУНКЦИОНАЛЬНЫХ МОДУЛЕЙ.....	9
3.2 Модуль ФАБРИКА ДАННЫХ	9
3.3 Модуль АНАЛИЗ СОБЫТИЙ.....	10
3.4 Модуль МАШИННОЕ ОБУЧЕНИЕ.....	10
3.5 Модуль РАССЛЕДОВАНИЕ.....	11
3.6 Модуль РАБОЧИЙ СТОЛ	11
3.7 Модуль АВТОРИЗАЦИЯ	11
4. ПОДГОТОВКА К РАБОТЕ	12
4.1 ВХОД В JET DETECTIVE.....	12
4.2 ВЫХОД ИЗ JET DETECTIVE	12
4.3 ПОРЯДОК ПРОВЕРКИ РАБОТОСПОСОБНОСТИ	12
4.4 ОПИСАНИЕ ИНТЕРФЕЙСА ПОЛЬЗОВАТЕЛЯ.....	13
4.4.1 Окно веб-приложения.....	13
4.4.2 Типовые элементы управления	15
4.4.3 Индикация полей при вводе данных.....	16
4.4.4 Работа с табличными списками	17
4.4.5 Работа с иерархическими списками	18
4.4.6 Отказ от сохранения изменений	19
5. РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ.....	20
5.1 ОБЩИЕ СВЕДЕНИЯ.....	20
5.2 ПРОСМОТР СТАТИСТИКИ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ	20
5.2.1 Общее описание рабочего стола	20
5.2.2 Раздел Инциденты на расследовании.....	21
5.2.3 Раздел Инциденты за прошедший период	22
5.3 РАБОТА С ИНЦИДЕНТАМИ	23

5.3.1 Общие сведения	23
5.3.2 Просмотр записи инцидента	24
5.3.3 Расследование инцидента.....	28
5.4 РАБОТА С ПОЛЬЗОВАТЕЛЬСКИМИ ОБЪЕКТАМИ	30
5.4.1 Общие сведения	30
5.4.2 Просмотр записи объекта.....	31
5.4.3 Добавление записи объекта.....	32
5.4.4 Редактирование записи объекта.....	32
5.4.5 Удаление записи объекта	33
6. АДМИНИСТРИРОВАНИЕ JET DETECTIVE	34
6.1 НАСТРОЙКА МОДЕЛИ ДАННЫХ	34
6.1.1 Общие сведения	34
6.1.2 Просмотр объекта.....	35
6.1.3 Этапы создания объекта	36
6.1.4 Создание первичной конфигурации объекта	37
6.1.5 Настройка атрибутов объекта	39
6.1.6 Описание таблицы объекта	41
6.1.7 Настройка дополнительных опций объекта	45
6.1.8 Настройка использования атрибутов объекта в машинном обучении	47
6.1.9 Использование ETL-процессов	48
6.1.10 Создание таблицы объекта в БД. Подтверждение конфигурации объекта.....	51
6.1.11 Редактирование конфигурации объекта	51
6.2 МОДЕЛЬ РАСПРЕДЕЛЕНИЯ ПРАВ ДОСТУПА	51
6.2.1 Механизмы управления доступом	51
6.2.2 Разрешения	52
6.2.3 Инструменты для формирования наборов разрешений	53
6.2.4 Владения	54
6.3 НАСТРОЙКА МЕХАНИЗМОВ УПРАВЛЕНИЯ ДОСТУПОМ	58
6.3.1 Общие сведения	58
6.3.2 Дерево разрешений	58
6.3.3 Дерево владений.....	63
6.3.4 Дерево ролей.....	65
6.4 УПРАВЛЕНИЕ УЧЁТНЫМИ ЗАПИСЯМИ.....	70
6.4.1 Просмотр списка пользователей и учётной записи пользователя	70
6.4.2 Создание учётной записи пользователя	72

6.4.3	Порядок настройки прав доступа пользователя	73
6.4.4	Формирование набора разрешений пользователя.....	74
6.4.5	Формирование схемы владения пользователя	75
6.4.6	Редактирование учётной записи пользователя.....	78
6.4.7	Блокировка и разблокировка учётной записи пользователя	78
6.4.8	Удаление учётной записи пользователя	78
6.5	СЛУЖЕБНЫЕ СПРАВОЧНИКИ	79
6.5.1	Настройка списков.....	79
6.5.2	Настройка глобальных переменных.....	81
7.	НАСТРОЙКА МЕХАНИЗМОВ ВЫЯВЛЕНИЯ АНОМАЛИЙ	84
7.1	НАСТРОЙКА ПРАВИЛ ВЫЯВЛЕНИЯ АНОМАЛИЙ.....	84
7.1.1	Общие сведения	84
7.1.2	Настройка правил выявления.....	85
7.1.3	Настройка политик выявления.....	98
7.2	НАСТРОЙКА ИСПОЛЬЗОВАНИЯ И ОБУЧЕНИЕ МОДЕЛЕЙ ВЫЯВЛЕНИЯ.....	105
7.2.1	Общие сведения	105
7.2.2	Настройка обучающих выборок	105
7.2.3	Использования модели машинного обучения	105
7.3	ИСПЫТАНИЕ ПОЛИТИК ВЫЯВЛЕНИЯ.....	110
7.3.1	Общие сведения	110
7.3.2	Выполнение политик.....	110
7.3.3	Сравнение результатов выполнения политик	112
	ПРИЛОЖЕНИЕ А ПРИМЕРЫ СХЕМ ВЛАДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ	119

1. ОБЩИЕ СВЕДЕНИЯ

1.1 ОБЛАСТЬ ПРИМЕНЕНИЯ

Универсальное решение **Jet Detective** (далее – **Jet Detective**) разработано для применения в организациях и на предприятиях любых отраслей: банки, предприятия розничной торговли, промышленные предприятия и др.

Программное обеспечение **Jet Detective** предназначено для создания систем, автоматизирующих анализ и выявление аномалий в данных, поступающих в режиме реального времени из множества разнородных не связанных источников.

Автоматизированные системы на базе **Jet Detective** обеспечивают:

- минимизацию времени принятия человеком экспертного решения при расследовании выявленных аномалий;
- применение для обнаружения известных аномалий не только экспертных правил выявления, но и методов машинного обучения, с помощью которых можно прогнозировать новые виды аномалий;
- гибкость настройки и расширения модели данных;
- масштабируемость решения пропорционально увеличению количества источников и объемов поступающих данных, в том числе за счет применения технологий и инструментов больших 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, например, 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 основных категорий пользователей **Jet Detective** приведены в ТАБЛ. 1.

ТАБЛ. 1 – Требования к уровню подготовки пользователей

КАТЕГОРИЯ ПОЛЬЗОВАТЕЛЕЙ	ОСНОВНОЕ ДЕЙСТВИЕ	ТРЕБОВАНИЕ К УРОВНЮ ПОДГОТОВКИ
Расследователи	<ul style="list-style-type: none"> Расследование инцидентов (см. раздел 5) 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Настройка взаимодействия Jet Detective с внешними системами (выполняется с помощью программного обеспечения Pentaho Data Integration); настройка модели данных (см. раздел 6.1); управление учётными записями и правами доступа пользователей (см. разделы 6.2, 6.3, 6.4) 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Настройка экспертных правил выявления аномалий (см. раздел 7.1); настройка использования моделей машинного обучения в Jet Detective (см. раздел 7.2) 	<ul style="list-style-type: none"> Знание предметной области, в которой применяется Jet Detective, в части выявления аномалий; знание и опыт использования SQL-подобных языков запросов данных; знание и опыт разработки моделей машинного обучения

2. НАЗНАЧЕНИЕ JET DETECTIVE

В **Jet Detective** реализованы 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;
 - с нарушением бизнес-процессов и регламентов;
 - с отклонениями от обычного поведения участников бизнес-процессов;
 - с нарушениями работоспособности компонентов сложных систем;
 - с состояниями, выходящими за пороговые значения;
 - с обнаружением скомпрометированных сущностей.
- проведение пользователем расследования инцидентов, связанных с выявленными аномалиями, в том числе с использованием графических инструментов кросс-канального расследования и анализа связей, получение 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;**
- **Машинное обучение;**
- **Расследование инцидентов;**
- **Рабочий стол;**
- **Авторизация.**

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, обучающие выборки);
- интерфейсы пользователя для просмотра, поиска, анализа и манипулирования данными в виде форм, таблиц, графов, диаграмм;
- интерфейс пользователя 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: 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 и методы машинного обучения;
- 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, предназначенную для предоставления данных, используемых в анализе событий, и реализующую быстрый доступ и специальную стратегию обновления.

3.4 МОДУЛЬ МАШИННОЕ ОБУЧЕНИЕ

Модель выявления – это самосоздаваемая и самообучаемая прогнозная модель. Модель автоматически проводит оценку событий или цепочек событий.

Модуль **Машинное обучение** предназначен для создания и обучения модели выявления и реализует следующие функции:

- создание, обучение и проверка модели выявления;
- создание массивов данных для обучения и проверки модели выявления.

Модуль включает в себя:

- интерфейс пользователя для настройки параметров конфигурации модели, таких как:
 - периоды обновления;
 - периоды верификации;
 - количество записей, которых достаточно для обучения;
 - выбор вспомогательных моделей;
 - специальные параметры машинного обучения, которые применяются в процедурах извлечения признаков (Feature Extraction), выбора признаков (Feature Selection), создания признаков (Feature Engineering), построения ансамблей и прочих.
- приложение, которое выполняет обучение модели выявления;
- систему хранения, предназначенную для обучающих выборок.

3.5 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:

- для работы с карточкой инцидента. 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.

3.6 МОДУЛЬ РАБОЧИЙ СТОЛ

Модуль **Рабочий стол** предназначен для организации быстрого доступа к статистике и действиям, часто выполняемым во время расследования инцидентов. Модуль включает в себя интерфейс пользователя с диаграммами и графиками. С экранной формы рабочего стола можно перейти к тем или иным инструментам расследования.

3.7 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 пользователя для настройки разрешений, владений, ролей пользователей и учётных записей пользователей;
- пользовательский 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 (РИС. 1).
- 3) Установите флажок **Запомнить меня**, чтобы в последующем авторизация выполнялась без указания регистрационного имени и пароля – на основе сохраненных данных,
- 4) Нажмите кнопку **Войти**.

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

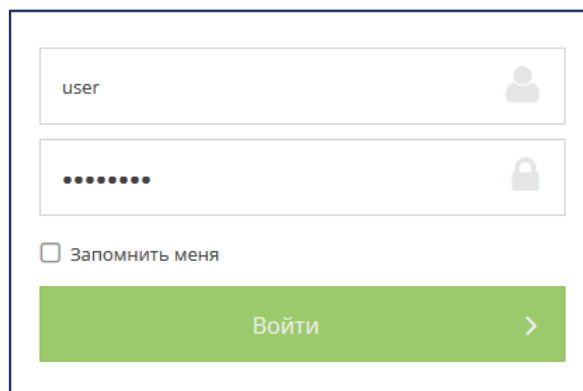



РИС. 1 – Вход в **Jet Detective**

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 готово 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 5.2).

4.4 ОПИСАНИЕ ИНТЕРФЕЙСА ПОЛЬЗОВАТЕЛЯ

4.4.1 Окно веб-приложения

Окно веб-приложения **Jet Detective** (РИС. 2) содержит следующие основные элементы интерфейса:

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

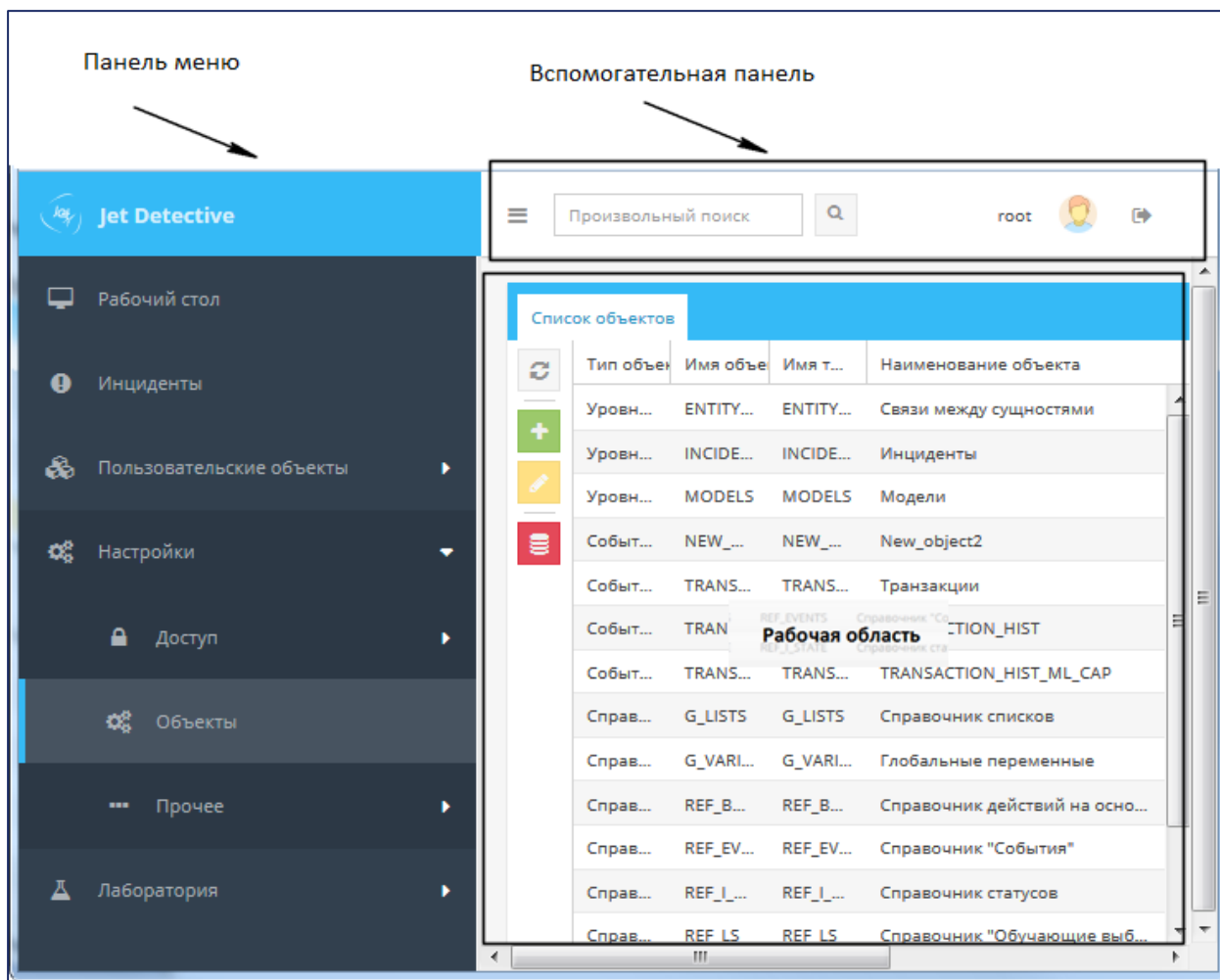


РИС. 2 – Общий вид окна веб-приложения

Интерфейс веб-приложения устроен единообразно – в *рабочей области* по умолчанию отображается вкладки со списком сущностей, соответствующих выбранному пункту меню, и формами. Исключение составляет интерфейс **Рабочего стола** (см. раздел 5.1).

Например:

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

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

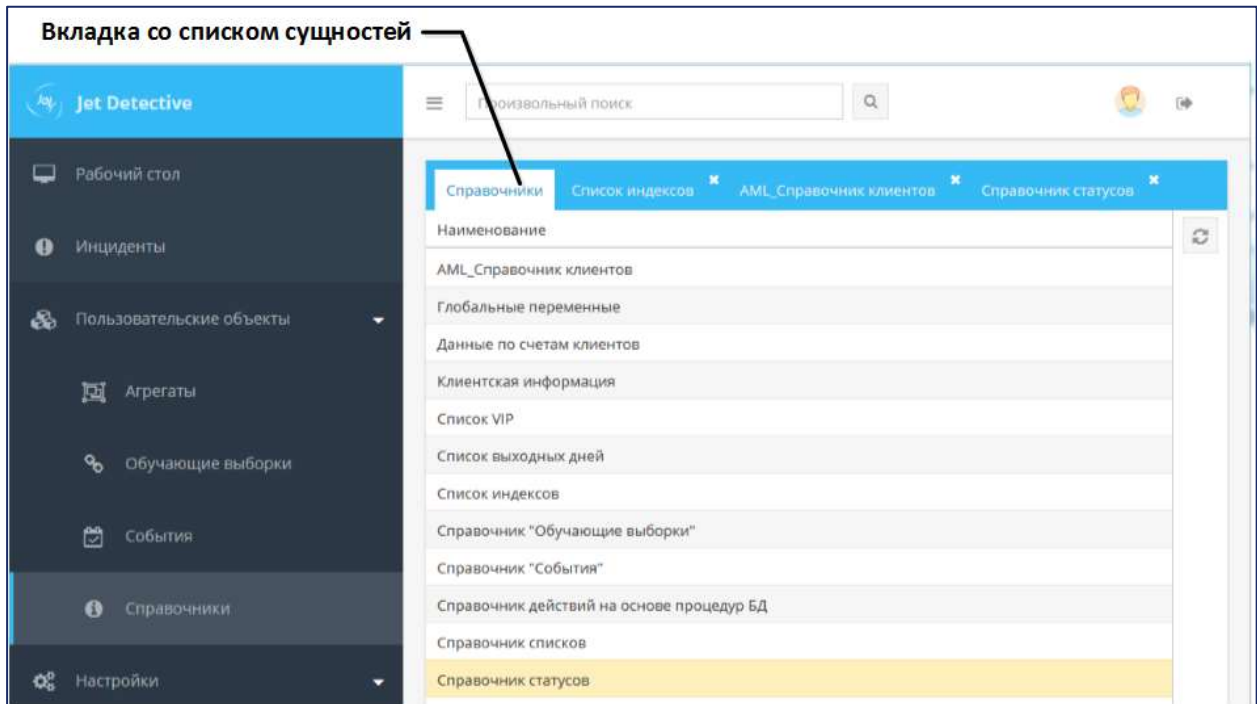


РИС. 3 – Пример списка экземпляров объекта с типом **Справочник**

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

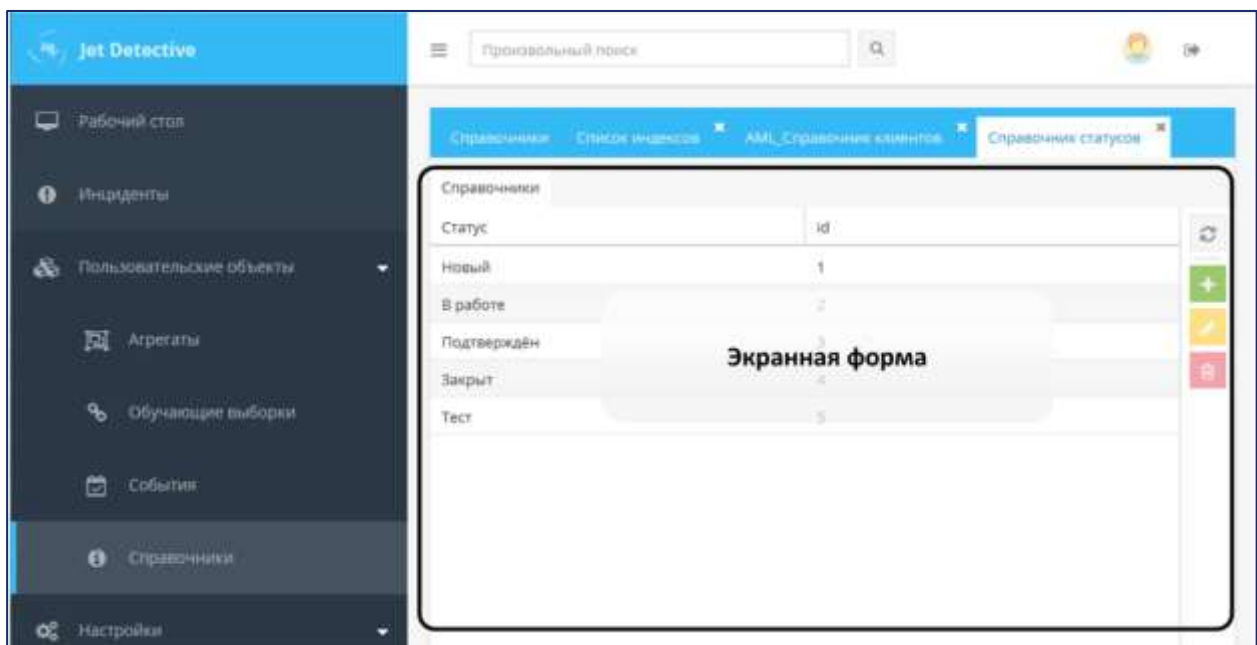





РИС. 4 – Пример вкладки с экранной формой выбранной сущности

Описание элементов вспомогательной панели приведено в ТАБЛ. 2.


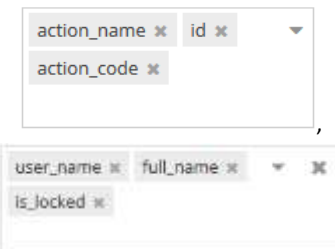



ТАБЛ. 2 – Описание вспомогательной панели







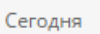
ЭЛЕМЕНТ ИНТЕРФЕЙСА	Тип	ДЕЙСТВИЕ
	Кнопка	Свернуть (развернуть) панель меню
	Кнопка	Настройка персонализации. Слева от кнопки отображается регистрационное имя пользователя работающего Jet Detective в настоящее время
	Кнопка	Выход из Jet Detective

4.4.2 Типовые элементы управления

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

ТАБЛ. 3 – Типовые элементы управления


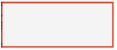



ЭЛЕМЕНТ УПРАВЛЕНИЯ	Тип или НАЗВАНИЕ	ОПИСАНИЕ ЭЛЕМЕНТА/ДЕЙСТВИЕ
	Кнопка Обновить	Используется, когда надо обновить отображаемую информацию, поступающую с сервера Jet Detective
	Поле	<p>Поле с раскрывающимся списком и множественным выбором элементов.</p> <p>Чтобы заполнить поле, выберите в раскрывающемся списке одно или несколько значений. Для выбора нескольких значений используйте клавишу Ctrl.</p> <p>Чтобы удалить из поля указанное ранее значение, нажмите кнопку  (находится в правой части поля).</p> <p>Чтобы в одно действие удалить все указанные значения, нажмите кнопку .</p> <p><i>Примечание:</i> такая возможность доступна не для всех полей</p>
	Кнопка Открыть , кнопка Редактировать	<p>Используется, когда надо открыть экранную форму выбранной в списке сущности (объекта, учётной записи пользователя и т. д).</p> <p>Экранную форму можно также открыть двойным щелчком по строке в списке сущностей</p>

ЭЛЕМЕНТ УПРАВЛЕНИЯ	Тип или название	ОПИСАНИЕ ЭЛЕМЕНТА/ДЕЙСТВИЕ
 	Поле с календарём	<p>Дату в поле можно указать как вручную, так и с помощью раскрывающегося календаря. Используемый формат – ДД.ММ.ГГГГ.</p> <p>Время можно указать только вручную, формат – чч:мм:сс. По умолчанию время автоматически устанавливается в значение 00:00:00. При необходимости его можно изменить.</p> <p>Чтобы раскрыть календарь, нажмите кнопку . Отобразится дата, выбранная ранее, или текущая дата – если поле с датой не заполнено.</p> <p>Чтобы перейти к любому месяцу и году:</p> <ul style="list-style-type: none"> • нажмите кнопку  в верхней части календаря; • в раскрывшемся списке выберите месяц и год; • нажмите ОК. <p>Для перехода к предыдущему или последующему месяцу используйте кнопки  и .</p> <p>Или: нажмите клавиши Ctrl+← или Ctrl+→.</p> <p>Для перехода к предыдущему или последующему году нажмите клавиши Ctrl+↓ или Ctrl+↑.</p> <p>Для выбора даты, соответствующей сегодняшнему дню, нажмите кнопку . Или нажмите клавишу пробела</p>

4.4.3 Индикация полей при вводе данных

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

ТАБЛ. 4 – Индикация полей

ЭЛЕМЕНТ ИНТЕРФЕЙСА	ОПИСАНИЕ
	Обязательное для заполнения поле
	Обязательное для заполнения поле, которое не было заполнено
 Да	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.

4.4.4.2 Настройка отображения столбцов

Можно включать столбцы в таблицу и исключать их.

Чтобы настроить состав отображаемых столбцов:

- 1) Наведите курсор на заголовок любого столбца.

В правой части заголовка отобразится кнопка  (РИС. 5).

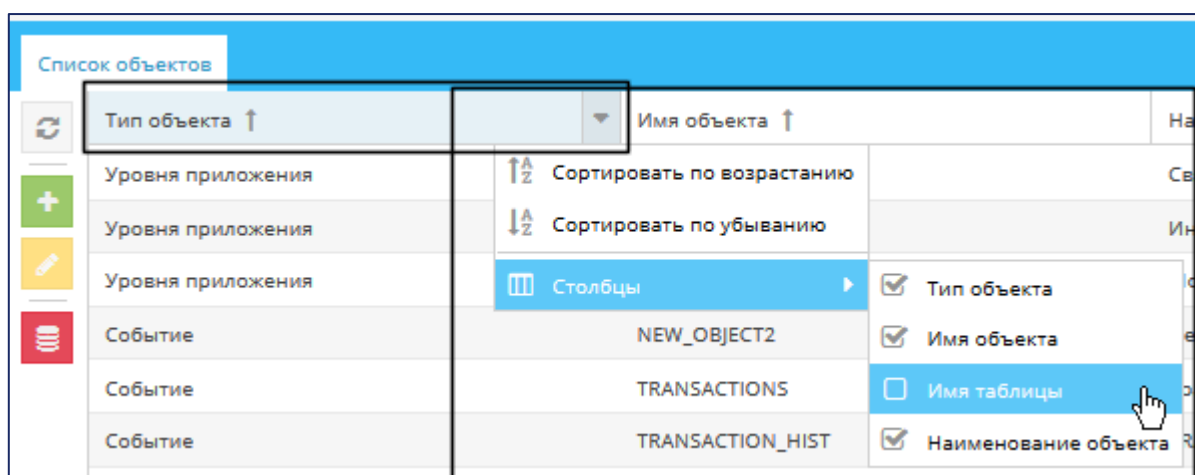


РИС. 5 – Настройка отображения столбцов

- 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.

4.4.4.3 Настройка порядка следования столбцов

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

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

Ширина столбца, расположенного слева, будет подобрана автоматически.

4.4.4.5 КНОПКИ ПЕРЕХОДА К СТРАНИЦАМ ТАБЛИЦЫ



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



ТАБЛ. 5 – Кнопки перехода к страницам таблицы


ЭЛЕМЕНТ УПРАВЛЕНИЯ	ТИП ИЛИ НАЗВАНИЕ	ДЕЙСТВИЕ
«	Кнопка Первая страница	Переход к первой странице таблицы
<	Кнопка Предыдущая страница	Переход к предыдущей странице таблицы
Страница  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 (РИС. 6).

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

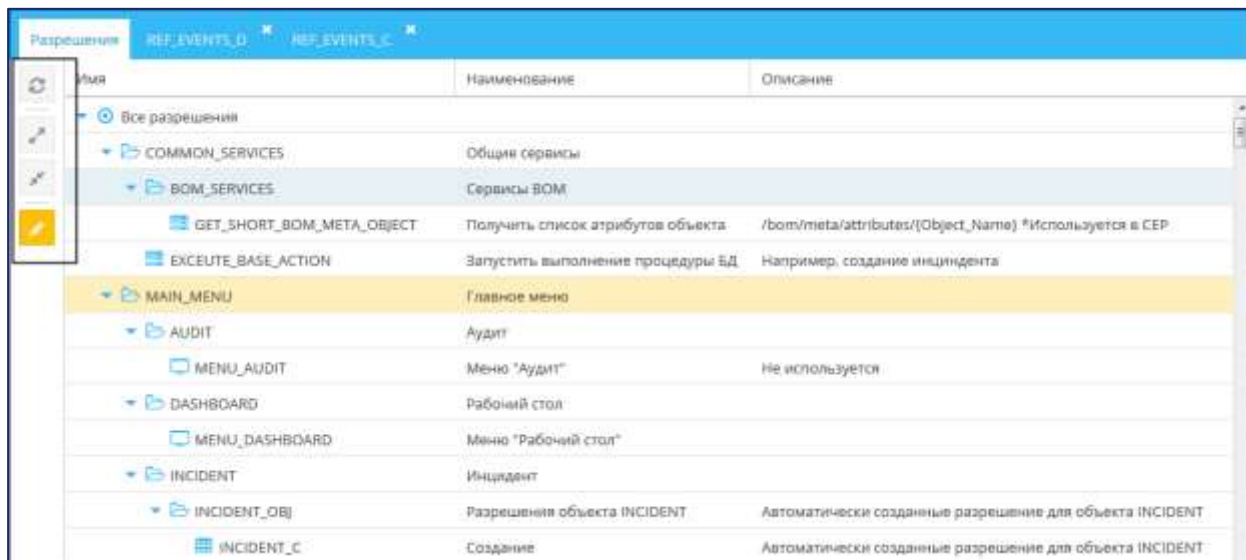


РИС. 6 – Пример полностью развернутого дерева разрешений

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.

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 анализа принимают решение, к какой категории отнести инцидент. Пример категорий при расследовании мошеннических действий: мошеннический, подозрительный или легитимный.

5.2 ПРОСМОТР СТАТИСТИКИ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ

5.2.1 Общее описание рабочего стола

Просмотр статистики расследования инцидентов выполняется на рабочем столе (РИС. 7).

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

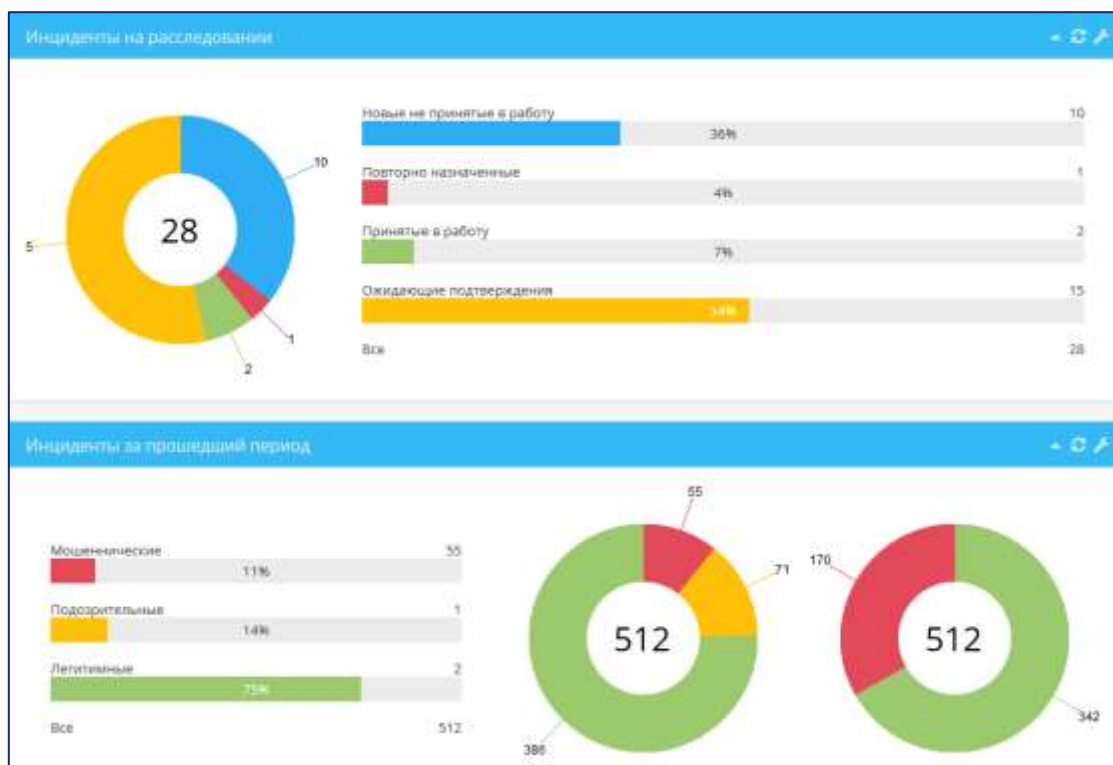






РИС. 7 – Экранная форма рабочего стола

На РИС. 7 представлен один из вариантов рабочего стола, который состоит из двух разделов:

- **Инциденты на расследовании** (см. раздел 5.2.2);
- **Инциденты за прошедший период** (см. раздел 5.2.3).

Строка заголовка каждого раздела содержит элементы управления, с помощью которых можно настроить отображение этого раздела (ТАБЛ. 6).

ТАБЛ. 6 – Описание элементов управления в строке заголовка раздела

ЭЛЕМЕНТ ИНТЕРФЕЙСА	Тип	ДЕЙСТВИЕ
	Кнопка	Свернуть раздел
	Кнопка	Развернуть раздел
	Кнопка	Обновить отображаемую информацию с сервера Jet Detective
	Кнопка	Настроить отображение информации

5.2.2 Раздел Инциденты на расследовании

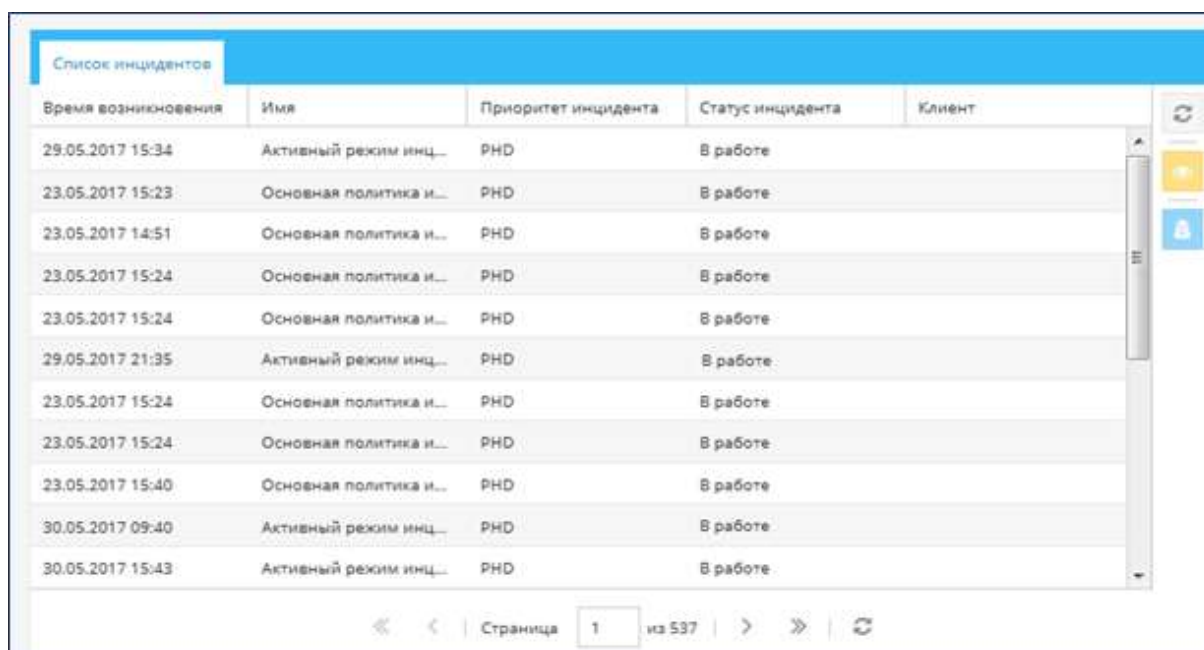
В разделе **Инциденты на расследовании** отображается статистика инцидентов, находящихся на расследовании у пользователя (РИС. 7).

Статистические данные расследуемых инцидентов представлены в виде:

- круговой диаграммы (слева);
- линейной диаграммы (справа).

Можно перейти от просмотра статистики к работе со списком соответствующих инцидентов. Для этого в разделе **Инциденты на расследовании** дважды щёлкните по шкале в линейной диаграмме.

На экране появится список инцидентов, находящихся на расследовании у пользователя (РИС. 8).



Время возникновения	Имя	Приоритет инцидента	Статус инцидента	Клиент
29.05.2017 15:34	Активный режим инц...	PND	В работе	
23.05.2017 15:23	Основная политика и...	PND	В работе	
23.05.2017 14:51	Основная политика и...	PND	В работе	
23.05.2017 15:24	Основная политика и...	PND	В работе	
23.05.2017 15:24	Основная политика и...	PND	В работе	
29.05.2017 21:35	Активный режим инц...	PND	В работе	
23.05.2017 15:24	Основная политика и...	PND	В работе	
23.05.2017 15:24	Основная политика и...	PND	В работе	
23.05.2017 15:40	Основная политика и...	PND	В работе	
30.05.2017 09:40	Активный режим инц...	PND	В работе	
30.05.2017 15:43	Активный режим инц...	PND	В работе	

РИС. 8 – Пример списка инцидентов при выборе шкалы **Новые не принятые в работу**

5.2.3 Раздел Инциденты за прошедший период

В разделе **Инциденты за прошедший период** отображается статистика инцидентов, с которыми расследователи завершили работу (РИС. 9).



РИС. 9 – Раздел **Инциденты за прошедший период** на экранной форме **Рабочий стол**

Статистические данные представлены в следующих формах:

- линейная диаграмма статистики расследованных инцидентов (РИС. 9, позиция А);
- круговая диаграмма статистики расследованных инцидентов (РИС. 9, позиция Б);
- график статистики расследованных инцидентов за период времени (РИС. 9, позиция Г). Чтобы увидеть количество инцидентов, относящихся к какой-либо категории, выявленных в том или ином месяце, наведите указатель мыши на соответствующую точку графика (РИС. 10);
- круговая диаграмма ложно-положительных срабатываний политик выявления, произошедших для расследованных инцидентов (РИС. 9, позиция В). Под ложно-положительным понимается результат применения политики, не совпавший с последующим решением расследователя.
- Можно перейти от просмотра статистики расследованных инцидентов к работе со списком соответствующих инцидентов.
- Для этого в разделе **Инциденты за прошедший период** дважды щёлкните по шкале А в диаграмме (см. РИС. 9). На экране откроется список инцидентов, с которыми работал расследователь (аналогичен списку на РИС. 8).



РИС. 10 – Пример просмотра сведений о количестве легитимных инцидентов за июнь

5.3 РАБОТА С ИНЦИДЕНТАМИ

5.3.1 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 добавляются в список инцидентов со статусом **Новый**. Статус меняется автоматически по нажатию кнопки **Взять в работу**.

5.3.2 Просмотр записи инцидента

Чтобы посмотреть запись:

1) Выберите пункт меню **Инциденты**.

В рабочей области отобразится одна или несколько вкладок:

- список инцидентов (РИС. 11);
- экранных форм записей инцидентов, открытых в этой сессии.

2) На вкладке со списком дважды щёлкните по строке с записью инцидента.

Карточка инцидента экранной формы записи инцидента откроется на отдельной вкладке (РИС. 12).

Краткое описание вкладок экранной формы инцидента приведено в ТАБЛ. 7, подробное описание – в разделах 5.3.2.1–5.3.2.3.

Время возникновения	Имя	Приоритет инцидента	Статус инцидента	Клиент
23.05.2017 14:51	Основная политика и...	Высокий	В работе	Банк
23.05.2017 15:23	Основная политика и...	Средний	В работе	Банк
23.05.2017 15:24	Основная политика и...	Низкий	В работе	Банк
23.05.2017 15:24	Основная политика и...	Низкий	В работе	Банк
23.05.2017 15:24	Основная политика и...	Средний	В работе	Банк
23.05.2017 15:24	Основная политика и...	Средний	В работе	Банк
23.05.2017 15:40	Основная политика и...	Низкий	В работе	Банк

РИС. 11 – Вкладка со списком инцидентов

Клиент:	Банк	Исполнитель:	Петров Игорь Иванович
Скор политики:	4	Имя:	Основная политика инцидент №11592
Время возникновения:	23.05.2017 15:24	Статус инцидента:	Новый
Приоритет инцидента:	Высокий	Владелец записи:	3

РИС. 12 – Вкладка Карточка инцидента

ТАБЛ. 7 — Краткое описание вкладок на экранной форме инцидента

Вкладка	Описание
Карточка инцидента	Общие сведения об инциденте (см. РИС. 12, ТАБЛ. 8)
Связанные события	Сведения связанных с инцидентом событий и сработавших правил выявления (см. раздел 5.3.2.2)
Ход расследования	Комментарии о проделанной работе при расследовании инцидента (см. раздел 5.3.2.3)

5.3.2.1 ПРОСМОТР КАРТОЧКИ ИНЦИДЕНТА

На вкладке **Карточка объекта** приведена общая информация инцидента (ТАБЛ. 8).

На этой вкладке можно изменить статус инцидента или перейти к инструменту расследования (см. раздел 5.3.3).

ТАБЛ. 8 — Описание полей вкладки **Карточка инцидента**

Поле	Описание
Клиент	Наименование клиента, в котором зарегистрирован инцидент
Скор политики	Бальная оценка выполнения политики выявления
Время возникновения	Дата и время выявления инцидента в формате ДД.ММ.ГГГГ чч:мм:сс.
Приоритет инцидента	Приоритет инцидента
Исполнитель	ФИО пользователя, ответственного за расследование инцидента
Имя	Составное название инцидента. Состоит из названия применяемой политики выявления и порядкового номера.
Статус инцидента	Статус инцидента.
Владелец записи	Код владения

5.3.2.2 ПРОСМОТР СВЯЗАННЫХ СОБЫТИЙ И СРАБОТАВШИХ ПРАВИЛ

На вкладке **Связанные события** экранной формы записи инцидента отображается:

- табличный список событий инцидента. Описание столбцов приведено в ТАБЛ. 9;
- список сработавших правил. Описание столбцов приведено в ТАБЛ. 10.

Информация правил появляется на экране при выборе события в табличном списке событий.

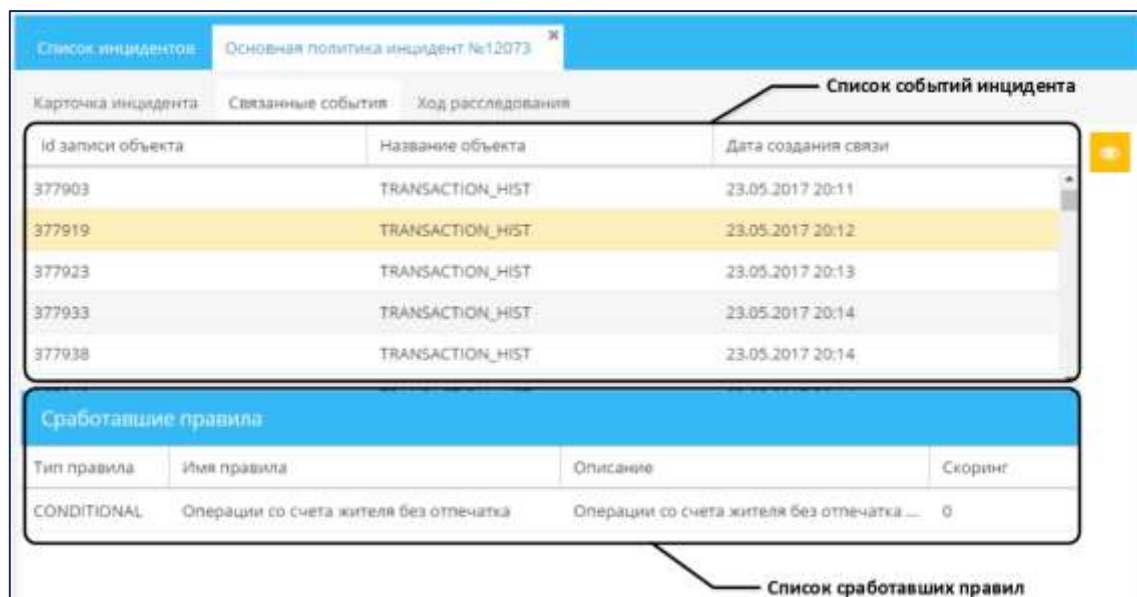
РИС. 13 – Вкладка **Связанные события**

ТАБЛ. 9 — Описание столбцов списка событий инцидента

Столбец	Описание
id записи объекта	Уникальный идентификатор события
Название объекта	Наименование объекта с типом событие, связанного с инцидентом. Просмотр полного списка событий – раздел 5.4; настройка объектов – раздел 6.1
Дата создания связи	Дата и время создания связи между инцидентом и событием в формате ДД.ММ.ГГГГ чч:мм:сс.

ТАБЛ. 10 — Описание столбцов списка сработавших правил

Столбец	Описание
Тип правила	Тип правила.
Имя правила	Имя правила. Подробнее про настройку правил в разделе 7.1
Описание	Описание правила
Скоринг	Бальная оценка

Чтобы посмотреть подробную информацию о связанном событии:

- 1) Откройте запись инцидента (см. раздел 5.3.2).
- 2) Перейдите на вкладку **Связанные события**.
- 3) Дважды щелкните по строке связанного события.

Отобразится окно **Информация о событии**. Пример окна приведён на РИС. 14. Его поля совпадают с полями объекта **Событие** (см. раздел 6.1).

Информация о событии «377919»

Номер счёта кредита:	3810165843525000	Баланс счёта кредита:	6000000
Обороты в валюте за день:	500000	Номер счёта дебета:	4567400034565060
enum_field:	C_enum	Баланс счёта дебета:	10000000
Идентификатор:	-2	Внешний ключ:	5
Дата, время последнего изменения:	29.05.2017 21:35	Разметка:	5
Владелец записи:	3	Автор последнего изменения:	Петров Игорь Иванович
ФИО плательщика:	Иванов Иван Иванович	Обороты по счёту за месяц:	15000000
ФИО получателя:	Петров Пётр Петрович	ДУЛ плательщика:	3705033791
Валюта операции:	RUB	ДУЛ получателя:	4603826261
Версия:	01	Сумма операции:	240000
		Дата операции:	01.01.2017 00:00

РИС. 14 – Окно **Информация о событии**

5.3.2.3 Ход расследования

На вкладке **Ход расследования** можно добавить комментарии к записи инцидента.

В левой части рабочей области отображается аватар пользователя, а в правой – текст комментария (РИС. 15). Все комментарии группируются по дням (датам).

Список инцидентов | Основная политика инцидент №11591

Карточка инцидента | Связанные события | **Ход расследования**

- Васильев Иван** Событие зарегистрировано. Принято в работу.
- Добавлен документ**
Подозрительное назначение платежа, Подозрительные время и место совершения операции.
- Петров Константин** добавил комментарий к событию
Звонок клиенту. Дозвониться не удалось. Клиент не берёт трубку.
- Зиновьев Алексей** повтор звонка
- Вчера**
- Добавлен комментарий**
Клиент не подтвердил проведение операции. Карта скомпрометирована, операция проведена третьими лицами


РИС. 15 – Инциденты. Вкладка **Ход расследования**

5.3.3 Расследование инцидента


Инструмент расследования находится в окне **Расследование**. Перейти к нему можно двумя способами:

- с вкладки со списком инцидентов;
- с вкладки **Карточка инцидента** экранной формы записи инцидента.

Чтобы открыть инструмент расследования с вкладки со списком инцидентов:

- 1) Откройте список инцидентов (см. раздел 5.3.2).
- 2) Выберите строку инцидента.
- 3) Нажмите кнопку **Открыть инструмент расследования**  в правой части рабочей области.

Чтобы открыть Инструмент расследования с вкладки **Карточка инцидента** экранной формы записи инцидента:

- 1) Откройте запись инцидента (см. раздел 5.3.2).
- 2) На вкладке **Карточка инцидента** нажмите кнопку **Открыть инструмент расследования**  (находится в нижнем правом углу рабочей области).

В окне **Расследование** (РИС. 16) отобразится:

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



РИС. 16 – Инциденты. Окно **Расследование**

5.3.3.1 ПАНЕЛЬ КРОСС-КАНАЛЬНОГО РАССЛЕДОВАНИЯ

Панель состоит из двух частей (РИС. 17):

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

Графики имеют временные 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.

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, 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 щёлкните 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.

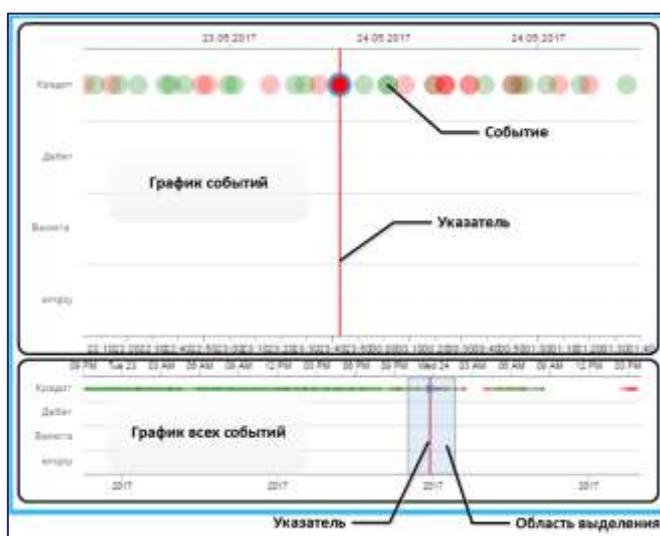


РИС. 17 – Панель кросс-канального расследования

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 о поступающих событиях. 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 (РИС. 18).

Статус	id
Не подтвержён	23
Закрыт	4
Подтверждён	3
В работе	2
Новый	1

РИС. 18 – Отображение объекта в виде таблицы

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.
- Можно перейти от просмотра статистики расследованных инцидентов к работе со списком соответствующих инцидентов.

- Для этого в разделе **Инциденты за прошедший период** дважды щёлкните по шкале **A** в диаграмме (см. РИС. 9). На экране откроется список инцидентов, с которыми работал расследователь (аналогичен списку на РИС. 8).

Можно перейти от просмотра статистики расследованных инцидентов к работе со списком соответствующих инцидентов.

Для этого в разделе **Инциденты за прошедший период** дважды щёлкните по шкале **A** в диаграмме (см. РИС. 9). На экране откроется список инцидентов, с которыми работал расследователь (аналогичен списку на РИС. 8).

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 **Пользовательские объекты – Справочники**.

В рабочей области отобразится одна или несколько вкладок:

- списка справочников (РИС. 19);
- справочников, открытых в этой сессии.

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

Экранная форма справочника откроется на отдельной вкладке (РИС. 20).

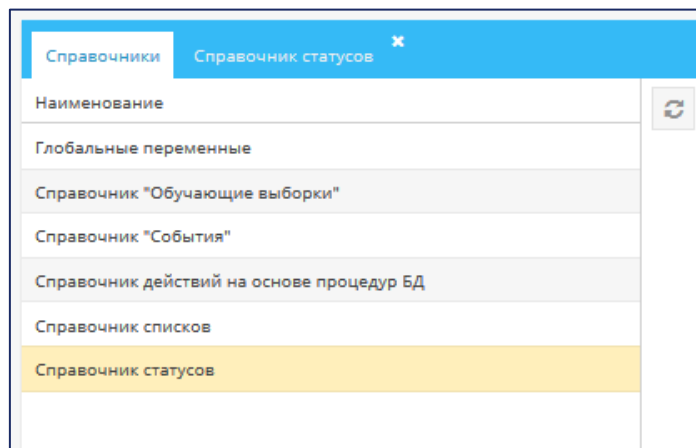


РИС. 19 – Вкладка со списком справочников

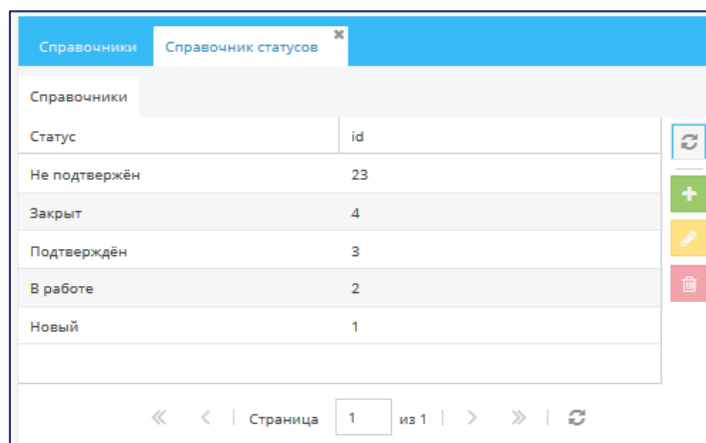



РИС. 20 – Вкладка с экранной формой справочника

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**  (РИС. 20).

Откроется вкладка **Добавление новой записи** выбранного справочника (РИС. 21).

- 3) Введите значения атрибутов.

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

- 4) Нажмите кнопку **Сохранить**.

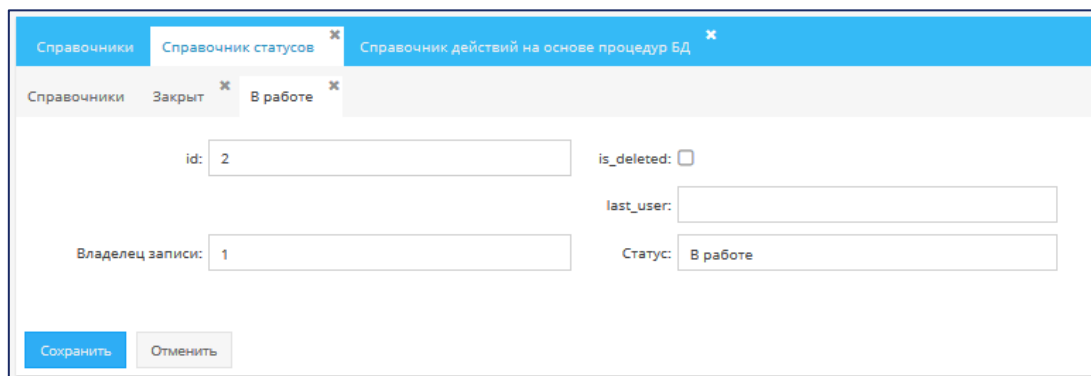


РИС. 21 – Добавление записи в справочник

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. (РИС. 22). Поля, флажки и прочие элементы этой вкладки соответствуют атрибутам справочника.

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

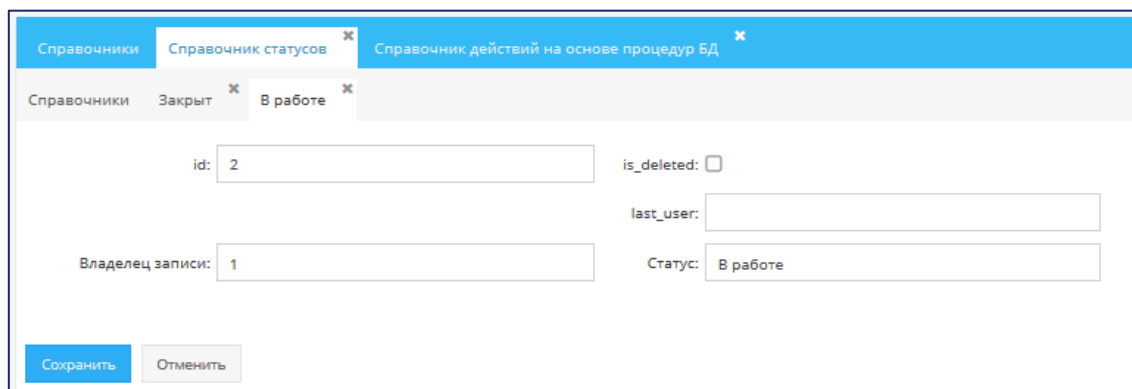



РИС. 22 – Справочник статусов. Пример экранной формы записи **В работе**

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** (РИС. 20).
- 3) Нажмите кнопку **Удалить** .
- 4) Нажмите кнопку **Да** в появившемся запросе на удаление.

6. АДМИНИСТРИРОВАНИЕ JET DETECTIVE

6.1 НАСТРОЙКА МОДЕЛИ ДАННЫХ

6.1.1 Общие сведения

Операции в **Jet Detective** выполняются над 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, PostgreSQL), так и нереляционные распределенные системы хранения, в том числе поддерживающие концепцию больших данных (например, HBase).

Существуют следующие типы объектов:

- *событие*. Объекты этого типа используются для хранения данных о событиях, поступающих из внешних систем;
- *справочник*. Справочные данные используются для обогащения поступающих событий;
- *агрегат*. Объекты этого типа используются для хранения результатов агрегации данных;
- *обучающая выборка*. Объекты этого типа являются служебными и предназначены для хранения обучающих выборок данных, которые использует модуль **Машинное обучение** для обучения, контроля и проверки моделей выявления;
- *уровень приложения*. Объекты этого типа относятся к служебным и являются встроенными в **Jet Detective**. К объектам уровня приложения относятся инциденты, модели, связи между объектами.

Можно настроить атрибуты объекта для их использования в машинном обучении. Дополнительно при настройке можно добавить ETL-процессы в конфигурацию объекта.

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;
- настройка использования атрибутов объекта в машинном обучении;
- настройка использования ETL-процессов.

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 6.1.10).

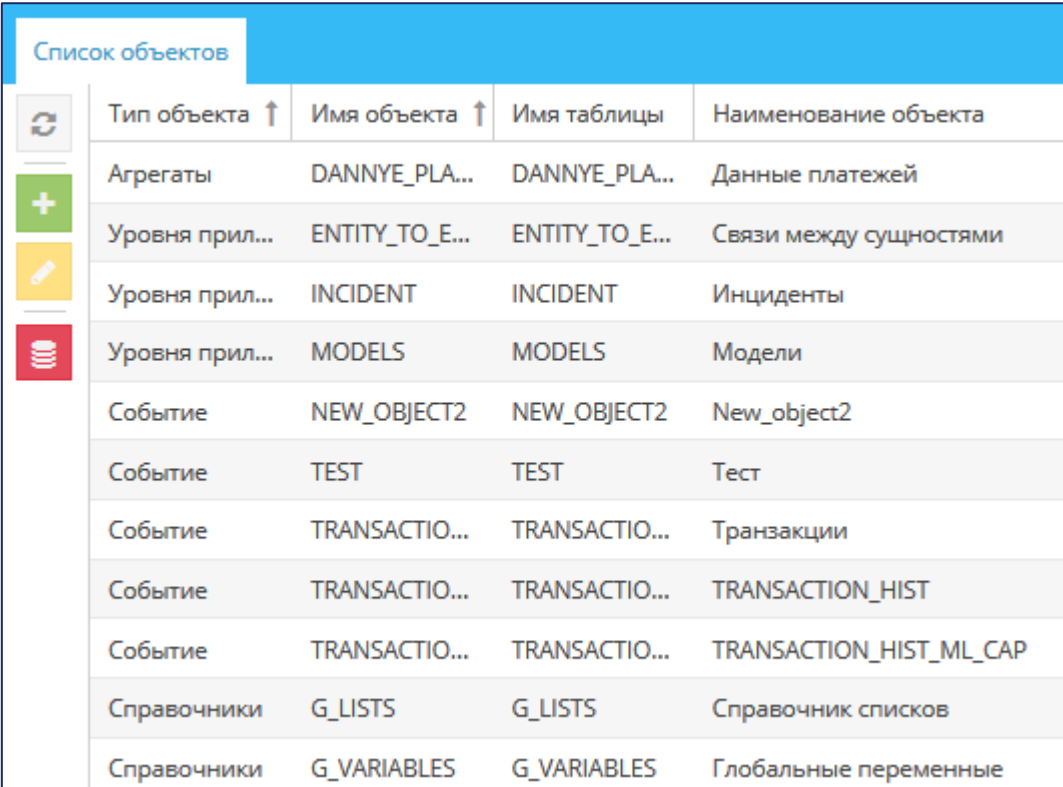
6.1.2 Просмотр объекта

Чтобы посмотреть объект:

- 1) Выберите пункт меню **Настройки – Объекты**.

В рабочей области отобразится одна или несколько вкладок:

- списка объектов (РИС. 24);
- конфигураций объектов, открытых в этой сессии.



Тип объекта ↑	Имя объекта ↑	Имя таблицы	Наименование объекта
Агрегаты	DANNYE_PLA...	DANNYE_PLA...	Данные платежей
Уровня прил...	ENTITY_TO_E...	ENTITY_TO_E...	Связи между сущностями
Уровня прил...	INCIDENT	INCIDENT	Инциденты
Уровня прил...	MODELS	MODELS	Модели
Событие	NEW_OBJECT2	NEW_OBJECT2	New_object2
Событие	TEST	TEST	Тест
Событие	TRANSACTION...	TRANSACTION...	Транзакции
Событие	TRANSACTION...	TRANSACTION...	TRANSACTION_HIST
Событие	TRANSACTION...	TRANSACTION...	TRANSACTION_HIST_ML_CAP
Справочники	G_LISTS	G_LISTS	Справочник списков
Справочники	G_VARIABLES	G_VARIABLES	Глобальные переменные

РИС. 23 – Пример списка объектов

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

Экранная форма конфигурации объекта откроется на вкладке **Объект** (РИС. 24). Сведения о конфигурации объекта распределены по нескольким вкладкам (ТАБЛ. 11).

Описание полей всех вкладок приведены в разделах 6.1.4 – 6.1.9.

Список объектов HOLIDAYS

Объект Атрибуты Поля Дополнительные опции Визуализация Машинное обучение ETL

Тип объекта: Справочники ?

Хранение: PostgreSQL ?

Имя: HOLIDAYS ?

Таблица: HOLIDAYS ?

Наименование: Список выходных дней ?

Скрыть: ?

РИС. 24 – Экранная форма конфигурации объекта. Вкладка **Объект**

ТАБЛ. 11 – Краткое описание вкладок на экранной форме с конфигурацией объекта

Вкладка	ОПИСАНИЕ
Объект	Общие сведения об объекте (см. РИС. 24, ТАБЛ. 12)
Атрибуты	Сведения об атрибутах объекта и инструменты для настройки атрибутов и соответствующих им полей таблицы объекта (см. раздел 6.1)
Поля	Сведения о полях таблицы объекта и инструменты для настройки полей (см. раздел 6.1.6)
Дополнительные опции	Инструменты для настройки дополнительных опций объекта (см. раздел 6.1.7)
Машинное обучение	Инструменты для настройки использования атрибутов объекта в машинном обучении (см. раздел 6.1.8)
ETL	Инструменты для использования ETL-процессов (см. раздел 6.1.9)

6.1.3 Этапы создания объекта

Создание объекта выполняется в несколько этапов:


- 1) Создание первичной конфигурации объекта (см. раздел 6.1.4).
- 2) Добавление и настройка атрибутов объекта и создание описаний, соответствующих атрибутам полей таблицы объекта (см. раздел 6.1.5).
- 3) Настройка дополнительных опций объекта (см. раздел 6.1.7).
- 4) Настройка использования атрибутов объекта в машинном обучении (см. раздел 6.1.8).
- 5) Добавление ETL-процессов в конфигурацию объекта и их использование (см. раздел 6.1.9).
- 6) Создание таблицы объекта в БД (см. раздел 6.1.10). Таблица создаётся автоматически после подтверждения.

Примечание. Создание таблицы объекта можно инициировать в любой момент после создания первичной конфигурации.

6.1.4 Создание первичной конфигурации объекта

При создании первичной конфигурации объекта, в числе прочего указывают имя объекта и имя таблицы объекта, которая в последствии будет создана в БД. Именование таблиц следует выполнять согласно правилам, принятым для выбранной базы данных. Объекту и таблице объекта рекомендуется давать одинаковые имена.

Чтобы создать конфигурацию объекта:

- 1) Выберите пункт меню **Настройки – Объекты**.
- 2) На вкладке **Список объектов** нажмите кнопку **Добавить** .
- 3) В открывшемся окне **Новый объект** (РИС. 25) заполните поля (ТАБЛ. 12).
- 4) Выберите служебные. Для этого:
 - раскройте секцию **Опции**;
 - установите флажки или снимите флажки, предлагаемые по умолчанию (ТАБЛ. 12).
- 5) Нажмите кнопку **Создать**.

Экранная форма с первичной конфигурацией объекта откроется на отдельной вкладке (РИС. 26).

После создания первичной конфигурации объекта следует выполнить настройку его атрибутов (см. раздел 6.1.5).

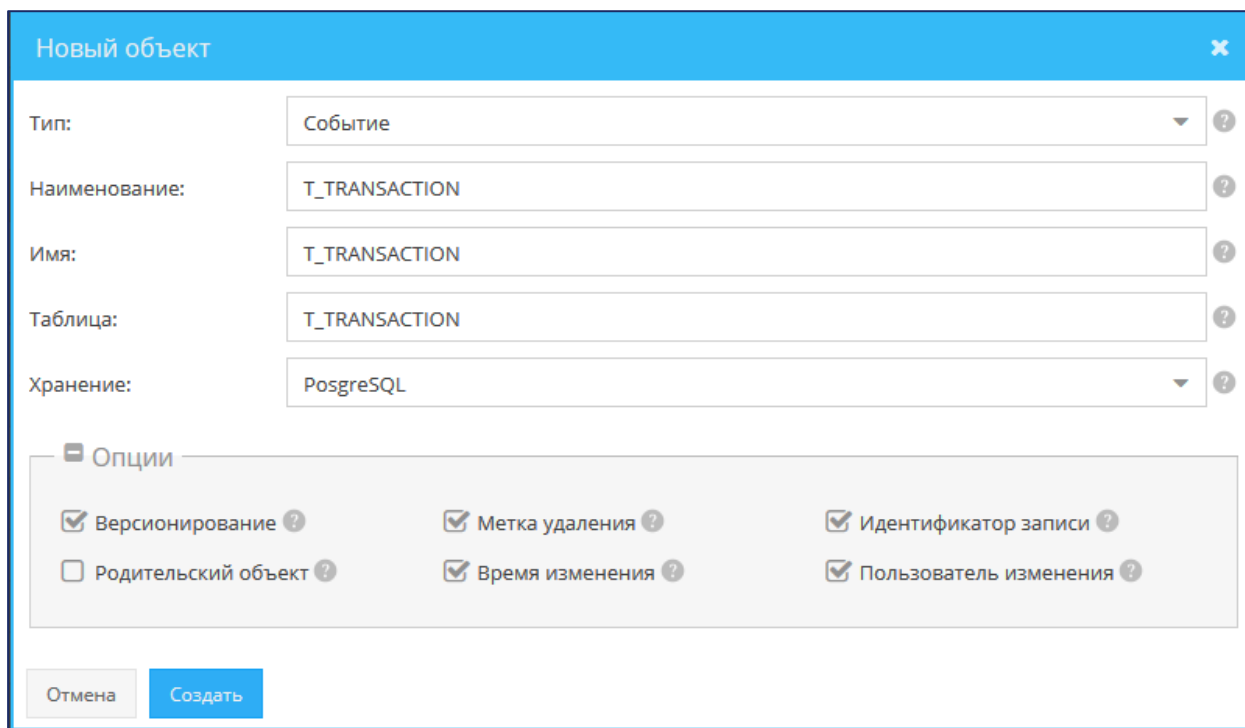


РИС. 25 – Окно **Новый объект**

ТАБЛ. 12 – Описание окна **Новый объект**

ЭЛЕМЕНТ ИНТЕРФЕЙСА	ОПИСАНИЕ
Поле Тип	Тип создаваемого объекта. Сведения о назначении того или иного типа объектов см. в разделе 6.1.1
Поле Наименование	Название объекта
Поле Имя	Имя объекта
Поле Таблица	Имя таблицы объекта
Поле Хранение	БД, в которой в последующем следует создать таблицу объекта
Флажок Версионирование	Если флажок установлен, то будут созданы атрибут и описание поля для хранения номера версии записи в таблице объекта. Атрибуту и полю автоматически присваивается имя
Флажок Родительский объект	Если флажок установлен, то будут созданы атрибут и описание поля для хранения ссылки на родительский объект при построении иерархии объектов. Атрибуту и полю автоматически присваивается имя
Флажок Метка удаления	Если флажок установлен, то будут созданы атрибут и описание поля для хранения отметки об удалении записи в таблице объекта. Атрибуту и полю автоматически присваивается имя is_deleted
Флажок Время изменения	Если флажок установлен, то будут созданы атрибут и описание поля для хранения даты и времени последнего изменения записи в таблице объекта. Атрибуту и полю автоматически присваивается имя last_change
Флажок Идентификатор записи	Если флажок установлен, то будут созданы атрибут и описание поля для идентификатора записи в таблице объекта. Атрибуту и полю автоматически присваивается имя id
Флажок Пользователь изменения	Если флажок установлен, то будут созданы атрибут и описание поля для хранения ссылки на учётную запись пользователя –автора последнего изменения записи в таблице объекта. Атрибуту и полю автоматически присваивается имя last_user

Список объектов T_TRANSACTION

Объект | Атрибуты | Поля | Дополнительные опции | Визуализация | Машинное обучение | ETL

Тип объекта: ?

Хранение: ?

Имя: ?

Таблица: ?

Наименование: ?


Скрыть: ?

РИС. 26 – Экранная форма с первичной конфигурацией объекта

6.1.5 Настройка атрибутов объекта

6.1.5.1 ДОБАВЛЕНИЕ АТТРИБУТА

Чтобы добавить атрибут объекта:

- 1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.1.2).
- 2) На вкладке **Атрибуты** нажмите кнопку **Добавить атрибут** .

В табличный список добавится строка с новым атрибутом. Его свойствам присвоятся автоматически сгенерированные значения.

- 3) Настройте свойства атрибута (см. раздел 6.1.5.2).
- 4) Нажмите кнопку **Сохранить**.

6.1.5.2 НАСТРОЙКА СВОЙСТВ АТТРИБУТА

Чтобы настроить свойства атрибута объекта:

- 1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.1.2).
- 2) На вкладке **Атрибуты** выберите строку с атрибутом.

В правой части рабочей области отобразится экранная форма, на которой приведены свойства атрибута (далее – *панель свойств атрибута*, РИС. 27).

- 3) Настройте свойства атрибута (ТАБЛ. 13).
- 4) Настройте описание полей (см. раздел 6.1.6).
- 5) Нажмите кнопку **Сохранить**.

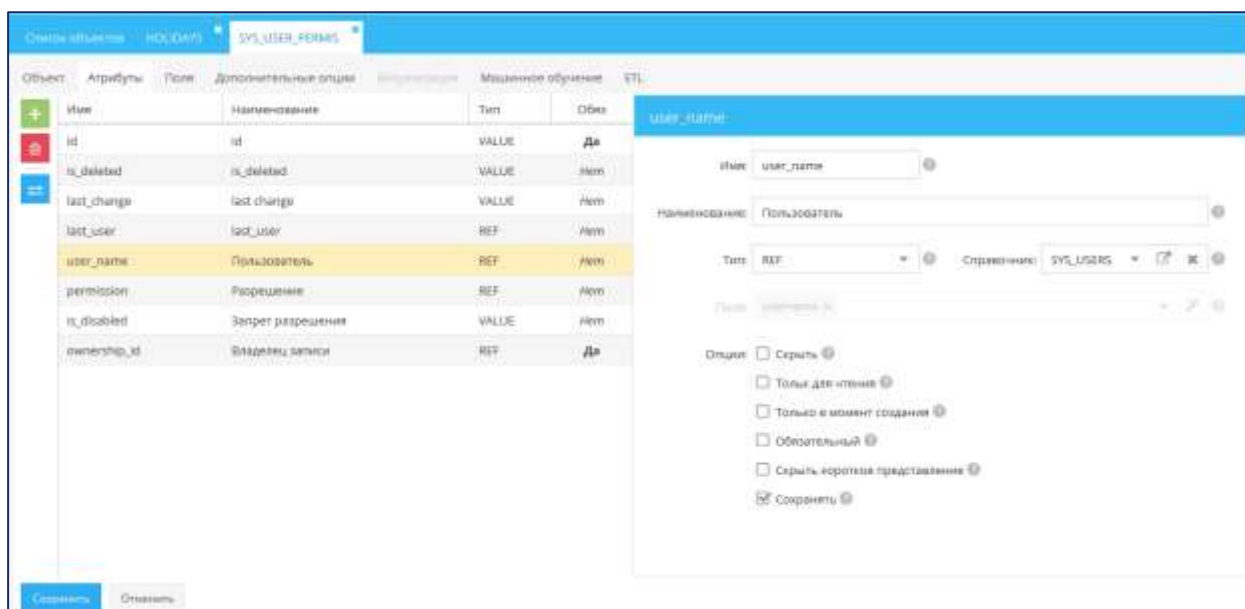



РИС. 27 – Просмотр свойств атрибута

ТАБЛ. 13 – Описание панели свойств атрибута

ЭЛЕМЕНТ ИНТЕРФЕЙСА	ОПИСАНИЕ
Поле Имя	Системное имя атрибута (далее – <i>имя атрибута</i>)
Поле Наименование	Название атрибута
Поле Тип	<p>Тип атрибута. Атрибуты бывают двух типов:</p> <ul style="list-style-type: none"> • VALUE – значение; • REF – ссылка на справочный объект. <p>Чаще всего в качестве справочного объекта используется объект с типом Справочник, но можно использовать объекты других типов. Если установлена ссылка на справочный объект, то атрибуту можно присвоить значения только из указанного объекта.</p> <p>На уровне БД ссылка на справочный объект означает установленную связь между полем атрибута объекта и полем идентификатора записи в таблице справочного объекта</p>
Поле Справочник	Имя справочного объекта, на который дается ссылка в атрибуте с типом REF . Значение выбирается в раскрывающемся списке
Поле Поля	<p>Имя атрибута в таблице справочного объекта:</p> <ul style="list-style-type: none"> • VALUE может соответствовать одно или несколько полей; • REF всегда соответствует одно поле
Флажок Скрыть	Если флажок установлен, то атрибут скрыт в интерфейсе пользователя при показе экземпляра объекта
Флажок Только для чтения	Если флажок установлен, то запрещено изменять значение атрибута в интерфейсе пользователя
Флажок Только в момент создания	Если флажок установлен, то значение атрибута определяется в момент создания записи в таблице объекта и его невозможно изменить впоследствии
Флажок Обязательный	Если флажок установлен, то атрибуту обязательно должно быть присвоено значение
Флажок Скрыть короткое представление	Если флажок установлен, то краткое представление атрибута скрыто в интерфейсе пользователя
Флажок Сохранять	Если флажок установлен, то значение атрибута сохраняется в таблице объекта

6.1.5.3 УДАЛЕНИЕ АТТРИБУТА

Чтобы удалить атрибут объекта:

- 1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.1.2).
- 2) На вкладке **Атрибуты** выберите строку с атрибутом.
- 3) Нажмите кнопку **Удалить атрибут** .
- 4) Нажмите кнопку **Да** в появившемся запросе.

Атрибут удалится из конфигурации объекта. Соответствовавшие атрибуту поля и их описания не будут удалены из таблицы объекта в БД (см. раздел 6.1.6).

6.1.6 Описание таблицы объекта

6.1.6.1 ОБЩИЕ СВЕДЕНИЯ

Формирование таблицы объекта заключается в следующем:

- описание 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 (см. РИС. 28, ТАБЛ. 14).

Объект	Атрибуты	Поля	Дополнительные опции	Визуализация	Машинное обучение	ETL		
	Имя	Используется в атрибутах	Тип	Размер	Точность	Список	По умолчанию	Полнотекстовый поиск
	id	id	NUMBER	19	0			Нет
	is_deleted	is_deleted	BOOLEAN	1	0			Нет
	last_change	last_change	DATE_TIME	0	0			Нет
	last_user	last_user	VARCHAR	255	0			Нет
	ownership_id	ownership_id	NUMBER	19	0			Нет

РИС. 28 – Просмотр описания таблицы объекта

ТАБЛ. 14 – 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

6.1.6.2 ДОБАВЛЕНИЕ ПОЛЯ

Существует три способа добавить поле в конфигурацию объекта:

- На панели свойств атрибута – с помощью мастера создания поля.
В этом случае при добавлении поля автоматически устанавливается соответствие между атрибутом и полем.
- На вкладке **Поля**.
В этом случае потребуется вручную установить соответствие между атрибутом и полем;
- На вкладке **Атрибуты** – с помощью специальной кнопки.
Поля, соответствующие атрибутам с типом **REF**, можно создать только таким способом. В результате выполнения операции для каждого атрибута, которому не поставлено в соответствие ни одно поле, автоматически создается по одному полю и устанавливается соответствие между атрибутами и полями.

Чтобы добавить поле на панели свойств атрибута:

- 1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.1.2).
- 2) На вкладке **Атрибуты** выберите строку с атрибутом.
- 3) На панели свойств атрибута, в поле **Поля**, нажмите кнопку **Открыть мастер создания поля**  (находится в левой части поля).

Откроется окно **Создание нового поля** (РИС. 29).

- 4) Настройте свойства поля (см. ТАБЛ. 14).
- 5) Нажмите кнопку **Добавить**.

Имя поля добавится в поле **Поля** (вкладка **Атрибуты**), а само поле – на вкладке **Поля**;

- 6) Нажмите кнопку **Сохранить**.

Поле добавится в конфигурацию объекта. Автоматически заполненное поле **Поля** (на вкладке **Атрибуты**) установит соответствие между атрибутом и полем объекта.

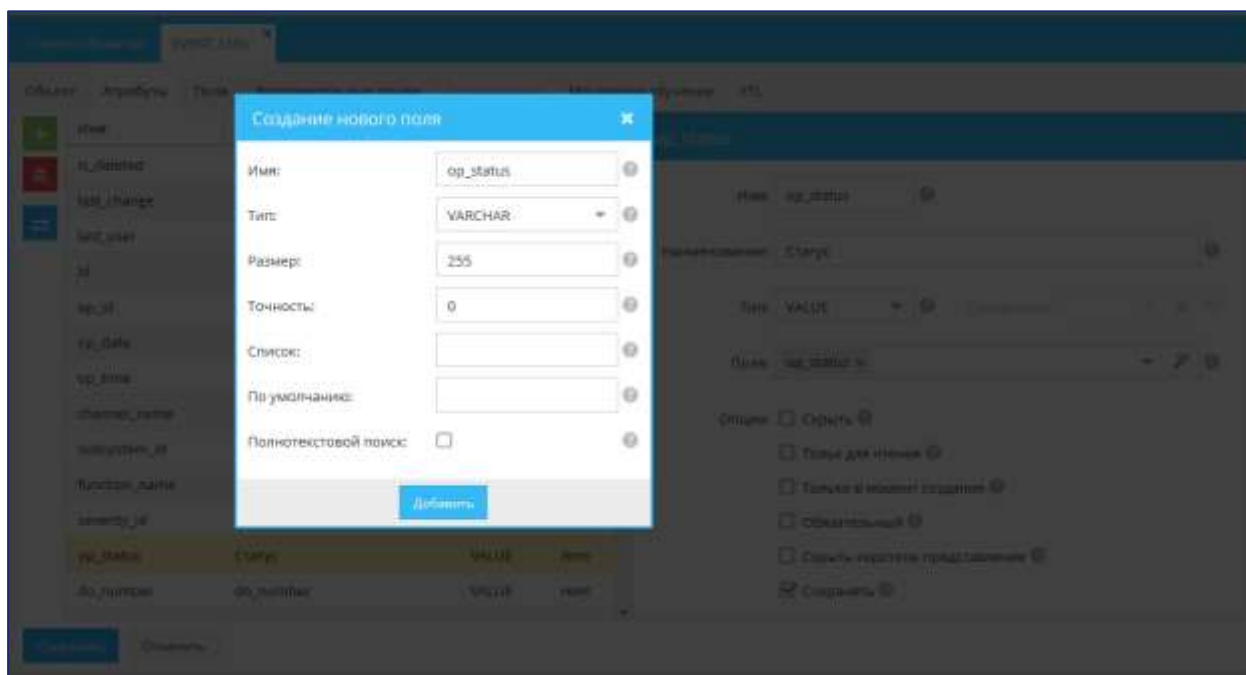



РИС. 29 – Добавление описания поля на панели свойств атрибута

Чтобы добавить поле на вкладке **Поля**:

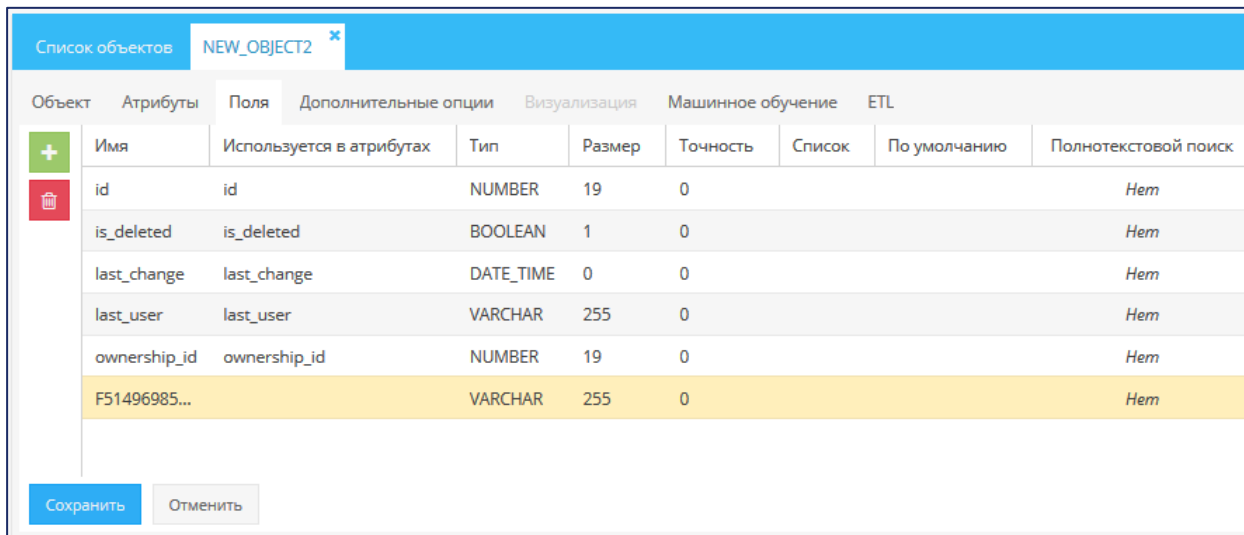
- 1) Нажмите кнопку **Добавить поле** .



В табличный список добавится строка с новым полем, а его свойствам присвоятся автоматически сгенерированные значения (РИС. 30).

- 2) Настройте свойства поля (см. ТАБЛ. 14) – укажите значения в соответствующих столбцах (кроме столбца **Используется в атрибутах**).

Примечание. Значение в столбце **Используется в атрибутах** указывается автоматически в результате установки соответствия между атрибутом и полем.

- 3) Установите соответствие между атрибутом и полем (см. раздел 6.1.6.3).
- 4) Нажмите кнопку **Сохранить**.




Объект	Атрибуты	Поля	Дополнительные опции	Визуализация	Машинное обучение	ETL		
	Имя	Используется в атрибутах	Тип	Размер	Точность	Список	По умолчанию	Полнотекстовый поиск
	id	id	NUMBER	19	0			Нет
	is_deleted	is_deleted	BOOLEAN	1	0			Нет
	last_change	last_change	DATE_TIME	0	0			Нет
	last_user	last_user	VARCHAR	255	0			Нет
	ownership_id	ownership_id	NUMBER	19	0			Нет
	F51496985...		VARCHAR	255	0			Нет

Сохранить Отменить

РИС. 30 – Добавление описания поля на вкладке **Поля**

Чтобы добавить недостающие поля:

- 1) На вкладке **Атрибуты** нажмите кнопку **Создать недостающие поля для атрибутов** .

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

Новые поля добавятся в конфигурацию объекта. Соответствие между атрибутами и добавленными полями установится автоматически.

- 3) На вкладке **Поля** настройте свойства полей (см. ТАБЛ. 14) – укажите значения в соответствующих столбцах.
- 4) Нажмите кнопку **Сохранить**.

6.1.6.3 УСТАНОВКА СООТВЕТСТВИЯ МЕЖДУ АТТРИБУТОМ И ПОЛЕМ И ОТМЕНА УСТАНОВЛЕННОГО СООТВЕТСТВИЯ

Для атрибутов с типом **VALUE** можно вручную установить соответствие между атрибутом и одним или несколькими полями таблицы объекта.

Чтобы установить соответствие:

- 1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.1.2).
- 2) На вкладке **Атрибуты** выберите строку с атрибутом.
- 3) На панели свойств атрибута в поле **Поля** выберите одно или несколько значений (РИС. 31).
- 4) Нажмите кнопку **Сохранить**.

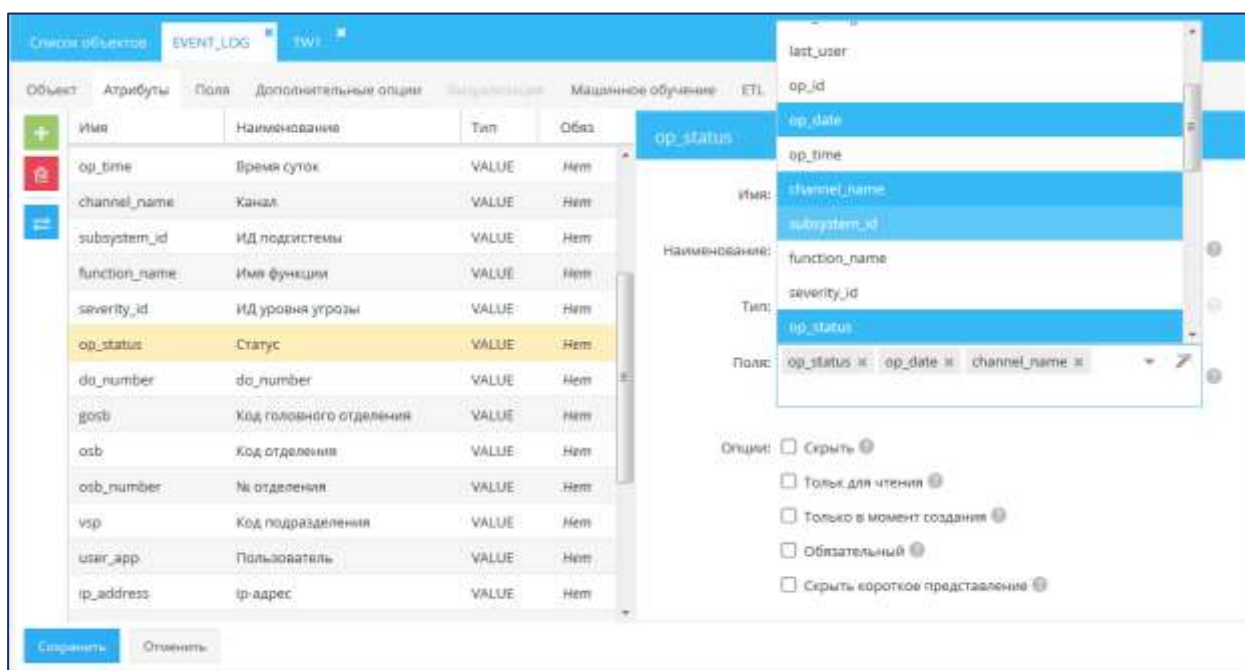


РИС. 31 – Выбор нескольких соответствующих атрибуту полей

Чтобы отменить соответствие:

- 1) На вкладке **Атрибуты** выберите строку с атрибутом.
- 2) На панели свойств атрибута в поле **Поля** нажмите кнопку **x** справа от имени поля (РИС. 32).
- 3) Нажмите кнопку **Сохранить**.

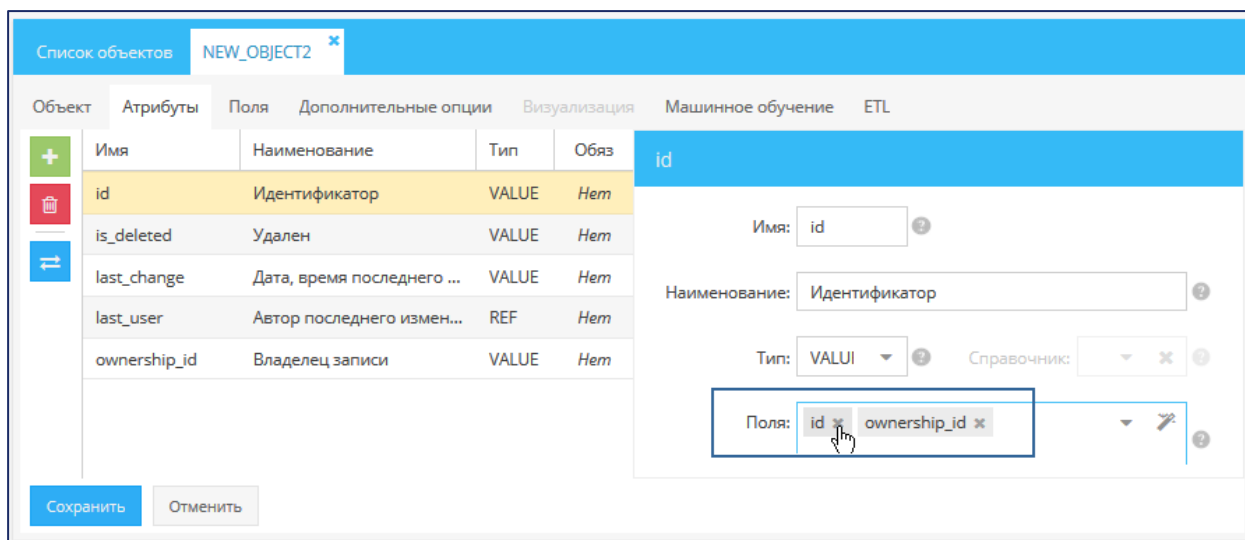



РИС. 32 – Отмена соответствия между атрибутом и полем

6.1.6.4 УДАЛЕНИЕ ПОЛЯ

Чтобы удалить поле из конфигурации объекта:

- 1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.1.2).
- 2) На вкладке **Поля** выберите строку поля.
- 3) Нажмите кнопку **Удалить поле** .
- 4) Нажмите кнопку **Да** в появившемся запросе.

Поле удалится из конфигурации объекта, но не из таблицы объекта в БД.

6.1.7 Настройка дополнительных опций объекта

Настройка дополнительных опций позволяет дифференцировать атрибуты объекта по их назначению. Например, любой атрибут может быть назначен идентификатором записи в таблице объекта.

Чтобы настроить дополнительные опции объекта:

- 1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.1.2).
- 2) На вкладке **Дополнительные опции** (РИС. 33) в раскрывающихся списках полей выберите имена атрибутов, которые следует задействовать (ТАБЛ. 15).
- 3) Нажмите кнопку **Сохранить**.

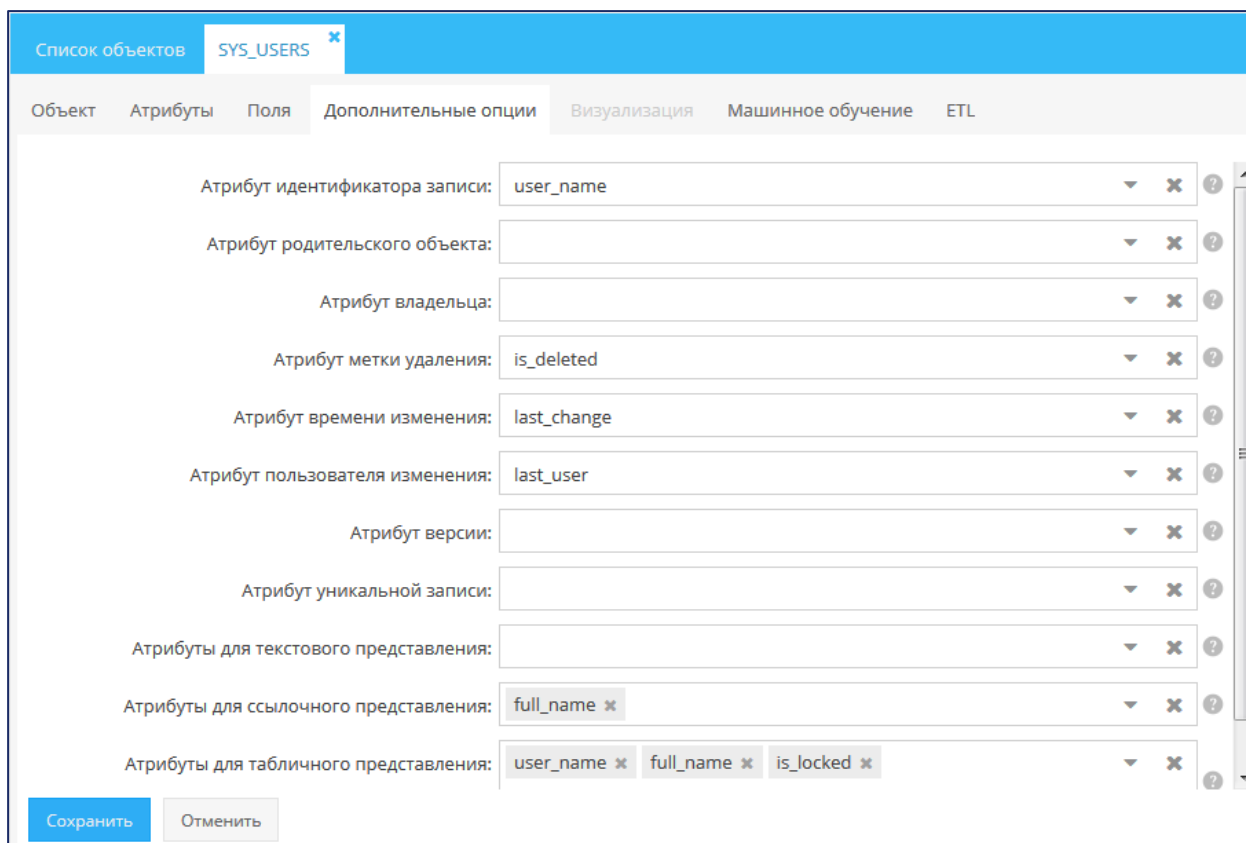


РИС. 33 – Настройка дополнительных опций объекта

ТАБЛ. 15 – Дополнительные опции объекта

Опция	ОПИСАНИЕ
Атрибут идентификатора записи	Идентификатор записи в таблице объекта
Атрибут родительского объекта	Хранение ссылки на родительский объект (при построении иерархии объектов)
Атрибут владельца	Хранение ссылки на владение (см. раздел 6.2.4)
Атрибут метки удаления	Хранение отметки об удалении записи в таблице объекта
Атрибут времени изменения	Хранение даты и времени последнего изменения записи в таблице объекта
Атрибут пользователя изменения	Хранение ссылки на пользователя – автора последнего изменения записи в таблице объекта
Атрибут версии	Хранение номера версии записи в таблице объекта
Атрибут уникальной записи	Хранение уникального идентификатора записи среди записей в таблице объекта, не отмеченных как удаленные
Атрибуты для текстового представления	Один или несколько атрибутов, которые следует использовать для текстового представления данных. Атрибуты используются в выгрузке данных в текстовый файл
Атрибуты для ссылочного представления	Один или несколько атрибутов, которые следует использовать для отображения в интерфейсе пользователя данных, запрашиваемых из другого объекта по ссылке (см. раздел 6.1.5.2, ТАБЛ. 13, поле Тип)

Опция	ОПИСАНИЕ
Атрибуты для табличного представления	Один или несколько атрибутов, которые будут использоваться для табличного представления данных объекта в интерфейсе пользователя

6.1.8 Настройка использования атрибутов объекта в машинном обучении

Атрибуты объекта можно настроить для использования в машинном обучении – в создании и обучении модели выявления. Модель выявления – это самосоздаваемая и самообучаемая прогнозная модель. Администратор **Jet Detective** классифицирует атрибуты объекта по типам значений и типам использования и тем самым формирует начальный состав признаков модели выявления (см. раздел 6.1.8). Модель автоматически проводит оценку событий или цепочек событий.

Чтобы настроить атрибуты для использования в машинном обучении:

- 1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.1.2)
- 2) На вкладке Машинное обучение (РИС. 34) установите флажок в столбце **МО** для атрибута.

Некоторые поля будут автоматически заполнены значениями по умолчанию.

- 3) Настройте параметры использования атрибута – укажите значения в соответствующих столбцах или используйте значения, предложенные по умолчанию (РИС. 36, ТАБЛ. 16).
- 4) Нажмите кнопку **Сохранить**.

Объект	Атрибуты	Поля	Дополнительные опции	Визуализация	Машинное обучение	ETL
Имя атрибута	Тип атрибута	МО	Тип значения	Тип использования	Тип данных	Тип трансформации
id	VALUE	<input type="checkbox"/>				
is_deleted	VALUE	<input checked="" type="checkbox"/>	text	keyField	string	
last_change	VALUE	<input type="checkbox"/>				
last_user	REF	<input type="checkbox"/>				
ownership_id	VALUE	<input type="checkbox"/>				

РИС. 34 – Настройка атрибутов для использования в машинном обучении

Объект	Атрибуты	Поля	Дополнительные опции	Визуализация	Машинное обучение	ETL
Имя атрибута	Тип атрибута	МО	Тип значения	Тип использования	Тип данных	Тип трансформации
id	VALUE	<input type="checkbox"/>				
is_deleted	VALUE	<input checked="" type="checkbox"/>	text	keyField	string	
last_change	VALUE	<input type="checkbox"/>			boolean	
last_user	REF	<input type="checkbox"/>			date-time	
ownership_id	VALUE	<input type="checkbox"/>			double	
A51496998852015	VALUE	<input type="checkbox"/>			integer	
					string	

РИС. 35 – Выбор типа данных атрибута (date-time) взамен предложенного по умолчанию (string)

ТАБЛ. 16 – Параметры использования атрибута

ПАРАМЕТР	ОПИСАНИЕ
Тип значения	continuous, flag, nominal, text
Тип использования	feature, keyField, skip, targetField
Тип данных	boolean, date-time, double, integer, string
Тип трансформации	oneToMany, profile

6.1.9 Использование ETL-процессов

6.1.9.1 ОБЩИЕ СВЕДЕНИЯ

В качестве платформы для работы с ETL-процессами используется Pentaho Data Integration (PDI). При настройке конфигурации объекта можно добавить ETL-процессы, подготовленные средствами PDI:

- из файлов формата KJB для ETL-процессов с типом **Transformation** (*преобразование*);
- из файлов формата KTR для ETL-процессов с типом **Job** (*задание*).

Примечание. ETL-процесс, связанный с объектом, не обязательно выполняет действия с этим объектом – он может только с ним ассоциироваться, но при этом воздействовать на какой-либо другой объект.

Сведения об ETL-процессах отображаются на вкладке **ETL** (см. РИС. 36, ТАБЛ. 17).

Имя файла	Имя	Описание	Версия	Дата создания	Создан	Статус
job load account.kjb	job load account	Задание: Загрузка информации по счетам	0.1	2016-11-05 12:09:22	-	loaded
Load account info.ktr	Load account info	Загрузка информации по счетам клиентное	0.1	2016-11-05 10:53:46	-	started

РИС. 36 – Просмотр сведений об использовании ETL-процессов

ТАБЛ. 17 – Атрибуты записи ETL-процесса

АТРИБУТ	ОПИСАНИЕ
Имя файла	Имя файла ETL-процесса, подготовленного средствами PDI
Имя	Служебное имя ETL-процесса
Описание	Краткое описание назначения ETL-процесса
Версия	Версия ETL-процесса

АТРИБУТ	ОПИСАНИЕ
Дата создания	Дата создания ETL-процесса
Создал	Автор ETL-процесса
Статус	Статус ETL-процесса в Jet Detective : <ul style="list-style-type: none"> • READY – процесс готов к выполнению; • RUNNING – процесс выполняется; • FAILURE – не удалось добавить процесса

6.1.9.2 ДОБАВЛЕНИЕ ETL-ПРОЦЕССА В КОНФИГУРАЦИЮ ОБЪЕКТА

Чтобы добавить ETL-процесс:

1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.1.2).

2) На вкладке **ETL** (см. РИС. 36) нажмите кнопку **Добавить процесс** .

Откроется табличный список файлов ETL-процессов (РИС. 37).

3) Выберите строку процесса.

4) Нажмите кнопку **Создать процесс**.

Сведения о добавленном ETL-процессе отобразятся на вкладке **ETL**. В случае успешного создания ETL-процессу присвоится статус READY, в противном случае – FAILURE.



Тип трансформации	Имя	Описание	Версия	Дата создания
TRANSFORM	Clean_data	Отчистка тестовых данных	0.1	
JOB	Job load account	Задание: Загрузка информации по счетам	0.1	2016-11-05 12:09:22
TRANSFORM	Load account info	Загрузка информации по счетам клиентов	0.1	2016-11-05 10:53:46
JOB	Load contact	Задание: загрузка контактной информации	0.1	
TRANSFORM	Load contact	Загрузка данных о контакте	0.1	2016-11-05 12:32:30
TRANSFORM	Stream_test_data	Тестовый поток данных		2016-10-18 10:17:57
JOB	Trans_cur_aggregate	Задание: обновление оборотов в валюте	0.1	
TRANSFORM	Trans_cur_aggregate	Сумма операций в валюте за день	0.1	
TRANSFORM	account_month_turn	Обороты по счету за последний час	0.1	

РИС. 37 – Выбор файла ETL-процесса

6.1.9.3 ПРОСМОТР СХЕМЫ ETL-ПРОЦЕССА

Чтобы посмотреть схему ETL-процесса:

1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.1.2).

2) На вкладке **ETL** выберите строку процесса.

3) Нажмите кнопку **Просмотреть схему ETL-процесса** .

Схема откроется в окне просмотра (РИС. 38).

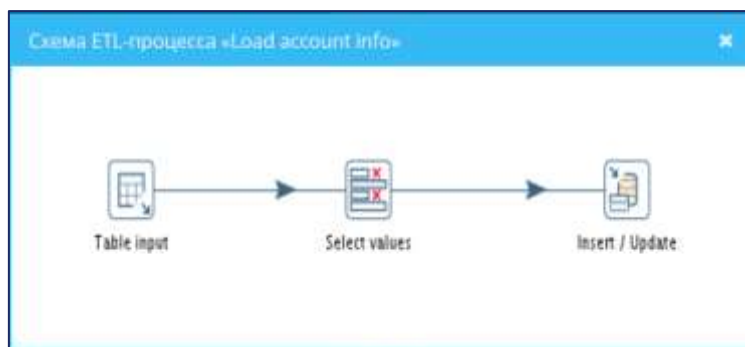



РИС. 38 – Просмотр схемы ETL-процесса

6.1.9.4 ЗАПУСК И ОСТАНОВКА ETL-ПРОЦЕССА

Чтобы запустить ETL-процесс на выполнение:


- 1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.1.2).
- 2) На вкладке **ETL** выберите строку процесса.
- 3) Нажмите кнопку **Запустить процесс** .
- 4) Нажмите кнопку **Да** в появившемся запросе.

ETL-процессу автоматически присвоится статус RUNNING.

После запуска ETL-процесса с типом **Преобразование** выполняются предписанные процессом операции с данными, после чего процесс автоматически завершается.

После запуска ETL-процесса с типом **Задание** выполняются предписанные процессом задачи согласно заданным файлу ETL-процесса условиям, например, по расписанию. Условия завершения процесса также заданы в его файле.


ETL-процесс любого типа можно остановить по команде пользователя. Для этого:

- 1) На вкладке **ETL** выберите строку процесса.
- 2) Нажмите кнопку **Остановить процесс** .
- 3) Нажмите кнопку **Да** в появившемся запросе.

ETL-процессу автоматически присвоится статус READY.

6.1.9.5 УДАЛЕНИЕ ETL-ПРОЦЕССА ИЗ КОНФИГУРАЦИИ ОБЪЕКТА


Чтобы удалить ETL-процесс:

- 1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.1.2).
- 2) На вкладке **ETL** выберите строку процесса.
- 3) Нажмите кнопку **Удалить процесс** .
- 4) Нажмите кнопку **Да** в появившемся запросе.

ETL-процесс удалится из конфигурации объекта.

6.1.10 Создание таблицы объекта в БД. Подтверждение конфигурации объекта

Таблица объекта создается в базе данных после подтверждения. Для этого:

- 1) Откройте вкладку **Список объектов** (см. раздел 6.1.2).
- 2) Нажмите кнопку **Применить изменения** .
- 3) Нажмите кнопку **Да** в появившемся запросе.

6.1.11 Редактирование конфигурации объекта

Чтобы изменить конфигурацию объекта:

- 1) Откройте экранную форму с конфигурацией объекта (см. раздел 6.1.2).
- 2) На вкладках экранной формы внесите изменения в конфигурацию объекта (см. разделы 6.1.5–6.1.9).
- 3) Нажмите кнопку **Сохранить**.

6.2 МОДЕЛЬ РАСПРЕДЕЛЕНИЯ ПРАВ ДОСТУПА

6.2.1 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 6.2.2) и владения (см. раздел 6.2.4).

Набор прав доступа каждого пользователя определяется установленными для него разрешениями в рамках владений, к которым он прикреплен (РИС. 39).

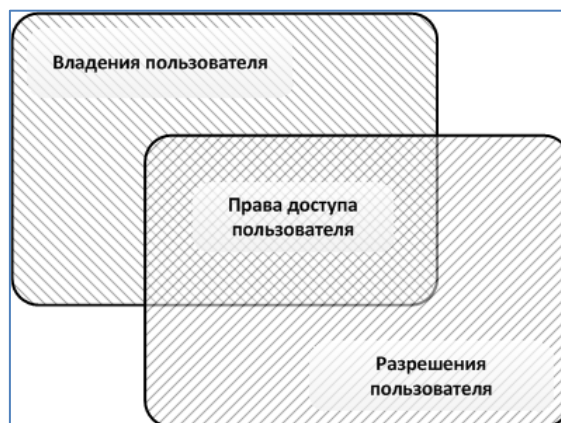


РИС. 39 – Права доступа пользователя определяются совокупностью владений и разрешений

6.2.2 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 определенного объекта.

Все возможные в **Jet Detective** разрешения представлены в виде *дерева разрешений* (РИС. 40). Такое представление позволяет группировать разрешения и выстраивать понятную и удобную для работы иерархию.

Имя	Наименование	Описание
Все разрешения		
COMMON_SERVICES	Общие сервисы	
BOM_SERVICES	Сервисы BOM	
GET_SHORT_BOM_META_OBJECT	Получить список атрибутов объекта	/Bom/meta/attributes/{Object_Name} *Используется в CEP *Возможно нигде не испол...
EXECUTE_BASE_ACTION	Запустить выполнение процедуры БД	Например, создание инцидента
MAIN_MENU	Главное меню	
AUDIT	Аудит	
MENU_AUDIT	Меню "Аудит"	Не используется
DASHBOARD	Рабочий стол	
MENU_DASHBOARD	Меню "Рабочий стол"	
INCIDENT	Инцидент	
INCIDENT_OBJ	Разрешения объекта INCIDENT	Автоматически созданные разрешения для объекта INCIDENT
INCIDENT_C	Создание	Автоматически созданные разрешения для объекта INCIDENT
INCIDENT_D	Удаление	Автоматически созданные разрешения для объекта INCIDENT
INCIDENT_R	Чтение	Автоматически созданные разрешения для объекта INCIDENT
INCIDENT_W	Запись	Автоматически созданные разрешения для объекта INCIDENT
MENU_INCIDENT	Меню "Инциденты"	

РИС. 40 – 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. Пользователю для выполнения соответствующей операции в **Jet Detective** необходимо 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 (см. раздел 6.3.2.1).

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 каждого пользователя. Существуют следующие инструменты для формирования набора разрешений:

- назначение пользователю одной или нескольких ролей (см. раздел 6.2.3.1);
- установка для пользователя одного или нескольких индивидуальных разрешений (см. раздел 6.2.3.2);
- установка запрета на одно или несколько разрешений (см. раздел 6.2.3.3).

6.2.3 Инструменты для формирования наборов разрешений

6.2.3.1 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.

6.2.3.2 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.

6.2.3.3 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 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.

Запреты устанавливаются администратором **Jet Detective** при настройке ролей и при настройке прав доступа пользователя.

6.2.4 Владения

6.2.4.1 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* (РИС. 41). 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.

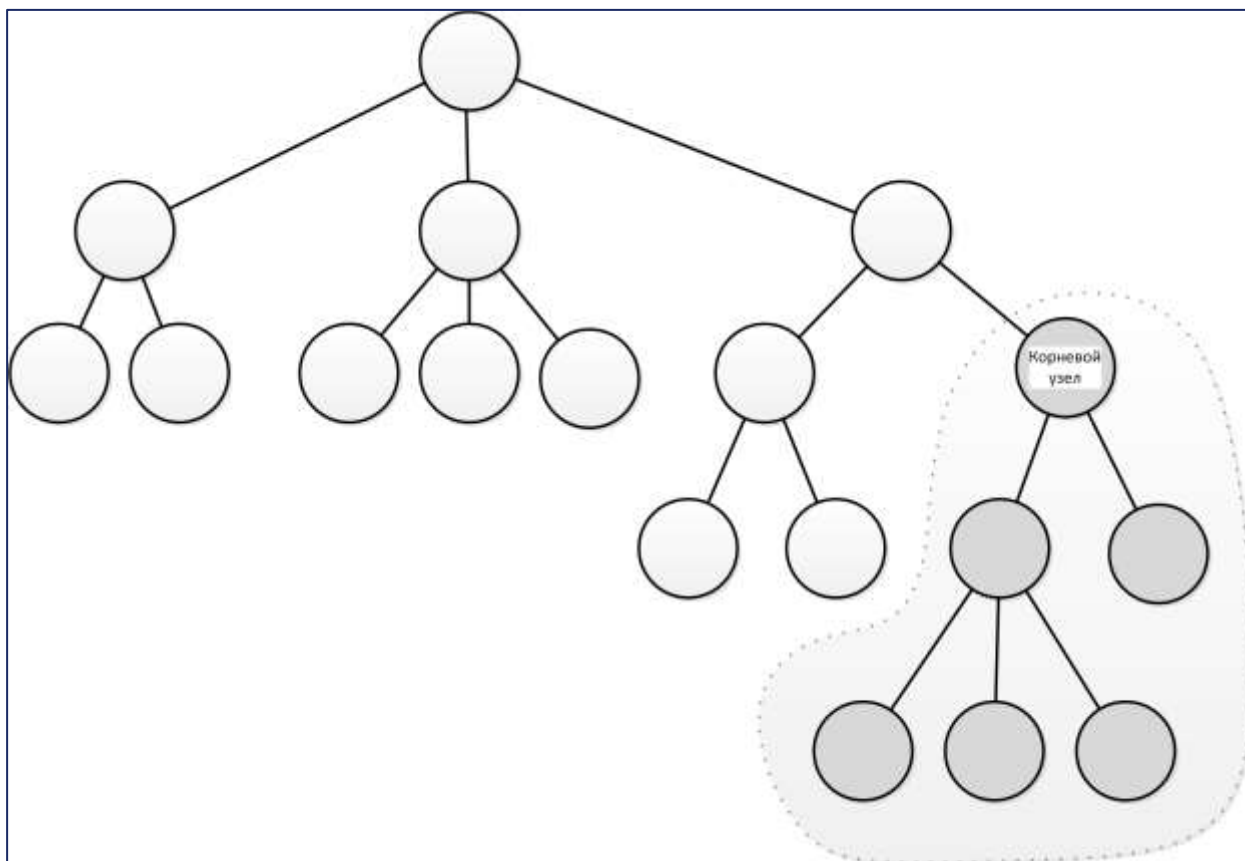


РИС. 41 – В дереве владений узел и его дочерние узлы образуют область владения

Схему владения пользователя образуют составляющие двух типов:

- область владения по умолчанию (см. раздел 6.2.4.2);
- области дополнительных владений (см. раздел 6.2.4.3).

Например, если на РИС. 42 область владения по умолчанию образована корневым узлом **А**, то области, образованные корневыми узлами **Б** и **В**, являются областями дополнительных владений.

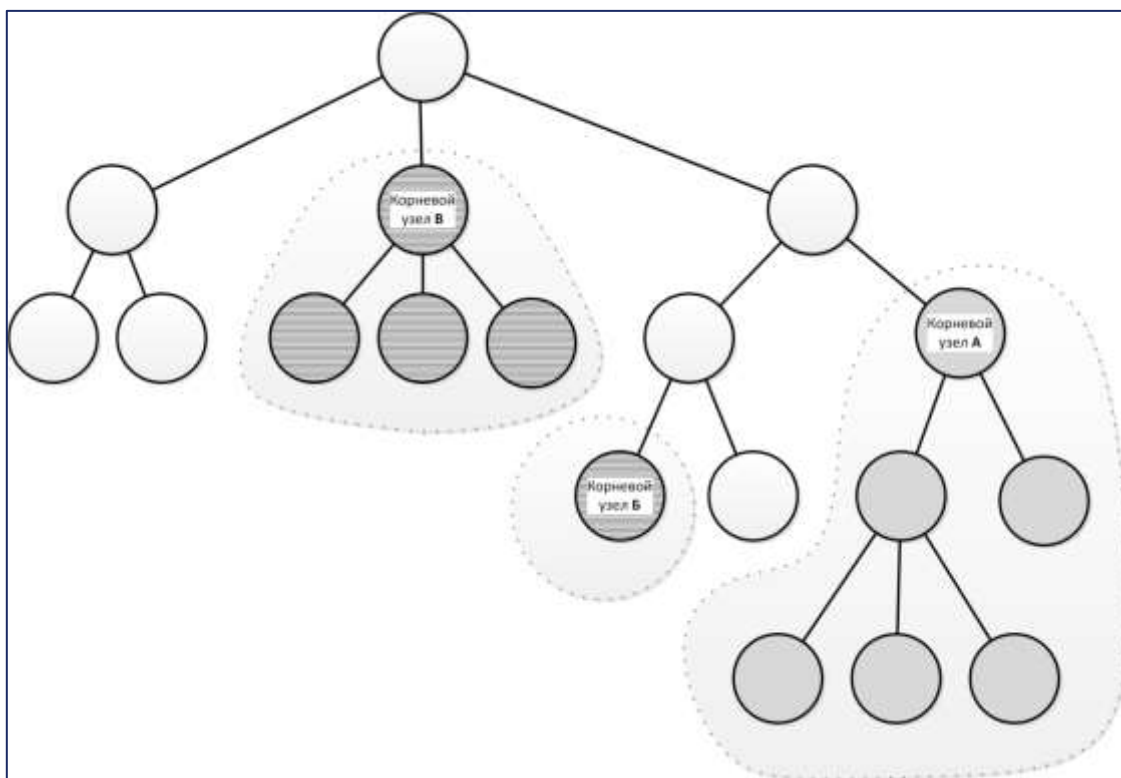


РИС. 42 – Схему владения пользователя образуют область владения по умолчанию и области дополнительных владений

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 РИС. 43 из области владения исключены дочерние узлы корневого узла **А**);
- узел вместе с дочерними узлами (например, на РИС. 44 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.

Примеры формирования схем владения пользователей см. в разделе Приложение А.

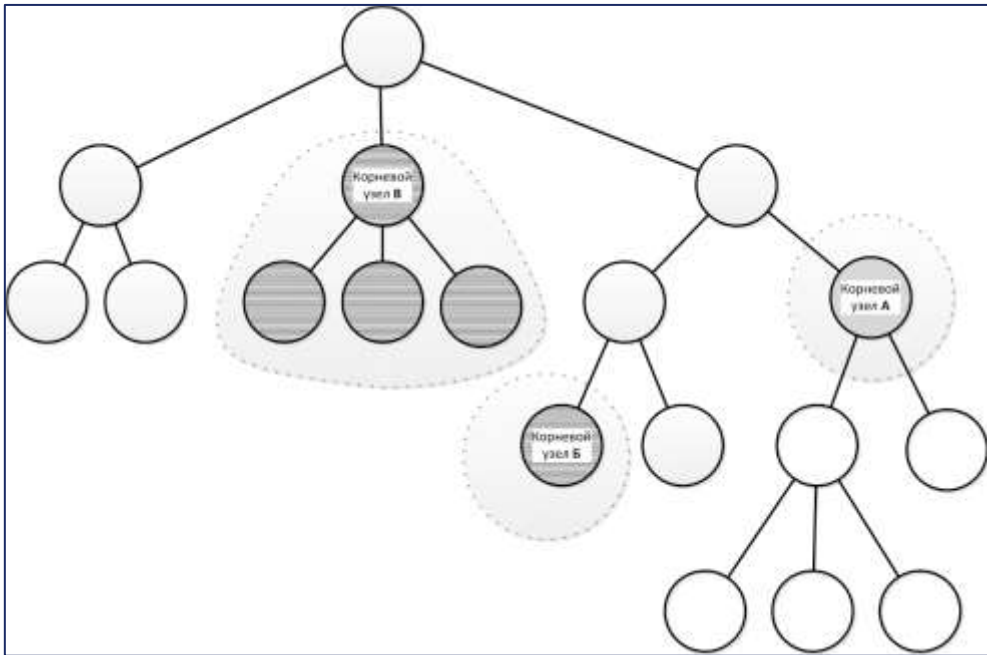


РИС. 43 – Из любой области владения можно исключить все дочерние владения

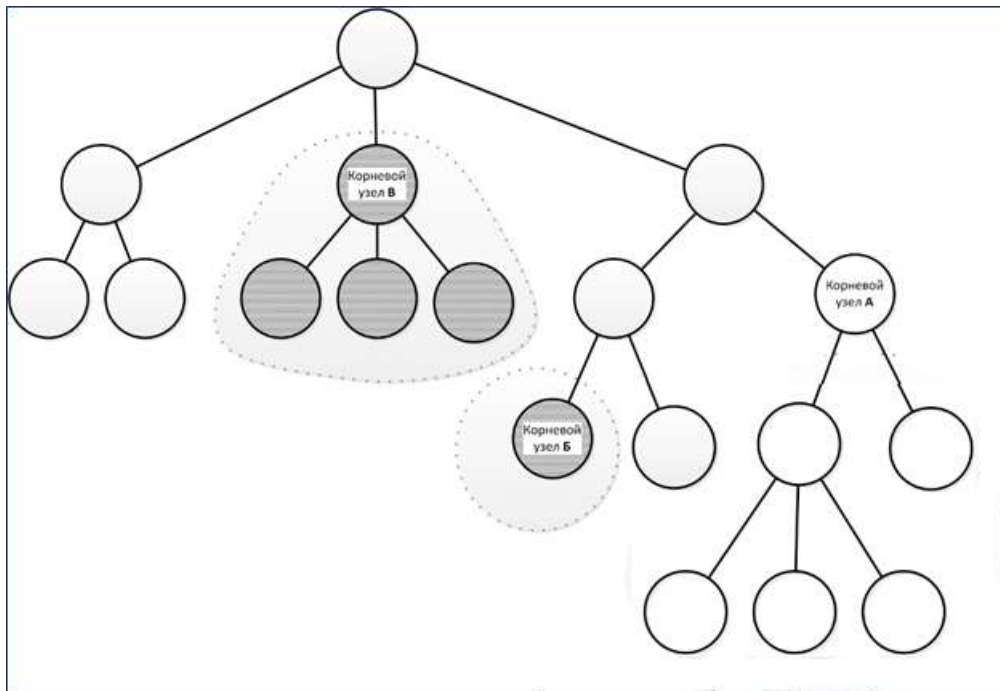


РИС. 44 – Из любой области владения можно исключить корневой узел

6.2.4.2 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. РИС. 41).

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 6.2.4.1 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 источника и содержания данных.

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.

6.2.4.3 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. РИС. 42).

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.

6.3 НАСТРОЙКА МЕХАНИЗМОВ УПРАВЛЕНИЯ ДОСТУПОМ

6.3.1 Общие сведения

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









На этапе внедрения администратор **Jet Detective** выполняет первичное построение:

- дерева разрешений (см. раздел 6.3.2).




Примечание. Изначально в **Jet Detective** уже присутствует дерево разрешений, которое охватывает все функции **Jet Detective**, кроме функций ведения пользовательских объектов и обучающих выборок, которые создаются автоматически во время создания объектов.

- дерева владений (см. раздел 6.3.3).
- дерева ролей (см. раздел 6.3.4).

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 6.4.5.1) 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.

6.3.2 Дерево разрешений

6.3.2.1 ПРОСМОТР ДЕРЕВА РАЗРЕШЕНИЙ, СВОЙСТВ ЕГО УЗЛОВ И ЛИСТЬЕВ

Общие сведения о дереве разрешений приведены в разделе 6.2.2.

Чтобы посмотреть дерево разрешений:

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

В рабочей области отобразится одна или несколько вкладок:

- дерева разрешений (РИС. 45);

- узлов дерева, открытых в этой сессии.

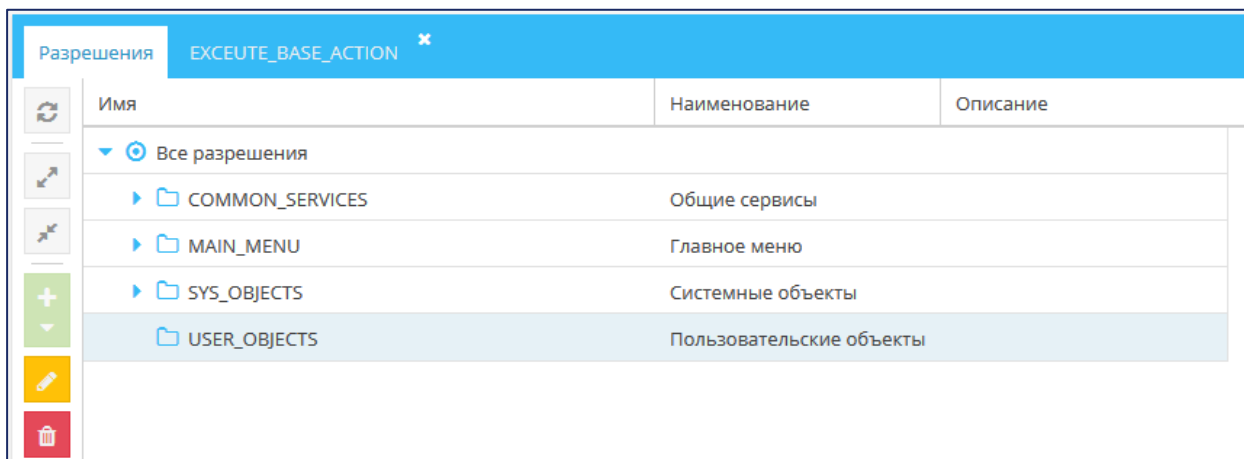


РИС. 45 – Пример дерева разрешений, развернутого на один уровень

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.

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

Экранная форма узла откроется на отдельной вкладке (РИС. 46).

Разрешение
Имя: USER_OBJECTS
Тип разрешения: Папка
Наименование: Пользовательские объекты
Описание:
Объект:

Сохранить Отменить

РИС. 46 – Вкладка с экранной формой узла USER_OBJECTS

Атрибуты узла описаны в ТАБЛ. 18.

ТАБЛ. 18 – Атрибуты узла дерева разрешений

АТРИБУТ	ОПИСАНИЕ
Имя	Системное имя узла (далее – <i>имя узла</i>)
Тип разрешения	Тип узла
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 (РИС. 47).

Экранная форма выбранной записи откроется на отдельной вкладке (РИС. 48).

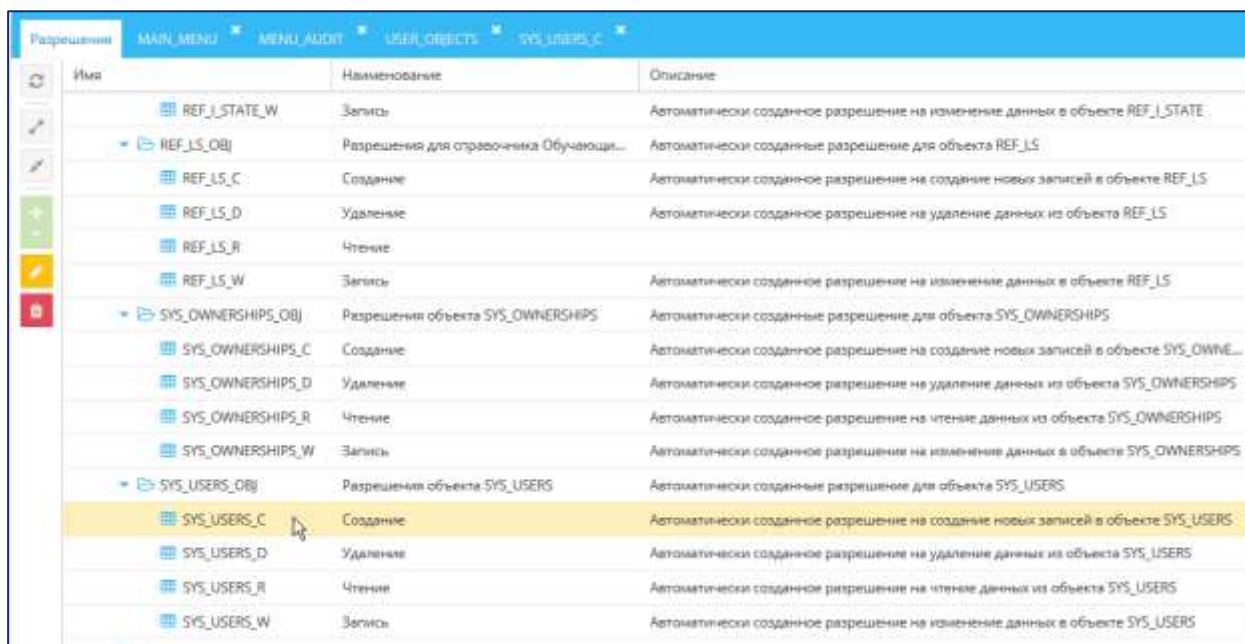


РИС. 47 – Выбор разрешения SYS_USERS_C

Разрешение

Имя: SYS_USERS_C

Тип разрешения: Объект

Наименование: Создание

Описание: Автоматически созданное разрешение на создание новых записей в объекте SYS_USERS

Объект: SYS_USERS

Сохранить Отменить

РИС. 48 – Экранная форма разрешения SYS_USERS_C

6.3.2.2 РЕДАКТИРОВАНИЕ СВОЙСТВ УЗЛА В ДЕРЕВЕ РАЗРЕШЕНИЙ И РАЗРЕШЕНИЯ

Можно отредактировать наименование и описание узла. Для этого:

- 1) Откройте экранные формы узла дерева разрешений и разрешения (см. раздел 6.3.2.1, РИС. 46, РИС. 48).
- 2) Измените наименование и описание узла.
- 3) Нажмите кнопку **Сохранить**.

6.3.2.3 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.

6.3.2.4 ДОБАВЛЕНИЕ УЗЛА И РАЗРЕШЕНИЯ В ДЕРЕВО РАЗРЕШЕНИЙ

Примечание: Изначально в **Jet Detective** уже присутствует дерево разрешений, которое охватывает все функции **Jet Detective**, кроме функций ведения пользовательских объектов и обучающих выборок. 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 (РИС. 49).

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

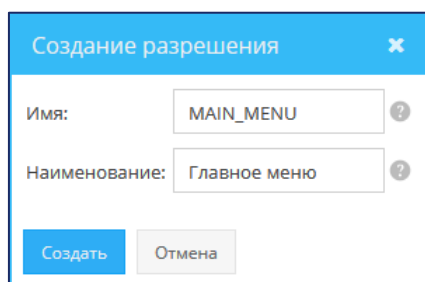



РИС. 49 – Создание разрешения

- 5) Нажмите кнопку **Создать**.
Узел добавится в дерево разрешений. Экранная форма узла откроется на отдельной вкладке.
- 6) Введите текст в поле **Описание** (РИС. 46).
- 7) Нажмите кнопку **Сохранить**.

6.3.2.5 УДАЛЕНИЕ УЗЛА ИЗ ДЕРЕВА РАЗРЕШЕНИЙ

Чтобы удалить узел из дерева разрешений:

- 1) Откройте экранную форму дерева разрешений (см. раздел 6.3.2.1).
- 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.

6.3.3 Дерево владений

6.3.3.1 ПРОСМОТР ДЕРЕВА ВЛАДЕНИЙ И ЕГО СВОЙСТВ

Общие сведения о дереве владений приведены в разделе 6.2.4.1.

Чтобы посмотреть дерево владений:

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

В рабочей области отобразится одна или несколько вкладок:

- дерева владений (РИС. 50);
- узлов дерева, открытых в этой сессии.

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

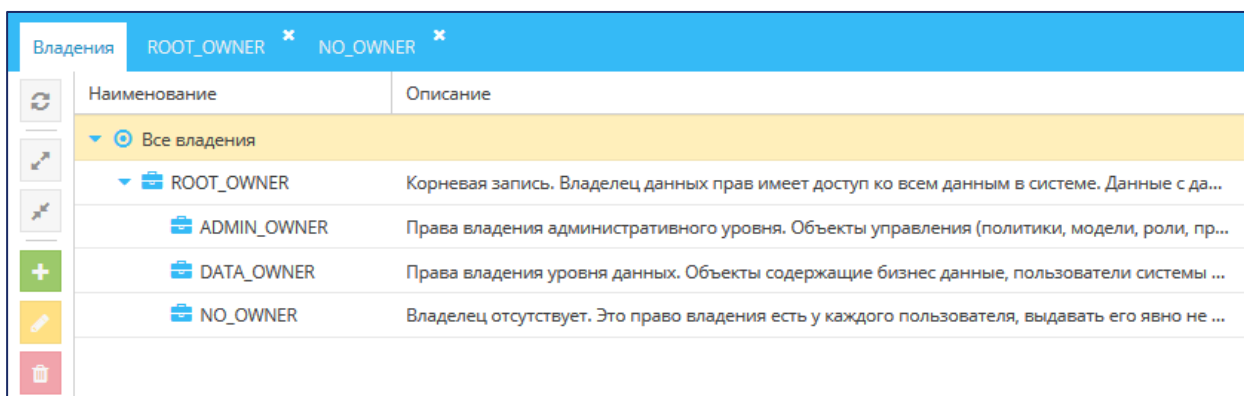


РИС. 50 – Пример дерева владений

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

Экранная форма владения откроется на отдельной вкладке (РИС. 51).

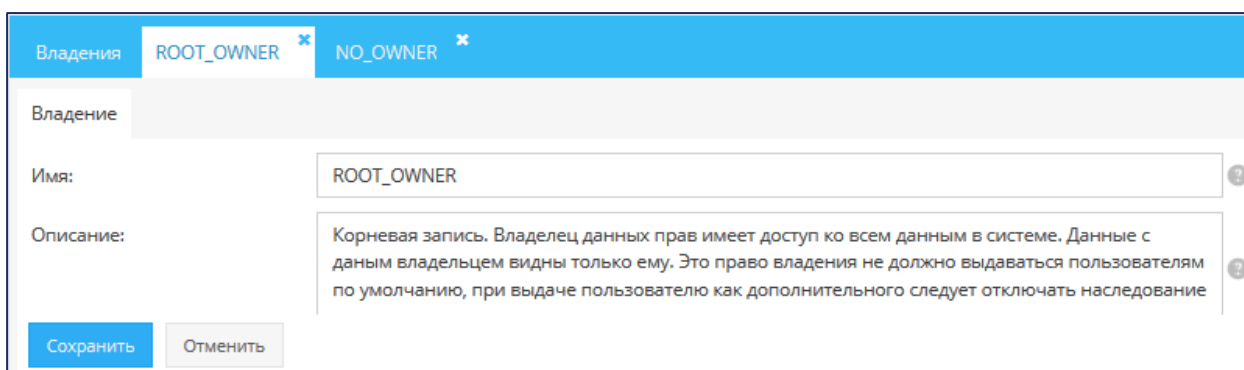


РИС. 51 – Вкладка с экранной формой узла ROOT_OWNER

Атрибуты записи владения описаны в ТАБЛ. 19.

ТАБЛ. 19 – Атрибуты записи владения

АТРИБУТ	ОПИСАНИЕ
Имя	Системное имя владения (далее – <i>имя владения</i>)
Описание	Описание владения

3) Чтобы посмотреть атрибуты записи владения:

- перейдите на вкладку **Владения**;
- дважды щёлкните по строке владения (РИС. 52).

Экранная форма выбранной записи откроется на отдельной вкладке (РИС. 53).

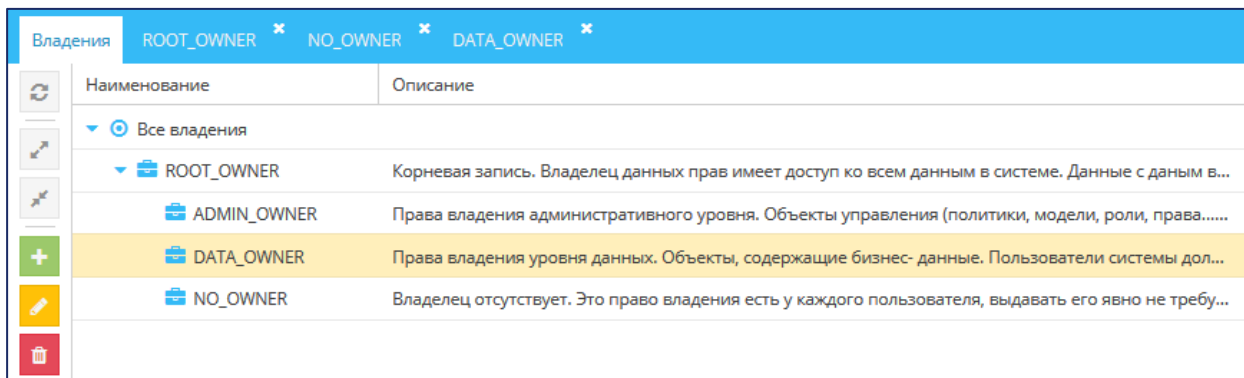


РИС. 52 – Выбор владения DATA_OWNER

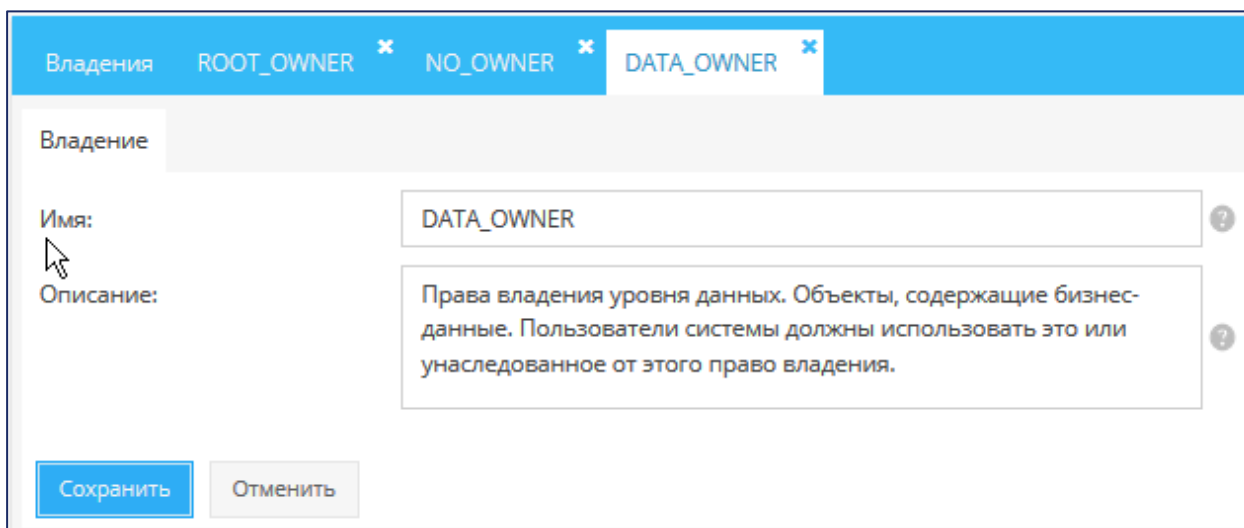


РИС. 53 –Экранная форма владения DATA_OWNER

6.3.3.2 РЕДАКТИРОВАНИЕ АТРИБУТОВ ЗАПИСИ ВЛАДЕНИЯ

Можно отредактировать описание владения. Для этого:


- 1) Откройте экранную форму узла владения и форму владения (см. раздел 6.3.3.1, РИС. 51 и РИС. 53).
- 2) Измените текст в поле **Описание** (ТАБЛ. 19).
- 3) Нажмите кнопку **Сохранить**.

6.3.3.3 ДОБАВЛЕНИЕ ВЛАДЕНИЯ

Администратор **Jet Detective** может добавлять владения в дерево владений.

Предварительно рекомендуется внимательно ознакомиться с общими сведениями о владениях (см. раздел 6.2.4), а также с примерами построения схем владения пользователей (см. раздел Приложение А).

Чтобы добавить владение в дерево владений:


- 1) Перейдите к просмотру дерева владений (см. раздел 6.3.3.1).
- 2) Выберите в дереве родительский узел для создаваемого владения (см. раздел 4.4.5).
- 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**.

6.3.3.4 УДАЛЕНИЕ ВЛАДЕНИЯ ИЗ ДЕРЕВА ВЛАДЕНИЙ

Чтобы удалить владение из дерева:

- 1) Откройте экранную форму дерева владений (см. раздел 6.3.3.1).
- 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 6.2.4) и не назначено пользователям (см. раздел 6.4.5).

6.3.4 Дерево ролей

6.3.4.1 ПРОСМОТР ДЕРЕВА РОЛЕЙ И РОЛИ

Общие сведения о дереве ролей см. в разделе 6.2.3.1.

Чтобы посмотреть дерево ролей:

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

В рабочей области отобразится одна или несколько вкладок:

- дерева ролей (РИС. 54);
- узлов дерева, открытых в этой сессии.

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

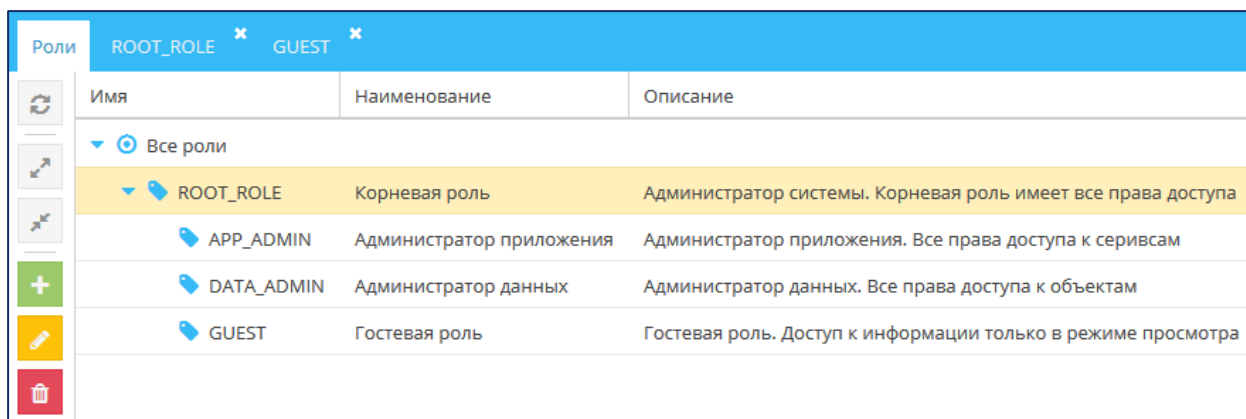


РИС. 54 – Пример дерева ролей

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. РИС. 55, ТАБЛ. 20);
- **Разрешения** – содержит дерево разрешений и инструменты установки разрешений и запретов для роли (см. раздел 6.3.4.5).

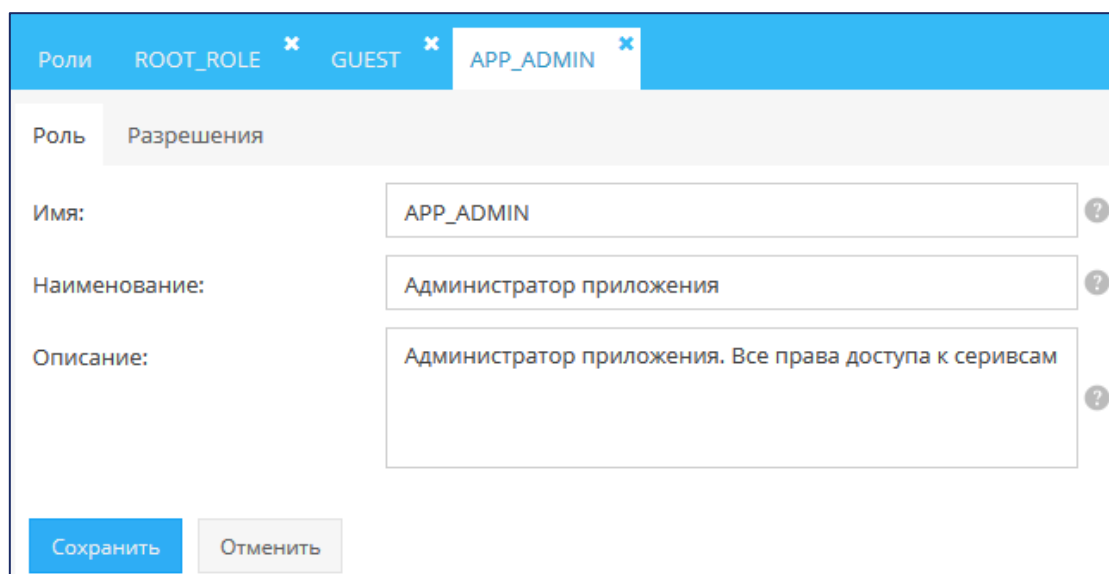
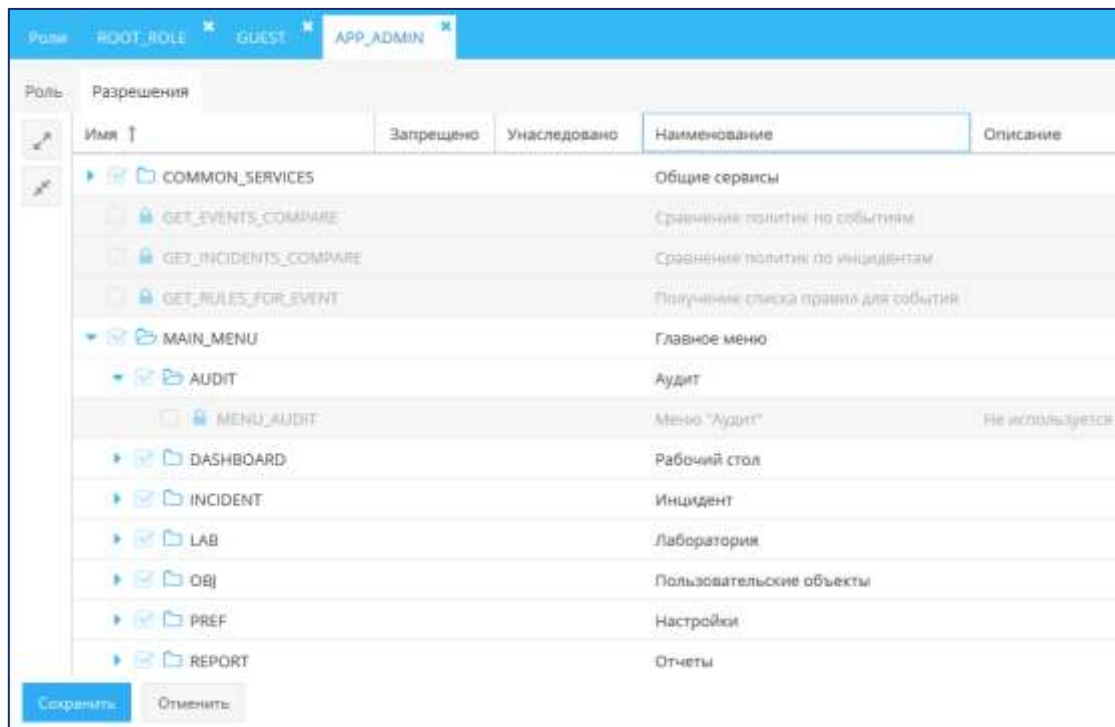
РИС. 55 – Вкладка **Роль**. Пример для APP_ADMIN

ТАБЛ. 20 – Атрибуты роли

АТРИБУТ	ОПИСАНИЕ
Имя	Системное имя роли (далее – <i>имя роли</i>)
Наименование	Название роли
Описание	Описание роли

РИС. 56 – Вкладка **Разрешения**. Пример для APP_ADMIN

6.3.4.2 РЕДАКТИРОВАНИЕ РОЛИ

Можно отредактировать наименование и описание роли. Для этого:

- 1) Откройте экранную форму роли (см. раздел 6.3.4.1, РИС. 55, РИС. 56).
- 2) Измените наименование и описание роли.
- 3) Нажмите кнопку **Сохранить**.

6.3.4.3 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.

6.3.4.4 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 (РИС. 57).
- 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 6.3.4.5).
 - 7) Нажмите кнопку **Сохранить**.

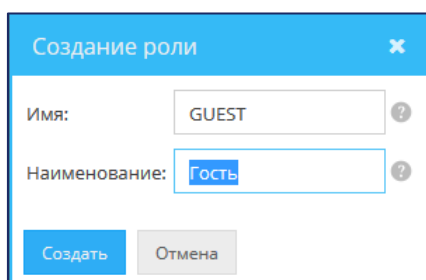
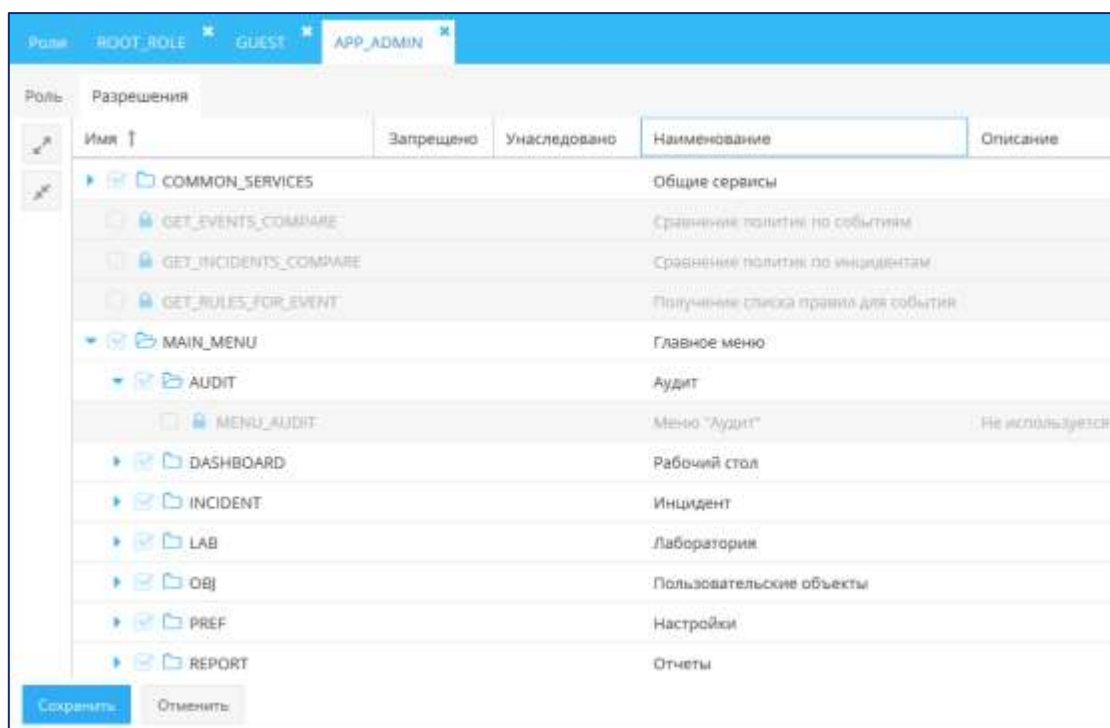


РИС. 57 – Создание роли

6.3.4.5 УСТАНОВКА РАЗРЕШЕНИЙ И ЗАПРЕТОВ ДЛЯ РОЛИ

Для каждой роли можно настроить набор разрешений и запретов. Общие сведения о разрешениях см. в разделе 6.2.2. Общие сведения о запретах см. в разделе 6.2.3.3.

Установка разрешений и запретов выполняется на вкладке **Разрешения** экранной формы роли (РИС. 58, ТАБЛ. 21).

РИС. 58 – Экранная форма роли. Пример вкладки **Разрешения**ТАБЛ. 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
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 (6.3.1).

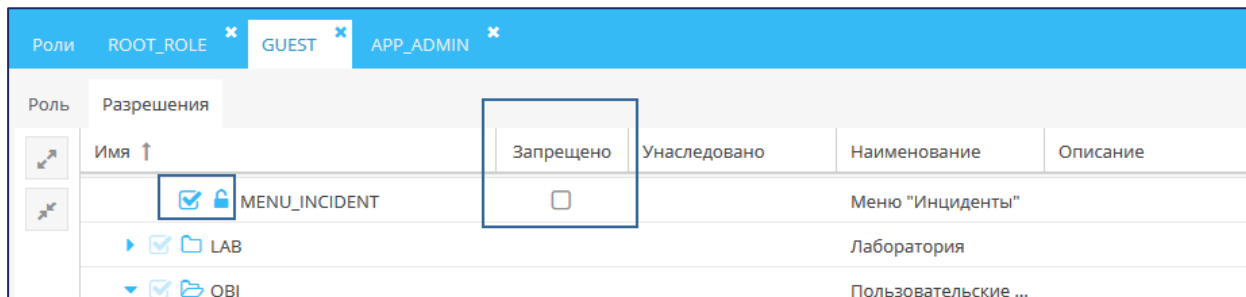
Чтобы установить разрешения и запреты для роли:

- 1) Перейдите на вкладку **Разрешения** (см. РИС. 58).
- 2) Чтобы установить какое-либо разрешение, явно установите флажок в соответствующем узле дерева.
- 3) Чтобы в одно действие установить разрешения во всех дочерних узлах какой-либо папки, явно установите флажок в узле с этой папкой.

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 явно установленными разрешениями имеют индикацию  и флажок в столбце **Запрещено** (РИС. 59).






Роль	Разрешения	Запрещено	Унаследовано	Наименование	Описание
	<input checked="" type="checkbox"/>  MENU_INCIDENT	<input type="checkbox"/>		Меню "Инциденты"	
	<input checked="" type="checkbox"/>  LAB			Лаборатория	
	<input checked="" type="checkbox"/>  OBJ			Пользовательские ...	

РИС. 59 – Поле для установки запрета


- 5) Нажмите кнопку **Сохранить**.

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

6.3.4.6 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 ролей:

- 1) Перейдите к просмотру дерева ролей (см. раздел 6.3.4.1).
- 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.

6.4 УПРАВЛЕНИЕ УЧЁТНЫМИ ЗАПИСЯМИ

6.4.1 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 (РИС. 60):

- списка пользователей

- учётных записей пользователей, открытых в этой сессии.

Имя ↑	Наименование	Заблокирован
guest	Гость	
root	Администратор	

РИС. 60 – Список пользователей

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

Экранная форма учётной записи откроется на отдельной вкладке (РИС. 61). Сведения о пользователе и его правах доступа размещены на нескольких вкладках формы. Краткое описание этих вкладок приведено в ТАБЛ. 22.

ТАБЛ. 22 – Краткое описание вкладок на экранной форме учётной записи пользователя

Вкладка	ОПИСАНИЕ
Пользователь	Общие сведения о пользователе (см. РИС. 60, ТАБЛ. 23)
Роли	Дерево ролей и инструменты для назначения пользователю ролей (см. раздел 6.4.4.2)
Разрешения	Дерево разрешений и инструменты установки для пользователя индивидуальных разрешений и запретов (см. раздел 6.2.3)
Права владения	Дерево владений и инструменты для прикрепления пользователя к дополнительным владениям, настройки областей владения и настройки прав доступа пользователя в каждой из областей владения (см. раздел 6.2.4)

Пользователь | Роли | Разрешения | Права владения

Имя:

Полное наименование:


Владение:

Дополнительные опции: Заблокировать

РИС. 61 – Экранная форма учётной записи. Вкладка **Пользователь**

6.4.2 Создание учётной записи пользователя

Чтобы добавить учётную запись пользователя:

- 1) Выберите пункт меню **Настройки – Доступ – Пользователи**.
- 2) На вкладке **Пользователи** (РИС. 60) нажмите кнопку **Добавить** .
- 3) В открывшемся окне **Создание пользователя** (РИС. 62) заполните поля (см. ТАБЛ. 23).

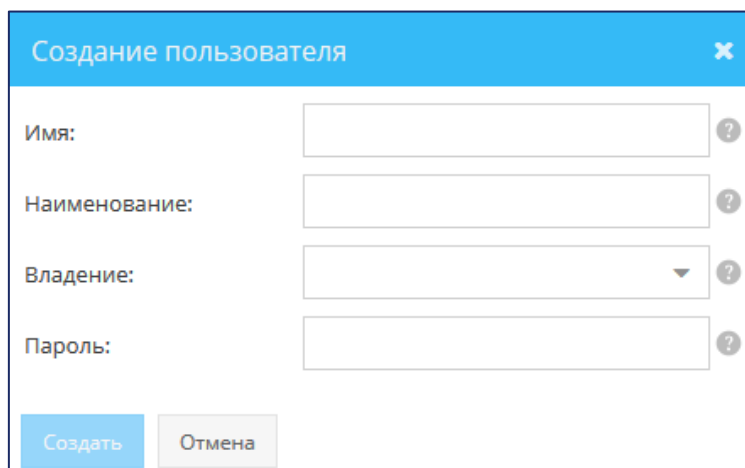


РИС. 62 – Создание учётной записи пользователя

ТАБЛ. 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
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 (РИС. 63).

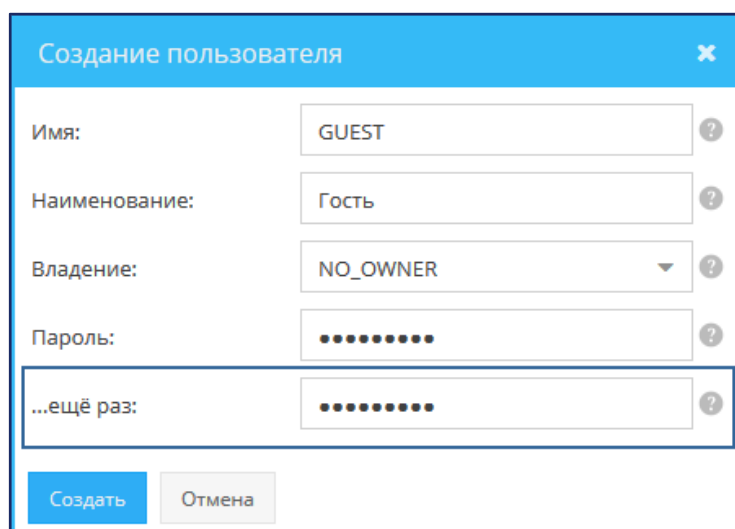


РИС. 63 – Поле для повторного ввода пароля. Пример новой учётной записи

4) Введите пароль повторно.

5) Нажмите кнопку **Создать**.

Экранная форма учётной записи будет открыта на отдельной вкладке (РИС. 64).

6) Нажмите кнопку **Сохранить**.

7) Настройте права доступа пользователя на вкладках **Роли**, **Разрешения**, **Права владения** (см. разделы 6.4.3 – 6.4.5).

РИС. 64 – Новая учётная запись пользователя. Вкладка **user**

6.4.3 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 6.2.3.1);
- если необходимо:
 - добавление в дерево ролей недостающих ролей (см. раздел 6.3.4.4) и установка для них разрешений и запретов (см. раздел 6.3.4.5).
 - установка для пользователя индивидуальных разрешений и запретов (см. раздел 6.4.4.2);

2) Формирование схемы владения пользователя:

- настройка области владения по умолчанию и прав доступа пользователя в области владения по умолчанию (см. раздел 6.4.5.1);
- если необходимо:
 - добавление в дерево владений недостающих владений (см. раздел 6.3.3.2);
 - прикрепление пользователя к дополнительным владениям;
 - настройка области дополнительных владений и прав доступа пользователя в каждой области дополнительных владений (см. раздел 6.4.5.1);
 - смена владения по умолчанию (см. раздел 6.4.5.2).

6.4.4 Формирование набора разрешений пользователя

6.4.4.1 НАЗНАЧЕНИЕ РОЛЕЙ ПОЛЬЗОВАТЕЛЮ

Использование ролей является основным способом установки разрешений для пользователей. Общие сведения о ролях см. в разделе 6.2.3.1.

Назначение ролей выполняется на вкладке **Роли** экранной формы учётной записи пользователя (РИС. 65).

Пользователь	Роли	Разрешения	Права владения
guest	Имя ↑	Наименование	Описание
	<input type="checkbox"/>	ROOT_ROLE	Корневая роль
	<input type="checkbox"/>	APP_ADMIN	Администратор приложения
	<input type="checkbox"/>	DATA_ADMIN	Администратор данных
	<input checked="" type="checkbox"/>	GUEST	Гостевая роль

Сохранить Отменить

РИС. 65 – 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 6.4.1).
- 2) Перейдите на вкладку **Роли** (РИС. 65).
- 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, установив для него индивидуальные разрешения и запреты (см. раздел 6.4.4.2).

6.4.4.2 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 6.2.3.2, общие сведения о запретах – в разделе 6.2.3.3.

Установка индивидуальных разрешений и запретов выполняется на вкладке **Разрешения** экранной формы учётной записи пользователя (РИС. 66).

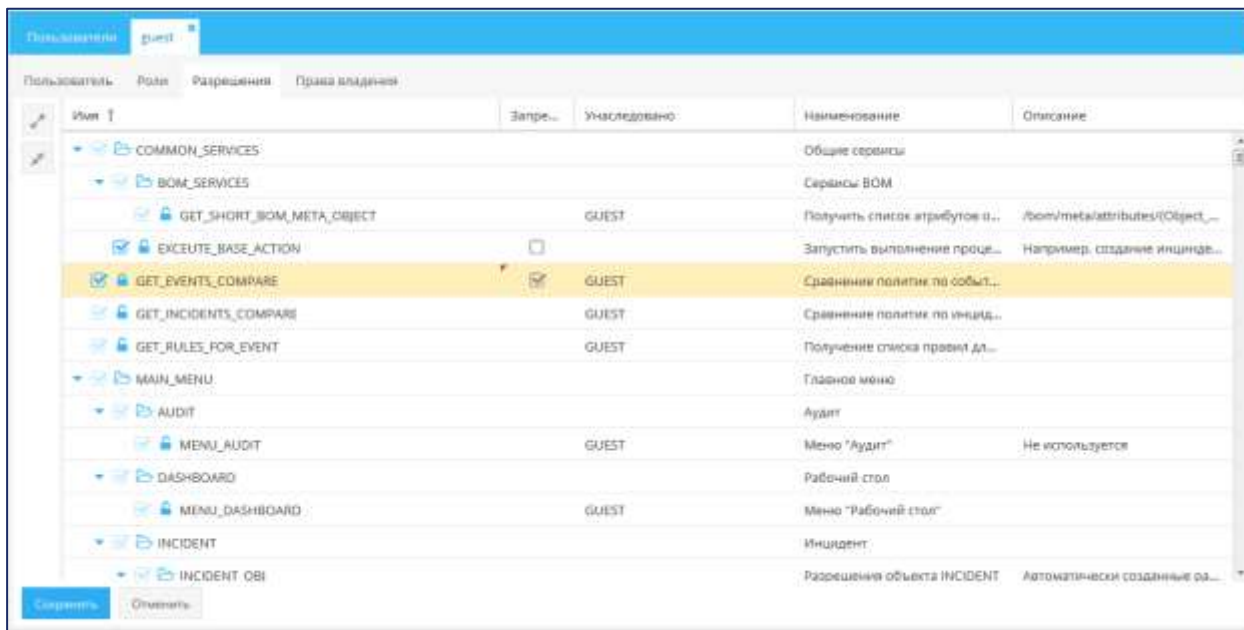



РИС. 66 – Экранная форма учётной записи пользователя. Вкладка **Разрешения**

Чтобы установить индивидуальные разрешения и запреты:

- 1) Откройте экранную форму учётной записи пользователя (см. раздел 6.4.1).
- 2) Перейдите на вкладку **Разрешения** (РИС. 66).
- 3) Чтобы установить одно индивидуальное разрешение, явно установите флажок в соответствующем узле дерева (см. раздел 6.3.1).
- 4) Чтобы установить индивидуальные разрешения сразу во всех дочерних узлах какой-либо папки, явно установите 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 явно установленными 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.

6.4.5 Формирование схемы владения пользователя

6.4.5.1 НАСТРОЙКА ОБЛАСТЕЙ ВЛАДЕНИЯ ПОЛЬЗОВАТЕЛЯ И НАСТРОЙКА ПРАВ ДОСТУПА ПОЛЬЗОВАТЕЛЯ В ОБЛАСТЯХ ВЛАДЕНИЯ

Общие сведения о владениях приведены в разделе 6.2.4. Сведения о том, к какому владению по умолчанию прикреплен пользователь, приведены на вкладке **Права владения** экранной формы учётной записи пользователя (см. РИС. 67).

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** (РИС. 67,

ТАБЛ. 24).

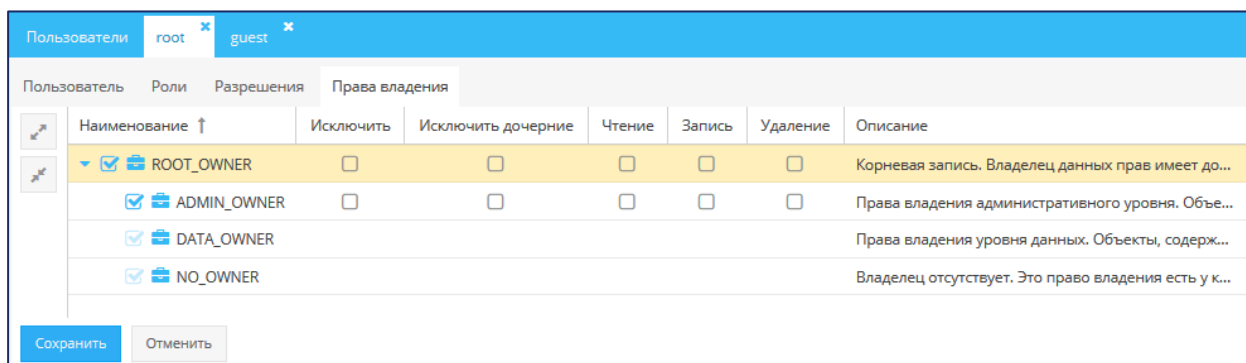


РИС. 67 – Экранная формы учётной записи пользователя. Вкладка **Права владения**

ТАБЛ. 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
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 6.3.1). Возможны следующие варианты:

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. ТАБЛ. 24).
- 4) ТАБЛ. 24).
- 5) Настройте права доступа пользователя в той или иной области владения – установите флажки в столбцах **Чтение, Запись, Удаление**.
- 6) Нажмите кнопку **Сохранить**.

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

6.4.5.2 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 6.4.1).
- 2) На вкладке **Пользователь**, в поле **Владение**, укажите другое владение по умолчанию – выберите значение в раскрывающемся списке (РИС. 68).
- 3) Нажмите кнопку **Сохранить**.

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 6.4.5.1).

The screenshot shows a web interface for user management. At the top, there are tabs for 'root' and 'guest'. Below the tabs, there are four main sections: 'Пользователь', 'Роли', 'Разрешения', and 'Права владения'. The 'Пользователь' section is active, showing fields for 'Имя:' (root), 'Полное наименование:' (Администратор), and 'Владение:' (ADMIN_OWNER). A dropdown menu is open under 'Владение:', showing options: ADMIN_OWNER (selected), ADMIN_OWNER, DATA_OWNER, NO_OWNER, and ROOT_OWNER. At the bottom, there are 'Сохранить' and 'Отменить' buttons.

РИС. 68 – Смена владения по умолчанию

6.4.6 Редактирование учётной записи пользователя

Чтобы отредактировать учётную запись пользователя:

- 1) Выберите пункт меню **Настройки – Доступ – Пользователи**.
- 2) На вкладке со списком пользователей (РИС. 60) дважды щёлкните по строке учётной записи.
- 3) Внесите изменения в поля на всех вкладках экранной формы.
- 4) Нажмите кнопку **Сохранить**.

6.4.7 Блокировка и разблокировка учётной записи пользователя

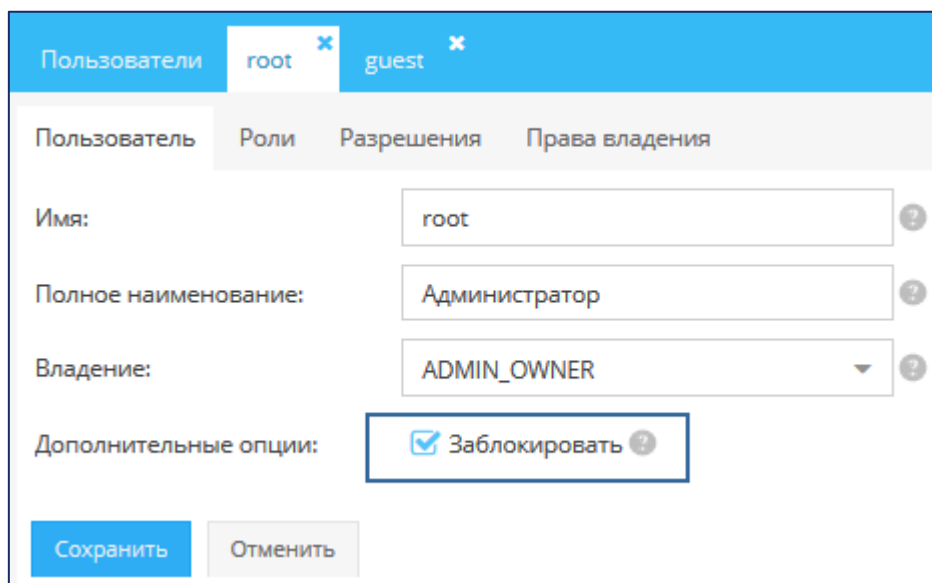
Администратор может заблокировать учётную запись пользователя. Такой пользователь теряет доступ к **Jet Detective** до тех пор, пока администратор не разблокирует его.

Чтобы заблокировать:

- 1) Откройте экранную форму учётной записи пользователя (см. раздел 6.4.1).
- 2) На вкладке **Пользователь** установите флажок **Заблокировать**.
- 3) Нажмите кнопку **Сохранить**.

Чтобы разблокировать:

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



The screenshot shows a web interface for user management. At the top, there are tabs for 'root' and 'guest'. Below this, there are tabs for 'Пользователь', 'Роли', 'Разрешения', and 'Права владения'. The 'Пользователь' tab is active. The form contains the following fields:


- Имя: root
- Полное наименование: Администратор
- Владение: ADMIN_OWNER
- Дополнительные опции: Заблокировать

At the bottom, there are two buttons: 'Сохранить' (Save) and 'Отменить' (Cancel). The 'Заблокировать' checkbox is highlighted with a blue box.

РИС. 69 – Блокировка учётной записи пользователя

6.4.8 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**  (РИС. 70).
- 4) Нажмите кнопку **Да** в появившемся запросе.

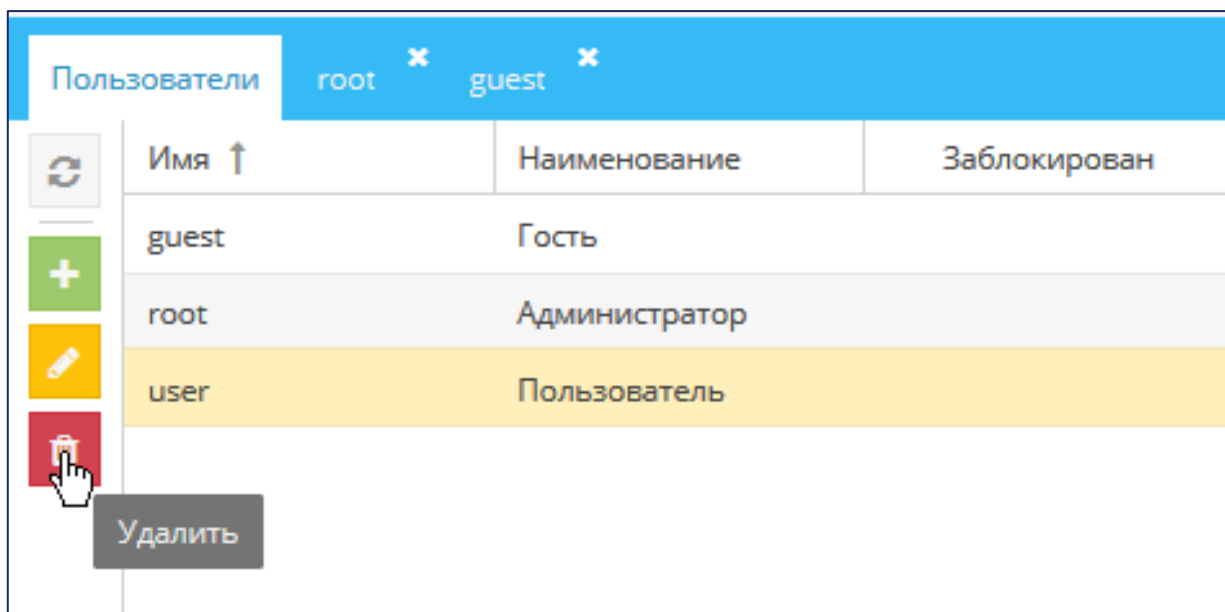


РИС. 70 – Переход к режиму удаления учётной записи пользователя

6.5 СЛУЖЕБНЫЕ СПРАВОЧНИКИ

6.5.1 Настройка списков

6.5.1.1 ПРОСМОТР ЗАПИСИ СПИСКА

Чтобы посмотреть запись в справочнике списков:

- 1) Выберите пункт меню **Настройки – Прочее – Списки**.

В рабочей области отобразится одна или несколько вкладок:

- перечня списков (РИС. 71);
- экранных форм списков, открытых в этой сессии.

- 2) На вкладке с перечнем дважды щёлкните по строке списка.

Экранная форма списка откроется на отдельной вкладке (РИС. 72).

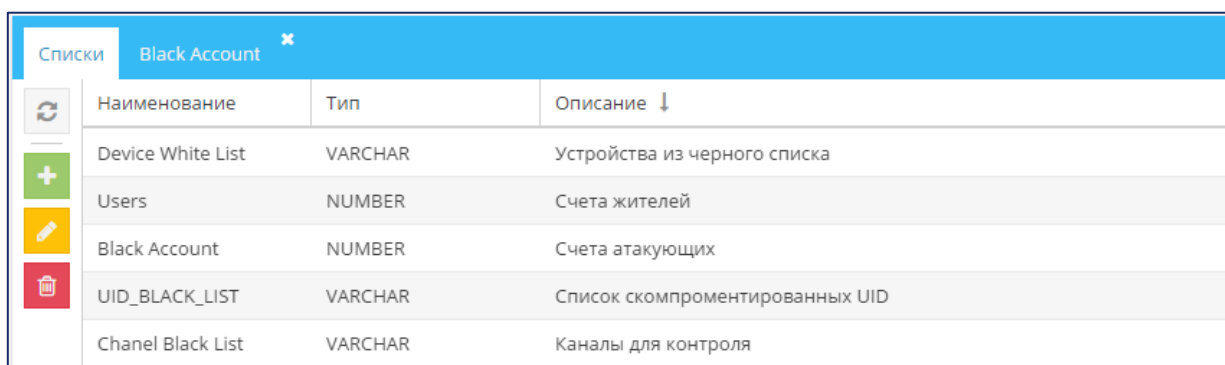


РИС. 71 – Вкладка с перечнем списков

The screenshot shows a web interface for editing a list. The title bar contains 'Списки' and 'Black Account'. The form has the following fields:

- Наименование: Black Account
- Тип: NUMBER
- Размер целой части: 19
- Размер дробной части: 0
- Описание: Счета атакующих

On the right, there is a 'Список значений' (List of values) section with a table:


Значение
104
105
108
85
111
106

At the bottom, there are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

РИС. 72 – Вкладка с экранной формой списка

6.5.1.2 ДОБАВЛЕНИЕ СПИСКА

Чтобы добавить список:

- 1) Откройте справочник **Списки** (см. раздел 6.5.1.1).
- 2) Нажмите кнопку **Добавить**  (см. РИС. 71).

Откроется вкладка **Создание списка**. В правой части находится панель значений списка (РИС. 73).

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

The screenshot shows the 'Создание списка' (Create list) form. The title bar contains 'Списки' and 'Создание списка'. The form has the following fields:

- Наименование: (empty text input)
- Тип: (empty dropdown menu)
- Описание: (empty text area)

On the right, there is a 'Список значений' (List of values) section with a table:

Значение

At the bottom, there are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

РИС. 73 – Вкладка **Создание списка**


6.5.1.3 РЕДАКТИРОВАНИЕ СПИСКА

Чтобы отредактировать запись в справочнике списков:

- 1) Откройте справочник **Списки** (см. раздел 6.5.1.1).
- 2) дважды щёлкните по строке записи списка.

Откроется вкладка выбранной записи (см. РИС. 72). Поля этой вкладки соответствуют атрибутам списка.

- 3) Внесите изменения в поля вкладки.
- 4) Внесите изменения на панели значений списка:
 - а) добавьте значения списка, для этого:


- на панели значений списка нажмите кнопку **Добавить** ;

Отобразится новая строка.

- введите значение в новую строку;
- нажмите кнопку **Применить**.

Добавится новое значение.


- б) удалите значения списка, для этого:

- на панели значений списка выберите строку;
- нажмите кнопку **Удалить** .

- 5) Нажмите кнопку **Сохранить**.

6.5.1.4 УДАЛЕНИЕ СПИСКА

Чтобы удалить запись из справочника:

- 1) Откройте справочник **Списки** (см. раздел 6.5.1.1).
- 2) Выберите запись на вкладке **Списки**.
- 3) Нажмите кнопку **Удалить** .
- 4) Нажмите кнопку **Да** в появившемся запросе.

6.5.2 Настройка глобальных переменных

6.5.2.1 ПРОСМОТР ГЛОБАЛЬНОЙ ПЕРЕМЕННОЙ

Чтобы посмотреть запись в справочнике глобальных переменных:

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

В рабочей области отобразится одна или несколько вкладок:

- списка переменных (РИС. 74);
- экранных форм переменных, открытых в этой сессии.

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

Экранная форма откроется на отдельной вкладке (РИС. 75).



Наименование	Тип	Значение	Описание
Test_gv	VARCHAR	Test_var	-
Test_gv_numb...	NUMBER	155	-
Test_gv_numb...	NUMBER	3	-

РИС. 74 – Вкладка со списком глобальных переменных



Наименование:

Тип:


Значение:

Описание:

РИС. 75 – Вкладка с экранной формой глобальной переменной

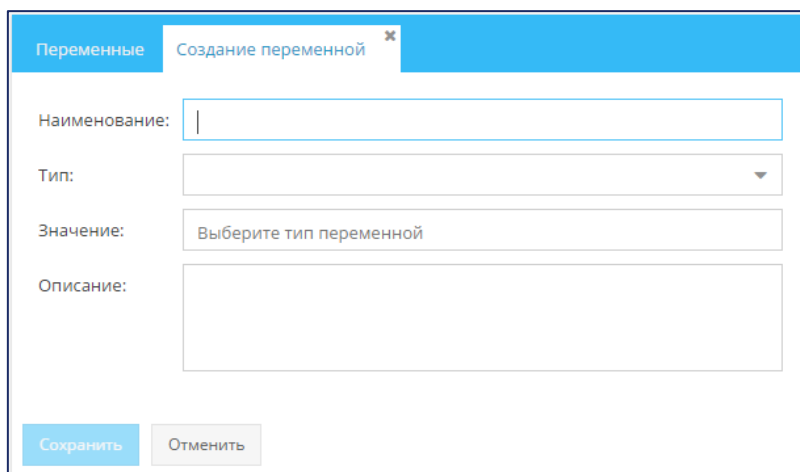
6.5.2.2 ДОБАВЛЕНИЕ ГЛОБАЛЬНОЙ ПЕРЕМЕННОЙ

Чтобы добавить глобальную переменную:

- 1) Откройте справочник **Переменные** (см. раздел 6.5.2.1).
- 2) нажмите кнопку **Добавить**  (см. РИС. 74).

Откроется вкладка **Создание переменной** (РИС. 76).

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



Наименование:

Тип:

Значение:

Описание:

РИС. 76 – Вкладка **Создание переменной**


6.5.2.3 РЕДАКТИРОВАНИЕ ГЛОБАЛЬНОЙ ПЕРЕМЕННОЙ

Чтобы отредактировать запись в справочнике глобальных переменных:

- 1) Откройте справочник **Переменные** (см. раздел 6.5.2.1).
 - 2) дважды щёлкните по строке переменной.
- Откроется вкладка выбранной записи (см. РИС. 75).
- 3) Внесите изменения в поля вкладки.
 - 4) Нажмите кнопку **Сохранить**.

6.5.2.4 УДАЛЕНИЕ ГЛОБАЛЬНОЙ ПЕРЕМЕННОЙ

Чтобы удалить запись из справочника:

- 1) Откройте справочник **Переменные** (см. раздел 6.5.2.1).
- 2) Выберите запись на вкладке **Переменные** (см. РИС. 74).
- 3) Нажмите кнопку **Удалить** .
- 4) Нажмите кнопку **Да** в появившемся запросе.

7. НАСТРОЙКА МЕХАНИЗМОВ ВЫЯВЛЕНИЯ АНОМАЛИЙ

7.1 НАСТРОЙКА ПРАВИЛ 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 аналитика¹ относится настройка этих правил² и политик³.

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;
- правило машинного обучения.

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*.

Правило машинного обучения представляет собой прогнозную модель, которая предназначена для выявления как известных, так и потенциальных аномалий. Правило машинного обучения составляется в отношении того или иного объекта с типом **Событие**. По аналогии с экспертными правилами, результатом применения правила машинного обучения к тому или иному событию является логическое значение ИСТИНА или ЛОЖЬ.

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. Для каждой строки матрицы определяют автоматические действия, которые должны быть выполнены, например:

- создать инцидент;
- информировать пользователей;

¹ Требования к уровню подготовки пользователей в разделе 1.3.

² См. раздел 7.1.2.

³ См. раздел 7.1.3.

- сформировать ответ во внешнюю информационную систему, являющуюся источником событий;
- выполнить программный сценарий и т. д.

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.

Чтобы посмотреть список групп правил:

- 1) Выберите пункт меню **Лаборатория – Политики – Правила выявления**.

В рабочей области отобразится одна или несколько вкладок:

- список групп правил (РИС. 77);
 - правил выявления, открытых в этой сессии.
- 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 .

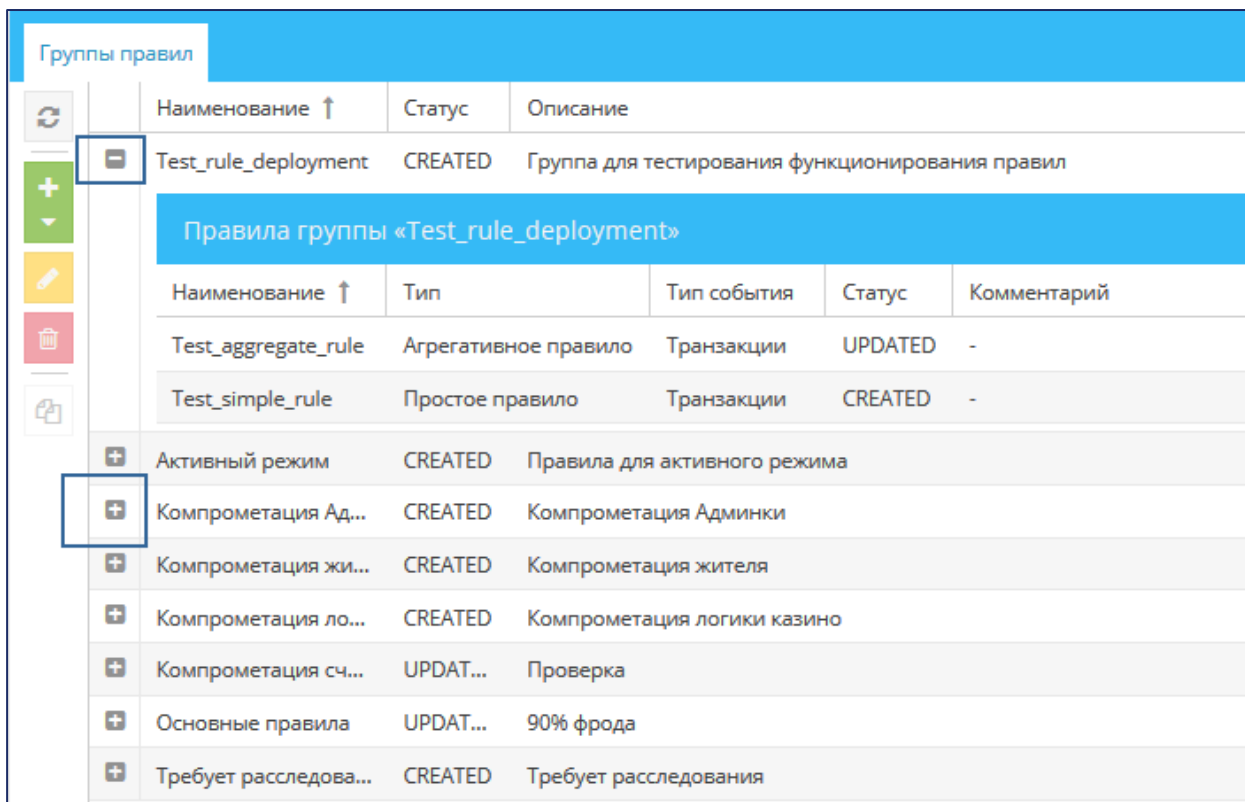


РИС. 77 – Вкладка со списком групп правил

Чтобы создать группу правил:

- 1) На вкладке со списком нажмите кнопку **Добавить**  и в раскрывшемся меню выберите пункт **Группа правил** (РИС. 78).

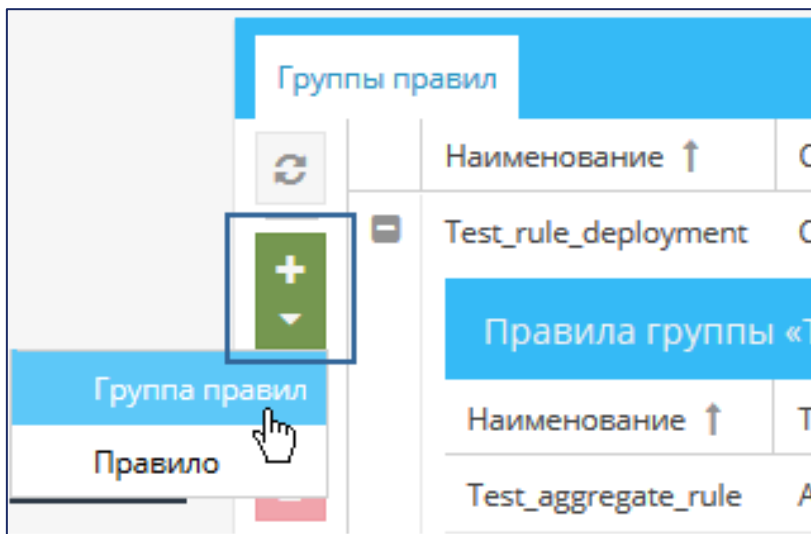


РИС. 78 – Переход к режиму создания группы правил

- 2) В открывшемся окне укажите наименование и описание группы (РИС. 79).
- 3) Нажмите кнопку **Сохранить**.

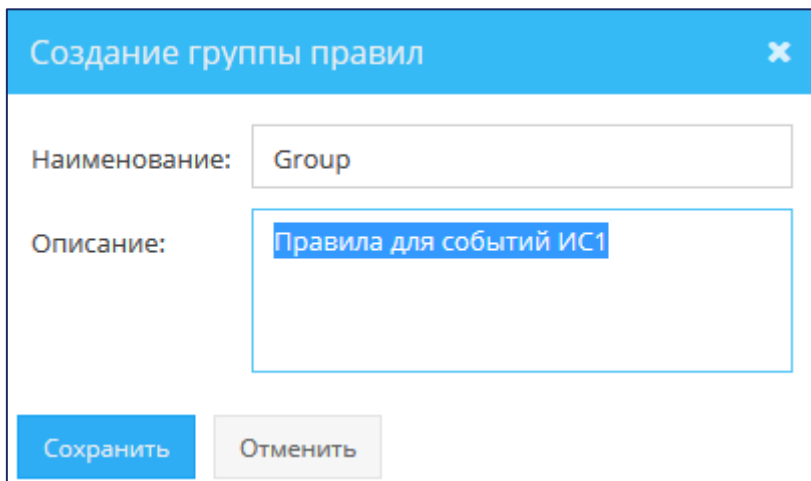


РИС. 79 – Создание группы правил

Чтобы отредактировать свойства группы правил:

- 1) На вкладке со списком выберите группу правил (см. РИС. 77).
- 2) Дважды щёлкните по строке группы.
- 3) В открывшемся окне внесите изменения в свойства группы (см. РИС. 79).
- 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.

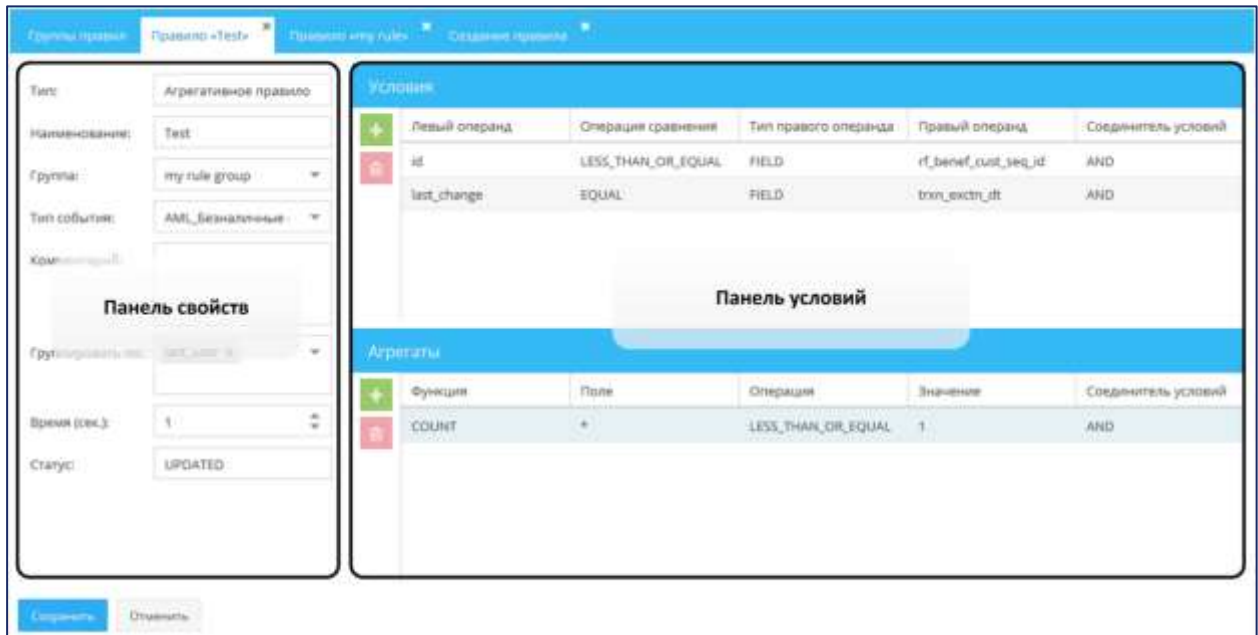


РИС. 80 – Экранная форма агрегативного правила выявления

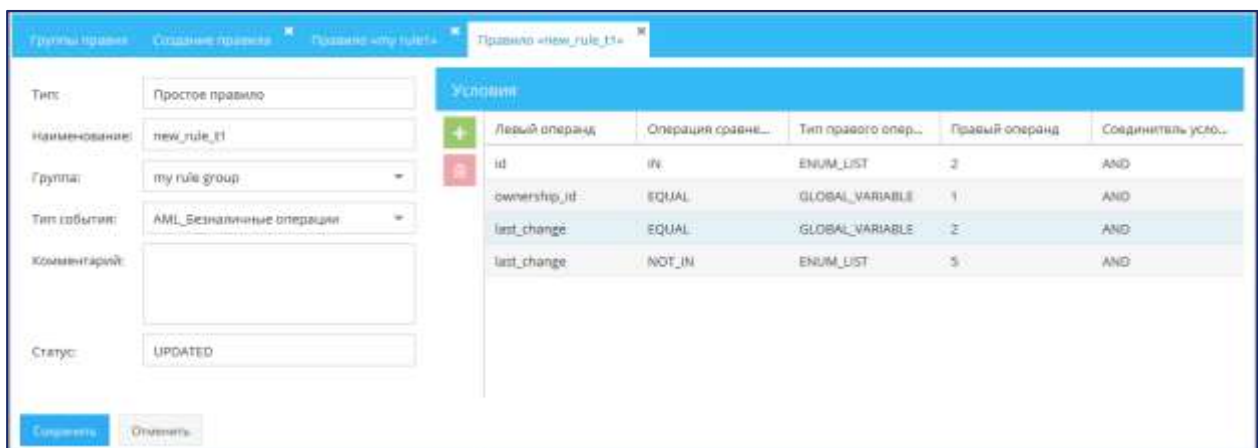


РИС. 81 – Экранная форма простого правила выявления

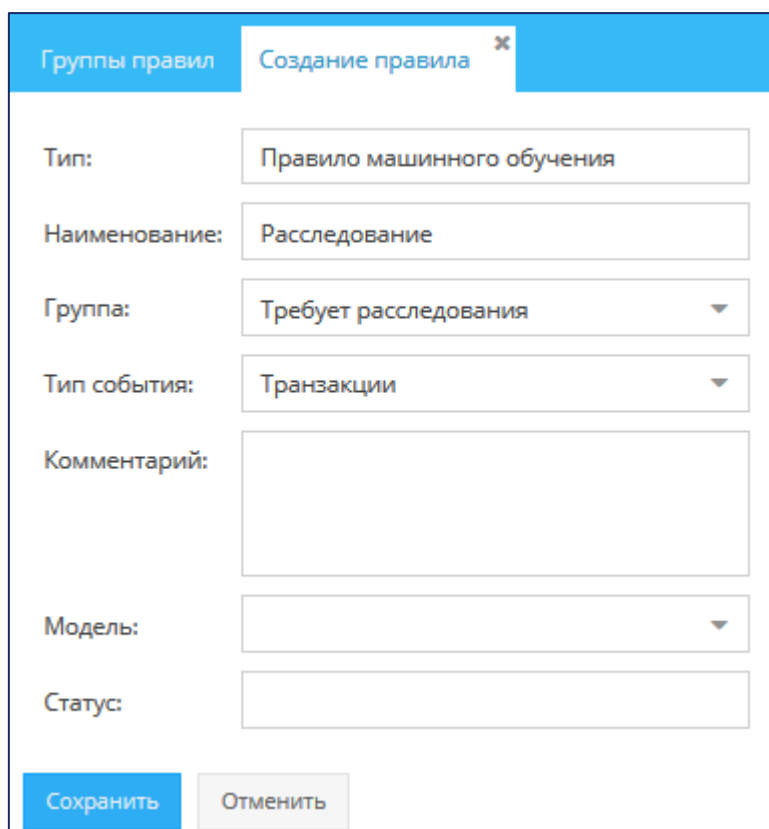


РИС. 82 – Экранная форма правила машинного обучения

У экранных форм всех типов правил есть *панель* свойств правил выявления. Для простого и агрегативного правила панель свойств отображается в левой части экранной формы (РИС. 81, РИС. 80). Экранная форма правила машинного обучения состоит только из панели свойств (РИС. 82).

В ТАБЛ. 25 описаны свойства, которые имеются у всех типов правил выявления. Специфические свойства каждого типа правил описаны ниже в разделах 7.1.2.4, 7.1.2.5, 7.1.2.6.

ТАБЛ. 25 – Поля правила выявления

Поле	ОПИСАНИЕ
Тип	Тип правила выявления
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)
Комментарий	Комментарий
Статус	Статус правила выявления в Jet Detective : <ul style="list-style-type: none"> • CREATED – правило создано; • UPDATED – правило изменено; • DELETED – правило удалено

В правой части экранной формы простого или агрегативного правила располагается *панель условий*. Для простого правила (РИС. 80) на панели условий составляют условия, выполнение которых будет проверяться при анализе входящего потока данных.

Панель условий агрегативного правила состоит из двух разделов (РИС. 81):

- **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 **Создать**  и в раскрывшемся меню выберите пункт **Правило**.
- 3) В открывшемся окне (РИС. 83) заполните поля **Тип** и **Тип события** (см. ТАБЛ. 25).

РИС. 83 – Создание правила выявления. Раскрывающиеся списки полей **Тип** и **Тип события**

- 4) Нажмите кнопку **Далее**.

Экранная форма правила откроется на отдельной вкладке (РИС. 80–РИС. 82).


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 7.1.2.4–7.1.2.6).
- 6) Нажмите кнопку **Сохранить**.

Примечания:

1. Простое правило можно сохранить только после добавления хотя бы одного условия.
2. Агрегативное правило можно сохранить только после добавления хотя бы одного условия в разделах **Условия** и **Агрегаты** на панели условий.
3. Правило машинного обучения можно сохранить, только если для него указана модель обучения.

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 7.1.2.4–7.1.2.6).
- 7) Нажмите кнопку **Сохранить**.

7.1.2.4 НАСТРОЙКА ПРОСТОГО ПРАВИЛА

Простое правило представляет собой набор условий, которые при анализе применяются к данным экземпляра объекта – к конкретному событию. Условия 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.

При настройке простого правила на панели свойств (РИС. 84) вручную указывают его свойства (см. ТАБЛ. 25), кроме типа и статуса правила.

РИС. 84 – Экранная форма простого правила выявления

Чтобы добавить в правило выявления условие и настроить его:


- 1) На панели условий нажмите кнопку **Добавить** . В список условий добавится пустая строка (РИС. 85).
- 2) В столбце **Левый операнд** укажите левый операнд условия – выберите атрибут события. При составлении условия левый операнд указывают всегда.

РИС. 85 – Строка для составления нового условия в разделе **Условия**

- 3) В столбце **Операция сравнения** укажите операцию – выберите значение в раскрывающемся списке:
 - условие может представлять собой операцию сравнения значения атрибута события – левого операнда (ТАБЛ. 26):
 - со значением другого атрибута события или с константой, или со значением глобальной переменной в качестве правого операнда;
 - со значениями из списка в качестве правого операнда;
 - с «пустым значением». Это унарная операция, которая не требует правого операнда.
 - в условии могут использоваться функции поиска по строковым данным (ТАБЛ. 27).
- 4) В столбце **Тип правого операнда** укажите тип правого операнда – выберите значение в раскрывающемся списке:
 - FIELD – атрибут события;
 - CONSTANT – константа;
 - GLOBAL_VARIABLE – глобальная переменная. О ведении справочника глобальных переменных см. в разделе 6.5.2;
 - ENUM_LIST – список. Ведение списков описано в разделе 6.5.1.

Примечание. В раскрывающемся списке отображаются только те типы правого операнда, которые совместимы с выбранной операцией сравнения (функцией поиска).

- 5) Если это требуется для используемой операции сравнения (функции поиска), в столбце **Правый операнд** укажите значение правого операнда. Значение константы указывают вручную, значения операнда другого типа выбирают в раскрывающемся списке. Типы данных у значений левого и правого операнда должны быть одинаковыми.
- 6) Чтобы завершить редактирование, нажмите кнопку **Применить** (находится над строкой, РИС. 86).

РИС. 86 – Условие, составленное в разделе **Условия**

- 7) Добавьте другие условия, если требуется.
- 8) Если правило содержит более одного условия, то в столбце **Соединитель условий** настройте логические операторы – выберите значения в раскрывающихся списках.
- 9) Нажмите кнопку **Сохранить**.

ТАБЛ. 26 – 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			
LESS_THAN_OR_EQUAL	Меньше или равно	Строковый, числовой, дата-время	event_attr LESS_THAN_OR_EQUAL 10
LESS_THAN	Меньше	Строковый, числовой, дата-время	event_attr LESS_THAN 10
EQUAL	Равно	Строковый, числовой, дата-время, логический	event_attr EQUAL 10
NOT_EQUAL	Не равно	Строковый, числовой, дата-время, логический	event_attr NOT_EQUAL 10
GREATER_THAN	Больше	Строковый, числовой, дата-время	event_attr GREATER_THAN 10
GREATER_THAN_OR_EQUAL	Больше или равно	Строковый, числовой, дата-время	event_attr GREATER_THAN_OR_EQUAL 10
СРАВНЕНИЕ ЗНАЧЕНИЯ АТРИБУТА СОБЫТИЯ СО ЗНАЧЕНИЯМИ ИЗ СПИСКА			
IN	Значение атрибута события входит в список	Строковый, числовой, дата-время	event_attr IN enum_list
NOT_IN	Значение атрибута не входит в список	Строковый, числовой, дата-время	event_attr NOT_IN enum_list

ОПЕРАЦИЯ	ОПИСАНИЕ	Типы данных, для которых применима операция	ПРИМЕР
СРАВНЕНИЕ ЗНАЧЕНИЯ АТТРИБУТА СОБЫТИЯ С «ПУСТЫМ ЗНАЧЕНИЕМ»			
IS_NULL	Значение атрибута «пустое значение»	Строковый, числовой, дата-время, логический	event_attr IS_NULL
IS_NOT_NULL	Значение атрибута не «пустое значение»	Строковый, числовой, дата-время, логический	event_attr IS_NOT_NULL

ТАБЛ. 27 – Справочные сведения о функциях поиска по строковым данным

Функция	ОПИСАНИЕ	Тип данных, для которого применима операция	ПРИМЕР
INSTR	Возвращает логическое значение ИСТИНА, если в любом месте строки левого операнда найдена подстрока, указанная в правом операнде	Строковый	event_attr INSTR 'перевод'
ENDS	Возвращает логическое значение ИСТИНА, если строка левого операнда заканчивается подстрокой, указанной в правом операнде	Строковый	event_attr ENDS 'перевод'
BEGINS	Возвращает логическое значение ИСТИНА, если строка левого операнда начинается с подстроки, указанной в правом операнде	Строковый	event_attr BEGINS 'перевод'
RE_INSTR	Возвращает логическое значение ИСТИНА, если в любом месте строки правого операнда найдена подстрока, указанная в левом операнде	Строковый	event_attr RE_INSTR 'акция промоакция'
RE_ENDS	Возвращает логическое значение ИСТИНА, если строка правого операнда заканчивается подстрокой, указанной в левом операнде	Строковый	event_attr RE_ENDS 'акция промоакция'
RE_BEGINS	Возвращает логическое значение ИСТИНА, если строка правого операнда начинается с подстроки, указанной в левом операнде	Строковый	event_attr RE_BEGINS ' 'акция промоакция'

7.1.2.5 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, а данные отобранных экземпляров группируются и агрегируются. 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 ТАБЛ. 28.

ТАБЛ. 28 – Общий порядок настройки агрегативного правила

№	Шаг	ОПИСАНИЕ
1.	Настройка основных свойств правила	При создании агрегативного правила, на панели свойств (РИС. 87) вручную указывают его основные свойства (см. ТАБЛ. 25), 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 . 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 поле Время (сек)
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 7.1.2.4)
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 . Описание действий приведено ниже в этом разделе

Скриншот экрана конфигурации агрегативного правила. Интерфейс разделен на две основные части: панель свойств и панель условий/агрегатов.

Панель свойств (слева):

- Тип: Агрегативное правило
- Наименование: Test_aggregate_rule
- Группа: Test_rule_deployment
- Тип события: Транзакции
- Комментарий: -
- Группировать по: source
- Время (сек.): 36000
- Статус: UPDATED

Панель условий (Условия):

Левый операнд	Операция сравнения	Тип правого операнда	Правый операнд	Соединитель условий
last_change	IS_NOT_NULL			AND

Панель агрегатов (Агрегаты):

Функция	Поле	Операция	Тип значения	Значение	Соединитель условий
COUNT	*	GREATER_THAN	GLOBAL_VARIABLE_ONLINE	Test_gv_number2	AND

В нижней части экрана расположены кнопки «Сохранить» и «Отменить».

РИС. 87 – Экранная форма агрегативного правила выявления

На панели условий, в разделе **Агрегаты**, настраивают функции агрегации данных и составляют условия, выполнение которых проверяется по отношению к агрегированным данным.

Чтобы добавить в раздел **Агрегаты** условие и настроить его:

- 1) На панели условий, в разделе **Агрегаты**, нажмите кнопку **Добавить** .

В список условий добавится пустая строка (РИС. 88).

- 2) В столбце **Функция** укажите вид агрегации – выберите значение в раскрывающемся списке:

- COUNT – подсчитать количество;
- AVG – вычислить среднее значение;
- SUM – вычислить суммарное значение;
- MAX – найти максимальное значение;
- MIN – найти минимальное значение.

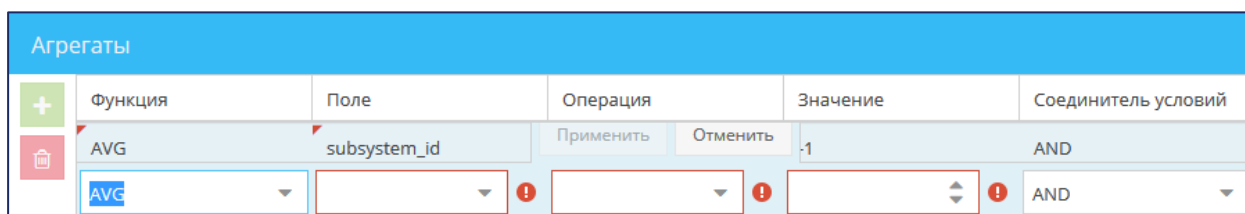


РИС. 88 – Строка для составления нового условия в разделе **Агрегаты**

- 3) В столбце **Поле** укажите левый операнд в операции сравнения – выберите значение в раскрывающемся списке. В качестве левого операнда используется атрибут события. При составлении условия левый операнд указывают для всех функций, кроме COUNT.
- 4) В столбце **Операция** укажите операцию сравнения – выберите значение в раскрывающемся списке (ТАБЛ. 29). Операция имеет сходство с HAVING, применяемой в SQL.
- 5) В столбце **Значение** укажите значение правого операнда. Правый операнд является константой числового типа.
- 6) Чтобы завершить редактирование, нажмите кнопку **Применить** (находится над строкой с условием, РИС. 89).

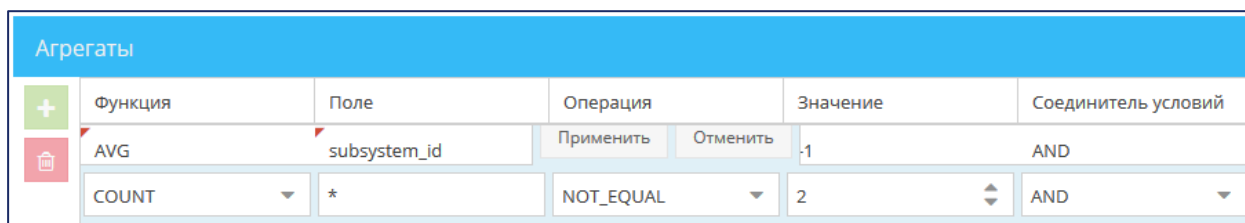


РИС. 89 – Условие, составленное в разделе **Агрегаты**

- 7) Добавьте другие правила, если требуется.
- 8) Если правило содержит более одного условия, то в столбце **Соединитель условий** настройте логические операторы – выберите значения в раскрывающихся списках.
- 9) Нажмите кнопку **Сохранить**.

ТАБЛ. 29 – Справочные сведения об операциях сравнения в агрегативном правиле

ОПЕРАЦИЯ	ОПИСАНИЕ
LESS_THAN_OR_EQUAL	Меньше или равно
LESS_THAN	Меньше
EQUAL	Равно
GREATER_THAN	Больше
GREATER_THAN_OR_EQUAL	Больше или равно

7.1.2.6 НАСТРОЙКА ПРАВИЛА МАШИННОГО ОБУЧЕНИЯ

Правило машинного обучения представляет собой прогнозную модель, которая при анализе применяется к данным экземпляра объекта, а именно, конкретного события. Результатом применения правила машинного обучения к тому или иному событию является логическое значение ИСТИНА или ЛОЖЬ.

При настройке правила машинного обучения на панели свойств (РИС. 90) вручную указывают его основные свойства (см. ТАБЛ. 25), кроме типа и статуса правила.

РИС. 90 – Экранная форма правила машинного обучения

Чтобы указать модель машинного обучения:

- 1) На панели свойств заполните поле **Модель** – выберите значение в раскрывающемся списке. В списке отображаются названия моделей, которые администратор создал в **Jet Detective** (см. раздел 7.2).
- 2) Нажмите кнопку **Сохранить**.

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 7.1.2.4–7.1.2.6, в зависимости от типа правила).
- 4) Нажмите кнопку **Сохранить**.

7.1.2.8 УДАЛЕНИЕ ГРУППЫ ПРАВИЛ ИЛИ ПРАВИЛА


Примечания:

1. Группу правил можно удалить, если в ней нет ни одного правила выявления, которое используется в политиках выявления.
2. 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.

7.1.3 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 7.1.3.5).

Чтобы посмотреть и отредактировать политику выявления:

1) Выберите пункт меню **Лаборатория – Политики – Настройка политик**.

В рабочей области отобразится одна или несколько вкладок:

- списка политик;
- экранных форм политик, открытых в этой сессии.

2) На вкладке со списком политик дважды щёлкните по строке политики.

Экранная форма политики откроется на отдельной вкладке (РИС. 91). В верхней части экранной формы отображаются свойства политики (ТАБЛ. 30). В нижней части отображается матрица срабатывания и инструменты для ее настройки.

Наименование: Test_deploymnet_policy

Описание: Политика для тестирования работоспособности СЕР

Сервер движка: Test engine

Правила: Test_simple_rule

Статус: UNDEPLOYED

Матрица срабатывания	
+	Наименование
	MR

Порядок срабатывания правил: Test_simple_rule

Сохранить Отменить

РИС. 91 – Экранная форма политики выявления

ТАБЛ. 30 – Поля политики выявления

Поле	ОПИСАНИЕ
Наименование	Уникальное название политики
Описание	Описание политики
Обработчик событий	Наименование экземпляра обработчика событий, который будет применять правила политики выявления к событиям. Наличие нескольких экземпляров обработчика событий позволяет организовать параллельную обработку событий
Правила	Перечень правил выявления, включенных в политику
Статус	CREATED – новая политика DEPLOYED – политика запущена UNDEPLOYED – политика остановлена

3) Чтобы посмотреть сведения о настройке строки матрицы срабатывания, в разделе **Матрица срабатывания** дважды щёлкните по строке.

Откроется окно **Строка матрицы срабатывания <наименование строки>** (РИС. 92). Окно состоит из двух вкладок:

- **Общие сведения** – содержит общие сведения о строке матрицы. В верхней части вкладки отображаются свойства строки (ТАБЛ. 31). Раздел **Действия** содержит инструменты для настройки перечня автоматических действий, которые должны быть выполнены в случае срабатывания строки;
 - **Порядок срабатывания правил** – содержит инструменты для настройки порядка срабатывания правил и настройки связей между событиями правил (см. раздел 7.1.3.3).
- 4) Внесите изменения в свойства политики.
- 5) Внесите изменения в матрицу срабатывания (см. раздел 7.1.3.3).
- 6) Нажмите кнопку **Сохранить**.

Наименование	Путь
Логирование возникновения фрода	/opt/afs/apache-tomcat-8.5.8/conf/cep-coordinator/scripts/SampleAction.groovy
Отправка почтового сообщения	/opt/afs/apache-tomcat-8.5.8/conf/cep-coordinator/scripts/SendMailAction.groovy
Создание инцидента по сработавшей строке ма...	/opt/afs/apache-tomcat-8.5.8/conf/cip-coordinator/scripts/CreateIncidentAction.groovy


РИС. 92 – Окно **Строка матрицы срабатывания**

ТАБЛ. 31 – Поля строк в матрице срабатывания

Поле	Описание
Наименование	Название строки
Описание	Описание строки
Интервал (сек)	<p>У каждого события имеется атрибут, в котором хранится время поступления события в Jet Detective. События связаны с правилами. Для строки матрицы срабатывания настраивают продолжительность интервала времени, предшествующего времени поступления события, которое связано с последним по порядку правилом (указано в строке матрицы срабатывания).</p> <p>Строка матрицы считается сработавшей, если:</p> <ul style="list-style-type: none"> сработали все указанные в строке матрицы правила; события правил появляются в указанной последовательности; все события, указанные в строке матрицы правил, находятся в указанном интервале

7.1.3.2 СОЗДАНИЕ ПОЛИТИКИ

Чтобы создать политику выявления:

- 1) Выберите пункт меню **Лаборатория – Политики – Настройка политик**.
- 2) На вкладке **Политики** нажмите кнопку **Создать** .

Экранная форма политики откроется на отдельной вкладке (РИС. 91).

- 3) Укажите свойства политики (см. ТАБЛ. 30), кроме ее статуса;
- 4) В поле **Правила** укажите все правила выявления, которые следует включить в политику – выберите их наименования в раскрывающемся списке.
- 5) Настройте матрицу срабатывания (см. раздел 7.1.3.3).
- 6) Нажмите кнопку **Сохранить**.

Политика выявления начнет применяться к входящему потоку данных после её запуска (см. раздел 7.1.3.4).

7.1.3.3 НАСТРОЙКА МАТРИЦЫ СРАБАТЫВАНИЯ

Настройка матрицы срабатывания заключается в добавлении одной или несколько строк. Политика выявления считается сработавшей, если в результате применения правил выявления сработала хотя бы одна строка матрицы срабатывания.

Для каждой строки настраивают:


- интервал времени (см. ТАБЛ. 31);
- перечень автоматических действий, которые должны быть выполнены в случае срабатывания строки матрицы;
- набор правил (из числа правил, включенных в политику выявления) и порядок их срабатывания;
- связи между правилами.

Строка матрицы считается сработавшей, если:

- сработали все указанные в строке матрицы правила;

- события правил появляются в указанной последовательности;
- все события, указанные в строке матрицы правил, располагаются в указанном интервале.

Чтобы добавить строку в матрицу срабатывания и настроить ее:

- 1) В экранной форме политики выявления, в разделе **Матрица срабатывания**, нажмите кнопку **Добавить**  (РИС. 91).

Откроется окно **Строка матрицы срабатывания**.

- 2) На вкладке **Общие сведения** укажите свойства строки (см. ТАБЛ. 31).

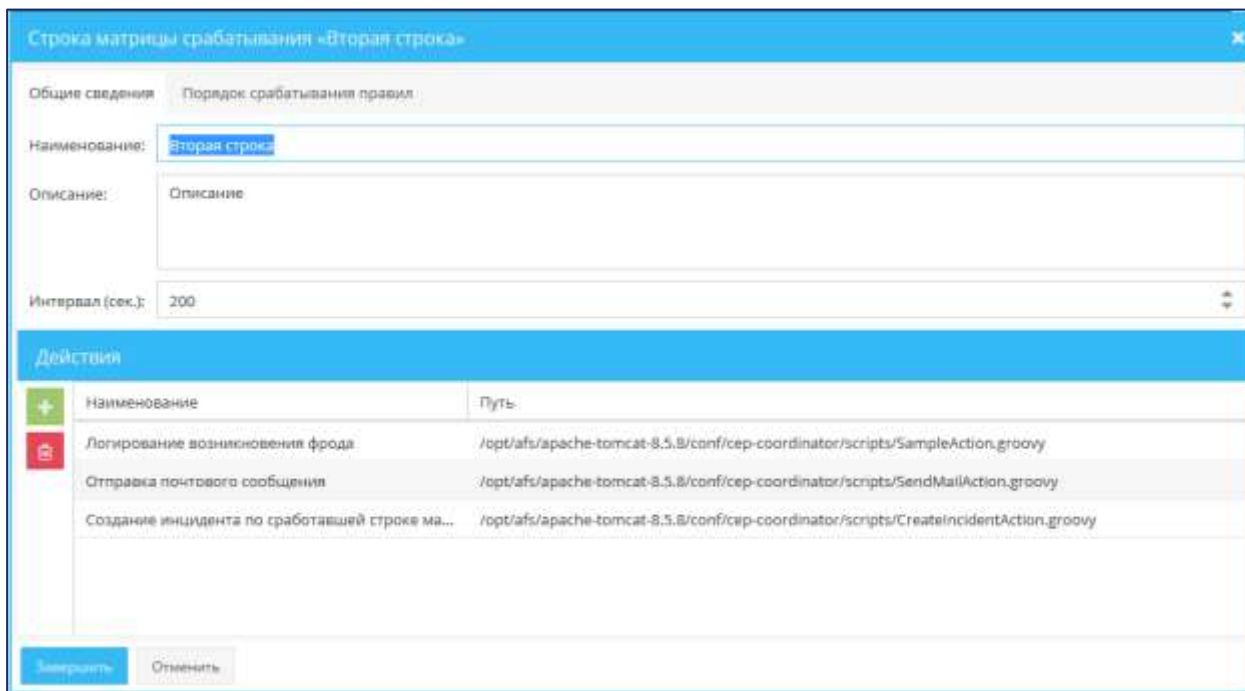



РИС. 93 – Окно **Строка матрицы срабатывания**

- 3) Чтобы настроить перечень автоматических действий, которые должны быть выполнены в случае срабатывания строки, в разделе **Действия** нажмите кнопку **Добавить** .
- 4) На раскрывшейся панели установите флажки рядом с наименованиями действий.

В результате установки того или иного флажка, в раздел **Действия** добавится строка с настройкой действия (РИС. 94).

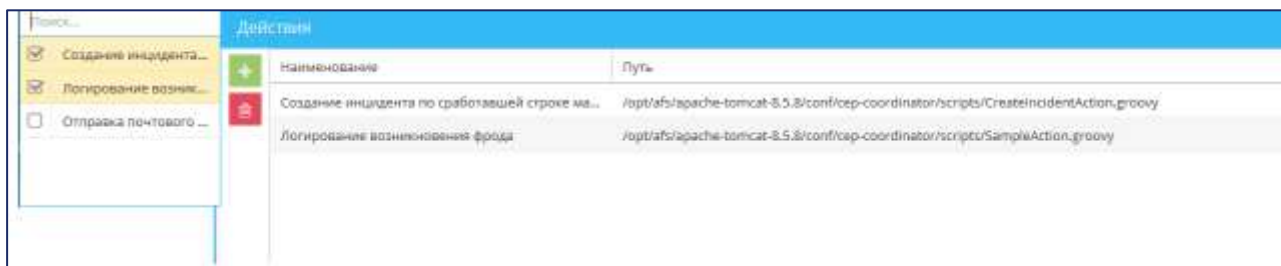


РИС. 94 – Настройка перечня автоматических действий

5) Перейдите на вкладку **Порядок срабатывания правил**.

Вкладка состоит из двух панелей:

- **Правила** – содержит инструменты для настройки порядка срабатывания правил;
- **Связи правила <наименование правила>** – содержит инструменты для настройки связывания правил.


6) Чтобы для строки матрицы настроить набор (перечень) правил и порядок их срабатывания, добавьте правила на панель **Правила** в том порядке, в котором они должны применяться:

- на панели **Правила** нажмите кнопку **Добавить** .

В перечень добавится пустая строка (РИС. 95);

- в столбце **Правило** выберите правило выявления в раскрывающемся списке. В списке отображаются названия только тех правил, которые включены в политику выявления и еще не добавлены в перечень;

5) Нажмите кнопку **Применить** (находится над или под позицией) (РИС. 96).

6) Чтобы удалить позицию, выберите ее в перечне и нажмите кнопку **Удалить** .

Можно удалить только позицию, которая была добавлена последней.

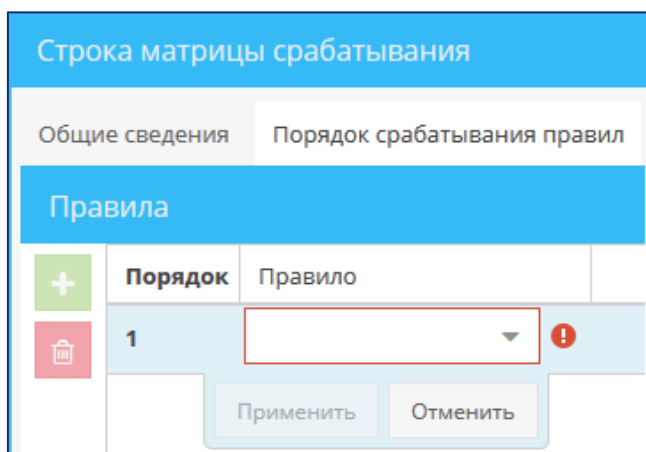


РИС. 95 – Строка для добавления правила при настройке порядка срабатывания правил

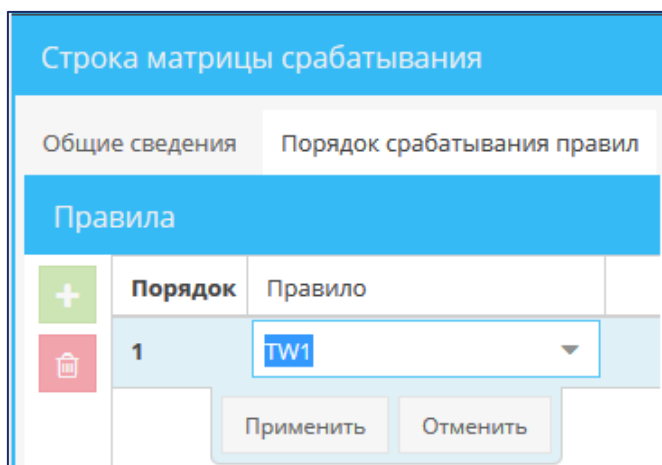



РИС. 96 – Правило, добавленное в перечень при настройке порядка срабатывания правил

- 7) Начиная со второй позиции в перечне правил следует настроить связь для каждого правила.
При связывании правил на самом деле связываются события правил. Такие связи необходимы для формирования логически связанных цепочек событий.

Чтобы настроить связь:

- на панели **Правила** выберите позицию с правилом;
 - на панели **Связи правила** <наименование правила> нажмите кнопку **Добавить** .
- В список связей добавится пустая строка (РИС. 97);
- в столбце **Связанное правило** укажите наименование правила, которое согласно настроенному порядку срабатывания проверяется раньше, – выберите значение в раскрывающемся списке;
 - в столбце **Поле текущего правила** укажите поле события этого правила – выберите значение в раскрывающемся списке;
 - в столбце **Операция сравнения** укажите операцию сравнения – выберите значение в раскрывающемся списке;
 - в столбце **Поле связанного правила** укажите поле события связанного правила– выберите значение в раскрывающемся списке;
 - нажмите кнопку **Применить** (РИС. 98).

Примечание. Из списка связей можно удалить только строку, которая была добавлена последней.

Чтобы удалить строку, выберите ее в списке связей и нажмите кнопку **Удалить** .

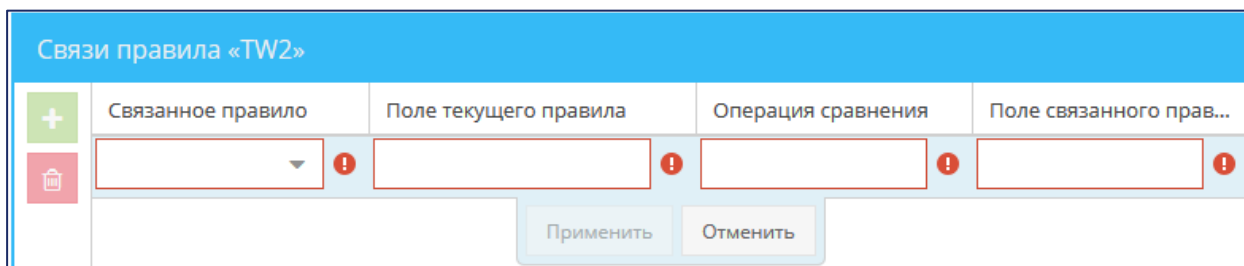


РИС. 97 – Добавления правила при настройке порядка срабатывания правил

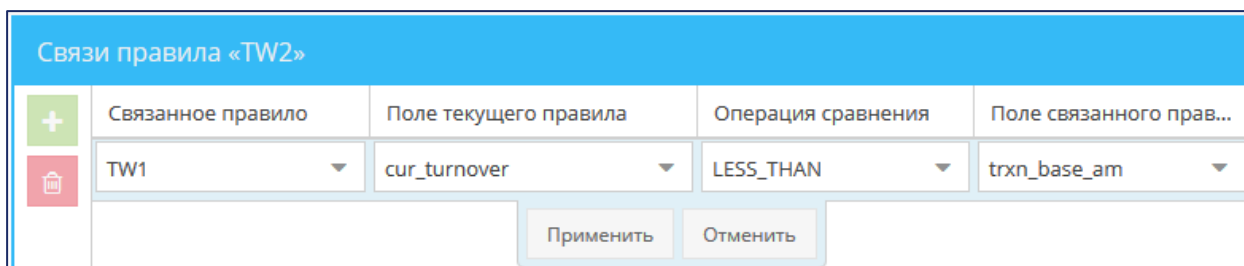


РИС. 98 – Добавления правила при настройке порядка срабатывания правил

- 8) Чтобы завершить настройку строки в матрице срабатывания, в окне **Строка матрицы срабатывания** нажмите кнопку **Завершить**.

Строка добавится в матрицу срабатывания (РИС. 99).

9) Нажмите кнопку **Сохранить**.

Наименование: TW Политика

Описание: TW Политика

Сервер джокс: Test engine

Правила: TW1 и TW2

Статус:

Матрица срабатывания


Наименование	Порядок срабатывания правил	
	TW1	TW2
Первая строка	1	2
Вторая строка	1	

Сохранить Отменить

РИС. 99 – Экранная форма политики выявления

7.1.3.4 Запуск политики


Политика выявления начнёт применяться к входящему потоку данных после её запуска. Чтобы запустить политику выявления на выполнение:

- 1) Выберите пункт меню **Лаборатория – Политики – Настройка политик**.
- 2) На вкладке **Политики** нажмите кнопку **Запустить** . Значение статуса политики поменяется на DEPLOYED.

7.1.3.5 Остановка политики

Администратор может прекратить применение политики к входящему потоку данных.

Для этого:

- 1) Выберите пункт меню **Лаборатория – Политики – Настройка политик**.
- 2) На вкладке **Политики** нажмите кнопку **Остановить** . Значение статуса политики поменяется на UNDEPLOYED.

7.2 НАСТРОЙКА ИСПОЛЬЗОВАНИЯ И ОБУЧЕНИЕ МОДЕЛЕЙ ВЫЯВЛЕНИЯ

7.2.1 Общие сведения

В **Jet Detective** настройка использования и обучение модели выявления проводится в модуле **Машинное обучение**.

Работа с функциями модуля выполняется в следующем порядке:

- подготовка массива данных для обучения – *обучающих выборок* (раздел 7.2.2);
- настройка использования модели машинного обучения (раздел 7.2.3);
- использование *Модели машинного обучения* – файла в формате PMML (Predictive Model Markup Language), разработанного с помощью специализированного программного обеспечения;
- обучение и дополнительная настройка модели выявления.

7.2.2 Настройка обучающих выборок

Обучающая выборка является одной из разновидностей пользовательского объекта.

Инструкции для работы с обучающими выборками приведено в разделе 5.4, инструкции для создания и настройки обучающей выборки – в разделе 6.1.

7.2.3 Использование модели машинного обучения

7.2.3.1 ПРОСМОТР МОДЕЛИ

Чтобы посмотреть модель:

- 1) Выберите пункт меню **Лаборатория – Модели – Настройка модели**.

В рабочей области отобразится одна или несколько вкладок:

- список моделей (РИС. 100);
- экранных форм моделей, открытых в этой сессии.

- 2) На вкладке со списком дважды щёлкните по строке модели машинного обучения.

Экранная форма модели откроется на отдельной вкладке (РИС. 101).

Список моделей		Дерево решений ×	
Имя модели	Название события	Статус модели	Название модели
NEW_MODEL	Транзакции	NEW	Новая модель
DECISION_TREE2	Транзакции	LEARNING	Дерево решений
Secon_model	Транзакции	NEW	Вторая модель
TREE_MODEL2	Транзакции	NEW	Дерево решений
SALARY_MODEL	Транзакции	NEW	Salary_model
MODEL_TREE	Транзакции	NEW	Дерево решений
HistModel	TRANSACTION_HIST_M...	READY	HistModel

<< < | Страница из 1 | > >> |

РИС. 100 – Вкладка со списком моделей

Список моделей		Дерево решений ×	
Общие сведения		Модель	
Название события:	<input type="text" value="Транзакции"/>	Описание модели:	<input type="text" value="Дерево решений"/>
Имя модели*:	<input type="text" value="DECISION_TREE2"/>	Статус модели:	<input type="text" value="LEARNING"/>
Название модели:	<input type="text" value="Дерево решений"/>	Владелец записи:	<input type="text" value="3"/>
			<input type="button" value="Сохранить"/>

РИС. 101 – Экранная форма модели. Вкладка **Общие сведения**

7.2.3.2 ДОБАВЛЕНИЕ МОДЕЛИ

Чтобы добавить модель:

- 1) Откройте список моделей (см. раздел 7.2.3.1).
- 2) Нажмите кнопку **Добавить** (РИС. 100).

Откроется вкладка **Общие сведения** экранной формы **Добавление новой записи** (РИС. 102).

- 3) Заполните поля вкладки **Общие сведения** (ТАБЛ. 32).
- 4) Перейдите на вкладку **Модель** (РИС. 103).

- 5) Нажмите на кнопку **Загрузить модель из файла** и выберите файл модели в формате PMML. Файл добавится в хранилище **Jet Detective**, а содержимое отобразится в *Конструкторе модели* (РИС. 103).
- 6) Выберите обучающую выборку в раскрывающемся списке. Список значений поля настраивается в пункте меню **Настройка обучающих выборок** (раздел 7.2.2).
- 7) Нажмите кнопку **Сохранить**.

The screenshot shows a web form titled 'Добавление новой записи' (Add new record) with a sub-tab 'Общие сведения' (General information). The form contains the following fields:

- Название события:** A dropdown menu.
- Описание модели:** A large text area.
- Имя модели*:** A text input field.
- Статус модели:** A text input field.
- Название модели:** A text input field.
- Владелец записи:** A text input field.

A blue 'Сохранить' (Save) button is positioned at the bottom right of the form.

РИС. 102 – Экранная форма **Добавление новой записи**. Вкладка **Общие сведения**ТАБЛ. 32 – Описание полей вкладки **Общие сведения**

Поле	ОПИСАНИЕ
Название события	Название события. Список значений поля настраивается в пункте меню События (раздел 5.4)
Имя модели	Системное имя модели
Название модели	Название модели
Описание модели	Описание модели
Статус модели	Статус модели машинного выявления в Jet Detective : <ul style="list-style-type: none"> • NEW – новая модель; • LEARNING – проводится обучение модели; • UNDERPLOYED – обучение остановлено; • READY – обучение проведено
Владелец записи	Код владения

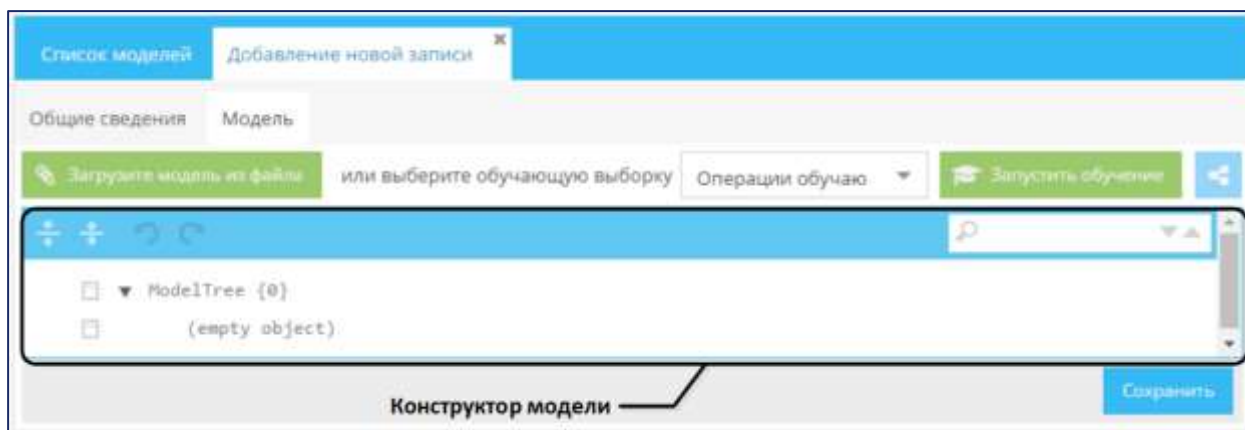


РИС. 103 – Экранная форма **Добавление новой записи**. Вкладка **Модель**

7.2.3.3 РЕДАКТИРОВАНИЕ МОДЕЛИ

Чтобы отредактировать модель:


- 1) Откройте модель (см. раздел 7.2.3.1).
- 2) Внесите изменения в поля вкладки **Общие сведения** (см. раздел 7.2.3.2).
- 3) На вкладке **Модели** выберите файл, обучающую выборку и внесите изменения в **Конструкторе модели**.
- 4) Нажмите кнопку **Сохранить**.

7.2.3.4 ЗАПУСК И ОСТАНОВКА ОБУЧЕНИЯ

Запустить обучение модели можно двумя способами:

- с вкладки со списком моделей;
- с вкладки **Модель** экранной формы модели.

Чтобы запустить обучение с вкладки со списком моделей:

- 1) Откройте список моделей (см. раздел 7.2.3.1).
- 2) Выберите модель и нажмите кнопку **Запустить** 

Процесс начнется, а статус модели поменяется на LEARNING (см. ТАБЛ. 32).


Чтобы запустить обучение с вкладки **Модель** экранной формы модели:

- 1) Откройте модель (см. раздел 7.2.3.1).
- 2) Перейдите на вкладку **Модель**.
- 3) Нажмите кнопку **Запустить обучение**.

Процесс начнется, а статус модели поменяется на LEARNING (см. ТАБЛ. 32).

- 4) Нажмите кнопку **Сохранить**.


Чтобы остановить обучение:

- 1) Откройте список моделей (см. раздел 7.2.3.1).
- 2) Выберите модель и нажмите кнопку **Остановить** .

Процесс остановится, а статус модели поменяется на UNDERPLOYED (см. ТАБЛ. 32).

7.2.3.5 ПРОСМОТР МОДЕЛИ В ГРАФИЧЕСКОМ ВИДЕ

Посмотреть модель в графическом виде можно только после её обучения, для этого:

- 1) Откройте модель (см. раздел 7.2.3.1).
- 2) Перейдите на вкладку **Модель**.
- 3) Нажмите кнопку .

Откроется окно **Дерево решений** с моделью в графическом виде (РИС. 104).

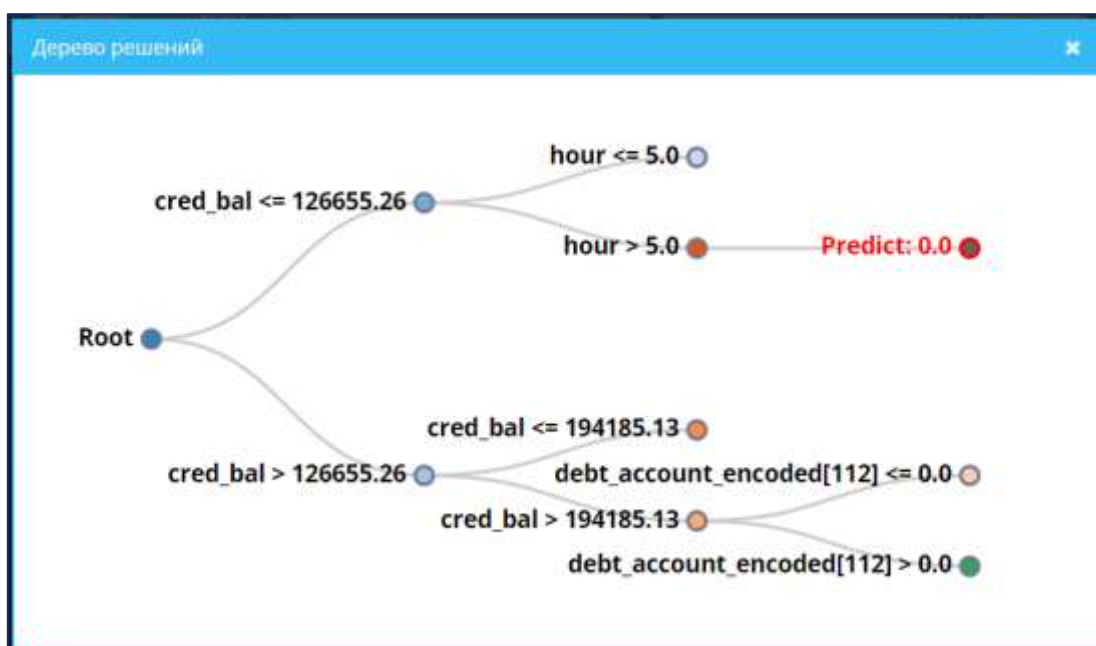



РИС. 104 – Окно **Дерево решений**

7.2.3.6 УДАЛЕНИЕ МОДЕЛИ

Чтобы удалить модель:

- 1) Откройте список моделей (см. раздел 7.2.3.1).
- 2) Выберите запись на вкладке **Список моделей**.
- 3) Нажмите кнопку **Удалить** .
- 4) Нажмите кнопку **Да** в появившемся запросе.

7.3 ИСПЫТАНИЕ ПОЛИТИК ВЫЯВЛЕНИЯ

7.3.1 Общие сведения

В **Jet Detective** можно сравнивать результаты работы политик и выбрать лучшую политику. Для этого реализованы следующие функции:

- Создание копии политики (см. раздел 7.1.2.3) с целью в дальнейшем внести в неё изменения и сравнить результаты её работы с результатами работы исходной версией политики.
- Определение выборки данных, в рамках которой будет проходить сравнение. Выполнение политик в тестовом режиме на хранимых в **Jet Detective** данных (см. раздел 7.3.2).
- Выбор двух политик или двух версий одной политики для сравнения результатов политик (см. раздел 7.3.3).

Для выполнения политик на хранимых данных в **Jet Detective** предусмотрены *объекты выполнения* (см. раздел 7.3.2), для хранения политик – *объекты сравнения* (см. раздел 7.3.3).

7.3.2 Выполнение политик

7.3.2.1 ПРОСМОТР ОБЪЕКТА ВЫПОЛНЕНИЯ

Чтобы посмотреть объект выполнения:

- 1) Выберите пункт меню **Лаборатория – Политики – Выполнение политик**.

В рабочей области отобразится одна или несколько вкладок:

- списка объектов выполнения (РИС. 105);
- экранных форм объектов выполнения, открытых в этой сессии.

- 2) На вкладке со списком объектов выполнения дважды щёлкните по строке объекта.

Экранная форма объекта выполнения откроется на отдельной вкладке (РИС. 106).

Политика	Период выполнения	Описание	Статус
Complex_policy_test	01.04.2017 00:00:00 - 31.05.2017 00:00:00	Проверка срабатывания политики со сложной ...	TESTED
Активный режим	01.05.2017 00:00:00 - 29.05.2017 00:00:00	Объект выполнения для активного режима	TESTED
Complex_policy_test	22.05.2017 00:00:00 - 23.05.2017 00:00:00	wer	TESTED
Test_deploymet_policy	01.04.2017 00:00:00 - 31.05.2017 00:00:00	-	TESTED

РИС. 105 – Список объектов выполнения

Объект выполнения «shushunov_policy_22_05_2017_2»

Политика: shushunov_policy_22_05_2017_2

Описание: 22.05.2017 14:25

Период выполнения: 02.02.2016 00:00:00 - 24.02.2016 00:00:00


Статус: TESTED

Создать Отменить

РИС. 106 — Вкладка с экранной формой объекта выполнения

7.3.2.2 СОЗДАНИЕ ОБЪЕКТА ВЫПОЛНЕНИЯ

Чтобы создать объект выполнения:

- 1) Откройте список объектов выполнения (см. раздел 7.3.2.1).
 - 2) Нажмите кнопку **Добавить** .
- Откроется экранная форма **Создание объекта выполнения**.
- 3) Заполните поля экранной формы (ТАБЛ. 33).
 - 4) Нажмите кнопку **Сохранить**.

Объекту выполнения автоматически присвоится статус CREATED, после чего объект добавится в список объектов выполнения.

ТАБЛ. 33 — Поля экранной формы **Создание объекта выполнения**

Поле	ОПИСАНИЕ
Политика	Политика, выполнение которой следует проверить на хранимых данных
Описание	Информативное описание объекта выполнения
Период выполнения	Интервал времени, за который проводится выборка данных для проверки политики. Заполнение поля см. в ТАБЛ. 3
Статус	Статус объекта выполнения (устанавливается автоматически): <ul style="list-style-type: none"> • CREATED – объект выполнения создан; • TESTING – идёт процесс проверки политики на хранимых данных; • TESTED – проверка политики завершена; • ERROR – во время проверки политики возникла ошибка; • DELETED – объект выполнения удалён (такой объект выполнения не отображается в интерфейсе пользователя)

7.3.2.3 РЕДАКТИРОВАНИЕ ОБЪЕКТА ВЫПОЛНЕНИЯ

Разрешается редактировать объекты выполнения, имеющие статус CREATED. Для этого:


- 1) Откройте объект выполнения (см. раздел 7.3.2.1).
- 2) Внесите изменения в поля объекта выполнения (см. ТАБЛ. 33). Внести изменения можно в любое поле экранной формы, кроме поля **Статус**, значение которого устанавливается автоматически.
- 3) Нажмите кнопку **Сохранить**.

7.3.2.4 ЗАПУСК ОБЪЕКТА ВЫПОЛНЕНИЯ

Чтобы начать проверку выполнения политики на хранимых данных, следует запустить объект выполнения. Операция запуска доступна только для объектов выполнения со статусом CREATED.

Чтобы запустить объект выполнения:

- 1) Откройте список объектов выполнения (см. раздел 7.3.2.1).


- 2) Выберите строку объекта и нажмите кнопку **Запустить** .
- 3) Нажмите кнопку **Да**.

Начнётся проверка выполнения политики выявления на хранимых данных. Объекту выполнения автоматически присвоится статус TESTING.

По завершении проверки объекту автоматически присвоится статус TESTED.

7.3.2.5 УДАЛЕНИЕ ОБЪЕКТА ВЫПОЛНЕНИЯ

Разрешается удалять объекты выполнения, имеющие статус CREATED, TESTED или ERROR. Для этого:

- 1) Откройте список объектов выполнения (см. раздел 7.3.2.1).
- 2) Выберите строку объекта выполнения.
- 3) Нажмите кнопку **Удалить** .
- 4) Нажмите кнопку **Да**.

7.3.3 Сравнение результатов выполнения политик

7.3.3.1 ОБЩИЙ ПОРЯДОК СРАВНЕНИЯ РЕЗУЛЬТАТОВ ВЫПОЛНЕНИЯ ПОЛИТИК

Сравнение результатов выполнения политик выполняется в следующем порядке:

- 1) Создание объекта сравнения.
- 2) Настройка параметров объекта сравнения и выбор политик.
- 3) Просмотр и анализ инцидентов, возникших в процессе выполнения политик.
- 4) Просмотр и анализ событий инцидента.

7.3.3.2 ПРОСМОТР ОБЪЕКТА СРАВНЕНИЯ

Чтобы посмотреть объект сравнения:

- 1) Выберите пункт меню **Лаборатория – Политики – Сравнение политик**.

В рабочей области отобразится одна или несколько вкладок:

- списка объектов сравнения;
- экранных форм объектов сравнения, открытых в этой сессии.

- 2) На вкладке со списком объектов сравнения (РИС. 107) дважды щёлкните по строке объекта сравнения.

Вкладка **Параметры** экранной формы объекта сравнения откроется на отдельной вкладке (РИС. 108).

Объекты сравнения Complex_policy_test и активная политика						
Наименование	Политика 1	Политика 2	Стат...	Период сравнения	Описание	
Сравнение политик	Complex_policy_test	Активный режим	NEW	01.05.2017 00:00:00 - 29.0...	Сравнение политик	
Сравнение Блэклист и Ос...	Проверка по BlackList	Основная политик...	NEW	22.05.2017 00:00:00 - 25.0...	-	
Complex_policy_test и акт...	Complex_policy_test	Активный режим	NEW	01.04.2017 00:00:00 - 29.0...	Сравнение срабатыва...	


РИС. 107 — Вкладка со списком объектов сравнения

Объекты сравнения Complex_policy_test и активная политика																									
Параметры																									
Наименование:	Complex_policy_test и активная политика																								
Описание:	Сравнение срабатывания политики со сложной матрицей и активной политики																								
Статус:	NEW																								
Период сравнения:	01.04.2017 00:00:00 - 29.05.2017 00:00:00																								
Политика 1	Политика 2																								
Complex_policy_test <input type="checkbox"/> По результатам расследования	Активный режим <input type="checkbox"/> По результатам расследования																								
<table border="1"> <thead> <tr> <th>Тип</th> <th>Период срабатывания</th> <th>Использовать в сравнении</th> </tr> </thead> <tbody> <tr> <td>PROD</td> <td>21.05.2017 06:20:18 - 21.05.201...</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>PROD</td> <td>21.05.2017 06:21:09 - 21.05.201...</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>PROD</td> <td>21.05.2017 06:21:13 - 21.05.201...</td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>	Тип	Период срабатывания	Использовать в сравнении	PROD	21.05.2017 06:20:18 - 21.05.201...	<input checked="" type="checkbox"/>	PROD	21.05.2017 06:21:09 - 21.05.201...	<input checked="" type="checkbox"/>	PROD	21.05.2017 06:21:13 - 21.05.201...	<input checked="" type="checkbox"/>	<table border="1"> <thead> <tr> <th>Тип</th> <th>Период срабатывания</th> <th>Использовать в сравнении</th> </tr> </thead> <tbody> <tr> <td>PROD</td> <td>24.05.2017 04:26:14 - 24.05.201...</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>PROD</td> <td>24.05.2017 04:28:15 - 24.05.201...</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>PROD</td> <td>24.05.2017 04:28:08 - 24.05.201...</td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>	Тип	Период срабатывания	Использовать в сравнении	PROD	24.05.2017 04:26:14 - 24.05.201...	<input checked="" type="checkbox"/>	PROD	24.05.2017 04:28:15 - 24.05.201...	<input checked="" type="checkbox"/>	PROD	24.05.2017 04:28:08 - 24.05.201...	<input checked="" type="checkbox"/>
Тип	Период срабатывания	Использовать в сравнении																							
PROD	21.05.2017 06:20:18 - 21.05.201...	<input checked="" type="checkbox"/>																							
PROD	21.05.2017 06:21:09 - 21.05.201...	<input checked="" type="checkbox"/>																							
PROD	21.05.2017 06:21:13 - 21.05.201...	<input checked="" type="checkbox"/>																							
Тип	Период срабатывания	Использовать в сравнении																							
PROD	24.05.2017 04:26:14 - 24.05.201...	<input checked="" type="checkbox"/>																							
PROD	24.05.2017 04:28:15 - 24.05.201...	<input checked="" type="checkbox"/>																							
PROD	24.05.2017 04:28:08 - 24.05.201...	<input checked="" type="checkbox"/>																							
Сохранить	Отменить Инциденты >																								

РИС. 108 — Вкладка **Параметры** объекта сравнения

7.3.3.3 СОЗДАНИЕ ОБЪЕКТА СРАВНЕНИЯ

Чтобы создать объект сравнения:

- 1) Откройте список объектов сравнения (см. раздел 7.3.3.2).
- 2) Нажмите кнопку **Добавить** .

Откроется вкладка **Параметры** экранной формы **Создание объекта сравнения** (РИС. 109).

В верхней части вкладки находится *панель свойств* объекта сравнения, в которой отображаются его свойства (см. ТАБЛ. 34). В нижней части вкладки расположена *панель выбора политики*, состоящая из двух идентичных частей – по одной для каждой политики.

- 3) Заполните поля панели свойств.
- 4) Выберите политики для сравнения (в поле со списком).

Отобразится список срабатываний политики на потоке данных (тип PROD) и объектов выполнения (тип SIMULATE).

- 5) Для каждой проверяемой политики установите флажок её срабатывания. Периоды срабатывания политик должны пересекаться.
- 6) Установите флажок **По результатам расследований**, если при сравнении политик необходимо учитывать статус инцидентов.
- 7) Нажмите кнопку **Сохранить**.

Объект сравнения появится в списке на вкладке **Объекты сравнения**. Также он станет доступным для редактирования его параметров и просмотра результатов сравнения – инцидентов и событий.

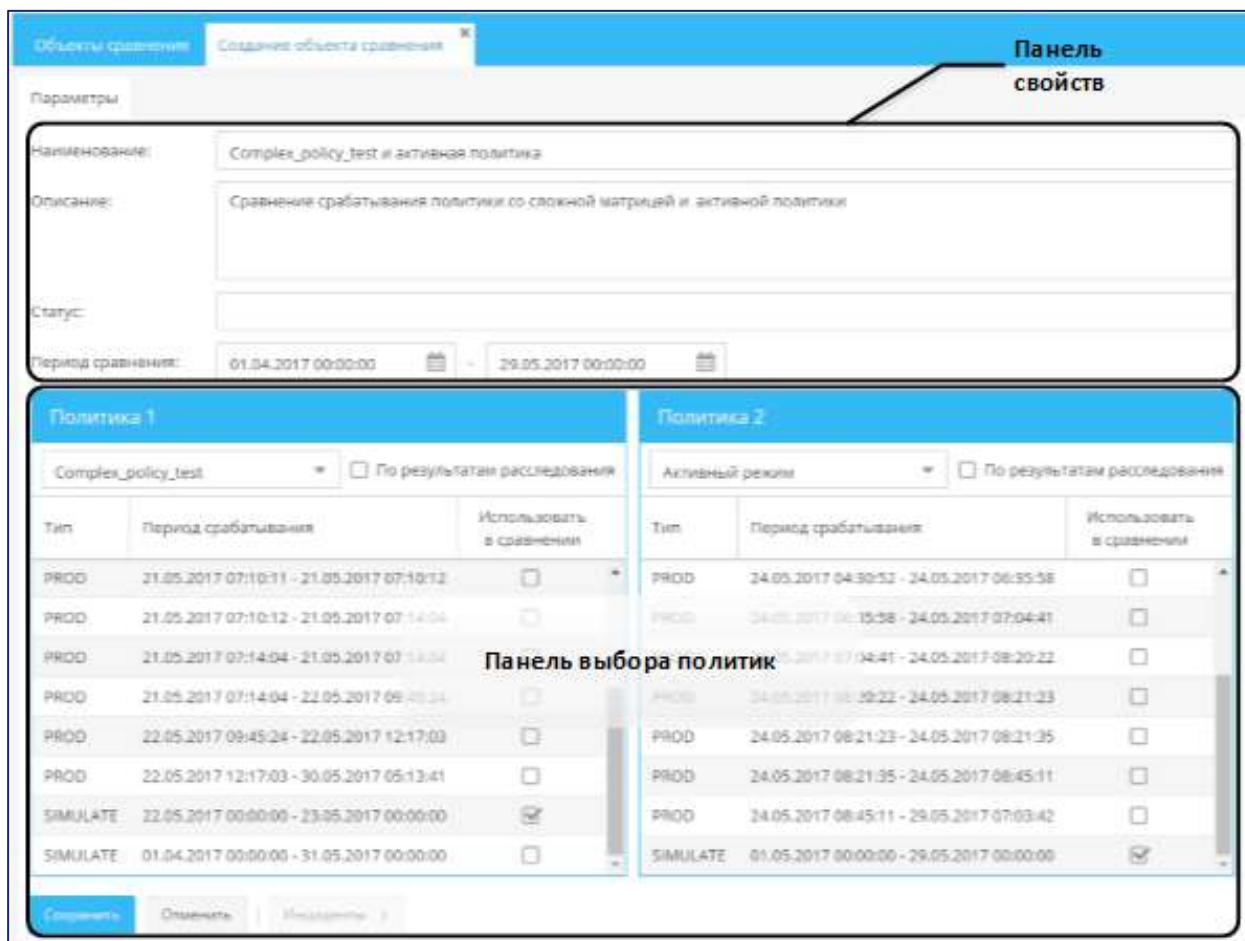


РИС. 109 — Экранная форма Создание объекта сравнения

ТАБЛ. 34 — Поля объекта сравнения

ЭЛЕМЕНТ ИНТЕРФЕЙСА	ОПИСАНИЕ
Наименование	Информативное название объекта сравнения
Описание	Информативное описание объекта выполнения
Период сравнения	Интервал времени, за который результаты проверки политик сравниваются. Заполнение поля см. в ТАБЛ. 3

7.3.3.4 РЕДАКТИРОВАНИЕ ПАРАМЕТРОВ ОБЪЕКТА СРАВНЕНИЯ

Чтобы отредактировать параметры объекта сравнения:

- 1) Откройте объект сравнения (см. раздел 7.3.3.2).
- 2) Внесите изменения в его поля (ТАБЛ. 34).
- 3) Нажмите кнопку **Сохранить**.

7.3.3.5 ПРОСМОТР РЕЗУЛЬТАТОВ. ИНЦИДЕНТЫ

Чтобы посмотреть инциденты, полученные в результате сравнения политик выявления:

- 1) Перейдите к просмотру объекта сравнения (см. раздел 7.3.3.2).
- 2) Нажмите кнопку **Инциденты**, чтобы открыть форму **Инциденты**.

Форма состоит из двух частей. В каждой части отображается табличный список инцидентов, возникших в результате выполнения политики, и *панель итогов* (РИС. 110).

Описание столбцов табличного списка приведено в ТАБЛ. 35. На панели итогов в поле **Количество событий** отражается сумма событий всех инцидентов. В поле **Сумма по инцидентам** – сумма денежных средств всех инцидентов.

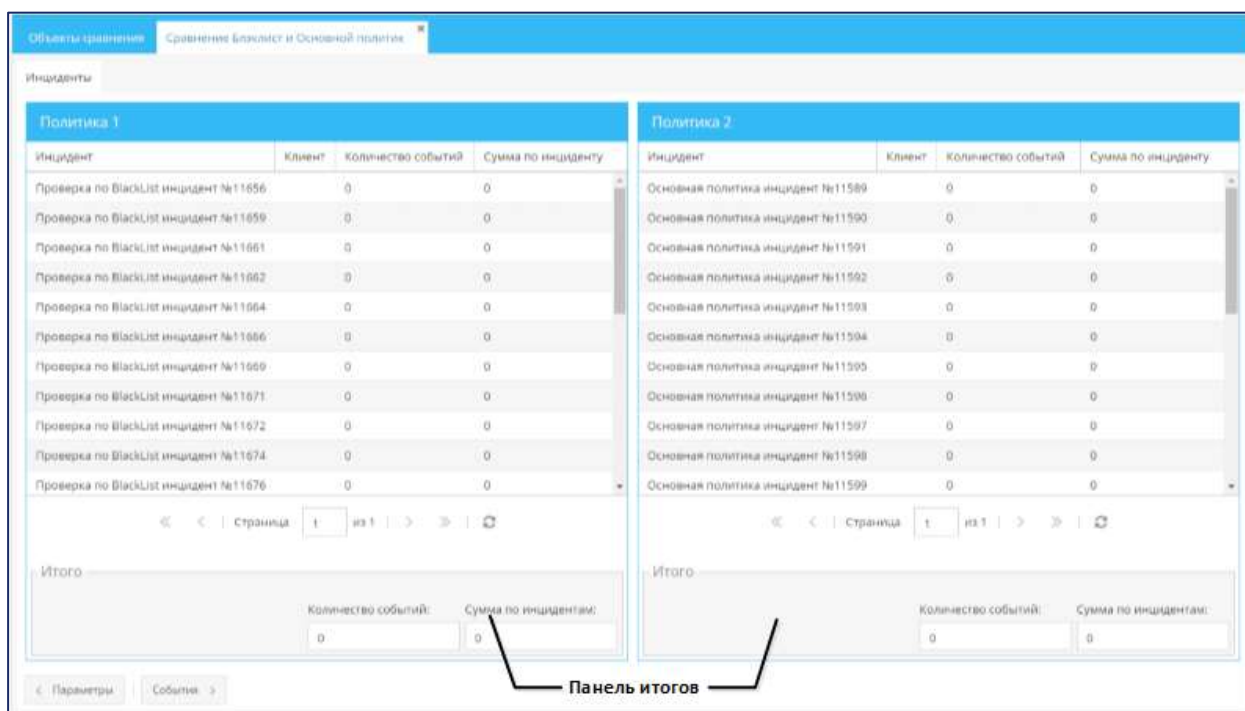


РИС. 110 — Сравнение политик. Форма **Инциденты**

ТАБЛ. 35 — Описание столбцов формы **Инциденты**

Столбец	Описание
Инцидент	Наименование политики выявления и порядковый номер инцидента
Клиент	Наименование клиента, в котором зарегистрирован инцидент
Количество событий	Количество событий инцидента
Сумма по инциденту	Сумма денежных средств

7.3.3.6 ПРОСМОТР РЕЗУЛЬТАТОВ. СОБЫТИЯ

Чтобы посмотреть события инцидентов, полученных в результате сравнения политик выявления:

- 1) Перейдите к просмотру объекта сравнения (см. раздел 7.3.3.2).
- 2) Нажмите кнопку **Инциденты**, чтобы открыть форму **Инциденты**.
- 3) Выберите инцидент.
- 4) Нажмите кнопку **События**, чтобы открыть форму **События**.

Форма состоит из двух частей (РИС. 111):

- табличный список событий в инцидентах (описание столбцов приведено в ТАБЛ. 36);
 - детальное описание проверки события.
- 5) Для просмотра детального описания выберите событие в табличном списке **События в инцидентах**.

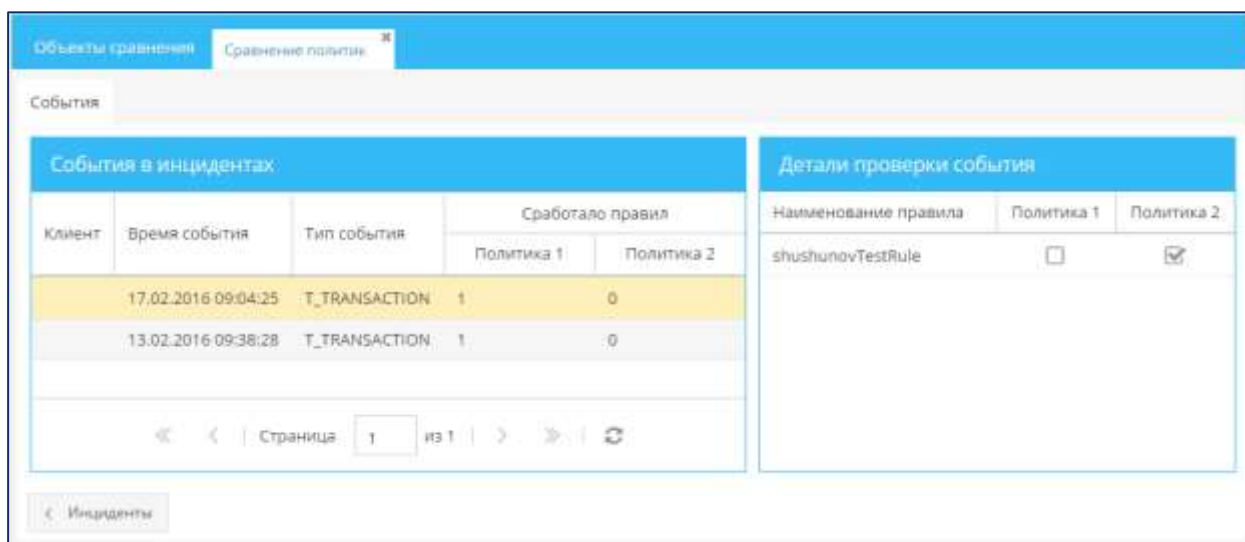


РИС. 111 — Сравнение политик. Форма **События**

ТАБЛ. 36 — Описание столбцов табличного списка **События в инцидентах**

Столбец	Описание
Клиент	Наименование клиента, в котором зарегистрирован инцидент
Время события	Дата и время события в формате ДД.ММ.ГГГГ чч:мм:сс
Тип события	Тип события из справочника
Сработало правил	Количество сработавших правил для первой и второй политики

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин/Сокращение	Описание
ETL	Extract, Transform, Load – процессы обработки данных
PDI	Pentaho Data Integration – система интеграции данных с открытым исходным кодом, разработка Hitachi Group Company
БД	База данных
СУБД	Система управления базами данных

ГЛОССАРИЙ

Агрегация данных – процесс вычисления обобщенных показателей массива данных: суммирование, вычисление среднего (максимального, минимального, медианного) значений и т. п. Является разновидностью обогащения данных.

Модели выявления – прогнозные модели, использующие, например, деревья решений.

Обогащение данных – процесс дополнения данных новой информацией, которая делает данные более полезными для дальнейшего использования. В частности, обогащение производится за счет данных из нескольких источников.

Очистка данных – процесс повышения качества данных с помощью выявления и устранения ошибок и несоответствия данных.

Связывание данных – процесс поиска и установки связей между сущностями. Является разновидностью обогащения данных.

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.

Business Object Model (модель бизнес-объектов) – совокупность сущностей в **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.

ПРИЛОЖЕНИЕ А ПРИМЕРЫ СХЕМ ВЛАДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ

В приложении рассматриваются примеры схем владения пользователями для вымышленной компании «Финсервис». Дерево владений компании «Финсервис» приведено на РИС. 112.

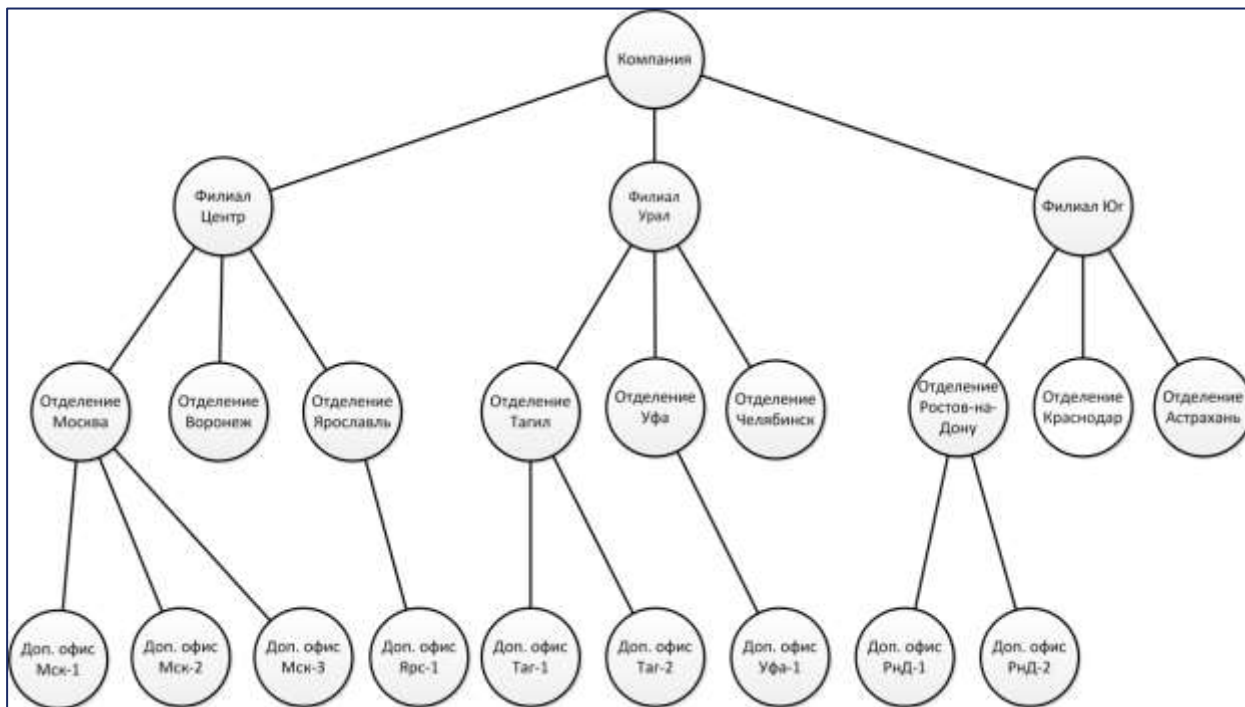


РИС. 112 – Дерево владений компании «Финсервис»

Служба информационной безопасности (ИБ) компании состоит из 11 человек (ТАБЛ. 37).

ТАБЛ. 37 – Сотрудники службы ИБ и их владения по умолчанию

Условное обозначение сотрудника	Условное обозначение владения по умолчанию	Описание владения по умолчанию
Директор ИБ	Компания	Компания «Финсервис»
Главный специалист ИБ-1	Филиал Урал	Филиал Уральский
Главный специалист ИБ-2	Филиал Центр	Филиал Центральный
Специалист ИБ-1	Отделение Москва	Отделение Москва
Специалист ИБ-2	Доп. офис Мск-2	Дополнительный офис Москва-2
Специалист ИБ-3	Доп. офис Мск-3	Дополнительный офис Москва-3
Специалист ИБ-4	Отделение Воронеж	Отделение Воронеж
Специалист ИБ-5	Отделение Тагил	Отделение Тагил
Специалист ИБ-6	Отделение Уфа	Отделение Уфа
Специалист ИБ-7	Отделение Ростов-на-Дону	Отделение Ростов-на-Дону

Условное обозначение сотрудника	Условное обозначение владения по умолчанию	Описание владения по умолчанию
Специалист ИБ-8	Отделение Астрахань	Отделение Астрахань

Наиболее интересными для рассмотрения являются схемы владения следующих пользователей:

- директор ИБ;
- главный специалист ИБ-1;
- специалист ИБ-1.

На схемах владений пользователей в рассматриваемых далее примерах приняты следующие обозначения прав доступа:

- (R) – права на чтение записей в таблицах объектов;
- (W) – права на редактирование записей в таблицах объектов;
- (D) – права на удаление записей из таблиц объектов.

Директор ИБ – главное должностное лицо в службе ИБ. В его обязанности входит общее управление и координация действий сотрудников службы. В целях выполнения служебных обязанностей ему необходим доступ ко всем данным компании. Однако в части данных филиала Юг его права ограничены только чтением данных. Для описанной ситуации схема владения директора ИБ состоит из следующих областей владения (РИС. 113):

- области владения по умолчанию с корневым узлом «компания» и настроенными правами доступа (RWD);
- дополнительной области владения с корневым узлом «филиал Юг» и настроенными правами доступа (R).

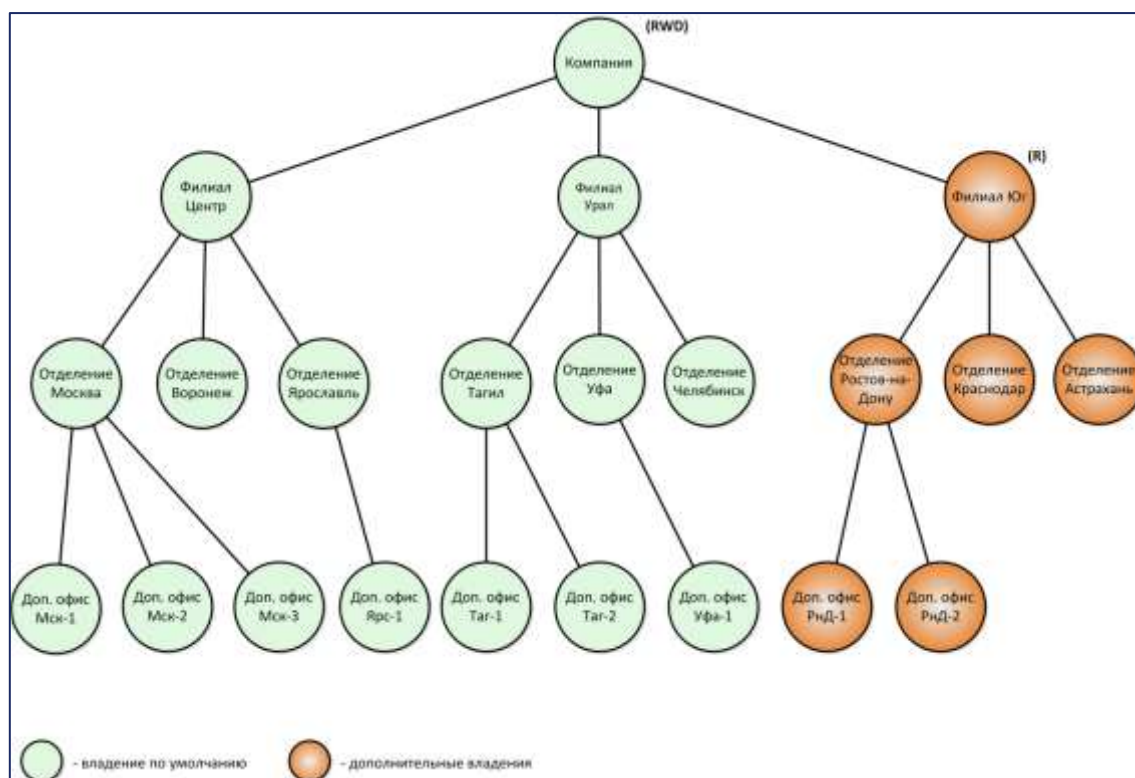


РИС. 113 – Схема владений директора ИБ

Главный специалист ИБ-1 курирует работу по расследованию инцидентов ИБ филиала Центр, а также по ряду вопросов замещает директора ИБ. Все данные, доступные директору ИБ, доступны главному специалисту ИБ-1 для чтения.

Для описанной ситуации схема владения главного специалиста ИБ-1 состоит из следующих областей владения (РИС. 114):

- области владения по умолчанию с корневым узлом «филиал Центр» и настроенными правами доступа (RWD);
- дополнительной области владения с корневым узлом «компания» и настроенными правами доступа (R).

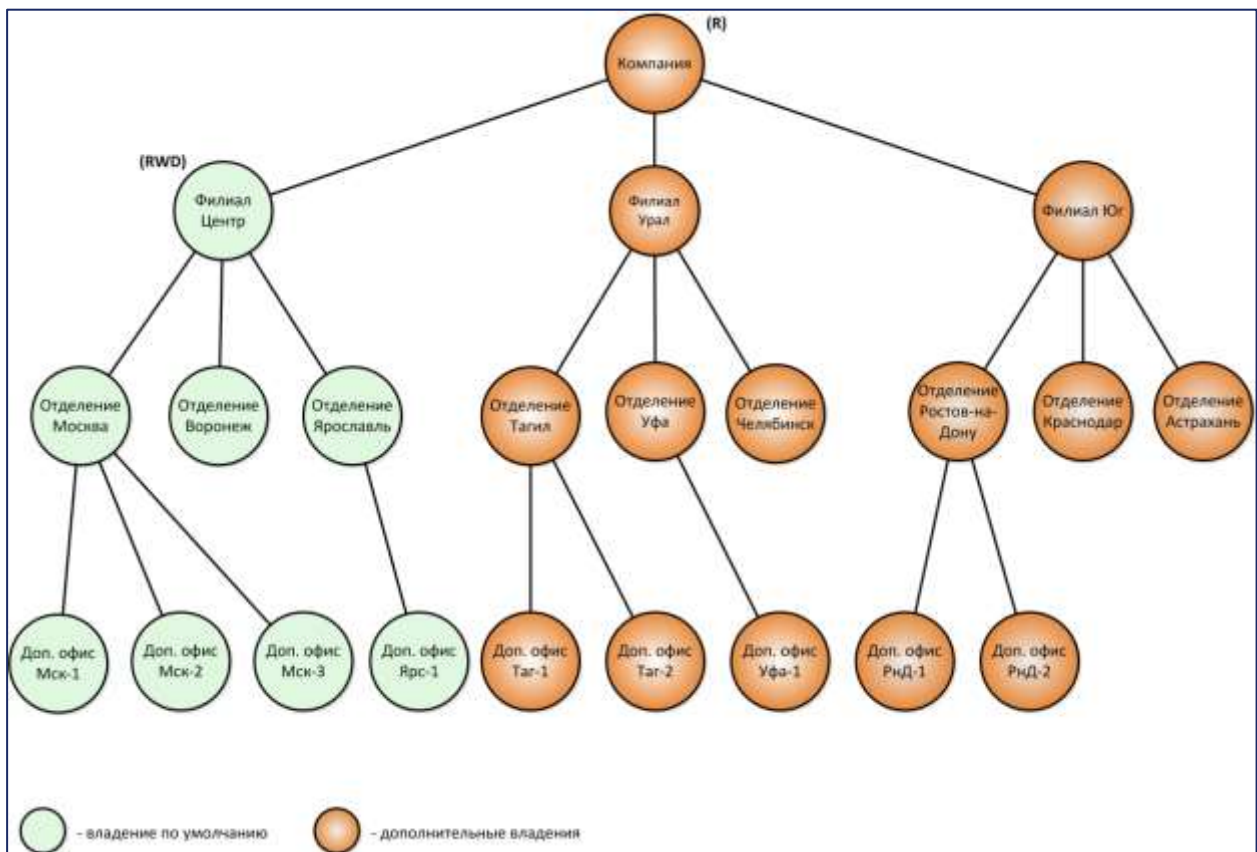


РИС. 114 – Схема владений главного специалиста ИБ-1

Специалист ИБ-1 расследует инциденты ИБ, связанные с отделением Москва и дополнительным офисом Москва-1. Данные этих подразделений доступны пользователю в полном объеме и с полными правами доступа.

Специалист ИБ-1 замещает главного специалиста ИБ-1. Исполняя обязанности заместителя, специалист ИБ-1 не имеет прав на удаление записей из таблиц объектов.

Для описанной ситуации схема владения специалиста ИБ-1 состоит из следующих областей владения (РИС. 115):

- области владения по умолчанию с корневым узлом «отделение Москва» и настроенными правами доступа (RWD);
- дополнительной области владения с корневым узлом «доп. офис Мск-2», для которой не установлены права доступа (-);

- дополнительной области владения с корневым узлом «доп. офис Мск-3», для которой не установлены права доступа (-);
- дополнительной области владения с корневым узлом «филиал Центр» и настроенными правами доступа (RW).

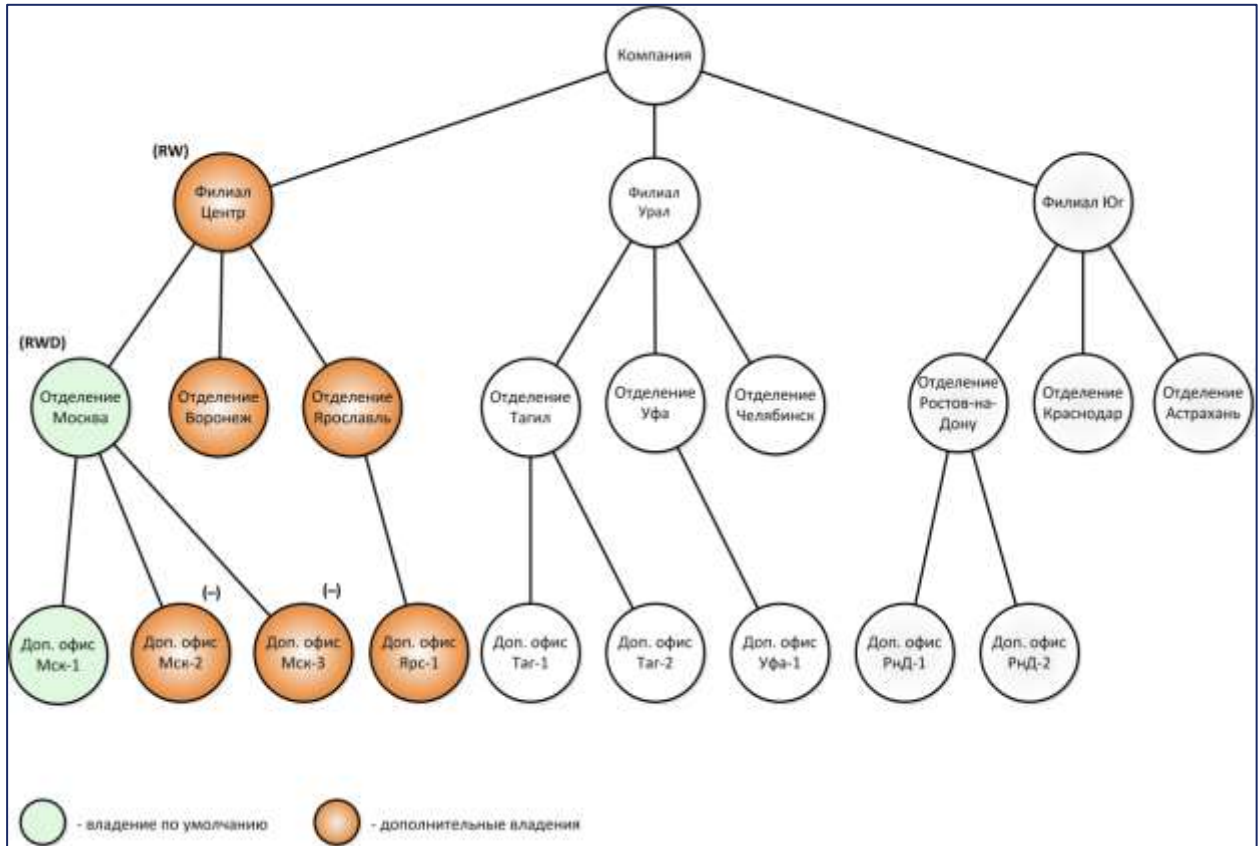


РИС. 115 – Схема владений специалиста ИБ-1