СИСТЕМА ХРАНЕНИЯ НОРМАТИВНЫХ ДАННЫХ

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ
11150642.3222106.00305.И3.01.1.М

СОДЕРЖАНИЕ

ГЛАВА

1 ВВЕДЕНИЕ

В главе приводится информация о назначении и основных функциях продукта.

1 Назначение

Продукт «Система хранения нормативных данных» (DRS) предназначен для накопления, хранения, обработки и поиска информации, необходимой уполномоченным органам для выполнения возложенных на них задач в порядке и случаях, установленных Федеральным законодательством.

2 Функции продукта

Продукт обеспечивает следующую функциональность:

- создание инфраструктуры для хранения данных;
- загрузка данных универсального (файлового) формата;
- управление системными задачами;
- управление пакетами данных;
- удаление данных;
- поиск данных;
- регистрация событий «прямого контроля» и оповещение пользователей об этих событиях;
- управление справочниками локального источника;
- мониторинг подсистем, входящих в состав продукта.

3 Рекомендации по квалификации персонала

Пользователь продукта должен иметь навыки работы с графическим пользовательским интерфейсом операционной системы.

Администратор продукта должен обладать навыками и знаниями по администрированию операционной системы, базовыми знаниями об администрировании Oracle, знаниями о конфигурации и настройках PHP, навыками работы с Apache и сертификатами (SSL).

4 Перечень эксплуатационной документации

Комплект эксплуатационной документации продукта включает:

- Массив входных данных (DRS-DOC_L6).
- Руководство по эксплуатации (DRS-DOC_G3) – текущий документ.
- Глоссарий (DRS-DOC_GLOSS).
- Настроечные параметры (DRS-DOC_SETUP_PRM).
- Руководство оператора на подсистемы:
  - «Рабочее место продукта DRS» (DRS_WEB);
  - «Шаблоны отчетов по соединениям» (R_SVC_CALLS);
  - «Шаблоны отчетов по платежам» (R_SVC_PAYM);
  - «Шаблоны отчетов по абонентам» (R_SVC_SUBS).
- Руководства системного программиста на подсистемы, входящие в состав продукта.

ГЛАВА

2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

В главе приводится описание возможностей и условий применения продукта.

1 Функциональные возможности продукта

- Формирование хранилища данных – локального источника для проведений поисков:
  - регистрация и сортировка поступающих в DRS файлов данных;
  - управление и контроль процесса загрузки в хранилище данных из внешних источников;
  - хранение информации о параметрах загрузки и характеристиках загруженных данных;
  - удаление данных.
- Поддержка документооборота при проведении поисков:
  - Создание и редактирование электронных заявок;
  - Создание и запуск на исполнение поисковых заданий;
  - Просмотр результатов выполнения поисковых заданий;
  - Формирование файлов отчетов по заявкам;
  - Формирование файлов отчетов по поисковым заданиям.
- Использование справочной информации при проведении поисков.
- Управление загрузкой данных и справочниками локального хранилища данных:
  - Конфигурирование справочников, использующихся в процессе загрузки и интерпретации загружаемых данных;
  - Настройка и управление источниками данных, в которых проводятся поиски.
- Регистрация событий «прямого контроля» и оповещение пользователей об этих событиях.
- Управление структурой подразделений и полномочиями пользователей:
  - Настройка структуры подразделений;
  - Настройка учетных записей пользователей;
  - Настройка привилегий пользователей.
- Аудит действий пользователей и системных событий.

2 Условия применения продукта

В разделе указаны условия, при выполнении которых обеспечивается применение продукта в соответствии с назначением.

1 Состав технических средств

Требования к аппаратной части зависят от:

- требований к объему хранимых данных;
- требований к количеству одновременно открытых пользовательских сессий;
- требований к скорости выполнения поисковых запросов;
- требований к скорости загрузки файлов соединений.

Аппаратная часть внутренней дисковой подсистемы каждого из серверов должна обеспечивать пропускную способность не ниже 2 Гбит/с.

Аппаратная часть дисковой подсистемы сервера хранилища данных должна обеспечивать пропускную способность не ниже 2 Гбит/с.

Для приблизительного расчета необходимого объема дискового пространства для хранилища данных рекомендуется использовать следующую формулу:

$$V_s = A_r \cdot P_d \cdot N_m \cdot K,$$

где:

- A_r – объем одной записи о соединении, загруженной в хранилище данных (в байтах);
- P_d – ежедневный поток записей в базу данных (записей в день);
- N_m – количество дней в месяце;

K – поправочный коэффициент (рекомендуемое значение – от 1.1 до 1.3).

2 Состав программных средств

Системные программные средства должны быть представлены лицензионными локализованными версиями операционных систем.

Сервер заявок и хранилище данных

Для работы каждого компьютера сервера заявок и хранилища данных требуются следующие установленные программные средства:

- Операционная система Red Hat Enterprise Linux Advanced Server 5 64-бит.
- Сервер баз данных: Oracle Enterprise Server версии не ниже 11.2.0.2.0 с включенной опцией Oracle Text.

Сервер пользовательского интерфейса

Для работы каждого компьютера сервера пользовательского интерфейса требуются следующие установленные программные средства:

- Операционная система Red Hat Enterprise Linux Advanced Server 5 64-бит.
- Клиент баз данных Oracle 11g.

Рабочее место пользователя

Для оснащения одного автоматизированного рабочего места требуются следующие установленные программные средства:

- Веб-обозреватель (один из перечисленных):
  - Microsoft Internet Explorer 8 и выше.
  - Mozilla Firefox версии с 10 по 15 включительно.
- Текстовый редактор для работы с отчетами, содержащими результаты выполнения поисковых заданий (один из перечисленных):
  - Microsoft Office Word версии не ниже 2003;
  - OpenOffice.org Writer версии не ниже 2.3.
- Табличный редактор для работы с отчетами, содержащими результаты выполнения поисковых заданий (один из перечисленных):
  - Microsoft Office Excel версии не ниже 2003;
  - OpenOffice.org Calc версии не ниже 2.3.

ГЛАВА

3 ПОДГОТОВКА К РАБОТЕ

В главе приводится информация о порядке установки и проверки работоспособности продукта.

1 Схемы развертывания DRS

DRS предусматривает два варианта развертывания.

В первом варианте развертывания устанавливаются:

1. Сервер заданий и сервер хранилища данных (может быть совмещенным).
2. Сервер пользовательского интерфейса для установки единого front-end.
3. Сервер конвертации данных.

Во втором варианте развертывания устанавливаются:

1. Сервер заданий и сервер хранилища данных (может быть совмещенным).
2. Сервер пользовательского интерфейса для установки HAS-сервера.
3. Сервер пользовательского интерфейса для установки web-серверов.
4. Сервер конвертации данных.

2 Полная установка

Для установки DRS следует последовательно установить необходимые подсистемы. Подробное описание установки см. в документах «Руководство системного программиста» для каждой подсистемы.

3 Обновление с предыдущей версии

Для обновления DRS следует последовательно обновить подсистемы, входящие в состав продукта, до требуемых версий. Подробное описание обновления см. в документах «Руководство системного программиста» для каждой подсистемы.

Перед проведением обновления необходимо остановить внешние процессы, помещающие файлы в каталоги IN файлового шлюза, а также дождаться окончания загрузки всех пакетов данных.

4 Настройка параметров

Описание настроечных параметров см. в документе «Настроечные параметры» (DRS-DOC_SETUP_PRM-RUS).

5 Порядок проверки работоспособности

Для проверки корректной установки следует убедиться в отсутствии ошибок в выводе скрипта установки после каждого этапа инсталляции.

Осуществить вход в пользовательский интерфейс системы через web-браузер (путем ввода URL вида `https://<IP-адрес компьютера web-интерфейса>:<порт Apache>`) с использованием логина и пароля администратора.

Для обеспечения доступа пользователей к заданному набору операций администратору после первого входа в систему рекомендуется зарегистрировать необходимое количество учетных записей и назначить им соответствующие права. Подробное описание прав и принципы их назначения см. в разделе «Модель прав доступа» настоящего документа.

О корректной установке продукта свидетельствуют также следующие факты:

- Зарегистрированы и запущены системные задачи. При обнаружении остановленных задач следует их запустить.

- Зарегистрирована и запущена служба файлового шлюза (при обнаружении остановленных служб следует их запустить).
- Запущен и работает HAS-сервер (при обнаружении неработающего HAS-сервера следует его запустить).

ГЛАВА

4 ОПИСАНИЕ ОПЕРАЦИЙ

В разделе приведено описание операций, доступных при помощи графического интерфейса пользователя, и описание операций по техническому обслуживанию DRS.

1 Операции, доступные через web-интерфейс

Через графический интерфейс пользователя доступны следующие операции:

- Управление заявками (только для режима работы с использованием заявок; режим можно выбрать при установке подсистемы DRS_RQS_API):
  - просмотр списка заявок;
  - поиск заявки по номеру;
  - добавление заявки;
  - редактирование заявки.
- Управление поисковыми заданиями:
  - просмотр списка заданий по заявке/ без привязки к заявке;
  - добавление поискового задания следующих видов:
    - «Карточка абонента»;
    - «Поиск карточки абонента по списку NN телефонов»;
    - «Идентификаторы абонентов»;
    - «Соединения»;
    - «Соединения по списку NN телефонов»;
    - «Соединения по базовым станциям»;
    - «Пополнения баланса»;
  - настройка полей форм поиска;
  - просмотр списка заданий источникам;
  - запуск поисковых заданий;
  - остановка поисковых заданий;
  - порождение задания на поиск соединений;
  - копирование поисковых заданий.
- Управление результатами поиска:
  - просмотр результатов поиска по заданию;
  - настройка формирования отчетов;
  - формирование отчета по всем заданиям заявки;
  - формирование отчета по выбранным заданиям;
  - просмотр файлов-отчетов, сформированных по результатам поиска;
  - импорт файлов-отчетов.
- Управление нормативно-справочной информацией:
  - работа со справочником номерной емкости операторов связи;
  - работа со справочником связанных диапазонов номеров;
  - работа со справочником базовых станций;
  - работа со справочником коммутаторов;

- работа со справочником транков;
- работа со справочником операторов связи;
- работа со справочником внутренних (особых) номеров;
- работа со справочником-картой типов соединений;
- работа со справочником-картой типов платежей;

- Управление источниками данных:
  - просмотр информации об источниках данных;
  - изменение статуса источника данных.
- Управление учетными записями пользователей:
  - просмотр списка пользователей;
  - добавление учетной записи пользователя;
  - редактирование учетной записи пользователя;
  - изменение статуса пользователя;
  - удаление учетной записи пользователя;
  - изменение пароля пользователя;
  - привязка пользователя к правовой группе;
  - смена подразделения пользователя;
  - настройка формирования отчетов для пользователя.
- Определение структуры подразделений:
  - просмотр списка подразделений;
  - добавление подразделения;
  - редактирование подразделения;
  - удаление подразделения.
- Разграничение прав пользователей:
  - просмотр списка групп прав;
  - добавление группы прав;
  - редактирование группы прав;
  - импорт прав доступа для группы прав;
  - настройка объектных привилегий группы прав;
  - настройка привилегий на доступ к блокам интерфейса для группы прав;
  - редактирование пользовательских ограничений;
  - изменение статуса группы прав;
  - удаление группы прав.
- Аудит действий пользователей:
  - Для режима работы с использованием заявок (режим можно выбрать при установке подсистемы `DRS_RQS_API`):
    - просмотр журнала заявок;
    - редактирование параметров заявки;
    - просмотр реквизитов санкции суда;
    - просмотр журнала аудита;
    - просмотр журнала сессий;
    - просмотр системного лога;
    - просмотр статистики поисков.
  - Для режима без использования заявок:
    - просмотр журнала аудита;

- просмотр журнала сессий;
- просмотр системного лога;
- просмотр статистики поисков.

- Специальные действия:
  - удаление данных.
- Управление загрузкой данных:
  - просмотр статистики по загруженным данным;
  - просмотр форматов загруженных данных;
  - изменение статуса формата загрузки;
  - работа с пакетами данных.

Подробное описание операций, доступных через web-интерфейс, см. в руководстве оператора, встроенном в подсистему DRS_WEB (доступно по нажатию кнопки ***Справка*** в web-интерфейсе).

2 Управление инфраструктурой хранения данных

В рамках управления инфраструктурой хранения данных доступны следующие операции:

- управление реестром серверов;
- регистрация и настройка в локальном хранилище данных нового оператора связи;
- подключение дополнительного локального источника данных;
- настройка параметров пользовательской сессии.

1 Управление реестром серверов

Для корректного отображения системных логов все сервера заявок и хранилищ данных, использовавшиеся для развертывания DRS, должны быть зарегистрированы в реестре DRS.

Для регистрации сервера в реестре DRS следует на базовом сервере заявок запустить утилиту RegisterServer или функцию AUTH.COMMON_DEPLOY_PG.InsertServer. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему SVC_DEPLOY_API.

Для получения информации об уже зарегистрированном сервере следует на базовом сервере заявок запустить процедуру AUTH.COMMON_DEPLOY_PG.GetServerByID.

Для удаления сервера из реестра следует на базовом сервере заявок запустить процедуру AUTH.COMMON_DEPLOY_PG.DeleteServer.

Для изменения информации о сервере в реестре следует на базовом сервере заявок запустить процедуру AUTH.COMMON_DEPLOY_PG.UpdateServer.

Подробное описание процедур и функций по управлению реестром серверов см. в документе «Руководство системного программиста» на подсистему SVC_DEPLOY_API.

2 Регистрация и настройка в локальном хранилище данных нового оператора связи

DRS предоставляет возможность настройки в локальном хранилище данных нового оператора связи.

1 Регистрация оператора связи

Для регистрации оператора связи, данные которого подлежат загрузке в хранилище, следует на сервере хранилища данных запустить утилиту RegisterTelco из состава утилит подсистемы DRS_DWH_REGISTRY_API. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему DRS_DWH_REGISTRY_API.

2 Регистрация стандарта связи

Для регистрации стандарта связи, поддерживаемого оператором, следует на сервере хранилища данных запустить утилиту SetTelcoStandarts из состава утилит подсистемы DRS_DWH_REGISTRY_API (утилита запускается для каждого стандарта, подлежащего

регистрации). Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему DRS_DWH_REGISTRY_API.

Для удаления стандарта связи из списка зарегистрированных стандартов следует запустить утилиту UnsetTelcoStandarts из состава утилит подсистемы DRS_DWH_REGISTRY_API (утилита запускается для каждого стандарта, подлежащего удалению). Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему DRS_DWH_REGISTRY_API.

Регистрация стандартов связи обеспечивает возможность поиска данных об абонентах и соединениях по заданному стандарту.

3 Регистрация универсальных форматов загрузки

Для регистрации универсальных (файловых) форматов загрузки данных об абонентах, соединениях и базовых станциях, предоставляемых оператором связи, следует на сервере хранилища данных запустить утилиту RegisterTelcoFormats из состава утилит подсистемы DRS_DWH_REGISTRY_API. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему DRS_DWH_REGISTRY_API.

4 Настройка приложений загрузки

Для настройки приложений загрузки следует:

1. В каталоге хранилища загружаемых файлов создать копию каталога GATE_EXAMPLE с именем, совпадающим с названием формата данных о соединениях (CALLS_XXXX, где XXXX – идентификатор оператора связи).
2. В каталоге хранилища загружаемых файлов создать копию каталога GATE_EXAMPLE с именем, совпадающим с названием формата данных о базовых станциях (STATIONS_XXXX, где XXXX – идентификатор оператора связи).
3. В каталоге хранилища загружаемых файлов создать копию каталога GATE_EXAMPLE с именем, совпадающим с названием формата данных об абонентах (SUBS_XXXX, где XXXX – идентификатор оператора связи).

Конфигурационные файлы форматов загрузки хранятся в базе данных хранилища данных. Для изменения конфигурации загрузки файлов с данными об абонентах, соединениях, базовых станциях следует запустить утилиту SetFileFormatConfig из состава утилит подсистемы DRS_DWH_REGISTRY_API. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему DRS_DWH_REGISTRY_API.

5 Настройка хранилища для загрузки данных оператора связи: определение параметров табличных пространств

В хранилище данных могут быть зарегистрированы несколько операторов связи. В этом случае шаги по настройке хранилища для загрузки данных оператора связи необходимо повторить для каждого оператора.

При определении параметров табличных пространств возможны два различных подхода:

- если все операторы, данные от которых должны поступать в систему, имеют примерно одинаковый объем данных, данный пункт может быть выполнен один раз для всех операторов связи;
- если операторы связи имеют достаточно сильно отличающиеся объемы данных, пункт должен быть выполнен индивидуально для каждого оператора, с различными параметрами (с последующим, для каждого оператора связи, выполнением создания партиционированных таблиц, так как настроенные параметры применяются при создании партиционированных таблиц).

В процессе работы с DRS допускается настраивать параметры создания табличных пространств, предназначенных для хранения логов и данных о соединениях. Настройка выполняется с помощью утилит SetStorageParams.

Изменение значений не влияет на параметры уже созданных табличных пространств – новые значения применяются только к табличным пространствам, созданным после запуска утилит.

По умолчанию табличные пространства для хранения логов DRS и данных о соединениях создаются с включенной опцией bigfile tablespace, а файлы данных именуются и

размещаются автоматически СУБД Oracle. Данная конфигурация рекомендуется при использовании базы данных с ASM.

Настройка параметров табличных пространств включает в себя:

- отключение/включение опции `bigfile tablespace`;
- изменение размера или приращения создаваемых табличных пространств;
- смену дисковой группы файлов, где создаются табличные пространства (при использовании базы данных с ASM);
- настройку шаблона именования файлов данных и путей для их размещения (только при использовании базы данных без ASM).

Для выполнения настройки параметров создания табличных пространств с логами следует запустить утилиту `SetStorageParams` из состава утилит подсистемы `SVC_BASE_API`. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему `SVC_BASE_API`.

Для выполнения настройки параметров создания табличных пространств с соединениями следует запустить утилиту `SetStorageParams` из состава утилит подсистемы `DRS_DWH_CALLS_API`. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему `DRS_DWH_CALLS_API`.

6 Настройка хранилища для загрузки данных оператора связи: создание партицированных таблиц для хранения соединений оператора связи

Предварительно следует убедиться, что зарегистрирован числовой идентификатор оператора связи в системе.

Для создания партицированных таблиц для хранения соединений оператора связи следует запустить утилиту `CreateEvTable4Telco` из состава утилит подсистемы `DRS_DWH_CALLS_API`. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему `DRS_DWH_CALLS_API`.

7 Настройка хранилища для загрузки данных оператора связи: расширение таблиц (партицирование)

Расширение таблиц может выполняться двумя способами: с помощью утилит (на год или на указанный период времени) или автоматически (в зависимости от значений соответствующих настроечных параметров).

1. Хранение логов.

Расширение таблицы для хранения логов рекомендуется выполнять не позже, чем за месяц до начала года, для которого добавляются партиции.

Для расширения таблицы с системным логом следует запустить утилиту `ExtentLogTable` из состава утилит подсистемы `SVC_BASE_API`. Количество запусков утилиты определяется количеством лет, за которые планируется хранить данные. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему `SVC_BASE_API`.

В случае если партицирование таблицы для хранения данных производится за текущий год в этом же году или за следующий год в последний день предыдущего года, то на время выполнения утилиты должны быть остановлены все источники записи в лог (системные задачи, маска имени которых – SSP%, службы файлового шлюза, службы адаптера SMD (538)).

Для включения функции автоматического расширения таблиц следует установить значение параметра `LOG_PARTITION_AUTOCREATE` равным `1`, а значение параметра `LOG_PARTITION_AUTOCREATE_COUNT` – отличным от нуля.

2. Хранение соединений.

Для расширения таблицы с данными о соединениях следует запустить утилиту `ExtentEvTable4Telco` из состава утилит подсистемы `DRS_DWH_CALLS_API`. Утилиту следует запускать для каждого оператора связи, чьи данные будут загружаться в хранилище данных. Количество запусков утилиты определяется числом операторов связи, соединения от которых заливаются в хранилище данных. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему `DRS_DWH_CALLS_API`.

Для включения функции автоматического расширения таблиц следует установить значение параметра CALLS_PARTITION_AUTOCREATE равным 1, а значение параметра CALLS_PARTITION_AUTOCREATE_COUNT – отличным от нуля.

8 Настройка временных периодов хранения соединений

Для того чтобы настроить периоды для хранения данных о соединениях за оперативный период (таблицы хранилища данных типа OPER) и данных в таблицах долговременного хранения (таблицы типа MAIN), следует настроить параметры, влияющие на определение границ архивного (долговременного) и оперативного периода хранения данных о соединениях.

Для каждого оператора связи в таблице EVENT_CUT_DATES подсистемы DRS_DWH_REGISTRY_SCR (подсистема DRS_DWH_REGISTRY_SCR устанавливается в схему REGISTRY) указываются следующие параметры по умолчанию:

- INS_IN_OPER_DEEP – количество дней, предназначенных для загрузки в таблицу оперативного хранения (OPER), начиная от текущей даты. Значение по умолчанию – 30 (последние 30 дней, считая от текущей даты);
- MOVE_OPER_START – количество дней от текущей даты до начала оперативного периода. Значение по умолчанию – 90 (данные в таблицах типа OPER хранятся не больше 90 дней до текущей даты);
- MOVE_OPER_END – количество дней от текущей даты до конца оперативного периода. Значение по умолчанию – 29 (в постоянное хранение переводятся данные, находящиеся в таблице типа OPER не меньше, чем 29 дней до текущей даты).

Рекомендуется значения параметров задавать таким образом, чтобы диапазоны дат: [sysdate - INS_IN_OPER_DEEP] и [MOVE_OPER_END-MOVE_OPER_START] были перекрываемыми, то есть чтобы выполнялось условие: MOVE_OPER_END = INS_IN_OPER_DEEP – 1.

Параметры настройки, влияющие на местоположение и размер создаваемых табличных пространств, хранятся в виде параметров системы в таблице BASE_APP_PARAMETERS схемы AUTH:

- EVENT_DATAFILENAME – DATAFILE для создания табличных пространств для хранения соединений;
- EVENT_TABLESPACE_SIZE – начальный размер табличного пространства для хранения соединений (например, 16 мегабайт – 16M, 1 гигабайт – 1G). Значение по умолчанию – 1M;

При установке DRS для ознакомления (без обработки промышленных объемов данных о соединениях) рекомендуемое значение EVENT_TABLESPACE_SIZE – 1M.

- EVENT_AUTOEXTEND_SIZE – величина автоматического расширения табличного пространства для хранения соединений. Значение по умолчанию – 1M.

При установке DRS для ознакомления (без обработки промышленных объемов данных о соединениях) рекомендуемое значение EVENT_AUTOEXTEND_SIZE – 1M.

9 Регистрация дополнительного формата загрузки данных о соединениях для зарегистрированного оператора связи

В случае если данные о соединениях одного оператора связи представлены в форматах разных версий, после регистрации основного формата следует:

1. Создать конфигурационный файл и файловое хранилище для пакетов дополнительного формата загрузки. Описание формата и элементов конфигурационного файла см. в документе «Руководство системного программиста» на подсистему DRS_GATEWAY.
2. Запустить утилиту RegisterCallsFormat из состава утилит подсистемы DRS_DWH_CALLS_API. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему DRS_DWH_CALLS_API.
3. Перезапустить службы файлового шлюза.

Утилита RegisterCallsFormat регистрирует дополнительный формат загрузки данных о соединениях с привязкой его к основному формату (основной формат регистрируется утилитой RegisterTelcoFormats).

Успешный запуск утилиты возможен, только если в таблице REGISTRY.DATA_FORMATS зарегистрирован следующий набор форматов данных о соединениях (поле DATA_FMT_TYPES_TYPE_ID):

1 – Вызовы;

4 – Типы вызовов;

5 – Коммутаторы;

7 – Транки;

12 – Роуминговые партнеры.

Если хотя бы один формат не зарегистрирован, в лог-файл setup.log выводится сообщение об ошибке вида:

Для оператора связи с Telco ID = <идентификатор оператора связи> не зарегистрирован набор форматов данных, требуемый для регистрации файлового формата загрузки соединений.

10 Удаление стандарта связи из списка стандартов, поддерживаемых данным оператором

Для удаления стандарта связи из списка зарегистрированных стандартов, поддерживаемых оператором связи, следует запустить утилиту UnsetTelcoStandarts из состава утилит подсистемы DRS_DWH_REGISTRY_API. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему DRS_DWH_REGISTRY_API.

3 Подключение дополнительного локального источника данных

В случае если в процессе работы возникла необходимость в создании нового локального источника (хранилища) данных, следует:

- на отдельном сервере установить и настроить подсистемы, обеспечивающие хранение данных;
- настроить взаимодействие сервера заявок с дополнительным хранилищем данных;
- зарегистрировать дополнительный сервер в реестре DRS;
- подготовить хранилище к загрузке данных;
- на сервере файловой загрузки создать экземпляры служб файлового шлюза, настроенные на соединение с дополнительным хранилищем данных, и подключить новые форматы загрузки.

3 Загрузка данных универсального формата

Загрузка данных универсального формата включает в себя выполнение следующих операций:

- Загрузка данных, полученных в файловом формате;
- Групповая загрузка файлов универсального формата (используется в специальных случаях, требует ручной настройки);
- Оптимизация загрузки данных о соединениях (требует ручной настройки).

В DRS загружаются файлы универсального (UNI) формата данных, содержащие:

- полный срез информации по всем абонентам оператора связи на момент выгрузки;
- обновления-срезы информации об абонентах, которые содержат данные об изменениях, которые были произведены с последнего сеанса загрузки среза или обновления-среза;
- информацию о соединениях;
- информацию об изменениях в составе базовых станций: новые базовые станции, отключенные базовые станции;
- информацию о платежах абонентов оператора связи.

Для корректной загрузки в хранилище данных и последующей обработки файлы должны быть представлены в текстовом формате. Подробное описание поддерживаемых форматов данных см. в документе «Система хранения нормативных данных. Массив входных данных [DRS-DOC_L6]».

1 Загрузка данных, полученных в файловом формате

Операция загрузки данных производится путем обмена файлами с сервером данных. Для загрузки данных, полученных в файловом формате, в хранилище данных следует:

1. Поместить в каталог \temp файл данных, удовлетворяющий требованиям выбранного формата данных (выполняется внешними по отношению к DRS механизмами).
2. Переместить файл в каталог \in (выполняется внешними по отношению к DRS механизмами).
3. Дождаться, пока файл будет автоматически перемещен в одну из папок (done, error, trash).
4. В зависимости от папки, в которую перемещен файл, выполнить дополнительные действия:

- \done – загрузка окончена, дополнительных действий не требуется;
- \error:
  - просмотреть лог-файлы загрузки (примеры сообщений в лог-файлах приведены в Приложении М);
  - изменить данные пакета с учетом выявленных в ходе анализа лог-файлов несоответствий;
  - произвести повторную загрузку пакета;
- \trash:
  - проверить формат именования файла, изменив его при необходимости;
  - повторить шаги 1-3.

2 Групповая загрузка файлов соединений универсального формата

Чтобы повысить скорость загрузки в хранилище данных файлов соединений универсального формата, возможна настройка на одновременную (групповую) загрузку нескольких пакетов (файлов).

Настройка выполняется отдельно для каждого формата загрузки.

Для настройки следует:

1. В таблице `REGISTRY.FILE_FORMATS` изменить параметры формата загрузки следующим образом:
   - в поле `GROUP_PACK_AMOUNT` указать максимальное количество пакетов в группе;
   - в поле `GROUP_PACK_SIZE` указать максимальный суммарный размер файлов, объединенных в группу, в байтах (значение параметра зависит от аппаратных возможностей сервера хранилища данных);
   - в поле `GROUP_DATE_MASK` задать маску для группировки файлов (один из указанных ниже символов) – в группу будут объединяться файлы, для которых совпадает дата, указанная в поле `REGISTRY.PACKAGES.DATED`:
     - `Y` – дата будет учитываться с точностью до года;
     - `M` – с точностью до месяца;
     - `D` – с точностью до дня;
     - `H` – с точностью до часа (совпадение года, месяца, дня и часа).

   Рекомендуемое значение маски для группировки файлов с данными о соединениях: `GROUP_DATE_MASK = D` (с точностью до дня).
2. Для изменения параметров существующей задачи загрузки запустить утилиту `RegisterLoaderJob` из состава дистрибутива подсистемы файловой загрузки в хранилище данных по технологии внешних таблиц Oracle (`SVC_FILE_ET_LOADER`), параметр `Enable multipack loading (0 - no, 1 - yes)?` установить в значение `1`.

О загрузке файла в составе группы свидетельствует `0` в поле `PACKAGES.DISABLE_GROUP` соответствующей записи.

Внимание! В текущей версии групповая загрузка поддерживается только для файлов с данными о соединениях.

3 Особенности загрузки файлов об абонентах

DRS предоставляет возможность загружать файлы с данными об абонентах в двух форматах:

- срез – содержит все записи, которые актуальны на момент загрузки;
- обновление-срез – содержит только записи, которые были добавлены, изменены или удалены в источнике после последней загрузки среза или обновления-среза.

Срезы и их обновления представляют собой пакеты, состоящие из записей, каждая из которых представляет собой полную информацию об абоненте. Дата, на которую эта информация была актуальна, единая для всего пакета, и называется датой актуальности пакета.

Обновления-срезы и срезы формируют единый поток данных различными способами. При обновлении данных учитывается удаление записей, в то время как при использовании полного среза данных запись является удаленной, если она отсутствует в наборе данных среза. При загрузке обновления-среза в случае изменений в паре клиент-абонент, для данного клиента в обновлении срезе требуется указать информацию по всем действующим парам клиент-абонент. Фактически при загрузке изменений по абоненту определенного клиента требуется выгрузить полный срез для данного клиента. В случае отсутствия в обновлении-срезе для данного клиента информации о действующих парах (хоть и не изменившихся с момента загрузки среза), данные пары будут считаться удаленными с момента загрузки обновления-среза.

Все записи, содержащиеся в обновлении-срезе, заносятся в хранилище данных с датой-временем начала интервала действия записи, совпадающей с датой актуальности файла из наименования файла. Дата окончания интервала действия записи устанавливается:

- в случае если запись была удалена, то равной дате актуальности;
- если запись является действующей, то равной 31.12.2999.

При загрузке обновлений-срезов:

1. Актуальные (не удаленные) записи из обновления-среза помещаются в исторические таблицы с датой начала действия записи, равной дате актуальности пакета, в котором содержатся. Датой окончания действия таких записей на момент вставки будет 31.12.2999.
2. Неактуальные (удаленные) записи из обновления-среза помещаются в исторические таблицы с датой начала и окончания действия, равной дате актуальности пакета.
3. После вставки записей производится изменение даты окончания действия на дату актуальности загружаемого пакета для записей, которые находятся в предыдущих пакетах и соответствуют парам клиент-абонент, которые входят в набор данных пакета обновления-среза.

Использование обновлений-срезов не позволяет восстановить полную историю записей из источника, т.к. обновление-срез передает только последнее состояние измененных записей. Если между двумя последовательными загрузками обновлений-срезов было произведено несколько изменений, то в последнее обновление-срез попадет только одна запись, являющаяся результатом последних изменений. Состояния записи после всех других модификаций (исключая конечную модификацию) будут утеряны.

SVC_BASE поддерживает алгоритм загрузки срезов и обновлений только "вперед", т.е. загружать можно только пакеты с датой актуальности большей, чем у пакетов, уже загруженных в хранилище. Первым для формата данных должен быть загружен срез, далее могут поступать как срезы, так и обновления. При загрузке пакета должно соблюдаться условие: среди загруженных или загружаемых в данный момент пакетов, относящихся к одному формату данных (поток данных), не должно быть пакетов с такой же датой актуальности, и загружаемый пакет должен быть последним (наиболее поздним) по дате актуальности.

В случае если один поток данных оператора связи прекращает поступать, и вместо него начинает поступать другой (например, при изменении структуры данных в БД оператора связи, после существенного изменения формата предоставления данных) для обеспечения корректности формирования истории изменения атрибутов абонентов необходимо завершить старый поток. Для завершения старого потока и закрытия исторических записей обо всех абонентах следует перед загрузкой первого среза нового формата загрузить фиктивный пустой срез с датой актуальности, равной первому срезу нового формата данных.

При загрузке срезов используется технология фильтров. Фильтр – это сохраненные ненормализованные данные пакета в том виде, в котором они поступают на загрузку, до выполнения этапа загрузки словарей. В качестве фильтра автоматически сохраняются данные последнего загруженного пакета отдельно для каждого формата данных. Сохранение фильтра производится после успешного окончания загрузки пакета, содержащего срез. Предыдущий фильтр удаляется в случае успешной загрузки как среза, так и его обновления.

Перед загрузкой срезов для уменьшения количества обрабатываемых данных вычисляется разница между срезом, который необходимо загрузить, и уже загруженным предыдущим срезом.

В случае если загружается срез, и предыдущий пакет был срезом, то к загружаемому срезу применяется фильтр. В случае отсутствия необходимого фильтра, фильтр будет загружен автоматически. Ручная загрузка фильтра не предусмотрена. При этом сначала будет загружен фильтр предыдущего пакета, следом после истечения периода времени, установленного в качестве значения параметра PACK_RELOAD_WAIT из таблицы AUTH.BASE_APP_PARAMETERS, будет выполнена загрузка самого пакета.

В случае если загружается срез, но предыдущий пакет не был срезом, или предыдущего пакета не было и, соответственно, нет сохраненного для него фильтра, срез будет загружен “как есть”.

В случае если производится загрузка обновления, то пакет загружается "как есть", без применения фильтра.

Результат фильтрации данных среза состоит из нескольких наборов строк (в процессе загрузки обрабатываются данные, находящиеся в таблице V_IMP_CLIENT_SUBS промежуточной схемы загрузки):

- Строки с новыми абонентами. Строки с такими идентификаторами абонентов (поле SUB_NO) отсутствуют в фильтре.
- Строки, в которых атрибуты абонента изменились. Изменение даты актуальности записи (поле ACT_DATE) при этом не учитывается, но она загружается в качестве атрибута абонента.
- Строки с информацией об удаленных абонентах. Удаленными являются абоненты, чьи идентификаторы (поле SUB_NO) присутствуют в фильтре, но отсутствуют в загружаемых данных. Для этих записей заполняются только поля SUB_NO, CMCT_STND_ID и DELETED. Поле DELETED заполняется датой актуальности загружаемого пакета.
- Строки с информацией об удаленных клиентах. Удаленными являются клиенты, чьи идентификаторы (поле CLNT_NO) присутствуют в фильтре, но отсутствуют в загружаемых данных. Для этих записей заполняются только поля CLNT_NO, JUR_TYPE_ID, DELETED. Поле DELETED заполняется датой актуальности загружаемого пакета.
- Дополнительно к процедуре фильтрации все полученные строки дополняются полями-флагами, в которых указывается, изменились ли в данной строке значения атрибутов, которые загружаются в словари, связанные с этой таблицей *_LOADS, по отношению к ее состоянию из предыдущего среза (из фильтра).

Для строк с информацией об удаленных клиентах и абонентах для определенности считается, что данные не изменились.

После загрузки большого количества данных в хранилище (например, первичная загрузка данных об абонентах для некоторого оператора связи, так и массовое изменение атрибутов абонентов в данных оператора связи), а также периодически в удобное время необходимо осуществлять сбор статистики оптимизатора Oracle по всем таблицам, их полям и индексам схемы SUBS_DATA. Рекомендуется использовать стандартную задачу сбора статистики GATHER_STATS_JOB.

4 Особенности загрузки данных о соединениях

Подробное описание загружаемых данных см. в документе «Система хранения нормативных данных. Массив входных данных [DRS-DOC_L6]».

При необходимости загрузки данных о соединениях, в которых длины полей превышают значения, указанные в описании формата данных, следует вручную настроить размерность таблиц. Подробнее см. в разделе «Настройка размерности таблиц для загрузки данных о соединениях».

5 Настройка размерности таблиц для загрузки данных о соединениях

Настройка размерности полей таблиц для хранения данных о соединениях осуществляется для каждого оператора связи в отдельности. Для этого необходимо вручную заполнить таблицу DATASRV.EVENT_TAB_STRUCT, указав размерность полей в таблицах соединений и наличие индекса по этим полям по каждому оператору связи.

Изменение размерности полей или изменение информации об использованных индексах в таблице DATASRV.EVENT_TAB_STRUCT не означает автоматических изменений в структуре данных соответствующих таблиц и требует ручного выполнения операции `alter table` или `create(drop) index` над соответствующими таблицами с данными.

После изменения размерности таблиц следует вручную изменить длины соответствующих полей в конфигурационных файлах загрузки информации о соединениях.

6 Оптимизация загрузки данных о соединениях

При загрузке данных о соединениях выполнение процесса перестройки индексов на таблице с данными, подготовленными для обмена партициями с партицированной таблицей, занимает продолжительное время.

Для сокращения времени перестройки индексов и оптимизации процесса загрузки реализована поддержка параллельного выполнения блоков PL/SQL-кода в одной сессии Oracle. Величина временного выигрыша в данном случае напрямую зависит от аппаратного обеспечения DRS.

По умолчанию DRS настроен на последовательную перестройку индексов с указанием коэффициента параллельности.

Для включения режима поддержки параллельного выполнения блоков PL/SQL-кода при загрузке данных о соединениях следует:

1. Создать группу задач для управления параллельным выполнением, запустив утилиту AddTaskHandle из состава утилит подсистемы SVC_BASE_API. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему SVC_BASE_API. При вызове утилиты рекомендуется:
   - для параметра Handler count указать значение не меньше 12;
   - в случае если планируется использовать данную группу задач только для управления параллельным перестроением индексов, указать значение параметра Correlation ID – произвольный набор символов, который будет использован для фильтрации при выборке блоков PL/SQL-кода.
2. В таблице REGISTRY.EVENT_CUT_DATES изменить значение поля IDX_REBUILD_MODE на 2.
3. В случае если создана группа системных задач, предназначенная только для управления параллельным перестроением индексов при загрузке соединений, в поле CORRELATION_CODE этой же таблицы указать соответствующий идентификатор корреляции.

4 Управление пакетами данных

DRS предоставляет возможность управления пакетами данных, включающего следующие действия:

- Отвержение пакета.
- Повторная загрузка.

Данные операции доступны через web-интерфейс. Если работа с web-интерфейсом по каким-либо причинам невозможна, для выполнения операций следует воспользоваться приведенными ниже рекомендациями.

1 Отвержение пакета

Отвержение пакета представляет собой исключение данных, поступивших в пакете, из общего массива хранимой и обрабатываемой информации.

Для того чтобы отвергнуть пакет, следует:

1. Запустить утилиту RejectPack из состава утилит подсистемы DRS_DWH_REGISTRY_API. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему DRS_DWH_REGISTRY_API.
2. Убедиться, что на стороне хранилища данных отвергнутый пакет находится в состоянии «Отвергнут», а операция над пакетом – в статусе «Выполнено» (в таблице PACKAGES схемы REGISTRY для пакета с заданным идентификатором поле CURRENT_STATUS_ID = 9, а поле OPERATION_STATUS_ID = 3).

Внимание! Пакет с информацией об абонентах может быть отвергнут, только в случае если отвергнуты все пакеты, загруженные после заданного. Отвержение пакетов следует производить последовательно, начиная с последнего.

2 Повторная загрузка

Повторная загрузка может быть выполнена только для отвергнутых пакетов.

Для того чтобы повторно загрузить ранее отвергнутый пакет данных, следует:

1. Запустить утилиту ReloadPack из состава утилит подсистемы DRS_DWH_REGISTRY_API. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему DRS_DWH_REGISTRY_API.
2. Убедиться, что на стороне хранилища данных загруженный пакет находится в состоянии «Доступ ограничен», а операция над пакетом – в статусе «Выполнено» (в таблице PACKAGES схемы REGISTRY для пакета с заданным идентификатором поле CURRENT_STATUS_ID = 5, а поле OPERATION_STATUS_ID = 3).

Внимание! Пакет с информацией об абонентах может быть загружен повторно, только в случае если загружены все пакеты, отвергнутые до заданного. Повторную загрузку пакетов следует производить последовательно, начиная с первого незагруженного (последнего отвергнутого).

5 Управление справочниками локального источника

DRS предоставляет возможность заполнения справочников-карт автоматически при загрузке данных о соединениях и платежах, а также путем выполнения операций добавления, объединения, разделения и удаления деталей сущностей посредством пользовательского интерфейса. При этом не нарушается целостность загруженных данных.

1 Возможности по редактированию справочников-карт

В базе данных хранилища данных каждый справочник-карта представляет собой две таблицы (XXX – название справочника-карты):

- XXX_MAP (мастер-таблица) – содержит атрибуты, не изменяемые во времени. Записи в мастер-таблицу добавляются только при загрузке данных о соединениях и платежах. В целях поддержания целостности загруженных данных добавление, редактирование и удаление записей через web-интерфейс невозможно.
- XXX_MAP_DET (детальная таблица) – содержит атрибуты, изменяющиеся с течением времени. Над записями детальной таблицы возможно выполнение следующих операций:
  - добавление;
  - редактирование;
  - удаление;
  - разделение на две записи (с указанием даты разделения);
  - объединение двух записей (с указанием записи, атрибуты которой будут у получившейся записи).

Операции добавления, объединения, разделения и удаления деталей сущностей доступны для следующих справочников:

- Коммутаторы;
- Транки;
- Роуминговые партнеры (недоступен для просмотра через web-интерфейс);
- Типы соединений;
- Типы платежей.

При выполнении загрузки данных загружаемые данные помещаются в буферные таблицы, где данные мапируются, после чего загружаются в хранилище данных. При мапировании учитывается дата-время записей в загружаемых данных.

При создании, редактировании, загрузке интервалов действия деталей справочников-карт не допускается создание пересекающихся по времени интервалов для одной и той же мастер-записи карты. В случае попытки создать или изменить перекрывающийся интервал через web-интерфейс выдается ошибка с сообщением о недопустимости таких действий. При загрузке данных в случае обнаружения в загружаемых данных записей с интервалом действия, пересекающимся с уже существующими в хранилище данных интервалами, в результате загрузки существующие интервалы в справочнике:

- не изменяются (если загружаемый интервал и интервал в хранилище данных совпадают по датам начала и конца);
- расширяются (если атрибуты деталей совпадают, или загружаемые атрибуты пусты);

Управление режимами расширения интервалов действия записей справочников при загрузке интервала действия с пустыми атрибутами осуществляется с помощью настроечных параметров CALLS_MAPS_EXTEND_MODE и PAYM_MAPS_EXTEND_MODE, определяющих, расширяются ли примыкающие интервалы, либо же производится добавление новой записи.

- не изменяются, но добавляются смежные интервалы (если атрибуты деталей не совпадают и временной интервал загружаемых деталей шире).

Например, если коммутатор с некоторым идентификатором присутствует в загружаемых данных о соединении за 01.01.2009 10:11:55, то считается, что этот коммутатор был активен весь день 01.01.2009. В случае если запись с таким идентификатором коммутатора и идентификатором формата данных в основной таблице отсутствует, то добавляется запись в мастер-таблицу и в детальную таблицу с периодом действия записи за весь указанный день.

В случае если запись с такими идентификаторами и идентификатором формата данных в основной таблице присутствует, то дальнейшие действия будут зависеть периодов действия соответствующих ей записей в детальной таблице:

- если в детальной таблице присутствует запись с периодом, включающим дату 01.01.2009 (например, 15.12.2008-15.01.2009), период действия записи в детальной таблице останется неизменным;
- если в детальной таблице присутствует запись с периодом, примыкающим к дате 01.01.2009 (например, 02.01.2009-10.01.2009), период действия записи в детальной таблице будет расширен (т.е. новый период действия – 01.01.2009-10.01.2009);
- если в детальной таблице отсутствуют записи, периоды действия которых включают или примыкают к дате 01.01.2009, будет добавлена новая запись с периодом действия за 01.01.2009.

При загрузке данных из внешних источников приоритет имеют интервалы действия, уже имеющиеся в хранилище данных. Например, если загружается интервал действия за сутки, за которые уже имеется интервал действия в хранилище данных, то загрузка интервала за эти сутки из внешнего источника (файла и т.д.) фактически не происходит.

Допускается существование мастер-записи любого справочника-карты без деталей, т.е. возможно удаление последней детали справочника.

2 Настройка карты типов соединений

После загрузки архива информации о соединениях оператора связи необходимо настроить карту типов соединений. Карта типов соединений создается при загрузке в DRS данных о соединениях и представляет собой набор последовательностей вида x-y-z, где:

- x – код типа соединения в учетных записях о соединениях, полученных от оператора связи;
- y – код дополнительной услуги в учетных записях оператора связи;
- z – тип абонента, к которому относится детальная информация.

Для корректной обработки поисковых запросов и отражения результатов поиска информации о фактах телефонных соединений необходимо после загрузки в DRS первоначального объема фактов соединений отредактировать элементы построенной к этому моменту карты типов соединений, привязав каждый из них к зарегистрированному типу соединения, направлению соединения и действию над услугой.

Действия по настройке и редактированию элементов карты типов соединений необходимо повторять по мере появления в данных, поступающих от оператора связи, новых комбинаций вида x-y-z (типа соединения – кода дополнительной услуги – типа абонента).

6 Управление системными задачами

DRS предоставляет возможность управления системными задачами, включающего следующие действия:

- просмотр;
- диагностика;
- запуск;
- деактивация;
- останов;

- запуск вне расписания;
- повторный запуск;
- добавление дополнительных экземпляров поисковых задач.

1 Просмотр системных задач

Полный перечень задач, зарегистрированных для функционирования DRS, содержится в представлении AUTH.V_BASE_SCHEDULER_JOBS. Информация о задачах может быть получена с помощью запроса, выполненного на базах хранилища данных и сервера заявок от имени администратора Oracle:

```
SELECT t.JOBSET_NAME, -- Имя шаблона Job-a
       t.OWNER,       -- схема -  владелец Job-a
       t.JOB_NAME,    -- Имя Job-a
       t.JOB_CLASS,   -- Имя Класса Job-a
       t.COMMENTS,    -- Комментарий Имя Job-a
       t.ENABLED,     -- Признак того что Job активен
       t.REPEAT_INTERVAL, -- Интервал запуска
       t.LAST_START_DATE, -- Последний запуск
       t.NEXT_RUN_DATE     -- Следующий запуск
FROM auth.v_base_scheduler_jobs t
Order by t.JOB_NAME
```

2 Диагностика состояния системных задач

Для диагностики состояния задач Oracle следует обратиться к представлению ALL_SCHEDULER_JOBS, выполнив на базах хранилища данных и сервера заявок следующий SQL-запрос от имени администратора Oracle:

```
select t.Owner, t.Job_Name, t.State, t.run_count, t.failure_count
  from All_Scheduler_Jobs t
where t.Job_Name like 'SSP%'
order by t.Owner, t.Job_Name;
```

Представление содержит следующие поля:

- OWNER – схема - владелец задачи;
- JOB_NAME – имя задачи;
- STATE – текущее состояние задачи. Значение DESABLED является признаком остановки задачи;
- RUN_COUNT – общее количество запусков задачи;
- FAILURE_COUNT – количество запусков задачи, завершившихся ошибкой. Увеличение значения в поле при выполнении запроса является признаком некорректного выполнения задачи.

3 Запуск системных задач

Для запуска заданной системной задачи следует запустить процедуру AUTH.BASE_JOBWORK_PG.EnableJob подсистемы SVC_BASE_API.

1 Формат:

```
procedure EnableJob(
   pi_sJobName in base_jobs.Job_name%type);
```

2 Параметры:

- pi_sJobName – имя задачи.

4 Деактивация системных задач

Для деактивации заданной системной задачи следует запустить процедуру AUTH.BASE_JOBWORK_PG.DisableJob подсистемы SVC_BASE_API.

1 Пример вызова процедуры:

```
begin
base_jobwork_pg.disablejob(pi_sjobname => 'имя задачи',
                           pi_bforce => true);
```

```
base_jobwork_pg.stopjob(pi_sjobname => 'имя задачи',
                        pi_bforce => true);
end;
```

2 Параметры:

- pi_sJobName – имя задачи;
- pi_bForce – признак необходимости деактивации задачи в любом случае:
  - TRUE – деактивируется и работающая задача;
  - FALSE – деактивируется только незапущенная в данный момент задача – для запущенной задачи формируется сообщение об ошибке.

  Значение по умолчанию FALSE.

5 Останов задачи

Для останова заданной системной задачи следует запустить процедуру AUTH.BASE_JOBWORK_PG.StopJob подсистемы SVC_BASE_API.

1 Формат:

```
procedure StopJob(
   pi_sJobName     in base_jobs.job_name%type,
   pi_bForce       in boolean,
   pi_bWaitForStop in boolean default true);
```

2 Параметры:

- pi_sJobName – имя задачи;
- pi_bForce – флаг останова задачи, если она запущена [TRUE/FALSE];
- pi_bWaitForStop – флаг ожидания остановки задачи [TRUE/FALSE]. Значение по умолчанию TRUE (ожидать).

6 Запуск задачи вне расписания

Для однократного запуска задачи вне расписания следует запустить процедуру AUTH.BASE_JOBWORK_PG.RunJob подсистемы SVC_BASE_API.

1 Формат:

```
procedure runjob(
   pi_sjobname in base_jobs.job_name%type)
```

2 Параметры:

- pi_sjobname – имя задачи.

7 Повторный запуск всех системных задач

В случае если часть системных задач не выполняется или выполняется некорректно, рекомендуется перезапустить все задачи с помощью утилиты RestartAllJob подсистемы SVC_BASE_API. В результате выполнения данной утилиты все задачи будут сначала остановлены, а затем запущены заново согласно расписанию. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему SVC_BASE_API.

1 Повторный запуск поисковых задач

В случае если не выполняются или некорректно выполняются только поисковые задачи на сервере хранилища данных (с именами SSP_STASK_%), рекомендуется перезапустить их с помощью утилиты RestartSearchJob из состава дистрибутива подсистемы DRS_DWH_REGISTRY_API. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему DRS_DWH_REGISTRY_API.

8 Добавление дополнительных экземпляров поисковых задач

При регистрации источника создается несколько системных задач (не менее двух), обеспечивающих выполнение поисковых запросов. В случае если их количества недостаточно (например, обнаружено, что растет очередь поисковых заданий источнику, увеличивается время обработки заданий из-за задержки их выборки из очереди заданий источнику и т.д.), следует запустить утилиту AddSearchJobs из состава подсистемы DRS_DWH_REGISTRY_API. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему DRS_DWH_REGISTRY_API.

Значение параметра СУБД Oracle JOB_QUEUE_PROCESS должно быть не меньше общего количества системных задач, запускаемых на базе хранилища данных.

7 Создание сертификатов для работы с HAS_SERVER

В случае истечение срока действия сертификатов необходимо создать сертификаты заново. Создание сертификатов включает в себя следующие этапы:

1. Подготовка сертификационного центра для хранения сертификатов Certificate Authority (CA) (выполняется только в том случае если необходимо заменить все ранее используемые сертификаты, включая корневые сертификаты).
2. Создание сертификатов для работы с Apache;
3. Создание сертификатов для работы с HAS-сервером;
4. Создание дополнительной структуры для хранения сертификатов.

Подтвержденные сертификаты, оставшиеся от предыдущих инсталляций, должны быть удалены.

1 Подготовка сертификационного центра

Для подготовки нового сертификационного центра следует создать каталог [[ROOT_PKI]] – корневой каталог сертификационного центра, распаковать архив подсистемы SVC_CERT. Структура каталогов следующая:

- ca.db.index – база выписанных корневых сертификатов;
- ca.db.serial – порядковый номер выписываемого сертификата;
- openssl_ca_root.conf – конфигурационный файл для формирования запроса на генерацию самоподписного корневого сертификата;
- openssl_ca_client.conf – конфигурационный файл для формирования запроса на генерацию корневого сертификата, необходимого для удостоверения клиентских сертификатов;
- openssl_ca_root_sign.conf – конфигурационный файл для подписания запросов корневым самоподписным сертификатом;
- openssl_ca_server.conf – конфигурационный файл для формирования запроса на генерацию корневого сертификата, необходимого для удостоверения серверных сертификатов;
- ca.db.certs – каталог с выписанными корневыми сертификатами;
- center.client – каталог для формирования клиентских сертификатов;
  - ca.db.index – база выписанных клиентских сертификатов;
  - ca.db.serial – порядковый номер выписываемого сертификата;
  - openssl_ca_client_sign.conf – конфигурационный файл для подписания клиентского сертификата;
  - openssl_req_client.conf – конфигурационный файл для формирования запроса на генерацию клиентского сертификата;
  - ca.db.certs – каталог с выписанными клиентскими сертификатами;
- center.has – каталог для формирования сертификатов для работы с HAS-сервером;
  - ca.db.index – база выписанных сертификатов для работы с HAS-сервером;
  - ca.db.serial – порядковый номер выписываемого сертификата;

- `openssl_req_client.conf` – конфигурационный файл для формирования запроса на генерацию клиентского сертификата, необходимого при доступе к HAS;
- `openssl_ca_client_sign.conf` – конфигурационный файл для подписания клиентского сертификата, необходимого при доступе к HAS;
- `openssl_req_server.conf` – конфигурационный файл для формирования запроса на генерацию серверного сертификата HAS;
- `openssl_ca_server_sign.conf` – конфигурационный файл для подписания серверного сертификата HAS;
- `openssl_ca_root.conf` – конфигурационный файл для формирования запроса на генерацию самоподписного корневого сертификата HAS;
- `ca.db.certs` – каталог с выписанными сертификатами для HAS;

- `center.server` – каталог для формирования серверных сертификатов;
  - `ca.db.index` – база выписанных серверных сертификатов;
  - `ca.db.serial` – порядковый номер выписываемого сертификата;
  - `openssl_req_server.conf` – конфигурационный файл для формирования запроса на генерацию серверного сертификата;
  - `openssl_ca_server_sign.conf` – конфигурационный файл для подписания серверных сертификатов;
  - `ca.db.certs` – каталог с выписанными серверными сертификатами.

Все серверные сертификаты (и клиентский сертификат для HAS) выдаются сроком на 5 лет, клиентские сертификаты выдаются на 1 год, CRL формируется на 1 месяц. Для корректной работы серверов CRL необходимо перегенерировать каждый месяц. Для обновления CRL Apache может периодически взаимодействовать с сертификационным центром (CA) через HAS_SERVER, описание взаимодействия приводится в документации на HAS.

2 Сертификаты для работы с Apache

Количество создаваемых сертификатов для работы с Apache зависит от того, как будет осуществляться доступ к DRS. Кроме того, следует учитывать наличие развернутого центра сертификации.

1 Самоподписной корневой сертификат

Самоподписной сертификат рекомендуется создавать только при отсутствии развернутого центра сертификации.

В условиях уже созданного центра сертификации следует изменить значения параметров `certificate` и `private_key` в файле `[[ROOT_PKI]]/openssl_ca_root_sign.conf` дистрибутива подсистемы SVC_CERT (где `[[ROOT_PKI]]` – корневой каталог центров сертификации), указав наименования существующих файлов сертификата и ключа.

Для создания самоподписного сертификата следует:

1. Установить права доступа к корневому каталогу центров сертификации `[[ROOT_PKI]]` только для пользователя `root` (операцию следует выполнять только в среде Red Hat Enterprise Linux):

   ```
   chown -R root:root [[ROOT_PKI]]
   find [[ROOT_PKI]] -type d | xargs chmod 700
   find [[ROOT_PKI]] -type f | xargs chmod 600
   ```

2. Перейти в каталог [[ROOT_PKI]] и сформировать запрос на получение сертификата:

   ```
   openssl req -new -newkey rsa:2048 -keyout ca_root.key -x509 -nodes -days 1825
   -out ca_root.crt -config openssl_ca_root.conf
   ```

3. В случае необходимости изменить значения параметров, запрашиваемых в процессе генерации сертификата. В качестве значения `Common Name (CN)` рекомендуется указывать легко распознаваемое и доступное для понимания наименование: например, `Root CA DRS`.

2 Подчиненный серверный сертификат

Для создания серверного сертификата следует:

1. Перейти в каталог `[[ROOT_PKI]]` и сформировать запрос на получение сертификата:

```
openssl req -new -newkey rsa:2048 -nodes -keyout ca_server.key -days 1825 -out
ca_server.csr -config openssl_ca_server.conf
```

2. В случае необходимости изменить значения параметров, запрашиваемых в процессе генерации сертификата. В качестве значения Common Name (CN) рекомендуется указывать легко распознаваемое и доступное для понимания наименование: например, Server DRS.
3. Подписать запрос:
```
openssl ca -out ca_server.crt -config openssl_ca_root_sign.conf -notext -infiles
ca_server.csr
```
4. Перенести созданные файлы ca_server.key и ca_server.crt в каталог [[ROOT_PKI]]/center.server.

3 Подчиненный клиентский сертификат

Для создания клиентского сертификата следует:

1. Перейти в каталог [[ROOT_PKI]] и сформировать запрос на получение сертификата:
```
openssl req -new -newkey rsa:2048 -nodes -keyout ca_client.key -days 1825 -out
ca_client.csr -config openssl_ca_client.conf
```
2. В случае необходимости изменить значения параметров, запрашиваемых в процессе генерации сертификата. В качестве значения Common Name (CN) рекомендуется указывать легко распознаваемое и доступное для понимания наименование: например, CA Client DRS.
3. Подписать запрос:
```
openssl ca -out ca_client.crt -config openssl_ca_root_sign.conf -notext -infiles
ca_client.csr
```
4. Перенести созданные файлы ca_client.key и ca_client.crt в каталог [[ROOT_PKI]]/center.client.

4 Серверный сертификат для Apache WebInterface

Для создания серверного сертификата, обеспечивающего аутентификацию Apache в случае доступа к DRS через web-интерфейс, следует:

1. Перейти в каталог [[ROOT_PKI]]/center.server и сформировать запрос на получение сертификата:
```
openssl req -new -newkey rsa:2048 -nodes -keyout server_apache_web.key -days 1825
-out server_apache_web.csr -config openssl_req_server.conf
```
2. Изменить значения параметров, запрашиваемых в процессе генерации сертификата, руководствуясь следующими рекомендациями:
   - указать значение Organization Unit Name (например, Apache WebInterface);
   - в качестве значения Common Name (CN) указать доменное имя сайта.
3. Подписать запрос:
```
openssl ca -out server_apache_web.crt -config openssl_ca_server_sign.conf -notext
-infiles server_apache_web.csr
```

3 Сертификаты для работы с HAS-сервером

Для обеспечения безопасной работы с HAS-сервером следует создать самоподписной корневой сертификат, серверный сертификат, а также клиентский сертификат для аутентификации Apache WebInterface в качестве клиента при доступе к HAS-серверу;

1 Самоподписной корневой сертификат

Для создания сертификата следует:

1. Перейти в каталог [[ROOT_PKI]]/center.has и сформировать запрос на получение сертификата:
```
openssl req -new -newkey rsa:2048 -nodes -keyout ca_root_has.key -x509 -days 1825
-out ca_root_has.crt -config openssl_ca_root.conf
```
2. В случае необходимости изменить значения параметров, запрашиваемых в процессе генерации сертификата. В качестве значения Common Name (CN) рекомендуется указывать легко распознаваемое и доступное для понимания наименование: например, HAS CA DRS.

2 Серверный сертификат

Для создания сертификата следует:

1. Перейти в каталог `[[ROOT_PKI]]/center.has` и сформировать запрос на получение сертификата:
   ```
   openssl req -new -newkey rsa:2048 -nodes -keyout server_has.key -days 1825 -out server_has.csr -config openssl_req_server.conf
   ```
2. В случае необходимости изменить значения параметров, запрашиваемых в процессе генерации сертификата, руководствуясь следующими рекомендациями:
   - в качестве значения `Common Name` (CN) указать доменное имя HAS-сервера.
3. Подписать запрос:
   ```
   openssl ca -out server_has.crt -config openssl_ca_server_sign.conf -notext -infiles server_has.csr
   ```

3 Клиентский сертификат для Apache WebInterface

Для создания сертификата следует:

1. Перейти в каталог `[[ROOT_PKI]]/center.has` и сформировать запрос на получение сертификата:
   ```
   openssl req -new -newkey rsa:1024 -nodes -keyout client_apache_web.key -days 1825 -out client_apache_web.csr -config openssl_req_client.conf
   ```
2. В случае необходимости изменить значения параметров, запрашиваемых в процессе генерации сертификата, руководствуясь следующими рекомендациями:
   - в качестве значения `Common Name` (CN) указать легко распознаваемое и доступное для понимания наименование: например, `Client HAS WebInterface`.
3. Подписать запрос:
   ```
   openssl ca -out client_apache_web.crt -config openssl_ca_client_sign.conf -notext -infiles client_apache_web.csr
   ```
4. Конвертировать сертификат в формат PKCS#12:
   ```
   openssl pkcs12 -in client_apache_web.crt -inkey client_apache_web.key -export -out client_apache_web.p12
   ```

После проверки работы HAS-сервера файл client_apache_web.p12 следует удалить (см. раздел «Размещение сертификатов на HAS-сервере»).

4 Дополнительная структура для хранения сертификатов

Чтобы упростить процедуру установки сертификатов на web-серверах Apache, следует в корневом каталоге центров сертификации создать отдельный каталог с сертификатами для каждого сервера.

1 Структура для Apache WebInterface

Чтобы обеспечить хранение сертификатов, необходимых для работы Apache WebInterface, следует:

1. Создать каталог `[[ROOT_PKI]]/for_apache_web`.
2. Скопировать в созданный каталог следующие файлы:
   - `[[ROOT_PKI]]/center.has/ca_root_has.crt`;
   - `[[ROOT_PKI]]/center.server/server_apache_web.crt`;
   - `[[ROOT_PKI]]/center.server/server_apache_web.key`;
   - `[[ROOT_PKI]]/center.has/client_apache_web.crt`;
   - `[[ROOT_PKI]]/center.has/client_apache_web.key`.
3. Переименовать скопированные файлы:
   - `ca_root_has.crt` в `CAcertificate.crt`;
   - `server_apache_web.crt` в `server.crt`;
   - `server_apache_web.key` в `server.key`;
   - `client_apache_web.crt` в `client.crt`;

- client_apache_web.key в client.key.

4. Скопировать в файл CAcertificate.crt содержимое следующих файлов:
   - [[ROOT_PKI]]/ca_root.crt;
   - [[ROOT_PKI]]/center.server/ca_server.crt.
5. В каталоге [[ROOT_PKI]]/for_apache_web создать PEM-файл клиентского сертификата для проксирования экспорта пользовательских файлов на HAS-сервер с помощью Apache WebInterface:
   5.1. Создать файл proxy.pem.
   5.2. Скопировать в созданный файл содержимое файлов client.crt и client.key.

8 Создание дополнительной учетной записи администратора

При необходимости создать дополнительного пользователя с минимальным набором прав, необходимым для начала работы с DRS через web-интерфейс, следует запустить утилиту AdditionalAdmin из состава утилит подсистемы DRS_HAS_API. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему DRS_HAS_API.

9 Удаление данных

Для удаления доступны данные, дата актуальности которых входит в период для удаления, т.е. не превышает граничную дату глубины хранения. Глубина (срок) хранения данных задается настроечными параметрами RTASK_RESULTS_STORAGE_DEPTH, CALLS_STORAGE_DEPTH, REQ_REPORTS_STORAGE_DEPTH, REQUESTS_STORAGE_DEPTH, AUDIT_STORAGE_DEPTH, LOG_STORAGE_DEPTH, RTASKS_STORAGE_DEPTH (подробнее см. в документе «Настроечные параметры [DRS-DOC_SETUP_PRM]»).

Для изменения предустановленного значения какого-либо параметра следует запустить процедуру SetDepthStorage. Параметры вызова процедуры см. в документе «Руководство системного программиста» на подсистему DRS_CMN_API.

1 Типы удаляемых данных

Типы удаляемых данных организованы в древовидную структуру. При удалении данных родительского типа всегда удаляются и данные дочерних (зависимых) типов, поэтому глубина хранения данных дочернего типа не должна превышать глубину хранения данных родительского типа.

Ниже приводится краткое описание типов данных для удаления.

1 CALLS

Данные о соединениях (хранятся на сервере хранилища данных).

Удалению подлежат записи индивидуальных таблиц хранения оператора связи: EVENTS_<TELCO_ID>_MAIN, EVENTS_<TELCO_ID>_PRED и EVENTS_<TELCO_ID>_OPER схемы DATASRV (где <TELCO_ID> – идентификатор оператора связи). В качестве даты актуальности удаляемых данных принимается дата начала соединения.

Записи удаляются только если пакет, в котором они поступили, находится в состоянии «Доступен» или «Доступ ограничен».

При удалении данных о соединениях удаляются также пакеты, в которых поступили удаляемые записи. Если пакет содержит хотя бы одну запись о соединении, дата актуальности которой выходит за рамки периода удаления, то ни одна запись о соединениях из этого пакета не удаляется.

2 BASE_LOG

Данные системного лога (хранятся на сервере заявок и сервере хранилища данных).

Удалению подлежат записи таблицы AUTH.BASE_LOG. В качестве даты актуальности удаляемых данных принимается дата записи в лог.

При удалении данных системного лога удаляются также следующие объекты:

- контексты, на которые ссылаются удаляемые записи;

- записи о сессиях лога, дата открытия которых меньше граничной даты глубины хранения и которые не имеют дочерних записей в журнале лог.

3 AUDIT

Журнал аудита (хранится на сервере заявок).

Удалению подлежат записи таблицы AUTH.SYS_AUDIT. В качестве даты актуальности удаляемых данных принимается дата записи в журнал аудита.

При удалении записей журнала аудита удаляются также записи о сессиях, дата закрытия которых меньше граничной даты глубины хранения и которые не имеют дочерних записей в журнале аудита.

4 REQUESTS

Заявки с заданиями (хранятся на сервере заявок).

Удалению подлежат записи таблицы SSP_DOCS.REQUESTS. В качестве даты актуальности удаляемых данных принимается дата создания заявки.

При удалении заявок удаляются также следующие объекты:

- поисковые задания и отчеты, связанные с удаляемой заявкой;
- задания источникам, связанные с удаляемыми заданиями.

5 RTASKS

Поисковые задания (хранятся на сервере заявок).

Удалению подлежат записи таблицы REQUEST_TASKS схемы REQSRV. В качестве даты актуальности удаляемых данных принимается дата создания поискового задания.

6 RTASK_RESULTS

Результаты поиска (хранятся на сервере заявок).

Удалению подлежат записи таблиц MOBILE_CDRS_RESPONSE, PAGING_CDRS_RESPONSE, STATIONARY_CDRS_RESPONSE, DATA_CDRS_RESPONSE, SUBS_RESPONSE и PAYM_RESPONSE схемы REQSRV. В качестве даты актуальности удаляемых данных принимается дата создания поискового задания, которому принадлежат результаты.

Поисковое задание, для которого удалены результаты, переводится в статус TASK_ARCHIVED (заархивировано) – формирование отчета по такому заданию невозможно.

Результаты поиска удаляются также при удалении соответствующих поисковых заданий.

7 REQUESTS_REPORTS

Отчеты по заявкам (хранятся на сервере заявок).

Удалению подлежат записи таблицы SSP_DOCS.REQUEST_REPORTS. В качестве даты актуальности принимается дата создания отчета.

Файлы отчетов удаляются также при удалении соответствующих заявок (с заданиями).

2 Автоматическая очистка устаревших данных

Автоматическая очистка устаревших данных производится для типов данных CALLS, BASE_LOG.

Процесс автоматической очистки регулируется:

- для типа данных CALLS – настроечными параметрами относительной суммарной наполненности файлов данных CALLS_HIGH_WATERMARK, CALLS_LOW_WATERMARK;
- для типа данных BASE_LOG – настроечными параметрами относительной суммарной наполненности файлов данных LOG_HIGH_WATERMARK, LOG_LOW_WATERMARK.

Описание настроечных параметров см. в документе «Настроечные параметры» (DRS-DOC_SETUP_PRM-RUS).

Попытка удаления устаревших данных по соединениям производится либо после загрузки пакета данных по соединениям, либо при работе системных задач «Перенос необработанных партиций оперативного периода» и/или «Перенос обработанных партиций», либо по созданной пользователем задаче на удаление устаревших данных.

Попытка удаления устаревших данных системного лога производится либо периодически, в 00:05 каждого дня, либо по созданному пользователем вручную заданию на удаление устаревших данных.

10 Поиск данных

Поиск данных выполняется через web-интерфейс. Подробное описание действий, необходимых для проведения поиска, см. в руководстве оператора, встроенном в web-интерфейс. В данном разделе рассматриваются особенности обработки данных при проведении поиска.

1 Поиск данных о соединениях

DRS предоставляет возможность поиска данных о соединениях по следующим наборам параметров:

- по различным атрибутам абонента (номер телефона, IMSI, IMEI и пр.) или идентификаторам оборудования оператора связи;
- по атрибутам LAC и CELL базовых станций;
- по списку телефонных номеров.

1 Данные партнеров по роумингу

При поиске по базовой станции в результаты поиска не включаются записи, поступившие от роуминговых партнеров (загруженные из TAP-файлов). Если условия поиска содержат номер транка партнера по роумингу, поиск не выполняется (т.к. данные о транках не загружаются из TAP-файлов).

2 Стандарт связи соединения

При поиске соединений осуществляется определение стандарта связи для каждой записи о соединении, удовлетворяющей условиям поиска, по следующему правилу:

1. При наличии установленного стандарта связи для типа соединения, к которому привязана запись о соединении, за период времени, в который попадает запись о соединении, – за стандарт связи принимается стандарт, установленный для данного типа соединения;
2. Если для типа соединения стандарт связи не определен – за стандарт связи записи принимается стандарт, привязанный к формату загрузки пакета, в котором поступила запись о соединении.

2 Поиск абонентской информации

1 Тип клиента

При поиске идентификаторов абонентов по наименованию клиента, действует следующее правило. Клиент считается юридическим лицом, если поле `JUR_TYPE_ID` в таблице `SUBS_DATA.CLIENTS` для соответствующей записи принимает значение `0` (неизвестен), `2` (юридическое лицо), `3` (ИЧП) или `NULL`.

2 Стандарт связи абонента

Правила определения принадлежности абонента к стандарту связи зависят от способа загрузки данных. Загрузка данных производится с помощью подсистем универсальной (файловой) загрузки: если для оператора связи зарегистрирован один стандарт связи, все абоненты оператора в загружаемых файлах должны быть помечены тем же стандартом связи; если для оператора связи зарегистрированы несколько стандартов связи, то для каждого абонента в файле должен быть указан стандарт связи; Если в результате нештатной ситуации в хранилище данных был загружен абонент, не привязанный к стандарту связи, то при поиске действуют следующие правила:

- Абонент относится к стандарту GSM при выполнении следующих условий:
  - загружаемая запись об абоненте содержит IMSI или IMEI, а также телефонный номер;
  - загружаемая запись об абоненте не содержит MIN;
  - для оператора связи зарегистрирован стандарт GSM.
- Абонент относится к стандарту CDMA при выполнении следующих условий:

- загружаемая запись об абоненте содержит IMSI или IMEI, а также телефонный номер
- загружаемая запись об абоненте не содержит MIN;
- для оператора связи не зарегистрирован стандарт GSM;
- для оператора связи зарегистрирован стандарт CDMA.

- Абонент относится к стандарту PSTN при выполнении следующих условий:
  - загружаемая запись об абоненте содержит телефонный номер и адрес установки;
  - для оператора связи зарегистрирован стандарт PSTN.

Во всех остальных случаях абонент относится к стандарту связи по умолчанию: GSM.

Правила определения принадлежности соединения к стандарту связи зависят от количества стандартов, зарегистрированных для оператора, и состава загруженных данных. Если в хранилище данных для оператора связи зарегистрирован один стандарт связи, то все соединения, информация о которых поступает от этого оператора, относятся к этому стандарту. Если для оператора зарегистрировано несколько стандартов связи, то действуют следующие правила:

- Соединение относится к стандарту GSM, если запись о соединении не содержит MIN, но содержит IMSI или IMEI, а также телефонный номер, и для оператора связи в хранилище данных зарегистрирован стандарт GSM.
- Соединение относится к стандарту CDMA при выполнении одного из следующих вариантов условий:
  - запись о соединении не содержит MIN, но содержит IMSI или IMEI, а также телефонный номер, и для оператора связи в хранилище данных не зарегистрирован стандарт GSM, но зарегистрирован стандарт CDMA;
  - запись о соединении содержит MIN и для оператора связи в хранилище данных зарегистрирован стандарт CDMA.

Во всех остальных случаях соединение относится к стандарту связи по умолчанию: GSM.

3 Преобразование символов

Загружаемые данные могут содержать символы, одинаковые по начертанию, но относящиеся к различным алфавитам и имеющие разные коды. Например, латинская буква "c" одинакова по начертанию с русской "с", но отлична по коду символа из кодовой таблицы.

В этом случае обеспечивается поиск загруженных исходных данных с одинаковым начертанием символов, но разными их кодами, с помощью единственного поискового запроса, заданного на одном языке.

При нахождении в строке поиска определяющих символов только одного алфавита (символов из таблицы SUBS_DATA.ALPH_DEFINE_CHARS, принадлежащих к этому алфавиту), этот алфавит считается основным. К нему будет далее производиться преобразование похожих символов из всех других алфавитов.

Если строка содержит определяющие символы нескольких алфавитов, то основной алфавит считается неопределенным.

Если строка не содержит определяющих символов ни одного из алфавитов, то основным алфавитом считается тот, который указан в качестве значения настроечного параметра ALPH_CONV_DEF (только в случае, если строка содержит символы этого алфавита, указанные для него в таблице SUBS_DATA.ALPH_CHAR_CONV или SUBS_DATA.ALPH_DEFINE_CHARS). В противном случае основной алфавит считается неопределенным.

В случае успешного определения основного алфавита строки к нему производится преобразование одинаково выглядящих символов этой строки всех остальных алфавитов по правилам, которые заданы в таблице SUBS_DATA.ALPH_CHAR_CONV. Если основной алфавит не был определен, строка остается неизменной.

Каждая строка таблицы SUBS_DATA.ALPH_CHAR_CONV задает пары похожих символов CHAR1 (алфавит ALPH_APLH1_ID) и CHAR2 (алфавит ALPH_ALPH2_ID).

После определения основного алфавита строки из таблицы SUBS_DATA.ALPH_CHAR_CONV выбираются все символы из других алфавитов, похожие на символы основного алфавита, и производится преобразование символов из неосновных алфавитов к соответствующим им символам основного.

При поиске по маске преобразование символов поискового запроса не производится, и возможно отсутствие результатов, если при поиске используется точно скопированная из загружаемых данных часть слова.

Пример 1:

Загружены данные об абоненте «Иванов Антон Михайлович», причем в имени буква «А» введена латиницей. В этом случае строка с фамилией, именем и отчеством будет преобразована к кириллическому алфавиту и поиск даст результаты.

Пример 2:

Загружены данные об абоненте «Иваноff Антон Михайлович», причем в имени буква «А» введена латиницей. В этом случае строка с фамилией, именем и отчеством не будет преобразована к кириллическому алфавиту (т.к. невозможно определить основной алфавит), и поиск не даст результатов.

3 Обработка внутренних номеров в результатах поиска

Необходимость обработки внутренних номеров в результатах поиска задается настроечным параметром PRM_CHECKINSNUM (подробнее см. в документе «Настроечные параметры [DRS-DOC_SETUP_PRM]»).

В результатах поиска абонентской информации (таблица REQSRV.SUBS_RESPONSE) на наличие внутренних номеров проверяются следующие поля:

- основной номер телефона (NUM);
- контактный телефон (CLNT_CNCT_PHONE);
- телефон для доставки счета (DLVR_PHONE);
- внутренний номер телефона (SUBS_INT_NUMBER);
- перечень телефонов внутренних пользователей (INTERNAL_USERS_PHONES).

В результатах поиска данных о соединениях (таблица REQSRV.MOBILE_CDRS_RESPONSE – мобильная связь, таблица REQSRV.STATIONARY_CDRS_RESPONSE – фиксированная связь) на наличие внутренних номеров проверяются следующие поля:

- номер телефона абонента оператора связи (SUBS_PHONE_NUM);
- вызывающий номер телефона (A_PHONE_NUM);
- вызываемый номер телефона (B1_PHONE_NUM);
- номер переадресации (B2_PHONE_NUM).

В результатах поиска данных о платежах (таблица REQSRV.PAYM_RESPONSE) на наличие внутренних номеров проверяются следующие поля:

- основной номер телефона абонента (SUBS_PHONE_NUM);
- внутренний номер телефона абонента (SUBS_INT_NUMBER).

11 Мониторинг работы DRS

Продукт предоставляет возможность мониторинга с помощью методов SNMP. Общая схема мониторинга представлена на рис.1.

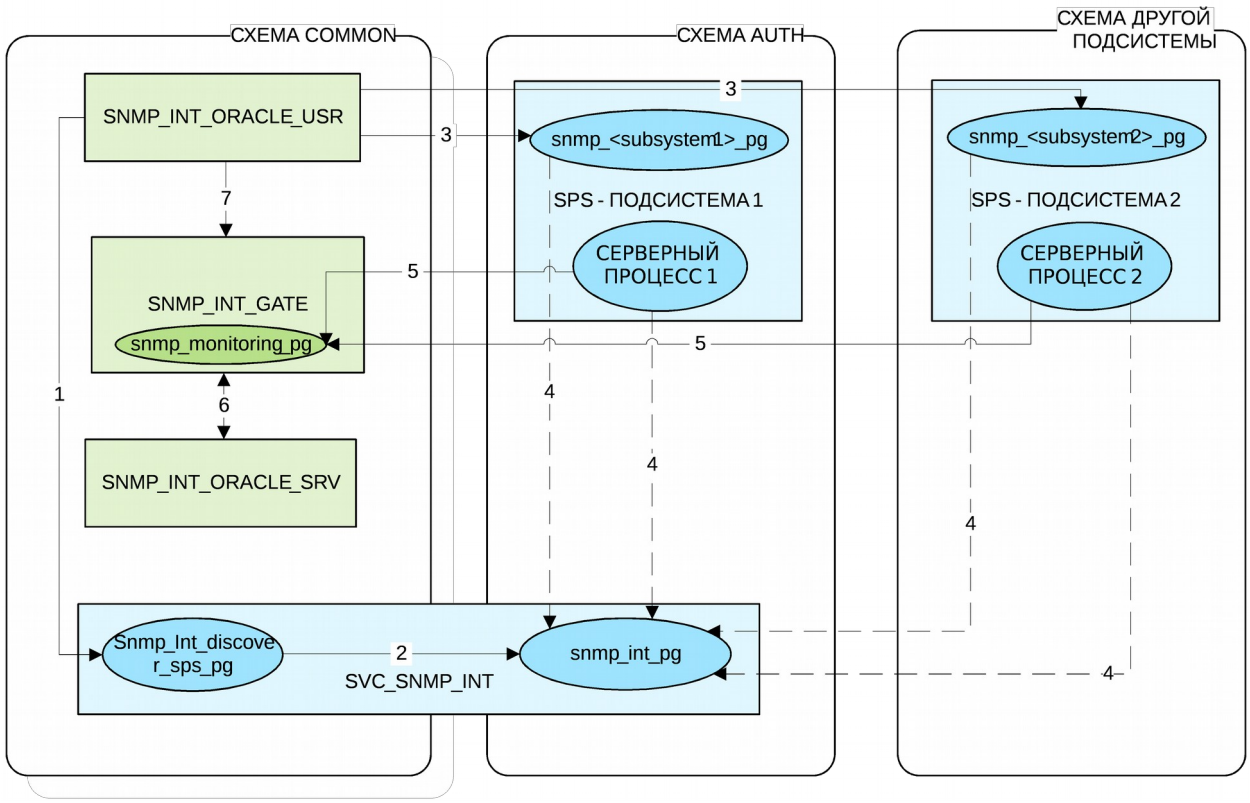

Рисунок 1 – Общая схема мониторинга

Стрелками на схеме обозначены направления вызовов для предоставления и получения данных. На схеме приняты следующие обозначения:

- SNMP_INT_ORACLE – подсистема «SNMP_INT Oracle интерфейс». Позволяет осуществлять SNMP мониторинг БД подсистем. Для получения детальной информации следует обратиться к документации на подсистему «SNMP_INT Oracle интерфейс» (SNMP_INT_ORACLE).
- SNMP_INT_GATE – подсистема «Шлюз к продукту SNMP_INT». Является прокси для вызовов серверной части подсистемы SNMP_INT_ORACLE. Может работать как заглушка при отсутствии установленной подсистемы SNMP_INT_ORACLE или выключенной поддержке SNMP.
- Snmp_monitoring_pg – пакет, предоставляющий доступ к SNMP_INT_ORACLE. Для получения детальной информации следует обратиться к документации на подсистему «Шлюз к продукту SNMP_INT» (SNMP_INT_GATE).
- SVC_SNMP_INT – подсистема «Поддержка SNMP мониторинга» (входит в состав SVC_BASE). Осуществляет интеграцию подсистемы «SNMP_INT Oracle интерфейс» (SNMP_INT_ORACLE) и подсистем, входящих в состав SVC_BASE. Устанавливается и регистрируется в схеме AUTH и в схеме, в которую установлена подсистема «Шлюз к продукту SNMP_INT» (SNMP_INT_GATE).
- Snmp_int_discover_sps_pg – пакет, имеющий имя и API, описанные в документации на подсистему SNMP_INT_ORACLE.
- Snmp_int_pg – пакет, предоставляющий для пакета Snmp_int_discover_sps_pg информацию об установленных подсистемах, а также управляет включением и выключением мониторинга в зависимости от наличия установленной опции.
- SPS–подсистема 1(2) – подсистема в составе продукта, для которой реализован мониторинг.
- Snmp_<subsystem1(2)>_pg – пакет подсистемы, через который можно получить значения параметров мониторинга подсистемы. Пакет при всех запросах метрик проверяет включенность опции SNMP. Для подсистемы SVC_SNMP_INT в этой роли выступает пакет Snmp_int_pg.

- Серверный процесс 1(2) – job или другой серверный процесс, который предоставляет о себе информацию для мониторинга.
- Взаимосвязи на схеме:
  - 1 – при старте сервера SNMP_INT_ORACLE пользовательская часть SNMP_INT_ORACLE запрашивает у пакета Snmp_int_discover_sps_pg список установленных подсистем.
  - 2 – пакет Snmp_int_discover_sps_pg запрашивает список установленных подсистем у пакета Snmp_int_pg.
  - 3 – «Прямой доступ» к метрикам мониторинга подсистемы. В MIB-файле описывается вызов пакета Snmp_<subsystem1(2)>_pg из схемы, в которую установлена подсистема.
  - 4 – проверка доступности опции SNMP.
  - 5 – серверные процессы помещают метрики мониторинга в SNMP_INT_ORACLE посредством вызовов SNMP_INT_GATE.
  - 6 – SNMP_INT_GATE проксирует вызовы методов сохранения и получения значений метрик мониторинга на подсистему SNMP_INT_ORACLE.
  - 7 – в MIB-файле описывается получение метрик, которые сохраняют серверные процессы.

Диагностирование является частью следующих подсистем:

- «Программный интерфейс подсистемы DRS_RQS_SCR» (DRS_RQS_API);
- «Интерфейс схемы справочников» (DRS_DICTS_API);
- «Программный интерфейс подсистемы DRS_DWH_REGISTRY_SCR» (DRS_DWH_REGISTRY_API);
- «Подсистема файловой загрузки в хранилище данных по технологии внешних таблиц Oracle» (SVC_FILE_ET_LOADER);
- «Программный интерфейс подсистемы DRS_DWH_CALLS_SCR» (DRS_DWH_CALLS_API);
- «Программный интерфейс подсистемы DRS_DWH_SUBS_SCR» (DRS_DWH_SUBS_API);
- «Программный интерфейс подсистемы DRS_DWH_PAYM_SCR» (DRS_DWH_PAYM_API);
- «Система регистрации файлов» (DRS_GATEWAY).

Возможность мониторинга подключается как дополнительная опция путем установки подсистемы «Мониторинг DRS» (DRS_KEYS.O_SRS_DIAGNOSTIC). Опция позволяет активировать процесс самодиагностики путем сбора, накопления и систематизации диагностической информации подсистем. Диагностическая информация подразделяется на три уровня: параметры работоспособности подсистемы в целом (level1), параметры ключевых функций (level2) и параметры мониторинга для детальной локализации проблемы (level3).

В случае необходимости автоматического опроса параметров мониторинга подсистемы «Система регистрации файлов» (DRS_GATEWAY) по расписанию следует использовать подсистему «SNMP_INT сервер» (SNMP_INT_SERVER). Для этого нужно скопировать MIB-файл в каталог MIB-файлов подсистемы «SNMP_INT сервер» либо в файле конфигурации подсистемы «SNMP_INT сервер» указать директорию расположения MIB-файлов подсистемы PS_SNMP_AGENT.

1 Параметры мониторинга подсистем

При мониторинге подсистем используются следующие параметры:

1. Сервер заявок:
   - Синхронизация справочников с источниками данных (таблица rqsDictsStatTable MIB-файла подсистемы DRS_RQS_API).
   - Таблица выполняющихся на данный момент запросов (таблица rqsExecSTaskTable MIB-файла подсистемы DRS_RQS_API).
   - Таблица ожидающих выполнения запросов (таблица rqsWaitSTaskTable MIB-файла подсистемы DRS_RQS_API).
   - Таблица источников данных и их состояний (таблица rqsSourcesTable MIB-файла подсистемы DRS_RQS_API).

- Таблица распределения данных по источникам данных (таблица `rqsTelcoSourcesTable` MIB-файла подсистемы `DRS_RQS_API`).
- Таблица типов запросов словарей (таблица `rqsDictsScenariosTable` MIB-файла подсистемы `DRS_RQS_API`).
- Таблица типов запросов сценариев (запрос справочников, поисковые запросы, управляющие команды) (таблица `rqsRequestScenariosTable` MIB-файла подсистемы `DRS_RQS_API`).

2. Хранилище данных:
   - Таблица статусов задач загрузки через `EXTRACT` (таблица `regExtractLoaderTable` MIB-файла подсистемы `DRS_DWH_REGISTRY_API`).
   - Таблица статусов задач отвержения пакетов (таблица `regRejectProcTable` MIB-файла подсистемы `DRS_DWH_REGISTRY_API`).
   - Таблица статусов задач обработки поисковых заданий (таблица `regSTaskProcTable` MIB-файла подсистемы `DRS_DWH_REGISTRY_API`).
   - Таблица задач загрузки из файлов пакетов данных (таблица `etldrLoaderTable` MIB-файла подсистемы `SVC_FILE_ET_LOADER`).
   - Таблица распределения данных о соединениях, полученных от оператора связи, по таблицам предварительного, оперативного и архивного хранения (таблица `callsArcStorageTable` MIB-файла подсистемы `DRS_DWH_CALLS_API`).
   - Состояние задач переноса данных из предварительного хранения в оперативное и архивное хранение, и из оперативного хранения в архивное хранение, а также задач удаления устаревших данных (таблица `callsMoveProcTable` MIB-файла подсистемы `DRS_DWH_CALLS_API`).
   - Таблица диапазона размеченных табличных пространств для хранения данных о соединениях оператора связи (таблица `callsPartitionsTable` MIB-файла подсистемы `DRS_DWH_CALLS_API`).
   - Таблица диапазона размеченных табличных пространств для хранения данных об истории услуг, предоставляемых абонентам операторов связи (таблица `subsServPartitionsTable` MIB-файла подсистемы `DRS_DWH_SUBS_API`).
   - Таблица диапазона размеченных табличных пространств для хранения данных о платежах клиентов операторов связи (таблица `paymPartitionsTable` MIB-файла подсистемы `DRS_DWH_PAYM_API`).
   - Таблица экземпляров файлового шлюза (таблица `gwInstanceTable` MIB-файла подсистемы `DRS_GATEWAY`).
   - Таблица статусов задач синхронизации событий прямого контроля (таблица `regDCEProcTable` MIB-файла подсистемы `DRS_DWH_REGISTRY_API`).
   - Таблица статистики по форматам загрузки (общее количество пакетов, количество пакетов, ожидающих загрузки) (таблица `regFormatsStatsTable` MIB-файла подсистемы `DRS_DWH_REGISTRY_API`).
   - Таблица файловых форматов (таблица `gwFileFormatsTable` MIB-файла подсистемы `DRS_GATEWAY`).
   - Таблица операторов связи (таблица `dictsTelcosTable` MIB-файла подсистемы `DRS_DICTS_API`).
   - Таблица форматов загрузки (таблица `regFormatsTable` MIB-файла подсистемы `DRS_DWH_REGISTRY_API`).

2 Методы мониторинга

Подсистема `SVC_SNMP_INT` содержит набор функций, предназначенных для сбора информации об установленных подсистемах.

1 Функция получения списка установленных подсистем (SNMP_INT_PG.GET_APPLICATIONS)

Возвращает список установленных подсистем.

Формат:

```
FUNCTION GET_APPLICATIONS
RETURN SYS_REFCURSOR
```

Результат:

Курсор, содержащий перечень установленных подсистем с указанием их версий.

2 Функция проверки опции DRS_KEYS.O_SPS_DIAGNOSTIC (SNMP_INT_PG.CheckOption)

Возвращает признак наличия опции `DRS_KEYS.O_SPS_DIAGNOSTIC`.

Формат:

```
FUNCTION CheckOption
    RETURN BOOLEAN
```

Результат:

`TRUE`, если установлена опция `DRS_KEYS.O_SPS_DIAGNOSTIC`.

ГЛАВА

5 МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

1 Модель прав доступа

Разграничение прав доступа достигается назначением каждому пользователю определенного набора прав (привилегий).

Набор привилегий пользователя определяется как объединение привилегий, назначенных группам прав, в которые входит пользователь.

Механизм группировки привилегий позволяет создавать типовые наборы привилегий, формируя предопределенные ограничения для пользователей системы.

1 Виды привилегий

В DRS реализованы следующие виды привилегий:

- объектные – обеспечивают возможность выполнять операции с конкретными объектами; типы объектов описаны в виде так называемого «дерева объектов», над каждым типом объектов определен набор действий-привилегий над этим типом объекта;
- интерфейсные – обеспечивают доступ к элементам пользовательского web-интерфейса.

2 Объектные привилегии: типы объектов, действия над объектами

Объектные привилегии представляют собой набор прав, определяющий доступные действия над объектами.

DRS поставляется со встроенным набором типов объектов и определенных для этих объектов привилегий.

Например:

В DRS зарегистрирован тип объекта «Виды запросов». Экземплярами объектов данного типа являются виды поисковых запросов.

Для данного типа объекта определены следующие объектные привилегии:

- Просмотр поисковых заданий указанного вида – определяет доступность действия: просмотр поискового задания с указанным видом запроса.
- Добавление поисковых заданий указанного вида – определяет доступность действия: создание поискового задания с указанным видом запроса.
- Добавление к заявке с недействительными реквизитами санкции суда – определяет доступность действия: добавление поискового задания с указанным видом запроса в рамках заявки, у которой не указаны или недействительны реквизиты санкции суда (например, истек срок). Доступно только для режима работы с использованием заявок (режим можно выбрать при установке подсистемы DRS_RQS_API).
- Запуск задания – определяет доступность действия: запустить поисковое задание с указанным видом запроса на исполнение.
- Отказ в выполнении задания – определяет доступность действия: отказать в выполнении поискового задания с указанным видом запроса.

3 Объектные привилегии: родительский объект для типа объекта

Тип объекта «Виды запросов» имеет фиксированный перечень экземпляров объектов данного типа. В DRS также есть типы объектов, количество экземпляров которых не является постоянным, а может увеличиваться в процессе эксплуатации. Для таких типов объектов важным для определения привилегий является родительский объект.

Например:

В DRS зарегистрирован тип объекта «Подразделения». Экземплярами объектов данного типа являются зарегистрированные подразделения. При поставке регистрируется корневое подразделение с наименованием SYSTEM. Остальные подразделения создаются в зависимости от сложности организационной структуры конкретной точки установки и необходимости разграничения полномочий пользователей разных подразделений на действия над другими объектами.

Для типа объекта «Подразделения» родительским объектом являются объекты того же типа, о чем говорит заголовок формы настройки объектных привилегий (см. Рисунок 2).

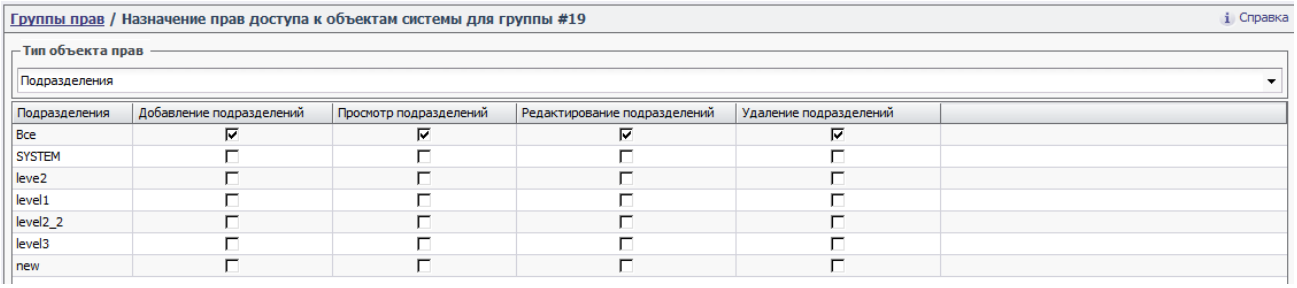

Рисунок 2 – Родительский объект

Для типа объекта «Подразделения» определены следующие объектные привилегии:

- Добавление подразделений – определяет доступность действия: добавление подразделения внутри указанного родительского подразделения.
- Просмотр подразделений – определяет доступность действия: просмотр подразделений внутри указанного родительского подразделения.
- Редактирование подразделений – определяет доступность действия: редактирование подразделений внутри указанного родительского подразделения.
- Удаление подразделений – определяет доступность действия: удаление подразделений внутри указанного родительского подразделения.

Если необходимо выдать привилегию на все экземпляры данного типа объекта, независимо от того, к какому родительскому объекту они относятся, используется специальный вид привилегии «Все».

4 Системные привилегии

В DRS существует ряд привилегий, которые условно названы «системными привилегиями». Эти привилегии регулируют выполнение действий, которые невозможно или нецелесообразно связывать с конкретным типом объектов, но регулировать права на выполнение этих действий необходимо. К числу системных привилегий относятся привилегии, объединенные типами «Системный объект» и «Специальные справочники»:

- Вход в систему – определяет доступность действия: регистрация пользователя при входе в систему.
- Изменение приоритетов – определяет доступность действия: изменение срочности заявки в рамках журнала заявок.
- Назначение ответственного оператора – определяет доступность действия: изменение ответственного оператора заявки в рамках журнала заявок.
- Ранее удаленные группы прав – определяет возможность просмотра ранее удаленных групп прав в рамках журнала заявок, журнала аудита, при просмотре списка заявок и при редактировании заявок.

- Ранее удаленные подразделения – определяет возможность просмотра ранее удаленных подразделений в рамках журнала заявок, журнала аудита, при просмотре списка заявок и при редактировании заявок.
- Ранее удаленные пользователи – определяет возможность просмотра ранее удаленных пользователей в рамках журнала заявок, журнала аудита, при просмотре списка заявок и при редактировании заявок.
- Добавление данных в справочник внутренних номеров – определяет доступность одноименного действия.
- Изменение данных в справочнике внутренних номеров – определяет доступность одноименного действия.
- Просмотр списка внутренних номеров – определяет доступность одноименного действия.
- Работа с результатами поиска с внутренними номерами – определяет доступность записей, содержащих внутренние (особые) номера, при просмотре результатов поиска и формировании отчетов с результатами.
- Удаление данных из справочника внутренних номеров – определяет доступность одноименного действия.

5 Полный перечень типов объектов

Типы объектов организованы в иерархическую структуру: каждый тип (за исключением системных привилегий) обладает родительским типом. Корневые типы объектов являются родительскими по отношению к себе. Для каждого типа объектов зарегистрированы одна или несколько привилегий. При установке привилегий права на действия над объектами устанавливаются через объекты родительских типов. Структура типов объектов представлена на Рисунке 3.

EMBED Visio.Drawing.11

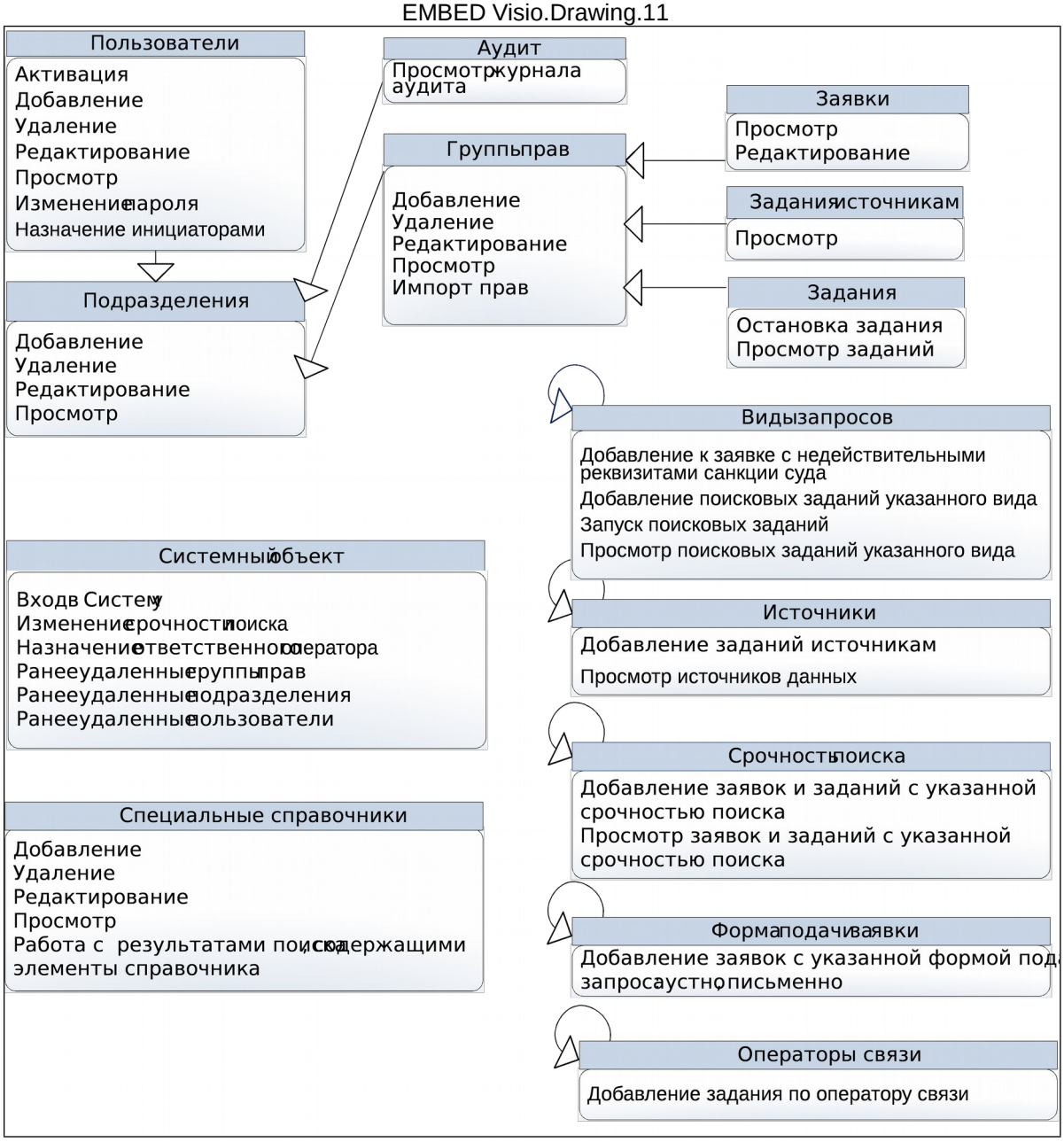

Рисунок 3 – Структура типов объектов

1 Тип объектов «Подразделения»

Тип объектов «Подразделения» представляет собой совокупность зарегистрированных структурных единиц для объединения пользователей.

Родительским объектом для подразделения является объект того же типа – родительское подразделение. Права на работу с дочерними объектами наследуются от прав на родительские подразделения.

При настройке привилегий флаг, установленный напротив наименования подразделения, означает наличие привилегии на выполнение действия над дочерними подразделениями, например: Редактирование подразделений, относящихся к родительскому подразделению с наименованием SYSTEM.

Возможные действия над объектами данного типа:

- Добавление подразделений. Обязательным условием добавления объекта типа «Подразделение» является его связь с родительским объектом такого же типа. При установке автоматически создается подразделение SYSTEM, являющееся корневым элементом в иерархической структуре объектов данного типа. Установка флага в данном поле возможна только совместно с флагом «Просмотр подразделений».

Возможность добавления подразделения первого уровня (без привязки к родительскому) поддерживается только в случае, если установлен флаг «Все» в столбце «Добавление подразделений».

- Просмотр подразделений.
- Редактирование подразделений. Установка флага в данном поле возможна только совместно с флагом «Просмотр подразделений».
- Удаление подразделений. Обязательным условием удаления объекта типа «Подразделение», кроме наличия привилегии на удаление, является отсутствие в системе дочерних объектов, связанных с данным подразделением: «Пользователи», «Группы прав». Удалять подразделение SYSTEM категорически не рекомендуется. Установка флага в данном поле возможна только совместно с флагом «Просмотр подразделений».

Для обеспечения полноты и достоверности информации, отображаемой в журнале аудита, журнале заявок, списке заявок и при редактировании заявок, записи обо всех когда-либо созданных подразделениях сохраняются в базе данных. В связи с этим при добавлении или редактировании подразделения не допускается присвоение ему наименования, как у уже зарегистрированного в том же родительском подразделении (в том числе удаленного).

Операция удаления подразделения, выполненная в web-интерфейсе, не приводит к фактическому удалению записи в базе данных – в результате выполнения операции заполняется поле DELETED в соответствующей таблице.

2 Тип объектов «Пользователи»

Тип объектов «Пользователи» объединяет зарегистрированных пользователей.

При установке автоматически создаются следующие пользователи:

- Administrator – пользователь, чья учетная запись используется для первого входа в систему и обладающий минимальным набором прав для начала работы с DRS;
- Поиск в локальной базе (LocalSearchSystem) – системная задача, обеспечивающая поиск в локальном источнике (хранилище данных);
- Поиск внешний (RemoteSearchSystem) – системная задача, обеспечивающая поиск в удаленных источниках;
- Процесс для запроса словарей (DictsRequestor) – системная задача, обеспечивающая синхронизацию справочников-карт и справочников на стороне источников данных.
- Управление поисковыми зад. (RQSJobs) – системная задача, обеспечивающая управление поисковыми заданиями.

Обязательным условием добавления объекта типа «Пользователи» является его связь с объектом типа «Подразделения». В каждый момент времени пользователь может быть привязан только к одному подразделению.

Родительским объектом для пользователей является объект типа «Подразделение» – родительское подразделение.

При настройке привилегий на действия над пользователями флаг, установленный напротив наименования подразделения, означает наличие привилегии на выполнение действия, например: Добавление пользователей в подразделение с наименованием SYS.

Возможные действия над объектами данного типа:

- Активация/блокировка учетной записи. Установка флага в данном поле возможна только совместно с флагом «Просмотр пользователей».
- Просмотр пользователей.
- Назначение пользователей инициаторами (проверяется при выборе пользователя-инициатора при добавлении заявки). Установка флага в данном поле возможна только совместно с флагом «Просмотр пользователей».
- Удаление пользователей. Установка флага в данном поле возможна только совместно с флагом «Просмотр пользователей».
- Добавление пользователей. Установка флага в данном поле возможна только совместно с флагом «Просмотр пользователей».

- Редактирование пользователей. Установка флага в данном поле возможна только совместно с флагом «Просмотр пользователей».
- Изменение паролей пользователей. Установка флага в данном поле возможна только совместно с флагом «Просмотр пользователей».

Для обеспечения полноты и достоверности информации, отображаемой в журнале аудита, журнале сессий, журнале заявок, списке заявок и при редактировании заявок, записи обо всех когда-либо созданных учетных записях пользователей сохраняются в базе данных. В связи с этим при добавлении или редактировании пользователя не допускается присвоение ему логина, ранее использовавшегося в DRS.

Чтобы пользователь не имел доступа к данным после удаления его учетной записи, при удалении ему автоматически присваивается другой пароль. В связи с этим удаление пользователя возможно, только в случае если инициатор действия обладает правом на изменение паролей пользователей данного подразделения.

Операция удаления пользователя, выполненная в web-интерфейсе, не приводит к фактическому удалению записи в базе данных – в результате выполнения операции заполняется поле DELETED в соответствующей таблице.

3 Тип объектов «Группы прав»

Тип объектов «Группы прав» представляет собой совокупность именованных объектов, которым назначается набор полномочий на доступ к объектам и элементам интерфейса.

Родительским объектом для группы прав является объект типа «Подразделения».

При добавлении объекта типа «Группа прав» его связь с объектом типа «Подразделение» не обязательна. Группы прав, не привязанные к подразделениям, используются для назначения общих привилегий, не зависящих от принадлежности к подразделениям. Для групп прав, привязанных к подразделениям, в каждый момент времени группа прав может быть привязана только к одному подразделению.

При установке автоматически создается группа прав, содержащая минимальный набор прав, необходимый для администрирования.

При настройке привилегий на действия над группами прав флаг, установленный напротив наименования подразделения, означает наличие привилегии на выполнение действия, например: Добавление групп прав в подразделение с наименованием SYS.

Для того чтобы было доступно действие добавление объекта типа «Группа прав» без привязки к подразделению, необходимо указать признак наличия привилегии напротив строки «Все».

Возможные действия над объектами данного типа:

- Просмотр групп прав.
- Добавление групп прав. Установка флага в данном поле возможна только совместно с флагом «Просмотр групп прав».
- Редактирование группы прав и принадлежности к ним пользователей. Установка флага в данном поле возможна только совместно с флагом «Просмотр групп прав».
- Удаление групп прав. Установка флага в данном поле возможна только совместно с флагом «Просмотр групп прав».
- Импорт прав для группы прав. Установка флага в данном поле возможна только совместно с флагом «Просмотр групп прав». Данное право позволяет пользователю импортировать права любой существующей группы прав в любую группу, при этом сам пользователь может не обладать привилегиями импортируемой группы прав.

Для обеспечения полноты и достоверности информации, отображаемой в журнале аудита, журнале заявок, списке заявок и при редактировании заявок, записи обо всех когда-либо созданных группах прав сохраняются в базе данных. В связи с этим при добавлении или редактировании группы прав не допускается присвоение ей наименования, ранее использовавшегося в DRS.

Операция удаления группы прав, выполненная в web-интерфейсе, не приводит к фактическому удалению записи в базе данных – в результате выполнения операции заполняется поле DELETED в соответствующей таблице.

4 Тип объектов «Аудит»

Тип объектов «Аудит» представляет собой совокупность записей системного журнала аудита, в котором фиксируются все действия пользователей.

Действия пользователей отображаются в журнале в следующих случаях:

- неудача проверки прав на выполнение операции;
- успех выполнения операции;
- неудача выполнения операции.

Для того чтобы было доступно действие просмотр записей журнала аудита о действиях системных пользователей (таких как Процесс поиска в локальном хранилище данных, Процесс для запроса словарей), необходимо указать признак наличия привилегии напротив строки «Все» или напротив строки с подразделением SYSTEM (в котором зарегистрированы системные пользователи).

Возможные действия над объектами данного типа:

- Просмотр аудита – просмотр записей о действиях пользователей, зарегистрированных в указанном подразделении.

5 Тип объектов «Заявки»

Тип объектов «Заявки» представляет собой совокупность зарегистрированных электронных документов, описывающих основания для проведения поиска информации. Доступен только в режиме работы с использованием заявок (режим можно выбрать при установке подсистемы `DRS_RQS_API`).

Обязательным условием добавления объекта типа «Заявка» является его связь с объектом типа «Группа прав». При создании объекта типа «Заявка» он связывается с одной из групп прав, к которым причислен пользователь, регистрирующий заявку. В каждый момент времени заявка может быть привязана только к одной группе прав. Значение поля «Группа-владелец», определяющее группу, которой принадлежал пользователь на момент создания заявки, постоянно и не меняется при назначении пользователю, создавшему заявку, другой группы прав. Таким образом, обеспечивается возможность просмотра всех заявок, созданных в момент времени, когда пользователи принадлежали заданной группе.

Родительским объектом для заявки является объект типа «Группа прав» – группа прав пользователя, регистрирующего заявку.

При настройке привилегий на действия над заявками флаг, установленный напротив группы прав, означает наличие привилегии на выполнение действия, например: Редактирование заявок, привязанных к указанной группе-владельцу, например: ALL2.

Возможные действия над объектами данного типа:

- Просмотр заявок.
- Редактирование заявок. Установка флага в данном поле возможна только совместно с флагом «Просмотр заявок».

Для выполнения действия <Добавление нового объекта типа «Заявка»> необходимо, чтобы пользователь обладал следующим минимальным набором объектных привилегий:

- Вход в систему (привилегия типа объекта «Системный объект»).
- Просмотр подразделений – просмотр подразделений, к которым привязаны группы прав, и пользователи-инициаторы, которые вводятся в параметрах заявки (привилегия типа объекта «Подразделения»).
- Просмотр пользователей (привилегия типа объекта «Пользователи»).
- Назначение пользователей инициаторами – возможность выбрать из списка пользователей пользователя-инициатора, от которого получен документ/распоряжение/санкция на проведение поиска (привилегия типа объекта «Пользователи»).
- Просмотр групп прав – возможность просмотра списка групп прав, к которым привязан пользователь, добавляющий заявку, с тем, чтобы выбрать из этого списка группу-владельца новой заявки (привилегия типа объекта «Группы прав»).
- Регистрация заявки с указанной формой подачи запроса – возможность видеть и выбирать в выпадающем списке «Форма подачи заявки» различные варианты (привилегия типа объекта «Форма подачи заявки»).

- Просмотр заявок и заданий с указанной срочностью поиска (привилегия типа объекта «Срочность поиска»).
- Добавление заявок и заданий с указанной срочностью поиска – возможность видеть и выбирать в выпадающем списке «Срочность поиска» различные варианты (привилегия типа объекта «Срочность поиска»).

Редактирование объекта типа «Заявки» в рамках аудита возможно, в случае если пользователь обладает следующим минимальным набором прав:

- Вход в систему (тип объектов «Системный объект»).
- Просмотр заявок (тип объектов «Заявки»).
- Редактирование заявок (тип объектов «Заявки»).
- Просмотр заявок и заданий с указанной срочностью поиска (тип объектов «Срочность поиска»).
- Просмотр пользователей (тип объектов «Пользователи»)
- Назначение ответственного оператора (тип объектов «Системный объект»).
- Изменение приоритетов (тип объектов «Системный объект»).

6 Тип объектов «Задания источникам»

Тип объектов «Задания источникам» представляет собой совокупность заданий на проведение поиска информации определенного типа в источниках данных, зарегистрированных в DRS.

Обязательным условием добавления объекта типа «Задания источникам» является его связь с объектом типа «Заявка», а через заявку – с группой прав, которая указана как группа-владелец заявки.

Родительским объектом для задания источникам является объект типа «Группа прав» – группа-владелец для заявки, в рамках которой создано задание источникам.

При настройке привилегий на действия над заданиями источникам флаг, установленный в напротив группы прав, означает наличие привилегии на выполнение действия.

Возможные действия над объектами данного типа:

- Просмотр заданий источникам. В текущей версии DRS данная объектная привилегия не реализована.

7 Тип объектов «Виды запросов»

Тип объектов «Виды запросов» представляет собой фиксированный набор сценариев поиска, в соответствии с которыми происходит выполнение поисковых заданий. «Вид запроса» – он же «Тип поискового задания» – выбирается пользователем при создании нового задания и не может быть изменен.

Родительским объектом для объекта «Виды запросов» является объект того же типа.

В DRS созданы следующие объекты типа «Виды запросов»:

- Запрос карточки Абонента.
- Команда: удаление задания.
- Поиск идентификаторов Абонента.
- Поиск пополнений Баланса.
- Поиск соединений.

Возможные действия над объектами данного типа:

- Действия, доступные в режимах с использованием и без использования заявок:
  - Просмотр поисковых заданий указанного вида. Действие возможно в рамках добавления заданий.
  - Добавление поисковых заданий указанного вида. Установка флага в данном поле возможна только совместно с флагом «Просмотр поисковых заданий указанного вида».
  - Запуск задания. Установка флага в данном поле возможна только совместно с флагом «Просмотр поисковых заданий указанного вида».
- Действия, доступные только в режиме с использованием заявок:

- Добавление к заявке с пустой санкцией – добавление задания с указанным видом запроса к заявке, в которой не заполнены поля с реквизитами санкции суда или истек период действия санкции суда. При отсутствии у пользователя права на данное действие DRS проверяет, что период, за который необходимо произвести поиск данных, входит в период действия санкции суда. При поиске информации «на данный момент» в качестве начальной и конечной даты поискового периода принимается текущая системная дата (время 00:00:00 и 23:59:59 соответственно). Установка флага в данном поле возможна только совместно с флагом «Просмотр поисковых заданий указанного вида».

8 Тип объектов «Задания»

Тип объектов «Задания» представляет собой совокупность заданий на проведение поиска информации определенного типа.

Родительским объектом для задания является группа прав пользователя, создающего задание (объект типа «Группы прав»).

Возможные действия над объектами данного типа:

- Просмотр поисковых заданий источникам. Действие возможно в рамках остановки заданий из списка заданий.
- Остановка задания. Установка флага в данном поле возможна только совместно с флагом «Просмотр поисковых заданий источникам».

9 Тип объектов «Источники»

Тип объектов «Источники» представляет собой совокупность логических разделов локального хранилища данных и внешних источников данных, в которых будет осуществляться поиск. По типу взаимодействия сервера заявок с источником выделены следующие типы источников:

3. Локальный источник – локальное хранилище данных.
4. Удаленный источник – удаленный источник данных.
5. По протоколу SMD/538 – удаленный источник, подключенный через адаптер SMD (538).

Родительским объектом для объекта «Источники» является объект того же типа «Источники».

При настройке привилегий на действия над «Источниками» флаг, установленный напротив источника, означает наличие привилегии на выполнение действия конкретно над этим объектом, например: Просмотр источника LOCAL_SOURCE.

Для того чтобы новые источники, подключаемые к DRS, становились видны без перенастройки привилегий объекта «Источники», достаточно указать признак наличия привилегии напротив строки «Все».

Возможные действия над объектами данного типа:

- Давать источникам задания на выполнение. Установка флага в данном поле возможна только совместно с флагом «Просмотр источников».
- Просмотр источников.

10 Тип объектов «Срочность поиска»

Тип объектов «Срочность поиска» задает варианты приоритетов поиска информации.

Родительским объектом для объекта «Срочность поиска» является объект того же типа «Срочность поиска».

В DRS созданы следующие экземпляры объектов типа «Срочность поиска»:

- АПК.
- Низкая.
- Нормальная.
- Высокая.
- Запрос справочников.
- Управляющая команда.

Возможные действия над объектами данного типа:

- Просмотр заявок и заданий с указанной срочностью поиска.

- Добавление заявок и заданий с указанной срочностью поиска. Установка флага в данном поле возможна только совместно с флагом «Просмотр заявок и заданий с указанной срочностью поиска».

Вид срочности «Запрос справочников» является наиболее приоритетным и используется при автоматической синхронизации справочников-карт и справочников на стороне источников данных. Не рекомендуется использовать данный вид срочности при добавлении заявок – следует ограничить права пользователей на его использование, настроив соответствующим образом интерфейсные и объектные привилегии.

11 Тип объектов «Форма подачи заявки»

Тип объектов «Форма подачи заявки» задает возможные варианты формы подачи заявки (доступен только в режиме работы с использованием заявок; режим можно выбрать при установке подсистемы DRS_RQS_API).

Родительским объектом для объекта «Форма подачи заявки» является объект того же типа.

В DRS созданы следующие экземпляры типа «Форма подачи запроса», которые могут быть выбраны при добавлении заявки:

- Устно.
- Письменно.

Возможные действия над объектами данного типа:

- Регистрация заявки с указанной формой подачи запроса.

12 Тип объектов «Операторы связи»

Тип объектов «Операторы связи» представляет собой совокупность зарегистрированных операторов связи. Родительским объектом для объекта типа «Операторы связи» является объект того же типа.

Возможные действия над объектами данного типа:

- Добавление задания по оператору связи.

Право на добавление задания по оператору связи реализуется при создании поискового задания. На этапе выбора оператора связи, в данных которого следует производить поиск, список операторов связи ограничивается в зависимости от выданных пользователю привилегий. Список включает тех операторов, по которым пользователь имеет право добавлять задания. Наличие объектной привилегии проверяется в момент сохранения поискового задания.

Привилегия распространяется только на добавление поискового задания и не ограничивает доступ к другим справочникам и таблицам, содержащим сводную справочную информацию, полученную от всех операторов связи.

13 Тип объектов «Системный объект»

Тип объектов «Системный объект» объединяет права на выполнение специфических действий, которые невозможно связать с экземплярами других типов объектов, но выполнение которых должно регламентироваться правами:

- Вход в систему – определяет доступность действия «Регистрация пользователя при входе в систему».
- Изменение приоритетов – определяет доступность действия «Изменение срочности заявки». Действие возможно только в рамках журнала заявок (только в режиме работы с использованием заявок; режим можно выбрать при установке подсистемы DRS_RQS_API).
- Назначение ответственного оператора – определяет доступность действия «Изменение ответственного оператора заявки». Действие возможно только в рамках журнала заявок (только в режиме работы с использованием заявок).
- Ранее удаленные группы прав – определяет возможность просмотра ранее удаленных групп прав. Действие возможно в рамках журнала заявок, журнала аудита, при просмотре списка заявок, при редактировании заявок.
- Ранее удаленные подразделения – определяет возможность просмотра ранее удаленных подразделений. Действие возможно в рамках журнала заявок, журнала аудита, при просмотре списка заявок, при редактировании заявок.

- Ранее удаленные пользователи – определяет возможность просмотра ранее удаленных пользователей. Действие возможно в рамках журнала заявок, журнала сессий, журнала аудита, при просмотре списка заявок, при редактировании заявок.

14 Тип объектов «Специальные справочники»

Тип объектов «Специальные справочники» объединяет права на выполнение действий со специальным справочником «Внутренние номера» и результатами проведения поиска, в которых были обнаружены внутренние номера.

Возможные действия над объектами данного типа:

- Добавление данных в справочник внутренних номеров – определяет доступность одноименного действия. Установка флага в данном поле возможна только совместно с флагом «Просмотр списка внутренних номеров».
- Изменение данных в справочнике внутренних номеров – определяет доступность одноименного действия. Установка флага в данном поле возможна только совместно с флагом «Просмотр списка внутренних номеров».
- Просмотр списка внутренних номеров – определяет доступность одноименного действия.
- Работа с результатами поиска с внутренними номерами – определяет доступность строк результатов поиска, содержащих внутренние (особые) номера. Установка флага в данном поле возможна только совместно с флагом «Просмотр списка внутренних номеров».
- Удаление данных из справочника внутренних номеров – определяет доступность одноименного действия. Установка флага в данном поле возможна только совместно с флагом «Просмотр списка внутренних номеров».

6 Интерфейсные привилегии

Интерфейсные привилегии представляют собой набор прав, определяющий доступные пользователю страницы/переходы/кнопки в web-интерфейсе. Описание действий по настройке интерфейсных привилегий см. в руководстве оператора, встроенное в web-интерфейс продукта DRS.

Настройка интерфейсных привилегий производится путем прямого указания признака доступности конкретных элементов интерфейса, представленных в виде иерархического списка (см. Рисунок 4).

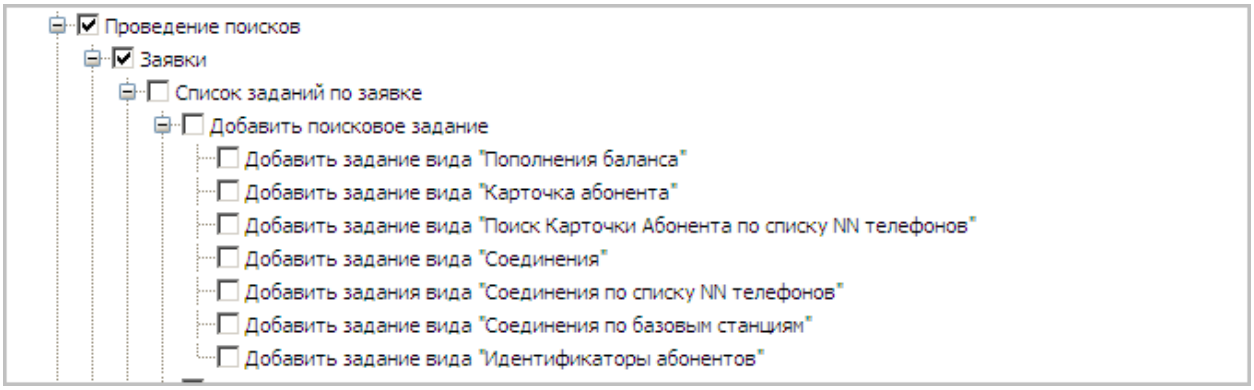

Рисунок 4 – Интерфейсные привилегии

7 Пользовательские ограничения

Пользовательские ограничения позволяют устанавливать максимально допустимое количество объектов, с которыми может работать пользователь.

Реализованы следующие пользовательские ограничения:

- ограничение на количество заданий за сутки;
- ограничение на количество заданий на поиск абонентов за сутки;
- ограничение на количество заданий на поиск платежей за сутки;
- ограничение на количество заданий на поиск соединений за сутки;
- ограничение на количество результатов по соединениям;

- ограничение на количество результатов поиска абонентской информации;
- ограничение на количество результатов поиска информации о платежах.

Если количество заданий, созданных пользователем в течение суток, достигло установленного ограничения, до окончания периода (суток) создание нового задания невозможно.

Ограничение на количество результатов поиска определяет максимальное количество доступных результатов, полученных в рамках выполнения одного задания источнику (т.е. результатов, полученных по одному поисковому заданию от одного источника). Если количество результатов по одному заданию источнику достигло установленного ограничения, то для такого задания в списке заданий в поле «Ограничение» будет указано «Да». Это означает, что часть результатов, полученных от данного источника, недоступна для просмотра.

При расчете максимально допустимого количества результатов поиска данных о соединениях сначала учитываются результаты по мобильной связи, а затем (если лимит не исчерпан) – результаты по фиксированной связи.

Ограничения устанавливаются для группы прав. В случае если пользователь привязан к нескольким группам прав, то для него применяется наименее жесткое ограничение из установленных для групп прав, к которым он привязан. Например, пользователь привязан к группам прав GROUP1 и GROUP2. Для группы прав GROUP1 установлено ограничение по количеству заданий за сутки, равное 10. Для группы прав GROUP2 установлено ограничение по количеству заданий за сутки, равное 20. Пользователь будет иметь возможность добавлять 20 заданий за сутки. Если для одной из групп прав установлены пользовательские ограничения, а для другой – нет, то ограничения накладываться не будут.

8 Использование групп для назначения прав пользователей

Выполнение сценариев взаимодействия с DRS через пользовательский интерфейс возможно только в случае, если пользователь обладает как объектными, так и интерфейсными привилегиями.

Права пользователя определяются набором привилегий, назначенных группам прав, в которые входит пользователь.

Для того чтобы назначить пользователю привилегии, следует связать его с одной или несколькими группами прав. Пользователь получает набор прав той группы, к которой он отнесен. В случае если пользователь отнесен к нескольким группам, он получает суммарный набор прав, определенных для указанных групп.

Если группам прав, к которым привязан пользователь, назначены пользовательские ограничения одного и того же типа, то для пользователя будет установлено максимальное (наименее жесткое) из них. Если хотя бы для одной из групп пользователя ограничение не установлено, для пользователя такое ограничение также не задается.

При создании правовых групп рекомендуется руководствоваться принципом атомарности, т.е. создавать группы, содержащие минимальные наборы прав, что позволит оперативно управлять привилегиями пользователей, избегая настройки самих правовых групп.

Чтобы назначить пользователю привилегии, рекомендуется:

1. Определить подразделение, к которому относится пользователь. Если подразделение не зарегистрировано в списке подразделений, зарегистрировать новое подразделение.
2. Определить группы прав, реализующие доступные пользователю действия. Если группы прав не зарегистрированы, создать их и назначить для них интерфейсные и объектные привилегии. В случае если необходимо выделить набор прав, характерный только для сотрудников конкретного подразделения, при создании группы таких прав указать привязку группы к этому подразделению и настроить привилегии со ссылкой на родительский объект – подразделение.
3. В списке пользователей создать учетную запись пользователя, которому будут назначаться привилегии, указав привязку к соответствующему подразделению.
4. Связать пользователя с требуемыми группами прав.

Для удобства назначения привилегий в DRS предусмотрена функциональность импорта (клонирования) привилегий для группы прав из одной группы прав в другую. Процесс импорта (клонирования) поддерживает следующие режимы привязки прав к сущностям, выбираемые при клонировании прав:

1. Привязка клонируемых прав ко «всем» объектам для привилегий, привязываемых к подразделениям или группам прав.

2. Привязка клонируемых прав к группам прав и подразделениям, выбранным пользователем, осуществляющим клонирование прав, для привилегий, привязываемых к подразделениям или группам прав.

Настройка привязки привилегий, связываемых с сущностями, отличными от групп прав и подразделений (например, срочность заданий, операторы связи, источники данных), осуществляется вручную после клонирования прав, при наличии такой необходимости. При клонировании прав привязка привилегий к таким объектам будет перенесена из группы прав - источника как есть, т.е. настройки связи привилегий с объектами, отличными от подразделений и групп прав, которые были в группе прав - источнике настроек, будут перенесены и в группу прав, в которую клонировались настройки.

При клонировании прав из одной группы в другую настройки привилегий группы прав, в которую осуществляется клонирование, не удаляются, т.е. копирование прав производится, дополняя ранее имевшиеся привилегии группы прав.

Пользовательские ограничения при клонировании прав из одной группы прав в другую не переносятся.

Импорт прав может выполняться из веб-интерфейса (см. встроенную документацию на подсистему DRS_WEB) или с помощью процедуры клонирования привилегий AUTH.CloneGroupPrivs (подробное описание параметров процедуры см. в документе «Руководство системного программиста» на подсистему SVC_AUTH_API).

ГЛАВА

6 АВАРИЙНЫЕ СИТУАЦИИ

В главе указываются возможные ошибки при работе с DRS и приводится перечень действий, которые следует предпринять пользователю при их возникновении.

1 Ошибки при установке

В случае если при установке какого-либо блока произошла ошибка, следует выяснить причину возникновения ошибки, проанализировав логи установки блока, на котором произошла ошибка; устранить причину ошибки и установить заново все подсистемы, подлежащие установке в данном блоке.

1 Ошибки обновления информации о пользователе в HAS

В случае если лог-файл при установке или обновлении front-end содержит сообщения об ошибках вида

Hot update access rights not performed. You need to restart HAS server <error_code>

где <error_code> – код ошибки, возвращаемой HAS-сервером, следует:

1. Провести детальный анализ проблемы. Подробное описание ошибок см. в документе «Подсистема «Высокопроизводительный сервер приложений». Руководство системного программиста [HAS_SERVER-DOC_ADMIN]».
2. Убедиться, что в конфигурационном файле HAS-сервера в качестве значения параметра `ssl_trusted` указан внешний IP базы, на которой развернута схема HAS (если база кластерная, следует указать IP обоих узлов кластера).
3. Перезапустить HAS-сервер.

2 Ошибки доступа к web-сайту

При попытке доступа к web-сайту пользователем может быть получено следующее сообщение системы безопасности:

- в Microsoft Internet Explorer:

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust certifying authority.

Сертификат выдан организацией, не входящей в состав доверенных. Откройте сертификат, чтобы уточнить доверие.

- в Mozilla Firefox:

Your browser does not recognize the Certificate Authority that issued the site's certificate.

К сертификату нет доверия, так как к сертификату его издателя нет доверия.

Данные сообщения возникают, в случае если серверный сертификат для Apache был подписан не доверенным центром сертификации (CA-центром).

Чтобы избежать получения указанных сообщений, следует импортировать созданный сертификат в хранилище доверенных CA-центров браузера.

Вход в систему невозможен: учетная запись пользователя заблокирована

20999: <LogID>43380</LogID>Вход в систему невозможен: Login fail

Причины возникновения ошибки: ввод некорректного пароля более трех раз подряд или отсутствие у пользователя права на вход в систему.

Рекомендации:

- Ввод некорректного пароля более трех раз подряд:
  - войти в базу, используя учетную запись пользователя-владельца схемы HAS;

- изменить значение поля SLRN_SLRN_ID таблицы SC_USERS для заблокированного пользователя на 0;
- обновить внутренний кеш прав доступа (дополнительную информацию см. в документе «Подсистема «Высокопроизводительный сервер приложений». Руководство системного программиста [HAS_SERVER-DOC_ADMIN]»).

- Отсутствие прав на соединение с системой:
  - назначить пользователю соответствующую объектную привилегию (тип объектов «Системный объект»).

3 Ошибки при добавлении поискового задания

При выборе источников в форме добавления поискового задания web-интерфейса может быть получено сообщение «Не найдено источников», в то время как точно известно, что искомые данные присутствуют в источнике, и источник зарегистрирован. Данная ситуация может возникать из-за остановки задач (jobs) Oracle с именами SSP_STASK_%.

Для решения указанной проблемы следует перезапустить поисковые задачи с помощью утилиты RestartSearchJob из состава дистрибутива подсистемы DRS_DWH_REGISTRY_API. Описание параметров запуска утилиты см. в документе «Руководство системного программиста» на подсистему DRS_DWH_REGISTRY_API.

4 Ошибки при удалении данных

Перед удалением данных выполняется проверка возможности удаления.

Если код типа удаляемых данных <DATATYPE> задан некорректно, то в лог выводится сообщение об ошибке вида:

Неподдерживаемый тип данных для очистки – <DATATYPE>

Если конечная дата периода для удаления данных <CLEAR_DATE>, заданная пользователем, превышает граничную дату глубины хранения (расчетную дату удаления) <MAX_CLEAR_DATE>, в лог выводится сообщение об ошибке вида:

Недопустимая глубина очистки <CLEAR_DATE>. Глубина очистки не может быть больше <MAX_CLEAR_DATE>

В процессе удаления данных выполняется обработка глубины хранения данных. Если не указано значение соответствующего настроечного параметра <PARAM_NAME> или параметр отсутствует, в лог выводится сообщение вида:

Не установлен параметр для допустимой глубины очистки типа данных <DATATYPE> (<PARAM_NAME>)

Логирование работы методов удаления выполняется от имени источника записи в лог с кодом DATA_CLEANING.

Приложение А. Утилиты

Подсистема DRS_RQS_API содержит утилиту регистрации удаленного источника (RegisterSRC538) (подробное описание параметров утилиты см. в документе «Руководство системного программиста» на подсистему).

Подсистема SVC_BASE_SCRIPT содержит скрипт для регистрации источника данных и запуска поисковых задач (SVC_BASE_SCRIPT.UTL_REGISTER_RQS) (подробное описание параметров скрипта см. в документе «Описание скрипта» на подсистему).

Подсистема SVC_DEPLOY_API содержит утилиту регистрации сервера (RegisterServer) (подробное описание параметров утилиты см. в документе «Руководство системного программиста» на подсистему).

Подсистема DRS_DWH_REGISTRY_API содержит следующие утилиты (подробное описание параметров утилит см. в документе «Руководство системного программиста» на подсистему):

- Утилита регистрации оператора связи (RegisterTelco).
- Утилита связывания оператора связи со стандартами связи (SetTelcoStandarts).
- Утилита регистрации форматов для загрузки данных оператора связи (RegisterTelcoFormats).
- Утилита регистрации конфигурации для зарегистрированного файлового формата (SetFileFormatConfig).
- Утилита удаления стандарта связи (UnsetTelcoStandarts).
- Утилита назначения операции «Отвержение» для указанного пакета данных (RejectPack).
- Утилита повторной загрузки пакета (ReloadPack).
- Утилита повторного запуска поисковых задач на базе хранилища данных (RestartSearchJob).
- Утилита изменения (увеличения) числа поисковых задач на сервере хранилища данных (AddSearchJobs).
- Утилита создания классов задач прерывания выполнения заданий (KILL_SESSION_JOB_CLASSES).

Подсистема SVC_BASE_API содержит следующие утилиты (подробное описание параметров утилит см. в документе «Руководство системного программиста» на подсистему):

- Утилита настройки параметров файлов для табличных пространств с логами (SetStorageParams).
- Утилита создания табличных пространств для хранения лога (ExtentLogTable).
- Утилита добавления задач для параллельного выполнения PL/SQL- блоков в одной сессии Oracle (AddTaskHandle).
- Утилита повторного запуска всех задач (RestartAllJob).

Подсистема DRS_DWH_CALLS_API содержит следующие утилиты (подробное описание параметров утилит см. в документе «Руководство системного программиста» на подсистему):

- Утилита настройки параметров файлов для табличных пространств с соединениями (SetStorageParams).
- Утилита создания таблиц для хранения данных о соединениях (CreateEvTable4Telco).
- Утилита партицирования таблиц (ExtentEvTable4Telco).
- Утилита регистрации дополнительного формата загрузки данных о соединениях (RegisterCallsFormat).

Подсистема DRS_DWH_PAYM_API содержит утилиту создания партиций (ExtentPaymsTable) (подробное описание параметров утилиты см. в документе «Руководство системного программиста» на подсистему).

Подсистема DRS_HAS_API содержит следующие утилиты (подробное описание параметров утилит см. в документе «Руководство системного программиста» на подсистему):

- Утилита создания дополнительного администратора (AdditionalAdmin).

- Утилита настройки рассылки сообщений по электронной почте (`SetSMTPSettings`).

Подсистема `SVC_FILE_ET_LOADER` содержит следующие утилиты (подробное описание параметров утилит см. в документе «Руководство системного программиста» на подсистему):

- Утилита регистрации/модификации задачи загрузчика (`RegisterLoaderJob`).
- Утилита удаления задачи загрузчика (`DeleteLoaderJob`).

Приложение Б. Системные задачи

В приложении приводится перечень и краткое описание системных задач, обеспечивающих выполнение функций DRS.

1 SSP_AUTODELETE_TASK_nn

Обозначения:

- <N> – порядковый номер экземпляра задачи.

Задача предназначена для запуска процедуры Job_Autodelete пакета AUTH.CMN_CLEAR_PG, реализующей автоматическое создание заданий на очистку данных.

Имя владельца задачи – AUTH.

Периодичность запуска – раз в сутки, в 00:45.

2 SSP_CLEAR_TASK_1

Задача предназначена для удаления данных и создается как на сервере заявок, так и на сервере хранилища данных.

Имя владельца задачи – AUTH.

Задача создается в одном экземпляре.

3 SSP_CLOSE_CLEAR_TASK_1

Задача предназначена для останова «зависших» задач удаления данных и создается как на сервере заявок, так и на сервере хранилища данных.

Имя владельца задачи – AUTH.

Задача создается в одном экземпляре.

4 SSP_CLOSESEARCHES

Задача предназначена для останова «зависших» поисковых процессов и создается на сервере заявок.

Имя владельца задачи – REQSRV.

Задача создается в одном экземпляре.

5 SSP_CLOSESESSIONS

Задача предназначена для останова пользовательских сессий, для которых истек таймаут, и создается на сервере заявок.

Имя владельца задачи – REQSRV.

Задача создается в одном экземпляре.

6 SSP_CTRL_PACK_LOAD_<N>

Обозначения:

- <N> – порядковый номер экземпляра задачи.

Задача предназначена для контроля загрузки пакетов данных и создается на сервере хранилища данных.

Имя владельца задачи – REGISTRY.

Задача создается в одном экземпляре.

7 SSP_EVENTSCLEAR_<TELCO_ID>

Обозначения:

- <TELCO_ID> – идентификатор оператора связи.

Задача предназначена для очистки партиций с данными о соединениях и создается на сервере хранилища данных.

Имя владельца задачи – DATASRV.

Количество создаваемых экземпляров задачи определяется количеством операторов связи, зарегистрированных в SVC_BASE. Для каждого зарегистрированного оператора связи создается один экземпляр задачи.

8 SSP_EVENTSMOVE_<TELCO_ID>_AP

Обозначения:

- <TELCO_ID> – идентификатор оператора связи.

Задача предназначена для переноса обработанных партиций с данными о соединениях и создается на сервере хранилища данных.

Имя владельца задачи – DATASRV.

Количество создаваемых экземпляров задачи определяется количеством операторов связи, зарегистрированных в SVC_BASE. Для каждого зарегистрированного оператора связи создается один экземпляр задачи.

9 SSP_EVENTSMOVE_<TELCO_ID>_OP

Обозначения:

- <TELCO_ID> – идентификатор оператора связи.

Задача предназначена для переноса необработанных партиций оперативного периода с данными о соединениях и создается на сервере хранилища данных.

Имя владельца задачи – DATASRV.

Количество создаваемых экземпляров задачи определяется количеством операторов связи, зарегистрированных в SVC_BASE. Для каждого зарегистрированного оператора связи создается один экземпляр задачи.

10 SSP_FILE_LDR_<job_name>

Обозначения:

- <job_name> – название системной задачи, указанное при запуске утилиты RegisterLoaderJob.

Задача предназначена для выполнения процедуры SVC_FILE_ET_LOADER.LOAD_PG.LoaderJob, с шаблоном набора аргументов, соответствующим аргументам процедуры SVC_FILE_ET_LOADER.LOAD_PG.LoaderJob.

Имя владельца задачи – SVC_FILE_ET_LOADER.

Периодичность запуска – каждые 5 секунд.

11 SSP_KILL_SESS_<SSS>_<RRRRRR>

Обозначения:

- <SSS> – идентификатор сессии;
- <RRRRRR> – SERIAL# сессии.

Задача предназначена для уничтожения сессии.

Имя владельца задачи – REGISTRY.

Создается и запускается служебной процедурой REGISTRY.KILL_SESSION_PG.KILL_SESSION.

12 SSP_LOG_DEPTH_TASK

Задача предназначена для удаления данных системного лога и запускает процедуру AUTH.BASE_STORAGE_DEPTH_CTRL_PG.CLEAR_JOB.

Имя владельца задачи – AUTH.

Задача создается в одном экземпляре.

Периодичность запуска – раз в сутки, в 00:05.

13 SSP_QUERYDICTS

Задача предназначена для запроса справочников, расположенных в источниках и создается на сервере заявок.

Имя владельца задачи – REQSRV.

Задача создается в одном экземпляре.

14 SSP_REJPACK_PROC

Задача предназначена для отвержения пакетов данных и создается на сервере хранилища данных.

Имя владельца задачи – REGISTRY.

Задача создается в одном экземпляре.

15 SSP_REPORT_ALL_<N>

Обозначения:

- <N> – порядковый номер задачи.

Задача предназначена для обработки заявок на формирование отчетов и запускает процедуру SSP_DOCS.REPORT_UTILS_PG.Report_Job. В случае установки на RAC следует привязать задачи обработки заявок на формирование отчетов к конкретному экземпляру БД Oracle.

Имя владельца задачи – SSP_DOCS.

Задача запускается каждую минуту.

16 SSP_RTASKS_DEPTH_TASK

Задача предназначена для удаления устаревших результатов поисковых запросов и поисковых запросов и запускает процедуру REQSRV.STORAGE_DEPTH_CTRL_PG.CLEAR_JOB.

Имя владельца задачи – REQSRV.

Задача создается в одном экземпляре.

Периодичность запуска – раз в сутки, в 00:15.

17 SSP_STASK_<DBNAME>_<TTT>_<NN>

Обозначения:

- <DBNAME> – имя базы данных, содержащей сервер заявок, в котором зарегистрировано хранилище;
- <TTT> – группа приоритетов заданий, обрабатываемая данной задачей (LPQ, HPQ, DQ, CQ);
- <NN> – порядковый номер задачи в разрезе сочетания DBNAME и TTT.

Имя владельца задачи – REGISTRY.

Задача предназначена для поиска данных.

Задача создается в четырех экземплярах, по одной для групп приоритетов HPQ, DQ, CQ, LPQ.

18 SSP_STASK_<RQS name>_<N>

Обозначения:

- <RQS name> – имя базы данных сервера заявок;
- <N> – порядковый номер экземпляра задачи.

Задача предназначена для маршрутизации поисковых заданий (перемещения их от сервера заявок к серверу хранилища данных) и создается на сервере хранилища данных.

Первоначально для каждого сервера заявок, для которого хранилище данных зарегистрировано в качестве локального источника, создается два экземпляра задачи. В дальнейшем количество экземпляров может быть увеличено с помощью утилиты AddSearchJobs из состава подсистемы DRS_DWH_REGISTRY_API.

19 SSP_SVC_EXT_CTRL<N>

Обозначения:

- <N> – порядковый номер экземпляра задачи.

Задача предназначена для загрузки данных об абонентах и платежах с помощью адаптеров загрузки и создается на сервере хранилища данных.

Имя владельца задачи – SVC_EXT_LOADER.

Для каждого формата загрузки, зарегистрированного в SVC_BASE, создается один экземпляр задачи. Общее количество создаваемых экземпляров определяется следующими факторами:

- количеством форматов загрузки, предназначенных для загрузки данных одного внешнего источника (в настоящее время поддерживается два формата для каждого источника);
- количеством внешних источников, подключенных посредством адаптеров загрузки.

ИСТОРИЯ ПУБЛИКАЦИИ ДОКУМЕНТА

Версия 001.00 от 23.11.2007

Документ создан.

Версия 002.00 от 15.01.2008

Глава «Подготовка к работе» изменена. Изменено описание порядка установки. Добавлены разделы «Предварительная настройка баз данных», «Настройка взаимодействия сервера заявок с хранилищем данных», «Установка подсистем, обеспечивающих загрузку данных», «Подключение новых форматов данных». Раздел «Установка подсистем, обеспечивающих хранение данных» изменен: удалены подразделы «Подготовка базы», «Подготовка Системы к загрузке данных», добавлен пункт о проверке объектов в состоянии INVALID. Раздел «Установка подсистем, обеспечивающих поиск правоохранительных органов» изменен: новое название «Установка подсистем, обеспечивающих обработку поисковых запросов правоохранительных органов», удален подраздел «Подготовка базы», добавлен пункт о проверке объектов в состоянии INVALID. Раздел «Установка подсистем, обеспечивающих поиск службы безопасности оператора связи» переименован, новое название «Установка подсистем, обеспечивающих обработку поисковых запросов службы безопасности оператора связи». Удален раздел «Установка подсистемы проведения поисков».

Глава «Описание операций» изменена. В разделе «Перечень операций» изменен список операций, доступных через веб-интерфейс. В разделе «Модель прав доступа» добавлено описание типа объектов «Специальные справочники», обновлен перечень объектов типа «Виды запросов», «Срочность поиска», изменен пример назначения привилегий.

Глава «Аварийные ситуации» изменена: добавлены разделы «Ошибки при установке Системы», «Ошибки при добавлении поискового задания».

Добавлена глава «Рекомендации по эксплуатации».

Версия 003.00 от 30.05.2008

Документ полностью переработан в соответствии с новым составом комплекта поставки продукта.

Версия 004.00 от 20.10.2008

Глава «Условия применения» изменена. В разделе «Минимальный состав технических средств» добавлено требование для поддержки протокола SMD (538).

Глава «Подготовка к работе» изменена. В раздел «Порядок установки Системы» добавлена информация об установке `PETER-SERVICE DRS_ADP_538`. Добавлены разделы «Настройка доступа к web-сайту» и «Настройка справочников-карт».

Глава «Описание операций» изменена. Удален заголовок «Перечень операций», в список операций добавлены просмотр протоколов системных событий, просмотр статистики загруженных пакетов и просмотр лога загрузки пакета. Удален раздел «Рекомендации по выполнению операций», информация перенесена в разделы «Настройка доступа к web-сайту» и «Настройка справочников-карт».

Глава «Аварийные ситуации» изменена. Добавлены разделы «Ошибки доступа к web-сайту», «Ошибки формирования графиков».

Версия 005.00 от 26.01.2009

Глава «Введение» изменена. В разделе «Возможности Системы» в перечень предоставляемых возможностей добавлено определение принадлежности номера телефона оператору связи.

Глава «Условия применения» изменена. В разделе «Минимальный состав программных средств» добавлено требование Adobe SVG Viewer для работы с графиками статистики.

Глава «Описание операций» изменена. В перечень операций добавлены определение принадлежности номера телефона оператору связи, просмотр и редактирование таких справочников локального источника, как «Номерная емкость» и «Связанные диапазоны номеров».

Глава «Аварийные ситуации» изменена. Добавлен раздел «Ошибки в работе адаптера SMD (538)».

Версия 006.00 от 18.08.2009

Глава «Введение» изменена. В разделе «Возможности Системы» добавлены функции управления глубиной хранения данных и поддержки протокола SMD (538).

Глава «Условия применения» изменена. В разделе «Минимальный состав программных средств» версия Microsoft Internet Explorer 6 SP1 изменена на Microsoft Internet Explorer 7 и выше.

Глава «Описание операций» изменена. В список операций в пункте «Добавление поискового задания» добавлены виды поисковых заданий. Также добавлены следующие операции: «Управление поисковыми заданиями: настройка формирования отчетов для пользователя», «Просмотр справочников локального источника: коммутаторы», «Удаление записей из справочников локального источника», «Управление учетными записями пользователей: настройка формирования отчетов», «Разграничение прав пользователей Системы: редактирование пользовательских ограничений», «Аудит действий пользователей Системы и системных событий: просмотр статистики поисков», «Специальные действия», «Управление форматами загрузки: просмотр журнала загруженных пакетов», «Управление пакетами загружаемых данных: просмотр информации о пакете».

Версия 007.00 от 15.10.2009

Глава «Введение» изменена. В разделе «Перечень эксплуатационной документации» добавлена ссылка на глоссарий.

Глава «Подготовка к работе» изменена. В разделе «Настройка справочников-карт» уточнено описание настройки карты типов платежей.

Глава «Описание операций» изменена. В список операций в пункте «Удаление записей из справочников локального источника» добавлены справочники коммутаторов, транков, типов соединений и типов платежей.

Глава «Аварийные ситуации» изменена. В разделе «Ошибки доступа к web-сайту» обновлен перечень аварийных ситуаций.

Версия 008.00 от 22.03.2013

Документ полностью переработан.