БУ ВО

«СУРГУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Ханты-Мансийского автономного округа – Югры»

Кафедра автоматизированных систем обработки информации и управления (АСОИУ)

ОТЧЁТ

по производственной практике, научно-исследовательская работа

«Изучение метода и средств доступа к идентификационным данным, разработка требований к автоматизированной системе поиска и исправления рассогласованности идентификационных данных центральной системы SAP Identity Management с данными конечных систем, требований к выходным данным и видам обеспечений, организационно-функциональной модели автоматизированной системы»

Выполнил студент гр. 606-71м

Боровков Дмитрий Евгеньевич

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись)

Научный руководитель:

профессор кафедры АСОИУ, д.т.н.,

Бушмелева Кия Иннокентьевна

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись)

Сургут, 2018

Оглавление

[ВВЕДЕНИЕ 3](#_Toc517381295)

[1. ПОСТАНОВКА ЦЕЛИ И ЗАДАЧ 4](#_Toc517381296)

[2. МЕТОДЫ И СРЕДСТВА ДОСТУПА К ИДЕНТИФИКАЦИОННЫМ ДАННЫМ 6](#_Toc517381297)

[2.1. Центр идентификации 6](#_Toc517381298)

[2.2. Виртуальный сервер каталогов 7](#_Toc517381299)

[2.3. Пользовательский интерфейс SAP IdM 7](#_Toc517381300)

[2.4. Потоки данных и задачи 8](#_Toc517381301)

[3. ОРГАНИЗАЦИОННО-ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ СИСТЕМЫ 11](#_Toc517381302)

[3.1. Методология IDEF0 11](#_Toc517381303)

[3.2. Контекстная диаграмма 12](#_Toc517381304)

[4. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ 14](#_Toc517381305)

[5. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ 16](#_Toc517381306)

[6. ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ 18](#_Toc517381307)

[ЗАКЛЮЧЕНИЕ 19](#_Toc517381308)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 20](#_Toc517381309)

[ПРИЛОЖЕНИЯ 21](#_Toc517381310)

[ПРИЛОЖЕНИЕ 1 ДЕКОМПОЗИЦИЯ КОНТЕКСТНОЙ ДИАГРАММЫ 21](#_Toc517381311)

# ВВЕДЕНИЕ

Для правильной организации работы разрабатываемой автоматизированной системы с идентификационными данными необходимо изучить метод и средства доступа к идентификационным данным как хранилища идентификаторов SAP Identity Management, так и конечных систем. При этом необходимо организовать так чтобы не расширять доступ к некоторым данным, которые не положены администратору по должностной инструкции, не противоречить федеральному закону №152 и трудовому кодексу РФ, при этом, не сужать полномочия администратора. Также разработаны первоначальные функциональные и не функциональные требования к системе, требования к выходным данным, правовому, программному и организационному обеспечениям.

# ПОСТАНОВКА ЦЕЛИ И ЗАДАЧ

Цель: изучить метод и средства доступа к идентификационным данным, разработать требования к автоматизированной системе поиска и исправления рассогласованности идентификационных данных центральной системы SAP Identity Management с данными конечных систем, требования к выходным данным и видам обеспечений, организационно-функциональную модель автоматизированной системы.

Задачи:

1. Разработать функциональные и нефункциональные требования к автоматизированной системе.
2. Разработать требования к выходным данным.
3. Описать метод и средства доступа к идентификационным данным.
4. Описать виды обеспечений.
5. Разработать контекстную диаграмму автоматизированной системы.
   1. Требования к автоматизированной системе

Функциональные требования:

* выдача предупреждающих сообщений при недоступности конечной системы или хранилища идентификаторов;
* автоматический запуск программы каждый час.

Нефункциональные требования:

* использование системы для поиска и исправления рассогласованности идентификационных данных SAP Identity Management с данными конечных систем SAP Human Resources, Directum, SAP Buisness Warehouse;
* минимизирование объема хранения промежуточных данных.
  1. Требования к выходным данным

Предоставление отчета о сравнении идентификационных данных в виде текстового документа или с помощью системы электронных таблиц

Предоставление исчерпывающей информации о пользователе, которому принадлежат рассогласованные идентификационные данные

# 2. МЕТОДЫ И СРЕДСТВА ДОСТУПА К ИДЕНТИФИКАЦИОННЫМ ДАННЫМ

SAP NetWeaver Identity Management (SAP IdM) состоит из двух компонент [1]:

1. Центр идентификации.
2. Виртуальный сервер каталогов.

## 2.1. Центр идентификации

Центр идентификации ‑ это основной компонент, используемый для управления идентификацией. Центр идентификации включает функции для обеспечения идентификации, workflow, управления паролями, ведения журнала и отчетности, управления заданиями (джобами). Он использует централизованный репозиторий, называемый хранилищем идентификаторов, для обеспечения единообразного представления данных независимо от исходного источника данных. Эта архитектура показана на рис. 1.

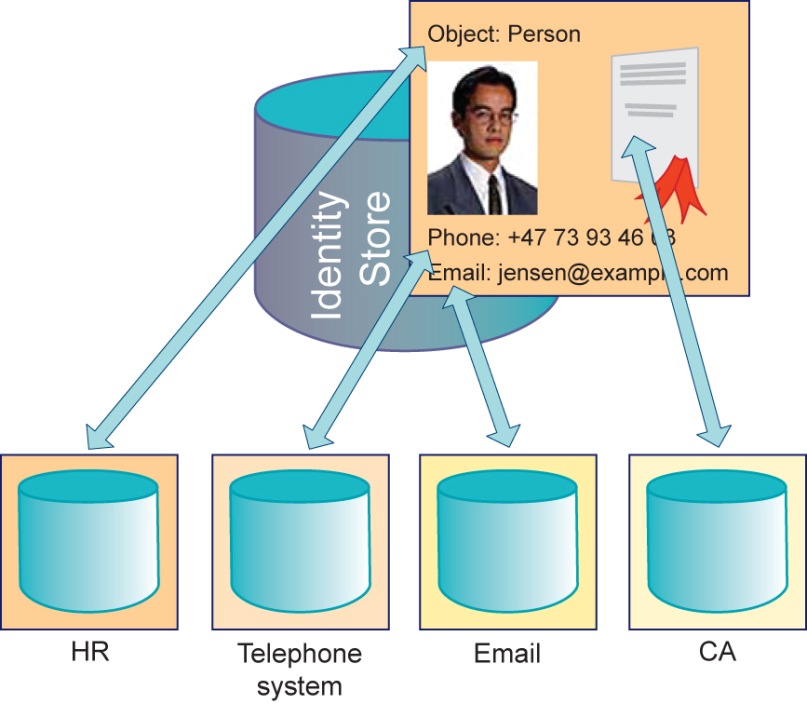


Рис. 1. Схема взаимодействия хранилища идентификаторов (Identity Store) с другими хранилищами (HR - Human Resource (система управления персоналом), Telephone System – система корпоративной телефонии, Email – корпоративная электронная почта)

Взаимодействие SAP IdM с различными SAP и не-SAP системами происходит с помощью коннекторов. Центр идентификации извлекает данные из различных репозиториев, консолидирует их, преобразует в необходимые форматы и публикует их обратно в репозитории.

## 2.2. Виртуальный сервер каталогов

Виртуальный сервер каталогов - это компонент, предоставляемый системой управления идентификацией SAP, который выступает в роли единой точки доступа для клиентов, получающих или обновляющих данные в нескольких хранилищах данных, поскольку он обеспечивает единообразное представление данных в режиме реального времени.

Его можно использовать, например, для объединения нескольких репозиториев в один источник данных, который подключен к Identity Center. Затем можно использовать Identity Center для предоставления и выполнения функций управления идентификацией для репозиториев через Virtual Directory Server.

Независимо от выбранной варианта подключения Sap IdM, необходимо соединить различные системы, содержащие идентификационные данные, с SAP IdM и продублировать данные в хранилища идентификаторов SAP IdM. Пользовательский ID является тем связующим параметром для всех систем, подключенных к SAP IdM. То есть, создается пользователь в Identity Center и ему присваивается свой ID, который однозначно идентифицирует пользователя. Далее, после консолидирования всех идентификационных данных, эти данные перезаписываются в подключенных системах.

## 2.3. Пользовательский интерфейс SAP IdM

Пользовательский интерфейс управления идентификацией SAP используется для управления идентификационными данными.

Существуют функции для регистрации пользователей и других задач самообслуживания, запросов на сброс пароля и утверждения задач. Он также содержит информацию о мониторинге для администраторов Центра идентификации.

Пользовательский интерфейс устанавливается как компонент на:

* AS Java, работающий в SAP NetWeaver 7.0;
* AS Java, работающий в выпусках SAP Composition Environment 7.10 / 7.11 или 7.2.

## 2.4. Потоки данных и задачи

В данном примере моделируется регулирование физического доступа в здание и в отдельные комнаты при помощи управления ролями [2].

Предполагается, что есть некоторый файл hr.csv, который имитирует идентификационные данные системы HR, подключенной к SAP IdM. Содержимое файла представлено на рис. 2.

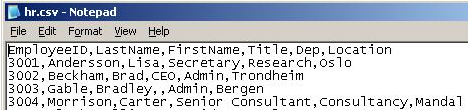


Рис. 2. Содержимое файла hr.scv (EmployeeID – идентификатор работника, LastName – Фамилия работника, FirstName – имя работника, Title – должность, Dep – отдел, Location – город)

Существует джоб (Employees to identity store), который считывает данные из файла hr.csv и обновляет записи в хранилище идентификаторов (рис. 3). Джоб запускается через Identity Center. Таким методом происходит вся работа с данными хранилища идентификаторов.

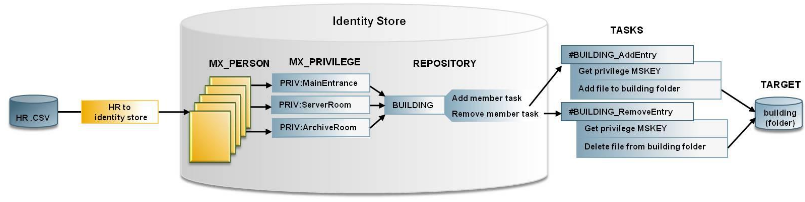


Рис. 3. Поток данных и задачи

В хранилище идентификаторов каждая запись в cr.csv является типом MX\_PERSON. MX\_PERSON ‑ запись с атрибутами, описывающими человека, такими как имя, фамилия, отдел, адрес электронной почты. Кроме того, он может быть назначен любому числу ролей и привилегий.

Создается три привилегии: PRIV:MainEntrance, PRIV:ServerRoom и PRIV:ArchiveRoom), которые можно назначить записям (каждому работнику):

1. PRIV:MainEntrance. Эта привилегия дает пользователям право доступа к зданию (основной вход).
2. PRIV:ServerRoom. Привилегия дает пользователю доступ к серверной комнате. Часто предоставляется ИТ-персоналу.
3. PRIV:ArchiveRoom. Привилегия дает пользователю доступ к архиву. Часто дается сотрудникам администрации.

Эти привилегии содержат ссылки на определения репозитория, которые содержат ссылки на задачи, выполняемые при назначении или удалении привилегии.

Для того чтобы процесс предоставления доступа к зданию или отдельным комнатам осуществился необходимо:

* + создать глобальную константу, содержащую путь к каталогу, в котором храниться источник данных hr.csv;
  + создать глобальную константу содержащую путь к каталогу, в котором должен быть размещен целевой репозиторий для файлов;
  + Когда пользователю предоставляется конкретная привилегия, выполняется джоб (рис. 4), который создает файл (содержащий временную метку, когда привилегия была назначена пользователю) и помещает его в соответствующую папку (рис. 5).

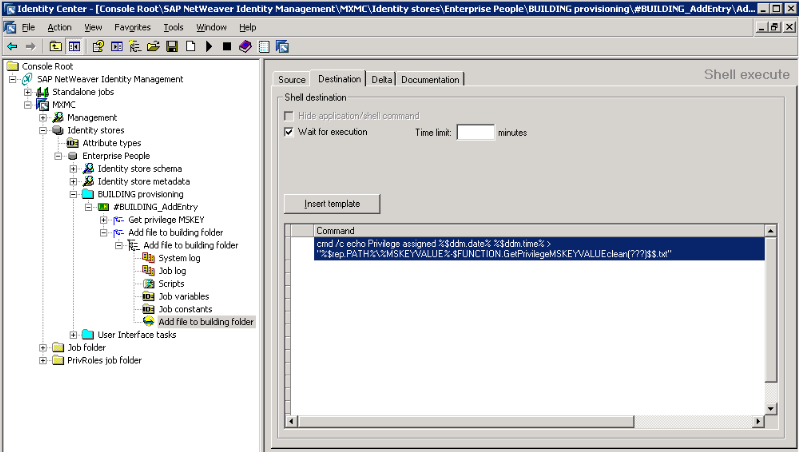


Рис. 4. Джоб BUILDING\_AddEntry

Джоб BUILDING\_AddEntry, состоящий из двух джобов: Get priviledge MSKEY, сохраняющий атрибут, который используется для идентификации работника, Add file to building folder, содержащий временную метку, когда привилегия была назначена пользователю

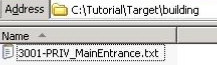


Рис. 5. Файл, созданный после назначения пользователю с MSKEY=3001 привелегии MainEntrance, который инициировал выполнение джоба BUILDING\_AddEntry

Файл сохраняется к директории, указанной в глобальной константе в Identity Center.

# 3. ОРГАНИЗАЦИОННО-ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ СИСТЕМЫ

## 3.1. Методология IDEF0

Методология IDEF0 используется для создания функциональной модели разрабатываемой системы, которая отображает структуру и функции системы, потоки информации и материальных объектов, преобразуемые этими функциями.

Функциональная схема представляет собой диаграмму. Основные элементы диаграммы представлены в таб.1.

*Таблица 1*

Основные элементы диаграммы

|  |  |  |
| --- | --- | --- |
| Элемент | Графическое отображение | Назначение элемента |
| Функциональный блок | Прямоугольник | Представляет функции, определяемые как деятельность, процесс, действие, преобразование |
| Интерфейсная дуга (стрелка) | Однонаправленная стрелка | Представляет данные, материальные объекты, связанные с функциями |

Общий вид функционального блока представлен на рис. 6.

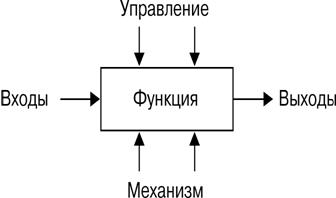


Рис. 6. Общий вид функционального блока

Стрелка “Входы” представляет входные данные, которые затем превращаются функциональным блоком в выходные данные, представленные стрелкой “Выходы”. Стрелка “Механизм” представляет то, с помощью чего осуществляется выполнение функций (ЭВМ, пользователь, БД, и т. д.). Стрелка “Управление” представляет то, что регулирует выполнение функции (документы, методы и т. д.).

Моделирование с помощью методологии IDEF0 начинается с контекстной диаграммы. Это диаграмма, представленная одним функциональным блоком и стрелок, изображающих окружение схемы. После описания контекстной диаграммы, проводится декомпозиция функционального блока с сохранением всех стрелок контекстной диаграммы. Декомпозиция проводится с целью детализации процессов, которые происходят в декомпозированном функциональном блоке [3].

## 3.2. Контекстная диаграмма

На рис. 7 представлена контекстная диаграмма разрабатываемой АС.

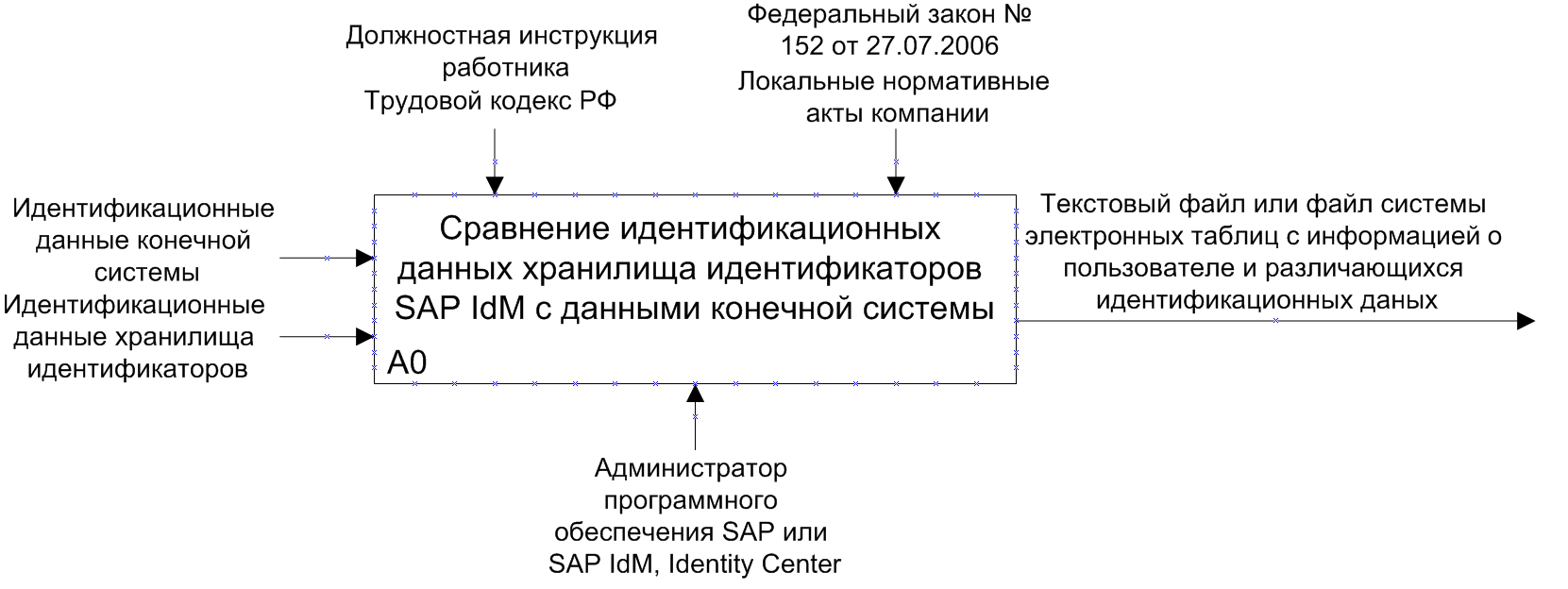


Рис. 7. Контекстная диаграмма автоматизированной системы

Запуск программы и последующую обработку выходных данных осуществляет администратор ПО SAP или SAP IdM. Запуск программы производится через Identity Center, расположенный на сервере IdM. Входными данными для разрабатываемой системы является таблица идентификационных данных конечной системы, формирующаяся сторонней программой. Выходные данные находятся вне системы SAP IdM в виде текстового файла или файла системы электронных таблиц. Администратор выполняет свои функции по должностной инструкции, следуя ограничениям, указанные в ТК РФ и ФЗ №152 от 27.07.2006, которые регулируют права и обязанности лица, владеющего доступом к персональным данным.

В приложении 1 указана декомпозиция контекстной диаграммы.

Для сравнения идентификационных данных конечной системы с данными, находящимися в хранилище идентификаторов необходимо сформировать временные таблицы с идентификационными данными конечной системы и идентификационными данными хранилища идентификаторов. Данные для временной таблицы идентификационных данных конечной системы берутся из сформированной сторонней программой таблицы данных конечной системы. Данные для временной таблицы идентификационных данных хранилища идентификаторов берутся из хранилища идентификаторов напрямую. Далее происходит вычитание данных временной таблицы идентификационных данных конечной системы из данных временной таблицы идентификационных данных хранилища идентификаторов. Оператор вычитания – «minus» является оператором языка PL\SQL. Оставшиеся после вычитания идентификационные данные конечной системы отображаются в виде текста в файле или в виде электронной таблицы в системе электронных таблиц.

# ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Системные требования для установки SAP IdM 7.2:

1. AS ABAP 4.6C или выше. Именно здесь выполняются фактические вычисления, оценки и другие операции. Необходимые для этого сведения запрашиваются с уровня базы данных. Новые входные данные обрабатываются на уровне приложения и передаются в базу данных. Уровень приложений представляет собой центр управления системой SAP R/3 [4].
2. AS Java/Portal: версия 6.40, 7.00, или 7.10 Также относится к уровню приложений, состоит из Java приложений предоставляющих бизнес-контент на уровень презентации.

Прямой доступ к хранилищу идентификаторов осуществляется через Oracle SQL Developer.

Oracle SQL Developer ‑ это бесплатная интегрированная среда разработки, которая упрощает разработку и управление Oracle Database как в традиционном, так и в облачном развертывании. SQL Developer предлагает полную сквозную разработку PL / SQL-приложений, рабочий лист для запуска запросов и сценариев, консоль администратора баз данных для управления базой данных (рис. 8) [5].

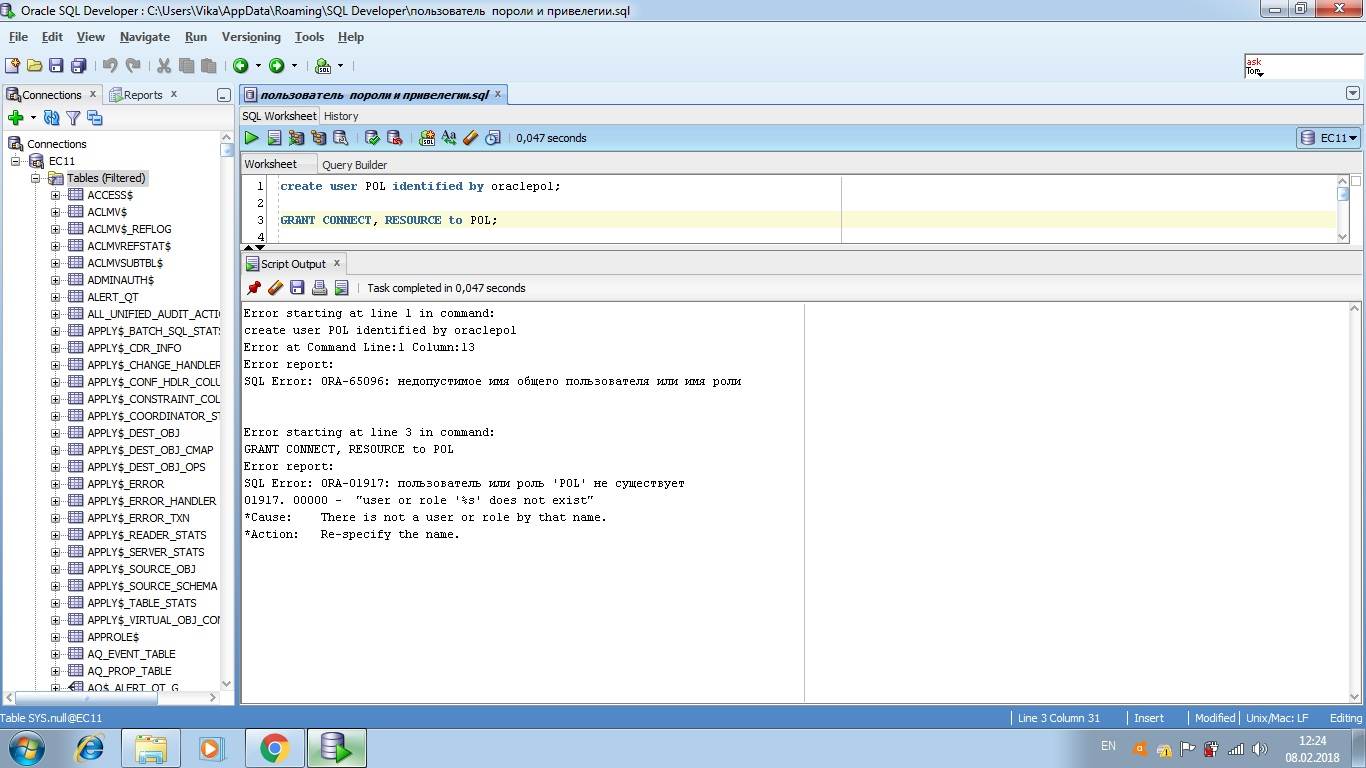


Рис. 8. Окно Oracle SQL Developer, слева – структура базы даны, состоящая из таблиц, триггеров, процедур и т. д.

Все запросы к базе данных пишутся на языке PL/SQL, разработанной компанией Oracle.

# ПРАВОВОЕ ОБЕСПЕЧЕНИЕ

Автоматизированная обработка персональных данных ‑ обработка персональных данных с помощью средств вычислительной техники

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

В соответствии с [6], обработка персональных данных осуществляется с согласия субъекта персональных данных. Но, при заключении трудового договора работник добровольно (без письменного согласия) предоставляет первоначальные данные, указанные в следующем перечне [7]:

* паспорт или иной документ, удостоверяющий личность;
* трудовую книжку;
* страховое свидетельство обязательного пенсионного страхования;
* документы воинского учета;
* документ об образовании;
* справку о наличии (отсутствии) судимости;
* справку о том, является или не является лицо подвергнутым административному наказанию.

Такой факт подтверждается ФЗ №152: обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации.

В соответствии с ТК РФ, необходимо разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций. Операторы или иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Необходимость усиления контроля за идентификационными данными пользователя подкрепляется ФЗ №152: оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

# ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Мониторинг расхождения идентификационных данных хранилища идентификаторов SAP IdM с данными конечных систем осуществляет администратор программного обеспечения SAP или конкретно SAP IdM.

Также администратору необходимо иметь доступ к системе AS Java, работающий в SAP NetWeaver 7.0 или к AS Java, работающий в выпусках SAP Composition Environment 7.10 / 7.11 или 7.2, так как на одном из них должен быть установлен пользовательский интерфейс.

Администратор должен иметь доступ к серверу с установленной системой Identity Center для ручного запуска джоба, если это необходимо.

Доступ к хранилищу идентификаторов также необходимо для ознакомления со структурой хранилища.

# ЗАКЛЮЧЕНИЕ

За время проведения производственной практики изучен метод доступа к идентификационным данным посредством вызова джобов через Identity Center. Изучены средства доступа к идентификационным данным: Identity Center, User Interface на SAP CE, Oracle SQL Developer. Также разработаны первоначальные функциональные и не функциональные требования к системе, требования к выходным данным и требовании к правовому, организационному и программному обеспечениям.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. SAP NetWeaver Identity Management Provisioning Framework for SAP Systems: Architectural Overview [Электронный ресурс]. URL: https://help.sap.com/viewer/53a1e172f3334c1db09d42ab4d185915/7.2/en-US
2. SAP NetWeaver Identity Management Identity Center [Электронный ресурс]. URL: https://www.sap.com/documents/2015/07/aaeb8454-5a7c-0010-82c7-eda71af511fa.html
3. Черемных, С. В. Моделирование и анализ систем. IDEFтехнологии: практикум / С. В. Черемных, И. О. Семенов, В. С. Ручкин. — М.: Финансы и статистика, 2006. — 192 с.
4. Сигрид Хагеман SAP R/3 Системное администрирование / Хагеман Сигрид. – М.: Лори, 2007. – 480 с.
5. Официальный сайт Oracle [Электронный ресурс]. URL: http://www.oracle.com/technetwork/developer-tools/sql-developer/overview/index.html
6. О персональных данных [Электронный ресурс]: федер. Закон от 27.07.2006 №152-ФЗ. URL: http://www.consultant.ru/document/cons\_doc\_LAW\_61801
7. Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ (принят ГД ФС РФ 21.12.2001) (ред. от 30.06.2003).

# ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1 ДЕКОМПОЗИЦИЯ КОНТЕКСТНОЙ ДИАГРАММЫ