Утвержден
RU.64509942.00214-01-ЛУ

Программное средство

«Система централизованного управления доступом пользователей»

(СЦУДП).

Описание программы

RU.64509942.00214-01 13 01

Листов 20

2021

Аннотация

Настоящий документ содержит описание Программного средства Система централизованного управления доступом пользователей (далее – СЦУДП, Система), включая описание функционального назначения, структуры программы и логики работы. В документе приведены общие сведения о программном средстве о его функциональном назначении, описание логической структуры, перечислены технические средства, которые используются при работе программного средства, описаны процессы вызова и загрузки программы, характер и организация входных и выходных данных.

СОДЕРЖАНИЕ

Перечень сокращений и условных наименований

Термин, сокращение	Определение
IdM	Identity Management – централизованное управление доступом
БД	База данных
Заявка	Объект Изделия, содержащий информацию о запрошенных пользователем или Изделием изменениях и процессах их согласования и выполнения
Изделие	Программное средство Система управления базой данных
ИТ-ресурс	Совокупность данных и правил доступа к ним в рамках автоматизации процессов
ОС	Операционная система
ПС	Программное средство
Право доступа, полномочие	Системные объекты в УС или в Изделии, ограничивающие права пользователя на выполнение функций и доступ к данным
СУБД	Система управления базами данных
СЦУДП, Система	Система централизованного управления доступом пользователей
УЗ	Учетная запись
УС	Управляемая система
Логические границы ПС	Перечень программных компонентов, которые входят в состав программного средства

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Обозначение и наименование программного средства

Полное наименование программного средства: Система централизованного управления доступом пользователей.

Сокращенное наименование: СЦУДП.

1.2. Программное обеспечение, необходимое для функционирования программного средства

Для функционирования Системы на серверном оборудовании должно быть установлено следующее программное обеспечение:

1) операционная система (см. Таблица 1);
2) СУБД – PostgreSQL версии 10 (и выше);
3) сервер приложений – Apache Tomcat версии 7, 8, 9;
4) серверы коннекторов – Connector Server .NET (для .net-коннекторов) и Connector Server Java (для .java-коннекторов);
5) JRE (Java 8).

Таблица 1 – Перечень совместимых ОС

Наименование операционной системы	Версии
Microsoft Windows	Microsoft Windows Server 2016
Astra Linux	Special Edition 1.6 (релиз «Смоленск»), Common Edition 2.12 (релиз «Орел»)
РЕД ОС	7.2
CentOS	7

В состав программного обеспечения компьютера должна входить программа-клиент, предоставляющая пользователю возможность навигации и просмотра web-ресурсов (браузер). Рекомендуемые браузеры:

- Chromium (версии 75-80);
- Google Chrome (версии 56-90);
- Microsoft Edge (версия 91);
- Яндекс Браузер (версии 20-21).

Языки программирования, на которых написано программное средство

При разработке ПС СЦУДП использовались следующие языки программирования:

- Java;
- C#;
- Groovy;
- JavaScript.

2. ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

Изделие, как программное средство класса Identity Management (IdM), автоматизирующее процессы контроля и управления правами доступа сотрудников в управляемых системах предприятия (далее - УС). С помощью ПС можно из кадровых систем предприятия получить все имеющиеся сведения о сотрудниках и далее управлять их учётными записями в различных УС предприятия.

Система обеспечивает выполнение следующих основных функций:

1) предоставление прав доступа к ИТ-ресурсам;
2) конфигурирование маршрутов согласования;
3) отзыв прав доступа к ИТ-ресурсам;
4) пересмотр прав доступа к ИТ-ресурсам;
5) блокирование и разблокирование доступа пользователя;
6) управление учетными записями и правами доступа пользователя при кадровых мероприятиях;
7) управление паролями учетных записей;
8) делегирование, эскалация согласования запросов на доступ;
9) ведение нормативно-справочной информации:

- ведение реестра ИТ-ресурсов;
- ведение каталога УС;
- ведение каталога ролей;
- ведение организационной структуры;
- ведение каталога работников;
- ведение матрицы конфликтов полномочий;
- управление рисками;
- ведение справочников в административном интерфейсе;

10) аудит прав доступа в ИТ-ресурсах:
11) аттестация прав доступа в ИТ-ресурсах:

12) информирование пользователей о событиях в Изделии;

13) отчетность.

Система обеспечивает выполнение следующих функций безопасности:

1) идентификация и аутентификация пользователей Изделия;

2) идентификация устройств (обеспечивается в Изделии с использованием функционала DNS, встроенного в ОС, по зарегистрированным логическим именам (FQDN) и логическим адресам (IP-адресам));

3) управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов пользователей Изделия;

4) управление средствами аутентификации пользователей Изделия, в том числе хранение, выдача, инициализация, блокирование средств аутентификации;

5) защита обратной связи при вводе аутентификационной информации;

6) управление (заведение, активация, блокирование и уничтожение) учётными записями пользователей, как самого Изделия, так и управляемых систем предприятия;

7) реализация необходимых методов управления доступом, типов и правил разграничения доступа;

8) разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование Изделия;

9) ограничение числа неуспешных попыток входа пользователей Изделия;

10) блокирование сеанса доступа в Изделие после установленного времени бездействия (неактивности) пользователя или по его запросу;

11) разрешение (запрет) действий пользователей Изделия, разрешённых до идентификации и аутентификации;

12) определение событий безопасности, подлежащих регистрации, и сроков их хранения;

13) определение состава и содержания информации о событиях безопасности, подлежащих регистрации;

14) регистрация событий безопасности.

3. ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ

3.1. Алгоритм программы

Система обрабатывает запросы на изменения учетных данных, инициируя соответствующие бизнес-процессы, в соответствии с конфигурацией, по результатам выполнения которых происходят необходимые изменения в подключенных системах, а также рассылаются уведомления о произошедших событиях.

Запросы на изменения учетных данных поступают в ПС Система централизованного управления доступом пользователе в виде:

– заявок, отправляемых пользователем из веб-интерфейса. Пользователь Системы может напрямую запросить изменения данных того или иного сотрудника из карточки пользователя. Также, пользователь может отправить заявку на добавление каких-либо ролей, которые будут предоставлены после успешного процесса согласования.

– заявок из внешних систем, подключенных в качестве источника данных (например, из кадровых систем). Из таких систем поступают данные о новых сотрудниках, данные об изменениях в организационно-штатной структуре, отпусках, увольнениях.

В зависимости от характера запрашиваемых изменений Система инициирует бизнес-процессы согласно настройкам системы и предоставляет инструменты для их настройки.

3.2. Используемые методы

Языки, используемые для разработки Системы приведены в разделе □.

В основе Системы лежит сервер приложений, который обеспечивает работу пользовательских веб-интерфейсов Системы, взаимодействует с подключенными УС и управляет выполнением фоновых задач. Подробнее о назначении компонентов Система приведено в разделе 3.3.

Все данные и метаданные, с которыми работает Система, являются объектами разных типов. Часть объектов выполняют служебные функции, другие являются проекциями объектов, получаемых из внешних управляемых систем, или представляют собой данные, с которыми работает Система. Объекты хранятся в базе данных, их можно экспортировать и импортировать в виде XML-документов.

Одна из важных функций Системы — автоматическая синхронизация атрибутов между внутренними объектами Системы и данными во внешних системах. Объектами, для которых возможна автоматическая синхронизация, являются пользователь, бизнес-роль, организация, подразделение, должность и трудоустройство.

Система может получать данные из кадровых и управляемых систем в нескольких режимах: ручном, по заданному расписанию или в режиме реального времени. Последний режим позволяет незамедлительно получать изменения из управляемых систем, обеспечивая тем самым непрерывность процесса управления и контроля прав доступа сотрудников. При этом Система взаимодействует с системами-источниками данных и УС с помощью коннекторов. Настройки взаимодействия (параметры подключения, схемы данных, правила обработки этих данных, правила синхронизации) с конкретной системой задаются в Системе в XML-описании этой системы.

В соответствии с заданными настройками, Система преобразует полученные данные в специальную структуру Ресурсный объект, что позволяет работать с объектами различных УС в едином формате. В Ресурсном объекте хранятся атрибуты УС – общие унифицирующие и специальные, определяемые для каждой УС отдельно.

При передаче данных применяются специальные правила, которые настраиваются при описании УС. Эти правила задают соответствие между данными в Системе и данными в других системах. Если данные передаются из других систем в нужные атрибуты конкретного объекта Системы, то срабатывают правила переноса данных из Ресурсного объекта в атрибуты объектов (inbound mapping). При обратной передаче срабатывают правила outbound mapping.

Обработка данных объекта в самой Системе выполняется в соответствии с правилами, заданными в шаблоне объектов. Для различных видов объектов можно задать разные шаблоны, где описаны алгоритмы и правила обработки атрибутов объекта, которые будут применяться ко всем объектам одного вида.

3.3. Структура программы

Система построена с использованием клиент-серверной архитектуры и состоит из следующих логических компонентов:

1) веб-интерфейс – предоставляет доступ пользователей к пользовательскому и административному интерфейсам Системы через веб-браузер. Включает в себя следующие программные компоненты:

- тонкий клиент пользовательского интерфейса;
- тонкий клиент административного интерфейса.

2) сервер приложений – обеспечивает работу пользовательских веб-интерфейсов Системы, взаимодействует с подключенными УС и управляет выполнением фоновых задач. Включает в себя следующие программные компоненты:

- графический интерфейс пользователя – программное решение, обеспечивающее работу в веб-интерфейсе пользователя;
- графический интерфейс администратора – программное решение, обеспечивающее работу веб-интерфейса администратора;
- приложение бизнес-логики и обработки фоновых заданий – программное решение, обеспечивающее целевую работу Системы.

3) сервер баз данных – обеспечивает централизованное хранение информации, необходимой для функционирования Системы:

- база данных – совокупность данных, хранимых в соответствии со схемой данных, манипулирование которыми выполняют в соответствии с правилами Системы.

4) сервер коннекторов – обеспечивает связь Системы с системами-источниками данных и УС с помощью коннекторов, специальных модулей, которые являются каналами передачи данных. Включает в себя следующие программные компоненты:

- сервер коннекторов Java – программное решение, позволяющее осуществить взаимодействие с системами-источниками данных и УС с помощью коннекторов, написанных на языке программирования Java;
- сервер коннекторов .NET – программное решение, позволяющее осуществить взаимодействие с системами-источниками данных и УС с помощью коннекторов, написанных на языке программирования C#.

5) коннекторы – набор независимых программных модулей – предоставляющих интерфейс определенного вида для обеспечения взаимодействия Системы с системами-источниками данных и УС.

Все данные и метаданные, с которыми работает Система, являются объектами разных типов. Часть объектов выполняют служебные функции, другие являются проекциями объектов, получаемых из внешних управляемых систем, или представляют собой данные, с которыми работает Система. Объекты хранятся в базе данных, их можно экспортировать и импортировать в виде XML-документов.

Логические границы ПС с указанием компонентов ПС, их взаимодействия, а также границ ПС и границ контролируемой зоны приведены на рисунке 1.

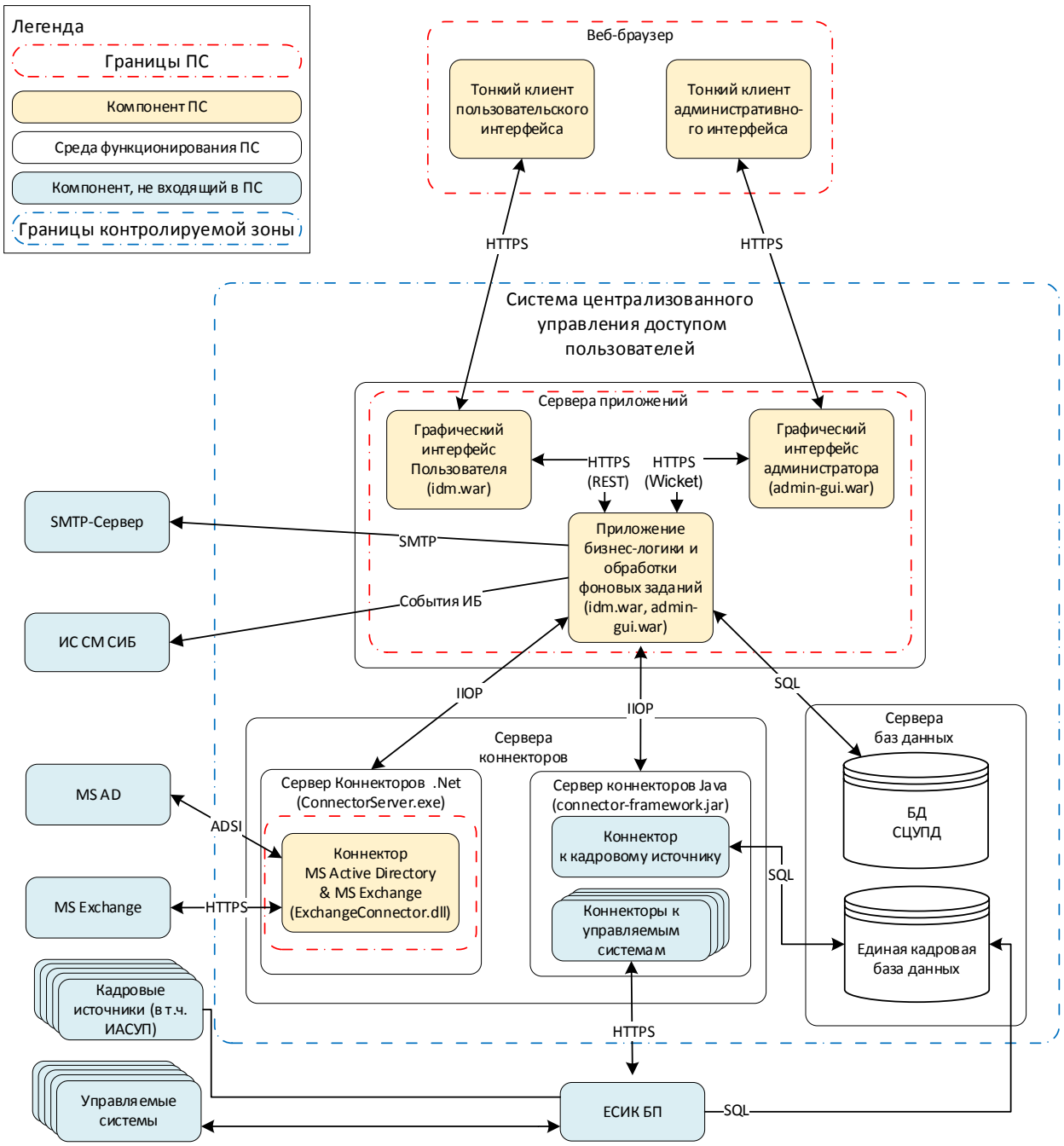

Рис. 1 – Логические границы ПС

Описание компонентов Системы централизованного управления доступом пользователей представлено в документе «Программное средство Система централизованного управления доступом пользователей (СЦУДП). Управление конфигурацией» RU.64509942.00214-01 89 01.

4. ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

Для функционирования ПС СЦУДП необходимо оборудование со следующими минимальными характеристиками:

Серверная часть:

1) 4-ядерный процессор Intel Xeon с тактовой частотой 2.5 ГГц;
2) объем оперативной памяти – 12 ГБ;
3) объем жесткого диска – 50 ГБ.

Клиентская часть:

1) 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 2 ГГц;
2) объем оперативной памяти – 2 ГБ;
3) объем жесткого диска – 20 ГБ.

5. ВЫЗОВ И ЗАГРУЗКА

Работа СЦУДП осуществляется через web-интерфейс. Входными точками в программу являются страницы авторизации web-интерфейсов администратора и пользователя.

Для работы с web-интерфейсом пользователя необходимо запустить браузер и ввести в адресной строке браузера адрес http://<host>:8080/idm, где host – адрес сервера, на который было установлено ПС Система централизованного управления доступом пользователей. Появится окно авторизации. Для входа необходимо ввести имя пользователя (логин), пароль и нажать кнопку Войти.

Для работы с веб-интерфейсом администратора необходимо запустить браузер и в адресной строке браузера ввести http://<host>:8081/admin-gui, где host – адрес сервера, на который было установлено ПС Система централизованного управления доступом пользователей. Появится окно авторизации. При первом входе в систему в окне авторизации следует указать логин и пароль по умолчанию: administrator/5ecr3t. После этого рекомендуется изменить пароль, а затем заново авторизоваться уже с новым паролем.

6. ВЫХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

6.1. Входные данные

Входными данными для Системы являются:

1) стартовая конфигурация системы, которая включает в себя следующий набор файлов:

- config.xml - файл, в котором хранятся параметры базовой конфигурации Системы:
  - параметры подключения к БД;
  - путь к каталогу с дополнительными коннекторами, которые загружаются в локальный сервер коннекторов Системы;
  - путь к хранилищу ключей, которыми шифруются пароли в Системе.
- keystore.jceks – файл с ключами для шифрования паролей в Системе. Расположение этого файла может задаваться в файле config.xml или при запуске Tomcat с помощью ключа -Djavax.net.ssl.trustStore=
- export – каталог, в котором хранятся файлы, генерируемые Системой (например, отчёты);
- icf-connectors – каталог для дополнительных коннекторов, которые должны работать на локальном сервере Системы. Расположение этого каталога может задаваться в файле config.xml;
- schema – каталог для файлов, описывающих расширения объектной модели Системы;
- tmp – каталог для временных файлов Системы;
- web – каталог, в котором хранятся данные, используемые при кастомизации внешнего вида Системы.

2) данные из доверенного источника кадровых данных: о сотрудниках, организациях, структурных подразделениях, должностях, трудоустройствах, которые могут быть получены одним из следующих способов:

- в формате *.csv файла;
- представления (view) в базе данных;
- промежуточная база данных;
- через программный интерфейс взаимодействия (API) (предпочтительно web-сервисы или хранимые процедуры, реализованные на стороне доверенного источника кадровых данных).

3) данные из подключенных УС: учетные записи, права доступа, которые могут быть получены одним из следующих способов:

- в формате *.csv файла;
- представления (view) в базе данных;
- через программный интерфейс взаимодействия (API) (предпочтительно web-сервисы или хранимые процедуры, реализованные на стороне доверенного источника кадровых данных).

4) команды пользователя из веб-интерфейса.

6.2. Выходные данные

Выходными данными для Системы являются:

1) информация, отображаемая пользователю в веб-интерфейсе как результат запроса к системе;

2) команды к подключенным внешним системам на исполнение операций по извлечению и модификации учетных данных:

- запрос списка всех УЗ;
- запрос атрибутов УЗ;

- запрос списка прав доступа;
- запрос атрибутов права доступа;
- создание УЗ;
- модификация УЗ:
- удаление УЗ;

3) записи в базе данных;

4) отчеты, построенные системой, по запросу пользователя, которые можно скачать через веб-интерфейс.

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					