Электронное Проектирование

УТВЕРЖДАЮ
Генеральный директор ООО «ЭП»
_____ И.Е. Мелодиев
«06» февраля 2026 г.

ООО «ЭЛЕКТРОННОЕ ПРОЕКТИРОВАНИЕ»
(наименование организации разработчика)

СЕРВИС КАТАЛОГИЗАЦИИ СЕМАНТИЧЕСКИХ АКТИВОВ
(наименование программы)

ВЕРСИЯ 1.0
(версия программы)

СКСА
(условное обозначение программы)

РУКОВОДСТВО ПО УСТАНОВКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
(наименование документа)

СКСА.ЭП.РУ.01
(условное обозначение документа)

Аннотация

В данном документе представлено описание процессов установки программного обеспечения Сервис каталога семантических активов.

Оглавление

Аннотация **2**
1. Общие сведения **4**
1.1 Обозначение и наименование программы 4
1.2 Программное обеспечение 4
1.3 Языки программирования, на которых написана программа 4
2. Функциональное назначение **5**
3. Установка СКСА **5**
3.1 Параметры конфигурации 5
3.2 Установка общесистемного ПО 6
3.2.1 Установка Liferay Portal 6
3.2.1.1 Общие сведения 6
3.2.1.2 Шаги установки Liferay Portal 6
3.2.1.3 Официальная документация по установке портала Liferay 8
3.2.2 Установка Keycloak 8
3.2.2.1 Общие сведения 8
3.2.2.2 Шаги установки Keycloak 8
3.2.3 Установка Virtuoso 12
3.2.3.1 Общие сведения 12
3.2.3.2 Шаги установки Virtuoso 12
3.2.4 Установка WebProtege 13
3.2.4.1 Общие сведения 13
3.2.4.2 Шаги установки WebProtege 13
3.3 Установка лицензионного программного обеспечения 15
3.3.1 Установка сервиса каталогизации семантических активов (СКСА) 15
3.3.1.1 Подготовка к установке 15
3.3.1.2 Шаги установки 15
4. Настройка **16**
4.1 Управление правами пользователей 16
4.2 Настройка авторизация Liferay Portal через OAuth сервер KeyCloak 17
4.3 Настройка сервиса каталогизации семантических активов 17
4.4 Настройка Nginx 18
5. Проверка работоспособности **18**
6. Сообщения администратору **18**
6.1 Ошибки в клиентском запросе 18
6.2 Ошибки сервера 18

1. Общие сведения

1.1 Обозначение и наименование программы

Наименование программы: Сервис каталогизации семантических активов.

Обозначение программы: СКСА.

1.2 Программное обеспечение

Программное обеспечение разработано в виде портлетов и сервисов Liferay Portal.

Для корректного функционирования программы СКСА на сервере должно быть установлено перечисленное ниже лицензионное программное обеспечение.

На сервере должны быть установлены следующие программные средства:

- Liferay Portal – рекомендуемая версия 7.3.6-ga7; Сайт продукта: https://www.liferay.com/; Ссылка на загрузку дистрибутива: https://github.com/liferay/liferay-portal/releases/download/7.3.6-ga7/liferay-ce-portal-tomcat-7.3.6-ga7-20210301155526191.tar.gz;
- Virtuoso Server Open Source Edition – рекомендуемая версия 7.2.9; Сайт продукта: https://virtuoso.openlinksw.com/; Ссылка на загрузку дистрибутива: https://github.com/openlink/virtuoso-opensource/releases/tag/v7.2.9;
- Nginx сервер – из состава дистрибутива Linux, рекомендуемая версия не ниже 1.18; Сайт продукта: https://nginx.org;
- Keycloak – рекомендуемая версия 20.0.2; Сайт продукта: https://www.keycloak.org/; Ссылка на загрузку дистрибутива: https://www.keycloak.org/archive/downloads-20.0.2.html;
- PostgreSQL – рекомендуемая версия 11.2; Сайт продукта https://www.postgresql.org/;
- WebProtege – доработанная версия 4.0.2; Сайт продукта https://protegewiki.stanford.edu/wiki/WebProtege; Доработанная версия WebProtege с интеграцией с СКСА поставляется в дистрибутиве. Для функционирования WebProtege необходима установка: (1) сервера приложений Tomcat – рекомендуемая версия 9.0.73. Сайт продукта https://tomcat.apache.org/. Ссылка на загрузку дистрибутива https://archive.apache.org/dist/tomcat/tomcat-9/v9.0.73/; (2) база данных MongoDB – рекомендуемая версия 7.0. Сайт продукта https://www.mongodb.com/. Ссылка на загрузку дистрибутива https://www.mongodb.com/docs/v7.0/tutorial/install-mongodb-on-ubuntu/.

Для управления пользователями используется открытое ПО, поддерживающие протокол авторизации OAuth 2.0 – «Keycloak» (открытое ПО для аутентификации и авторизации, а также управления ролями и правами пользователей). Для хранения графовых данных используется открытое ПО – СУБД «Virtuoso». Для хранения структурированных данных используется открытое ПО – СУБД «PostgreSQL». Для поддержки персистентности (устойчивости) универсальных идентификаторов ресурсов (URI) используется открытое ПО – веб-сервер Nginx.

1.3 Языки программирования, на которых написана программа

Программа разработана на языках Java и JavaScript (REACT).

2. Функциональное назначение

Сервис каталогизации семантических активов (СКСА) обеспечивает сбор, публикацию и распространение подготовленных для многократного использования наборов данных (наборов связанных данных, нСД) и описывающих их моделей (семантических активов, СА) для обеспечения семантической интероперабельности. СКСА обеспечивает формирование интегрированного рабочего пространства экспертного сообщества в части каталогизации СА/нСД.

СА публикуются как стандарты данных, используются для обеспечения семантической интероперабельности в гетерогенной информационной среде и являются основой для проектирования информационного обмена с использованием семантических методов. нСД публикуются как наборы данных, разработанные и опубликованные в виде связанных данных (Linked Data).

Функции СКСА обеспечивают:

- формирование и ведение каталогов СА/нСД;
- загрузку и публикацию в каталоге СА/нСД;
- классификацию, поиск и подбор СА/нСД;
- визуализацию СА/нСД;
- предоставление программных интерфейсов для взаимодействия с внешними сервисами и инструментами.

3. Установка СКСА

3.1 Параметры конфигурации

В данной документации используются параметры, которые должны быть заменены на актуальные значения при установке и настройке системы или выполнении команд.

Параметр	Описание	Пример значения
<url_сервера_liferay>	Имя или адрес сервера, на котором размещается Liferay Portal.	catalog.local
<url_сервера_keycloak>	Имя или адрес сервера, на котором размещается Keycloak.	keycloak.local
<url_сервера_virtuoso>	Имя или адрес сервера, на котором размещается хранилище RDF-графов СУБД Virtuoso.	virtuoso.local
<url_сервера_webprotege>	Имя или адрес сервера, на котором размещается WebProtege.	webprotege.local
<PASSWORD>	Пароль пользователя базы данных liferay.	P@ssw0rd!
<DB_PASSWORD>	Пароль пользователя базы данных keycloak.	P@ssw0rd!
<SSO_ADMIN_PASSWORD>	Пароль пользователя keycloak.	P@ssw0rd!

3.2 Установка общесистемного ПО

3.2.1 Установка Liferay Portal

3.2.1.1 Общие сведения

Liferay Portal является сервером приложений и основным общесистемным программным обеспечением сервиса каталогизации семантических активов.

Для установки требуется сервер с установленным ПО:

- OpenJDK – виртуальная машина Java на основе свободного и открытого исходного кода;
- PostgreSQL 11 – объектно-реляционная система управления базами данных, разработанной как open-source проект;
- liferay-ce-portal-tomcat-7.3.6-ga7-20210301155526191.tar.gz – дистрибутив общесистемного программного обеспечения Liferay Portal;

Для работы серверной части системы необходим сервис OpenLink Virtuoso.

3.2.1.2 Шаги установки Liferay Portal

3.2.1.2.1 *Установка OpenJDK*

Установка OpenJDK на сервере осуществляется выполнением следующей команды:

```
$ sudo apt install openjdk-11-jdk openjdk-11-jdk-headless openjdk-11-jre openjdk-11-jre-headless
```

3.2.1.2.2 *Проверка*

Проверка наличия OpenJDK и версии, установленной OpenJDK, осуществляется выполнением следующей команды:

```
$ java -version
```

3.2.1.2.3 *Установка PostgreSQL*

Установка PostgreSQL на сервере осуществляется выполнением следующей команды:

```
$ sudo apt install postgresql-11
```

В случае ошибки установки PostgreSQL необходимо на сервере добавить репозиторий с дистрибутивом PostgreSQL.

3.2.1.2.4 *Добавление репозитория с PostgreSQL*

Добавление репозитория PostgreSQL на сервере осуществляется выполнением следующих команд (включающих установку утилиты gnupg2 и добавления ключа репозитория):

```
$ sudo sh -c 'echo "deb http://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg main" > /etc/apt/sources.list.d/pgdg.list'
$ sudo apt -y install gnupg2
$ wget --quiet -O - https://www.postgresql.org/media/keys/ACCC4CF8.asc | sudo apt-key add -
```

3.2.1.2.5 *Обновление PostgreSQL до версии 11*
Обновление PostgreSQL до версии 11 на сервере осуществляется выполнением следующей команды:

```
$ sudo apt update
$ sudo apt install postgresql-11
```

3.2.1.2.6 *Настройка PostgreSQL*
После успешной установки PostgreSQL необходимо выполнить создание базы данных и пользователя для использования в Liferay Portal.

3.2.1.2.7 *Создание пользователя и базы для Liferay Portal*
Для создания пользователя и базы для Liferay Portal на сервере выполняются следующие команды:

```
$ sudo -u postgres psql
create user pgliferay WITH PASSWORD '<PASSWORD>';
CREATE DATABASE liferaydb;
GRANT ALL PRIVILEGES ON DATABASE "liferaydb" to pgliferay;
\q
exit
```

После создания пользователя и базы данных для Liferay Portal необходимо изменить portal-ext.properties указав в нём параметры соединения с PostgreSQL:

```
jdbc.default.driverClassName=org.postgresql.Driver
jdbc.default.password='<PASSWORD>'
jdbc.default.url=jdbc:postgresql://localhost:5432/liferaydb
jdbc.default.username=pgliferay
```

3.2.1.2.8 *Создание каталога и распаковка дистрибутива*
Установка Liferay Portal из установочного архива liferay-ce-portal-tomcat-7.3.6-ga7-20210301155526191.tar.gz осуществляется выполнением на сервере следующих команд:

```
$ wget https://github.com/liferay/liferay-portal/releases/download/7.3.6-ga7/liferay-ce-portal-tomcat-7.3.6-ga7-20210301155526191.tar.gz
$ sudo tar xvfz /opt/liferay-ce-portal-tomcat-7.3.6-ga7-20210301155526191.tar.gz -C /opt/
$ cd /opt
$ sudo ln -s liferay-ce-portal-tomcat-7.3.6-ga7 liferay-ce-portal
```

3.2.1.2.9 *Создание Systemd Unit*
Для автозапуска Liferay Portal необходимо создать скрипт автозапуска liferay.service.

Создание файла liferay.service:

```
root@catalog:/opt# nano /etc/systemd/system/liferay.service
[Unit]
Description=Liferay Apache Tomcat Web Application Container
After=network.target
[Service]
```

Type=forking
ExecStart=/opt/liferay-ce-portal/tomcat-9.0.40/bin/startup.sh
ExecStop=/opt/liferay-ce-portal/tomcat-9.0.40/bin/shutdown.sh
[Install]
WantedBy=multi-user.target

Добавление запуска Liferay Portal в автозагрузку осуществляется выполнением на сервере следующих команд:

$ sudo systemctl daemon-reload
$ sudo systemctl start liferay
$ sudo systemctl status liferay
$ sudo systemctl enable liferay

3.2.1.2.10 *Установка Nginx*
Установка Nginx на сервере осуществляется выполнением следующей команды:

$ sudo apt install nginx-extras

Проверка после установки осуществляется выполнением следующей команды:

$ curl -i http://localhost

В выводе результата проверки должно быть "200 OK"

3.2.1.3 Официальная документация по установке портала Liferay
Дополнительная информация об установке и настройке Liferay Portal представлена в официальной документации на открытое ПО, размещённой в сети Интернет по адресу https://help.liferay.com/hc/en-us/categories/360001750451-Liferay-DXP-7-2-Admin-Guide.

3.2.2 Установка Keycloak
Keycloak является общесистемным программным обеспечением для реализации технологии single sign-on (SSO) с возможностью управления доступом к сервису каталогизации семантических активов.

3.2.2.1 Общие сведения
Для установки требуется сервер с установленным ПО:

- Ubuntu – операционная система на базе Linux версии 22.04 LTS;
- OpenJDK – виртуальная машина Java на основе свободного и открытого исходного кода версии не ниже 11;
- PostgreSQL 11 – объектно-реляционная система управления базами данных, разработанная как open-source проект.

3.2.2.2 Шаги установки Keycloak

3.2.2.2.1 *Установка OpenJDK*
Установка OpenJDK на сервере осуществляется выполнением следующей команды:

$ sudo apt install openjdk-11-jdk openjdk-11-jdk-headless openjdk-11-jre openjdk-11-jre-headless

Проверка наличия OpenJDK и версии установленной OpenJDK осуществляется выполнением следующей команды:

$ java -version

Вывод результата проверки:

openjdk 11.0.30 2026-01-20
OpenJDK Runtime Environment (build 11.0.30+7-post-Ubuntu-1ubuntu122.04)
OpenJDK 64-Bit Server VM (build 11.0.30+7-post-Ubuntu-1ubuntu122.04, mixed mode, sharing)

3.2.2.2.2 *Установка PostgreSQL*
Установка PostgreSQL на сервере осуществляется выполнением следующей команды:

$ sudo apt install postgresql-11

В случае возникновения ошибки установки PostgreSQL необходимо на сервере добавить репозиторий с дистрибутивом PostgreSQL

3.2.2.2.3 *Добавление репозитория с PostgreSQL*
Добавление репозитория PostgreSQL на сервере осуществляется выполнением следующих команд (включающих установку утилиты gnupg2 и добавления ключа репозитория):

$ sudo sh -c 'echo "deb http://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg main" > /etc/apt/sources.list.d/pgdg.list'
$ sudo apt -y install gnupg2
$ wget --quiet -O - https://www.postgresql.org/media/keys/ACCC4CF8.asc | sudo apt-key add -

3.2.2.2.4 *Настройка PostgreSQL*
После успешной установки PostgreSQL необходимо выполнить создание базы данных и пользователя для использования в Keycloak. Создание пользователя и базы для Keycloak на сервере осуществляется выполнением следующих команд:

$ sudo -u postgres psql
=# create user keycloak with password '<DB_PASSWORD>';
=# create database keycloak owner keycloak;
=# grant all privileges on database keycloak to keycloak;
\q
exit

3.2.2.2.5 *Добавление пользователя и группы*
Создание системных пользователей и групп для Keycloak на сервере осуществляется выполнением следующих команд:

$ sudo groupadd -r keycloak
$ sudo useradd -m -d /var/lib/keycloak -s /sbin/nologin -r -g keycloak keycloak

3.2.2.2.6 *Скачивание дистрибутива*

Перед установкой Keycloak необходимо скачать дистрибутив Keycloak. Для скачивания дистрибутива на сервере выполняются следующие команды:

```
$ sudo mkdir -p /opt/
$ cd /opt/
$ sudo wget https://github.com/keycloak/keycloak/releases/download/20.0.2/keycloak-20.0.2.tar.gz -P /opt/
```

3.2.2.2.7 *Распаковка и назначение прав*

Распаковка Keycloak из дистрибутива и назначение прав на файлы выполняется на сервере следующими командами:

```
$ sudo tar xvfz /opt/keycloak-20.0.2.tar.gz -C /opt/
$ cd /opt
$ sudo chown -R keycloak. keycloak-20.0.2
$ sudo ln -s keycloak-20.0.2 keycloak
$ sudo chmod o+x /opt/keycloak/bin/
$ sudo chown keycloak. /opt/keycloak/keycloak/conf/server*
```

3.2.2.2.8 *Редактирование конфигурационного файла keycloak.conf*

Для настройки Keycloak необходимо отредактировать конфигурационный файл keycloak.conf, выполнив следующие команды:

```
$ sudo nano /opt/keycloak/keycloak-20.0.2/conf/keycloak.conf
```

Содержимое отредактированного файла:

```
# Database
# The database vendor.
db=postgres
# The username of the database user.
db-username=keycloak
# The password of the database user.
db-password=<DB_PASSWORD>
# The full database JDBC URL. If not provided, a default URL is set based on the
selected database vendor.
db-url=jdbc:postgresql://localhost:5432/keycloak
# Hostname for the Keycloak server.
hostname=<url_сервера_keycloak>
https-port=443
http-enabled=true
http-port=80
log-console-output=default
log=console,file
log-file=/tmp/keycloak.log
```

Окончательная настройка Keycloak включает задание логина и пароля администратора, создание конфигурационного файла, первый запуск Keycloak и импорт логина и пароля администратора в базу данных.

3.2.2.2.9 *Задание логина/пароля администратора*
Для первичного задания логина и пароля администратора необходимо выполнить на сервере следующие команды:

$ export KEYCLOAK_ADMIN=admin
$ export KEYCLOAK_ADMIN_PASSWORD= <SSO_ADMIN_PASSWORD>

3.2.2.2.10 *Создание конфигурационного файла*
Для автоматического создания конфигурационного файла необходимо выполнить на сервере следующую команду:

$ sudo bin/kc.sh build

3.2.2.2.11 *Первый запуск и импорт пары логин-пароль администратора в базу*
Первый запуск Keycloak производится следующей командой:

$ sudo -E bin/kc.sh start

При первом запуске происходит импорт в базу ранее заданных логина и пароля администратора. После успешного первичного запуска Keycloak, необходимо остановить процесс, используя (Ctrl+C).

Полная команда запуска Keycloak выглядит следующим образом:

$ sudo bin/kc.sh start --hostname=<url_сервера_keycloak>

3.2.2.2.12 *Создание Systemd Unit*
Для автозапуска Keycloak необходимо создать скрипт автозапуска keycloak.service.

Создание файла keycloak.service:

$ sudo nano /etc/systemd/system/keycloak.service

Содержимое файла:

[Unit]
Description=Keycloak
After=network.target
[Service]
Type=idle
User=keycloak
Group=keycloak
SuccessExitStatus=0 143
ExecStart=/opt/keycloak/bin/kc.sh start
TimeoutStartSec=600
TimeoutStopSec=600

[Install]
WantedBy=multi-user.target

3.2.2.2.13 *Запуск сервиса, просмотр статуса и добавление в автозагрузку*
Добавление запуска Keycloak в автозагрузку и запуск сервиса осуществляется выполнением на сервере следующих команд:

$ sudo systemctl daemon-reload
$ sudo systemctl enable keycloak
$ sudo systemctl start keycloak

Для просмотра статуса работы сервиса можно использовать следующую команду:

$ sudo systemctl status keycloak

3.2.2.2.14 *Официальная документация по установке Keycloak*
Дополнительная информация об установке и настройке Keycloak представлена в официальной документации на открытое ПО, размещённой в сети Интернет по адресу https://www.keycloak.org/documentation

3.2.3 Установка Virtuoso

Virtuoso является сервером графовой базы данных и общим общесистемным программным обеспечением для сервиса каталогизации семантических активов.

3.2.3.1 Общие сведения

Для установки требуется сервер с установленным ПО:

- Ubuntu – операционная система на базе Linux версии 22.04 LTS.

3.2.3.2 Шаги установки Virtuoso

Установка Virtuoso на сервере осуществляется выполнением следующих команд (включая распаковку дистрибутива):

3.2.3.2.1 *Распаковка дистрибутива*
$ cd /opt
$ wget https://github.com/openlink/virtuoso-opensource/releases/download/v7.2.9/virtuoso-opensource-7.2.9.tar.gz
$ sudo tar xvfz virtuoso-opensource-7.2.9.tar.gz -C /opt/
$ sudo ln -s virtuoso-opensource-7.2.9 virtuoso-opensource

3.2.3.2.2 *Создание Systemd Unit*
Для автозапуска Virtuoso необходимо создать скрипт автозапуска: virtuoso.service

Создание файла virtuoso.service:

$ nano /etc/systemd/system/virtuoso.service

Содержимое файла:

[Unit]
Description=Viruoso

After=network.target
[Service]
Type=forking
ExecStart=/opt/virtuoso-opensource/bin/virtuoso-t +configfile /opt/virtuoso-opensource/database/virtuoso.ini
[Install]
WantedBy=multi-user.target

3.2.3.2.3 *Запуск сервиса, просмотр статуса и добавление в автозагрузку*
Добавление запуска Virtuoso в автозагрузку и запуск осуществляется выполнением на сервере следующих команд:

$ sudo systemctl daemon-reload
$ sudo systemctl enable virtuoso
$ sudo systemctl start virtuoso

Для просмотра статуса работы сервиса можно использовать следующую команду:

$ sudo systemctl status virtuoso

3.2.3.2.4 *Официальная документация по установке Virtuoso*
Дополнительная информация об установке и настройке Virtuoso представлена в официальной документации на открытое ПО, размещённой в сети Интернет по адресу https://docs.openlinksw.com/virtuoso/conductorbar/

3.2.4 Установка WebProtege

WebProtege является бесплатной средой совместной разработки онтологий с открытым исходным кодом.

3.2.4.1 Общие сведения

Для установки требуется сервер с установленным ПО:

- Ubuntu – операционная система на базе Linux версии 22.04 LTS.

3.2.4.2 Шаги установки WebProtege

Установка WebProtege на сервере осуществляется выполнением следующих команд (включая распаковку дистрибутива):

3.2.4.2.1 *Установка дистрибутива Apache Tomcat*
Установка Apache Tomcat на сервере осуществляется выполнением следующих команд (включая создание каталога и распаковку дистрибутива):

$ sudo mkdir -p /opt/
$ cd /opt
$ wget https://archive.apache.org/dist/tomcat/tomcat-9/v9.0.73/bin/apache-tomcat-9.0.73.tar.gz
$ sudo tar xvfz apache-tomcat-9.0.73.tar.gz -C /opt/
$ sudo ln -s apache-tomcat-9.0.73 apache-tomcat

3.2.4.2.2 *Создание Systemd Unit*

Для автозапуска Apache Tomcat необходимо создать скрипт автозапуска apache-tomcat.service

Создание файла apache-tomcat.service

```
$ nano /etc/systemd/system/apache-tomcat.service
```

Содержимое файла:

```
[Unit]
Description=Apache Tomcat Web Application Container
After=network.target
[Service]
Type=forking
ExecStart=/opt/apache-tomcat/bin/startup.sh
ExecStop=/opt/apache-tomcat/bin/shutdown.sh
[Install]
WantedBy=multi-user.target
```

3.2.4.2.3 *Запуск сервиса, просмотр статуса и добавление в автозагрузку*

Добавление запуска Apache Tomcat в автозагрузку, запуск и просмотр статуса осуществляется выполнением на сервере следующих команд:

```
$ sudo systemctl daemon-reload
$ sudo systemctl enable apache-tomcat
$ sudo systemctl start apache-tomcat
```

Для просмотра статуса работы сервиса можно использовать следующую команду:

```
$ sudo systemctl status apache-tomcat
```

3.2.4.2.4 *Установка и запуск MongoDB*

Установка MongoDB на сервере осуществляется выполнением следующей команды:

```
$ sudo apt install mongodb-server
```

После установки запуск MongoDB на сервере осуществляется выполнением команды:

```
$ sudo systemctl start mongod.service
```

Проверить статус выполнения MongoDB на сервере можно выполнением команды:

```
$ sudo systemctl status mongod.service
```

3.2.4.2.5 *Установка дистрибутива WebProtege*

Установка WebProtege на сервере осуществляется выполнением следующих команд (включая создание каталога и распаковку дистрибутива):

```
$ cd /opt/apache-tomcat
$ cp /tmp/distrib/webprotege-server.war ./webapps/
$ unzip keycloak-tomcat-adapter-dist-9.0.0.zip -d ./lib/
```

3.2.4.2.6 *Перезапуск Apache Tomcat с установленным WebProtege*
Перезапуск Apache Tomcat осуществляется выполнением на сервере следующей команды:

$ sudo systemctl restart apache-tomcat

3.2.4.2.7 *Официальная документация по установке WebProtege*
Дополнительная информация об установке и настройке WebProtege представлена в официальной документации на открытое ПО, размещённой в сети Интернет по адресу https://github.com/protegeproject/webprotege/wiki/WebProt%C3%A9g%C3%A9-4.0.0-Installation.

3.3 Установка лицензионного программного обеспечения

3.3.1 Установка сервиса каталогизации семантических активов (СКСА)

3.3.1.1 Подготовка к установке
Для установки требуется сервер с установленным ПО:

- Liferay Portal (см. раздел 3.1.1);
- Keycloak (см. раздел 3.1.2);
- Virtuoso (см. раздел 3.1.3);
- WebProtege (см. раздел 3.1.4).

Должна быть настроена авторизация Liferay Portal через OAuth сервер KeyCloak (см. раздел 4.2).

3.3.1.2 Шаги установки
Установка СКСА заключается в установке расширения СКСА и первичной настройке. Расширение СКСА содержит:

- портлет каталога семантических активов;
- портлет визуализации;
- тему отображения;
- сервисы взаимодействия.

Первичная настройка расширения СКСА включает загрузку графов каталогов.

3.3.1.2.1 *Установка портлета каталога семантических активов*
Для установки портлета каталога семантических активов скопируйте файл дистрибутива ru.ep.csi.semantic.jar в каталог установки Liferay Portal /opt/liferay-ce-portal/deploy/.

3.3.1.2.2 *Установка портлета визуализации*
Для установки портлета визуализации скопируйте файл дистрибутива SetupView-portlet.war в каталог установки Liferay Portal /opt/liferay-ce-portal/deploy/.

3.3.1.2.3 *Установка темы отображения*

Для установки темы скопируйте файл дистрибутива statcat-theme.war в каталог установки Liferay /opt/liferay-ce-portal/deploy/.

3.3.1.2.4 *Установка сервисов взаимодействия*

Для установки сервисов (REST-сервис интеграции с внешними системами и инструментами разработки СА/нСД и OpenAPI) скопируйте файлы дистрибутива org.semanticpro.mposervice.api.jar, org.semanticpro.mposervice.service.jar, org.semanticpro.openapi.api.jar org.semanticpro.openapi.client.jar, org.semanticpro.openapi.impl.jar, org.semanticpro.openapi.test.jar в каталог установки Liferay Portal /opt/liferay-ce-portal/deploy/.

3.3.1.2.5 *Загрузка графов каталогов*

Для загрузки графов каталога семантических активов и каталога наборов данных, содержимого семантических активов и наборов данных, а также визуальных представлений загрузите данные в БД Virtuoso. Для этого используйте веб-интерфейс «Virtuoso Conductor», предоставляемый СУБД. Веб-интерфейс располагается на порту 8890 сервера с установленной БД Virtuoso и работает по протоколу HTTP. Для загрузки графов перейдите в раздел «Linked Data», затем в «Quad Store Upload» и загрузите файлы в соответствии с таблицей.

Имя файла (File)	**Имя графа (Named Graph IRI)**
SA.ttl	http://csi.semanticpro.org/ADMS
LD.ttl	http://csi.semanticpro.org/LD
Views.ttl	http://csi.semanticpro.org/VIEWS

Проконтролируйте наличие графов в базе данных в разделе «Linked Data», «Graphs».

Информация о загрузке графов приведена в операции «Импорт графа каталога» из блока сервисных функций руководства по эксплуатации (СКСА.ЭП.РЭ.01).

4. Настройка

4.1 Управление правами пользователей

Для настройки необходимо перейти по адресу https://<url_сервера_keycloak>/admin/master/console/ и ввести учётные данные администратора (учётная запись admin, созданная в момент установки keycloak в соответствии с п. 3.1.2 данного документа). В ходе настройки необходимо создать новый realm sksa. В созданном realm необходимо создать: (1) Клиента ***catalog*** для взаимодействия с ***Liferay Portal*** (2) группы ***LiferayAdmins*** (группа с административными правами) и ***LiferayUsers*** (группа с правами обычного пользователя); (3) роль user; (4) пользователей СКСА.

Информация о создании realm, групп и пользователей приведена в операции «Управление пользователями и разграничение прав доступа» из блока сервисных функций руководства по эксплуатации (СКСА.ЭП.РЭ.01).

4.2 Настройка авторизация Liferay Portal через OAuth сервер KeyCloak

Для настройки авторизация необходимо перейти в панель управления Liferay Portal, выбрать раздел System Settings и прейти в настройку SSO.

На вкладке "OpenID Connect" необходимо поставить "Включен" и сохранить изменения.

На вкладке "OpenID Connect Provider" необходимо настроить соединение с сервером авторизации KeyCloak. Для этого рекомендуется использовать следующие параметры:

Параметр	Описание	Рекомендуемое значение
Provider Name	Наименование провайдера	IDM
OpenID Connect Client ID	Наименование клиента	catalog
OpenID connect client secret	Секретный ключ клиента	
Области действия	Области действия (scopes), которые Liferay Portal будет запрашивать в Keycloack во время аутентификации	openid email profile
Authorization Endpoint	Конечная точка авторизации для KeyCloack	http(s):///realms/sksa/protocol/openid-connect/auth
Issuer URL	URL издателя	http(s):///realms/sksa/protocol/openid-connect/auth
JWKS URI	URI для доступа к JSON Web Key Set	http(s):///realms/sksa/protocol/openid-connect/certs
Token Endpoint	Конечная точка авторизации для доступа к токенам	http(s):///realms/sksa/protocol/openid-connect/token
User Information Endpoint	Конечная точка авторизации для доступа к информации о пользователе	http(s):///realms/sksa/protocol/openid-connect/userinfo

4.3 Настройка сервиса каталогизации семантических активов

Настройка СКСА описана операции «Добавление и настройка портлетов СКСА с использованием интерфейса Liferay» из блока сервисных функций руководства по эксплуатации (СКСА.ЭП.РЭ.01).

Получение информации об установке осуществляется выполнением следующей команды:

> $ curl -i http(s)://<*url_сервера_liferay*>*/api/jsonws/mpo.mpo/get_info*

Вывод результата проверки должен содержать ответ "HTTP/1.1 200" и строку с JSON-объектом, содержащий: (1) строку со значением hash установки (Hash); (2) флаг проверки лицензии (Licensed). Если значение флага не равно YES, необходимо обратится в ООО "Электронное проектирование" и передать строку с JSON-объектом.

4.4 Настройка Nginx

Настройка Nginx включает настройку прокси-сервера для общесистемного ПО Liferay и KeyCloak. Информация об установке и настройке Nginx представлена в официальной документации на открытое ПО, размещённой в сети Интернет по адресу https://nginx.org/ru/docs/.

5. Проверка работоспособности

Для проверки работоспособности необходимо обратиться браузером по адресам доменов, которые были указаны в параметрах конфигурации, и дождаться загрузки страниц общесистемного ПО. По адресу http(s):<*url_сервера_liferay*>/ дождаться загрузки страницы сервиса каталогизации семантических активов.

6. Сообщения администратору

Управление Сервисом каталогизации семантических активов предполагает отслеживание состояния веб-сервера Nginx.

В случае возникновения внештатных ситуаций веб-сервер Nginx производит запись в лог-файл следующих типов ошибок:

6.1 Ошибки в клиентском запросе

Код ошибки	Описание
400	Некорректный запрос (синтаксис/формат)
401	Требуется авторизация
403	Доступ запрещён
404	Ресурс не найден
405	Недопустимый метод запроса
406	Недопустимая кодировка
407	Требуется авторизация прокси
408	Истекло время ожидания запроса
409	Конфликт запросов
411	Не указана длина запроса
412	Не выполнено предусловие (precondition)
413	Превышен предел размера тела запроса
414	Слишком длинный URI
415	Неподдерживаемый тип медиа

6.2 Ошибки сервера

Код ошибки	Описание
500	Внутренняя ошибка сервера
501	Метод не реализован
502	Неверный шлюз
503	Сервис недоступен
504	Истекло время ожидания
505	Неподдерживаемая версия протокола HTTP