



CENTER
TECHNOLOGY COMPANY

Акционерное общество
«Технологическая Компания
«Центр»

Волгоградский пр-т, д. 43, корп.3,
Москва, 109316

Тел.: +7 (495) 204-85-00
Факс: +7 (495) 204-86-00

Программное обеспечение «Сервис налогового агента (Ортакс 1.0)»

Руководство для установки и эксплуатации программного обеспечения

Оглавление

1. Настройка программы	3
1.2. Настройка на состав программных средств.....	3
1.2.1. Настройка MariaDB	3
1.2.2. Установка и настройка JCP	3
I. Установка и первоначальная настройка CryptoPro JCP на сервере приложения	4
II. Экспорт ключей и сертификатов с защищенного носителя Rutoken в контейнер HDImageStore (процедуру необходимо выполнять на отдельной рабочей станции).....	4
III. Импорт ключа и сертификатов, экспортированных в п. 1. в контейнер HDImageStore на сервере приложения.....	5
1.2.3. Настройка Jetty	6
1.2.4. Настройка ключей и сертификатов	7
2. Развёртывание приложения на сервере.	7
3. Развёртывание приложения на сервере.	7
4. Конфигурационные файлы	8

1. Настройка программы

1.2. Настройка на состав программных средств

Приложение «Ortax-gateway» (Сервис налогового агента (Ортакс 1.0) требует дополнительной настройки Jetty. Предполагается что Jetty уже установлен на сервере и настроен как сервис. Так же предполагается что уже установлена СУБД MariaDB.

Далее приводится описание дополнительных настроек в Jetty и в MariaDB.

1.2.1. Настройка MariaDB

Должна быть создана БД web_gate_ortax и следующие пользователи:

- wg_ortax со следующими правами:

GRANT SELECT, UPDATE, LOCK TABLES, DELETE, EXECUTE, INSERT

- wg_ortax_vcs со следующими правами:

GRANT SELECT, UPDATE, ALTER, CREATE, CREATE ROUTINE, ALTER ROUTINE, LOCK TABLES, CREATE VIEW, DELETE, DROP, EVENT, EXECUTE, INDEX, INSERT, REFERENCES, TRIGGER, CREATE TEMPORARY TABLES

1.2.2. Установка и настройка JCP

Перед выполнением работ необходимо подготовить следующее аппаратно-программное обеспечение:

- скачать следующее программное обеспечение: CryptoPro JCP версии jcp-2.0.40132-A;

Программное обеспечение необходимо загрузить с Web-сайта поставщика:

<https://www.cryptopro.ru/products/csp/jcp/downloads>

Для загрузки, необходима учетная запись, которую можно создать по ссылке:

<https://www.cryptopro.ru/user/register>

- получить защищенные носители Rutoken для операторов АО ГСЛ и ООО Спортлото.

Вместе с носителями необходимо получить PIN коды пользователей (не Администраторов) на эти носители.

PIN код состоит из цифр и имеет вид: 81601011937.

Установка и конфигурация CryptoPro JCP состоит из следующих этапов:

1. Установка и первоначальная настройка CryptoPro JCP на сервере приложения;
2. Экспорт ключей и сертификатов с защищенного носителя Rutoken в контейнер HDImageStore (процедуру необходимо выполнять на отдельной рабочей станции);

3. Импорт ключа и сертификатов, экспортированных в контейнер HDImageStore на сервере приложения.

I. Установка и первоначальная настройка CryptoPro JCP на сервере приложения

Детально процедура установки и первоначальной настройки приведена в документации Сcryptopro JCP ЖТЯИ.00091-02 91 01-02. Инструкция по использованию. (Раздел 3. Установка ПО СКЗИ на ПЭВМ) (документация поставляется в составе скачанного дистрибутива - см директорию Дос/ЖТЯИ.00091-02-JCP).

Ниже приведен пример последовательности действий для установки на сервера Сервис налогового агента (Ортакс 1.0).

Последовательно на сервере приложения выполнить следующие действия:

1. Скопировать папку с дистрибутивом CryptoPro JCP в раздел для прикладного ПО: `$ cp -rf jcp-2.0.40132-A /opt/;`
2. Выдать права на запуск скриптов: `$ sudo chmod +x /opt/jcp-2.0.40132-A/*.sh;`
3. Перейти в директорию с установленным приложением: `cd /opt/jcp-2.0.40035/;`
4. Запустить конфигурационный скрипт `configure.sh` (требует root прав)
5. Ввести информацию о лицензии вызовом класса

```
ru.CryptoPro.JCP.tools.License -serial "serial_number" -company "company_name" -store,  
например:
```

```
java -cp .:*: ru.CryptoPro.JCP.tools.License serial "XXXXXX-XXXXXX-XXXXXX-XXXXXX" -  
company "ТК Центр" -store
```

6. Проверить установленную лицензию, вызвав `java -cp .:*: ru.CryptoPro.JCP.tools.License.`

II. Экспорт ключей и сертификатов с защищенного носителя Rutoken в контейнер HDImageStore (процедуру необходимо выполнять на отдельной рабочей станции).

Для импорта ключей и сертификатов с защищенного носителя Rutoken, необходимо:

1. На локальной рабочей станции (на любой поддерживаемой ОС) установить JDK 11 (не JRE), Сcryptopro JCP;

Процедура установки аналогична процедуре, описанной в разделе I, за исключением пунктов 5,6 - они не потребуются).

Последовательно, для Rutoken ГСЛ и Rutoken Спортлото выполнить действия 2-4

2. Вставить защищенный ключевой носитель Rutoken в USB порт;
3. Запустить панель управления JCP (под пользователем с правами администратора), исполнив файл ControlPane.sh / ControlPane.bat, передав в качестве аргумента путь к установленному JDK, например:

```
sudo ./ControlPane.sh /usr/lib/jvm/adoptopenjdk-11-hotspot/
```

4. Осуществить копирование ключевого контейнера Rutoken в контейнер HDImageStore (в файловую систему).

Процедура копирования описана в разделе 4.7.4. Копирование, удаление объектов и смена пароля, документа ЖТЯИ.00091-02 91 01-02. Инструкция по использованию.

При копировании, система JCP попросит установить имя контейнера и пароль. Эти данные необходимо использовать далее, при установке версии сервиса налогового агента (Ортакс 1.0), поэтому их необходимо сохранить или запомнить).

В качестве имен контейнеров, в целях унификации, на всех средах рекомендуется использовать следующие значения:

- GOSLOTO - для ключевого контейнера, импортированного с Rutoken выданного на имя "АО ГСЛ";
- SPORTLOTO - для ключевого контейнера, импортированного с Rutoken выданного на имя "ООО Спортлото".

5. В результате импорта, в файловой системе, по пути:
C:\Users\<USER_NAME>\AppData\Local\Crypto Pro

(или /var/opt/cprosp/keys/<USER_NAME> в случае Linux), будут созданы 2 директории, со следующими именами:

*.000, где * - последовательность из цифр, например:

10211231.000

10211243.000

Их необходимо скопировать, и далее использовать при импорте (см. этап III).

III. Импорт ключа и сертификатов, экспортированных в п.1. в контейнер HDImageStore на сервере приложения

Последовательно на сервере приложения выполнить следующие действия:

- Скопировать ключевые директории (директории с именем *.000) в каталог ключей jcp (/var/opt/cprosp/keys);

- Установить следующие права на скопированные объекты (владелец: root, права доступа rwx----- (700).

1.2.3. Настройка Jetty

В /home/jetty/resources/ требуется поместить прилагаемые к данной инструкции файлы: application.properties, system.properties и logback-stoloto.xml, а в home/jetty/webapps файл stoloto-gateway.xml. Так же требуется создать директорию /home/jetty/war и поместить туда war-файл приложения.

В файле **application.properties** требуется указать значения следующих параметров:

- **ortax.url** – путь к API ortax (<протокол>://<хост>:<порт>);
- **site.url** = – базовый путь к API сайта Столото (<протокол>://<хост>:<порт>);
- **inn.service.url** – базовый путь к API сервиса получения ИНН (<протокол>://<хост>:<порт>);
- **walletone.url** – базовый путь к API сервиса РНКО «Единая касса» (<протокол>://<хост>:<порт>);
- **site.link.successIdentUrl** – указать адрес на который будет происходить перенаправление пользователя в случае успешного прохождения сценария идентификации;
- **esia.url** = – базовый путь к сервису ЕСИА (<протокол>://<хост>:<порт>/);
- **spring.datasource.url** – jdbc-урл для подключения к БД web_gate_ortax (jdbc:mariadb://<хост>:3306/web_gate_ortax?serverTimezone=Europe/Moscow);
- **spring.datasource.password** – пароль для пользователя БД wg_ortax;
- **spring.liquibase.password** – пароль для пользователя БД wg_ortax_vcs;
- **email.host** – хост SMTP сервера;
- **esia.certificate.alias** – алиас сертификата в контейнере;
- **gsl.keystore.alias** – указать алиас ключевого контейнера АО ГСЛ, под которым он доступен в Cryptopro JCP;
- **sportloto.keystore.alias** – указать алиас ключевого контейнера ООО Спортлото, под которым он доступен в Cryptopro JCP.

В файле system.properties требуется указать значения следующих параметров:

- **javax.net.ssl.keyStore** – путь к хранилищу SSL ключей;
- **javax.net.ssl.keyStorePassword** – пароль к хранилищу SSL ключей;
- **javax.net.ssl.keyStoreType** – тип хранилища SSL ключей (p12 или jks) ;
- **javax.net.ssl.trustStore** – путь к хранилищу доверенных сертификатов (jks) ;
- **javax.net.ssl.trustStorePassword** – пароль к хранилищу доверенных сертификатов;
- **jcp.keystore.goslotoPersonalStorePassword** – необходимо указать значение, которое использовалось при сохранении ключевого носителя в контейнер HDImageStore для АО ГСЛ (см. раздел II инструкции по установке JCP);



- **jcp.keystore.sportlotoPersonalStorePassword** – необходимо указать значение, которое использовалось при сохранении ключевого носителя в контейнер HDImageStore для АО Спортлото (см. раздел II инструкции по установке JCP).

В файле stoloto-gateway.xml требуется в параметре “war” указать путь к war-файлу приложения.

1.2.4. Настройка ключей и сертификатов

1. Импортировать сертификат (ГОСТ 2012 ПРОД.cer для продуктивной среды или ТЕСИА ГОСТ 2012.cer для тестовой) в хранилище, указанное в свойстве javax.net.ssl.keyStore в system.properties. При импорте необходимо указать алиас, который необходимо записать или запомнить (будет использован в дальнейшем). Актуальную ссылку для скачивания сертификатов можно найти в пункте 3.1.2 методических рекомендации по использованию ЕСИА, доступных по адресу: <https://digital.gov.ru/ru/documents/6186/> На момент написания инструкции сертификаты доступны для скачивания по адресу: <https://esia.gosuslugi.ru/public/esia.zip>
2. Импортировать цепочку сертификатов портала ESIA (адреса портала для тестовых и продуктивной сред приведены в п.5, при описании параметра esia.url) в хранилище сертификатов, указанное в свойстве javax.net.ssl.trustStore;
3. Импортировать клиентский сертификат системы ORTAX в хранилище, указанное в свойстве javax.net.ssl.keyStore в system.properties;
4. Импортировать сертификат корневого доверенного центра авторизации используемого для API Ortax.

2. Развёртывание приложения на сервере.

Для развёртывания приложения необходимо:

1. Остановить сервер приложений jetty выполнив команду `systemctl stop jetty`;
2. Поместить war-файл приложения в каталог `/home/jetty/wars` и скорректировать имя war-файла в `stoloto-gateway.xml`;
3. Запустить сервер приложений jetty выполнив команду `systemctl start jetty`.





3. Развёртывание приложения на сервере.

Убедиться, что в логах в `/home/jetty/logs` присутствует строка `<ru.stoloto.StolotoApplication - Started StolotoApplication...>` и отсутствуют ошибки. Так же приложение должно открываться в браузере (слушает порт 8080).

4. Конфигурационные файлы

В таблице 1 прикреплены все необходимые конфигурационные файлы.

Таблица 1

№	Файл
1	 application.properties
2	 logback-stoloto.xml
3	 stoloto-gateway.xml
4	 system.properties