|  |
| --- |
|  |
|  |

СИСТЕМА

«IDЕСИА. ТИПОВОЕ РЕШЕНИЕ ДЛЯ

ВЗАИМОДЕЙСТВИЯ С ЕСИА»

Обработчик ИС

РУКОВОДСТВО АДМИНИСТРАТОРА

Листов 9

2025

СОДЕРЖАНИЕ

[1 Установка и обновление Обработчика ИС 3](#_Toc171507380)

[**1.1** **Установка Системы** 3](#_Toc171507381)

[1.1.1 Установка Java JRE 3](#_Toc171507382)

[1.1.1 Установка СУБД РБД 3](#_Toc171507383)

[1.1.2 Установка КриптоПро Java CSP и JCP 4](#_Toc171507384)

[1.1.3 Установка Apache Tomcat 4](#_Toc171507385)

[1.1.4 Установка Обработчика ИС 6](#_Toc171507386)

[**1.2** **Обновление Системы** 6](#_Toc171507387)

[1.2.1 Обновление прикладной части 6](#_Toc171507388)

[1.2.2 Обновление БД 7](#_Toc171507389)

[2 Настройка Обработчика ИС 8](#_Toc171507390)

1. **Установка и обновление Обработчика ИС**
   1. **Установка Системы**

Обработчик ИС предназначен для получения и обработки запросов ВИС банка. Он представляет собой стандартный java-сервлет работающий в среде виртуальной машины java под управлением сервера приложений Apache Tomcat.

Для корректной работы приложения необходимо, чтобы на сервер были установлены и настроены следующие компоненты:

* Java JRE версии 8;
* СУБД РБД версии 3.0;
* Apache Tomcat версии 8 или 9;
* КриптоПро JCP v.2.0;
* КриптоПро Java CSP v.5.0;
* КриптоПро CSP v.5.0;

Для того чтобы среда работала корректно необходимо организовать следующую структуру каталогов.

Таб.1

|  |  |
| --- | --- |
| **Название подкаталога** | **Описание подкаталога** |
| ../id-sys/ | Корневой каталог приложения, желательно размещать в корне диска (для Windows) или каталоге /opt (для Linux) |
| ../id-sys/db/ | Каталог (или символическая ссылка) файлов БД Системы |
| ../id-sys/rdb/ | Домашний каталог (или символическая ссылка) СУБД «Ред База Данных» |
| ../id-sys/tomcat/ | Домашний каталог (или символическая ссылка) Сервера приложений Apache Tomcat |
| ../id-sys/update/ | Каталог (или символическая ссылка) обновлений |

### Установка Java JRE

Установка JRE производится стандартным способом для выбранной операционной системы. В ОС семейства Windows обычно необходимо запустить исполняемый файл и следуя подсказкам установщика произвести дефолтную установку программы. В ОС семейства Linux можно либо произвести установку из доступных репозиториев, либо скачать архив и настроить систему на работу с данной версией.

Проверьте что после установки в переменный средах окружения используемой ОС семейства Windows была корректно установлена переменная JRE\_HOME. В ОС семейства Linux команда «java -version» должна выводить информацию об установленной версии java.

### Установка СУБД РБД

Для установки СУБД РДБ на любой операционной системе необходимо запустить исполняемый файл и следуя рекомендациям произвести установку.

Для СУБД версии 2.6 необходимо выбрать архитектуру **classic** при установке, для СУБД версии 3.0 архитектуру **super**.

В ОС семейства Windows необходимо в качестве каталога установки использовать Домашний каталог СУБД из таб.1. В ОС семейства Linux необходимо после установки создать символическую ссылку на корневой каталог СУБД, чтобы сохранялась структура каталогов указанная в таб.1.

### Установка КриптоПро Java CSP и JCP

При установке Java CSP будет произведена установка JCP в качестве дополнительного модуля, соответственно нет необходимости ставить его отдельно.

Для установки Java CSP необходимо запустить исполняемый файл для соответствующей операционной системы и руководствуясь подсказками выполнить установку JCSP и JCP, установив в качестве криптопровайдера по умолчанию JCSP.

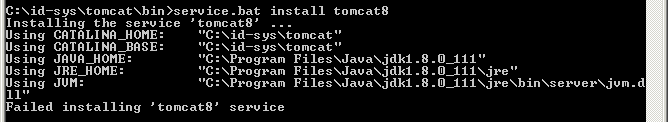
### Установка Apache Tomcat

Для установки Apache Tomcat необходимо поместить все файлы сервера приложений в Домашний каталог Сервера приложений из таб.1.

На ОС семейства Windows необходимо сделать Tomcat системной службой, для этого:

1. Запустите командную строку Windows (cmd.exe) с правами Администратора
2. В командной строке переместитесь в каталог «...\*id-sys\tomcat\bin»*
3. Выполните команду

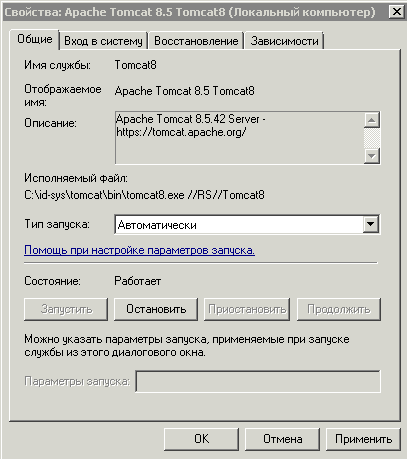
*..\id-sys\tomcat\bin>service.bat install*



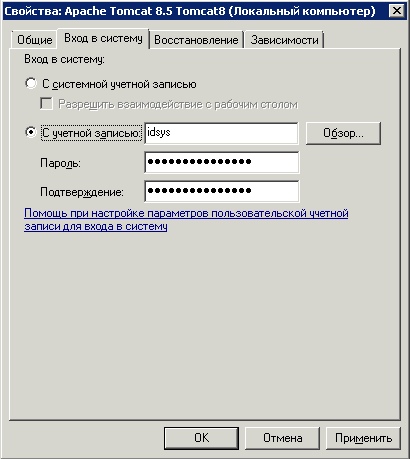
При успешном выполнении будет выведено сообщение

*The service «Tomcat8» has been installed.*

1. Откройте консоль управления службами Windows (Панель управления -> Администрирование -> Службы)
2. Найдите установленную службу Apache Tomcat и откройте на редактирование, дважды кликнув на ней
3. На вкладке «Общие» выберите «Тип запуска» равным «Автоматически»



1. На вкладке «Вход в систему» необходимо установить параметр «С учетной записью», указав имя и пароль той учетной записи, из-под которой устанавливался ключевой контейнер электронной подписи в реестр системы



1. Сохраните изменения и запустите службу

Так же необходимо произвести конфигурирование сервера приложений, добавив в настройки Tomcat параметры работы с виртуальной машиной java, для этого:

1. С помощью командной строки перейдите в каталог «..\id-sys\tomcat\bin» откройте настройки используемой службы выполнив команду:

C:\id-sys\tomcat\bin>tomcat8w.exe //ES//{Имя сервиса}

Где {Имя сервиса} это имя которое было задано при создании сервиса

1. В открывшемся окне перейдите не вкладку «Java»
2. В поле «Java Options» в самом конце с новой строки добавить следующие параметры

-Djava.awt.headless=true

-Xms4096m

-Xmx4096m

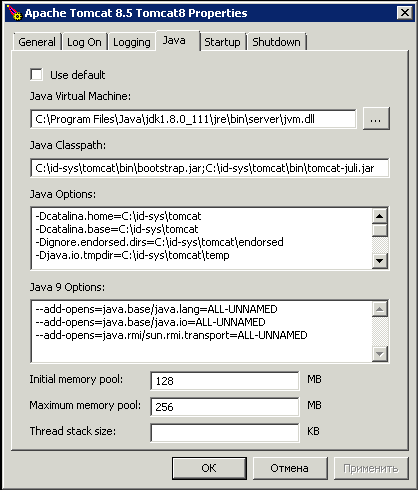
-XX:+CMSPermGenSweepingEnabled

-XX:MaxMetaspaceSize=512m

-XX:+UseG1GC

-XX:MaxGCPauseMillis=1000

-XX:G1HeapRegionSize=8m



**ПРИМЕЧАНИЕ**: Параметры Xms и Xmx указываются в мегабайтах, рекомендуется устанавливать в значение 75% от текущей доступной памяти на сервере. Так же значения Xmx и Xms желательно продублировать в параметрах «Initial memory pool» и «Maximum memory pool»

1. Сохранить изменения

В ОС семейства Linux для запуска сервиса Tomcat необходимо поместить скрипт  в среду используемого менеджера инициализации сервисов.

Так же необходимо произвести конфигурирование сервера приложений, добавив в настройки Tomcat параметры работы с виртуальной машиной java. Для этого откройте на редактирование файл «/opt/id-sys/tomcat/bin/catalina.sh» и укажите следующую строку java опций в начале файла (если подобная строка уже существует, то её стоит заменить):

CATALINA\_OPTS="-Djava.awt.headless=true -Xms4096m -Xmx4096m -XX:MaxMetaspaceSize=512m -XX:+CMSPermGenSweepingEnabled -XX:+UseG1GC -XX:MaxGCPauseMillis=1000 -XX:G1HeapRegionSize=8m -XX:OnOutOfMemoryEr ror=\"touch /tmp/tomcat\_suicide;kill -9 %p\" -verbose:class"

**ПРИМЕЧАНИЕ**: Параметры Xms и Xmx указываются в мегабайтах, рекомендуется устанавливать в значение 75% от текущей доступной памяти на сервере.

### Установка Обработчика ИС

Для установки Обработчика ИС необходимо выполнить следующие действия:

1. Содержимое файла «is\_dp\_online.war» (только вложенные в архив каталоги WEB-INF и META-INF со всем содержимым) необходимо извлечь в каталог «../tomcat/webapps/is\_dp\_online/» сервера приложений;
2. Базу данных «IS\_DP.FDB» (название может отличаться, но часть имени должно обязательно содержать «IS\_DP») разместить в каталоге Файлов БД из таб.1.
3. В конфигурационном файле СУБД «../rdb/aliases.conf» (databases.conf) добавить строку вида:

is\_dp=C:\id-sys\db\IS\_DP.FDB (для windows)

is\_dp=/opt/id-sys/db/IS\_DP.FDB (для linux)

При размещении файлов необходимо учитывать, что к файлам БД должны иметь доступ УЗ ОС из под которых работает СУБД. Так же БД должна быть доступна на чтение и запись.

* 1. **Обновление Системы**

Обновление Обработчика ИС может состоять из двух действий: обновления прикладной части, обновления БД. Обновление БД может не производиться, если в новой версии Обработчика не было изменений в структуре базы.

### Обновление прикладной части

Для обновления приложения Обработчика ИС необходимо произвести следующие действия:

1. Остановить сервер приложений Tomcat
2. Сохранить копию конфигурационного файла «../id-sys/tomcat/webapps/is\_dp\_online/WEB-INF/EsiaServerConfig.xml»
3. Удалить содержимое каталога «../id-sys/tomcat/webapps/is\_dp\_online/»
4. Содержимое файла новой версии приложения «is\_dp\_online.war» (только вложенные в архив каталоги WEB-INF и META-INF со всем содержимым) извлечь в каталог «../id-sys/tomcat/webapps/is\_dp\_online/»
5. Заменить конфигурационный файл «../id-sys/tomcat/webapps/is\_dp\_online/WEB-INF/EsiaServerConfig.xml» сохраненной на шаге 2 копией
6. Запустить сервер приложений Tomcat

### Обновление БД

Обновление БД необходимо производить специальной утилитой обновления, которую предоставит служба поддержки при необходимости. Утилиту необходимо поместить в каталог Обновления.

Для обновления БД Обработчика ИС необходимо произвести следующие действия:

1. Остановить сервер приложений Tomcat
2. Создать резервную копию текущей БД (на случай непредвиденных ошибок при обновлении)
3. В каталог «updates» утилиты обновления необходимо поместить файлы патчей БД (файлы с расширением «.upd»)
4. Запустить утилиту обновления следующей командой:

java -jar updater-1.0.jar -config <Путь до EsiaServerConfig.xml> -dir <Путь до каталога с .upd файлами> -type DB\_IS

дождаться завершения её выполнения

1. Запустить сервер приложений Tomcat
2. **Настройка Обработчика ИС**

Обработчик ИС является приложением без интерфейса, все настройки производятся через изменение конфигурационного файла «../id-sys/tomcat/webapps/is\_dp\_online/WEB-INF/EsiaServerConfig.xml».

Конфигурационный файл имеет XML-структуру и должен соответствовать определенной XSD-схеме. Готовый по структуре файл поставляется вместе с приложением, который необходимо только корректно заполнить.

Назначение настроек:

**Корневой блок <ESConfig>**

**Блок <ESIA>:**

**AuthServiceURL** - URL сервиса аутентификации ЕСИА, указать адрес сервиса ЕСИА к которому необходимо обращаться для формирования сессии аутентификации;

**MarkerServiceURL** - URL сервиса получения маркера идентификации ЕСИА, указать адрес сервиса ЕСИА к которому необходимо обращаться для получения маркера идентификации;

**UserDataServiceURL** - URL запроса сведений о пользователе ЕСИА, указать адрес сервиса ЕСИА к которому необходимо обращаться для получения сведений о пользователе;

**ClientSystemId** - Идентификатор системы-клиента, указать присвоенный в ЕСИА идентификатор;

**Timeout** - Таймаут сервера ЕСИА, указать таймаут в течении которого будет ожидаться получение ответа от сервисов ЕСИА;

**Redirect\_uri** - URI перенаправления, указать адрес Обработчика ЕСИА в формате:

http://ip\_address:8080/esia\_dp\_online/RedirectURI/&lt;id&gt;

где ip\_address – это IP-адрес сервера Обработчика ЕСИА.

**Scope** - Список областей доступа, указать список областей действия доступный банку в ЕСИА;

**Mnemonic** - Мнемоника ЕСИА, указать мнемонику в формате предоставленном ЕСИА;

**ClientCertificateHash** - Хеш сертификата (fingerprint сертификата) системы-клиента в hex–формате. Используемый для проверки подписи сертификат должен быть предварительно зарегистрирован в ЕСИА и привязан к УЗ системы-клиента в ЕСИА

**</ESIA>**

**Блок <ESKeys>:**

**ESIAKey** – Ключ ЭП, содержит атрибуты определяющие принадлежность ключа и доступ к нему;

***id*** - Идентификатор ключа, определяет принадлежность настройки, если указано «REQUEST», то это Ключ ЭП запросов к ЕСИА, если «CHECK», то это Ключ проверки ЭП запросов к ЕСИА;

***isActive*** – Признак активности, если «1» то активен, если «0» то не активен;

***container*** - Наименование контейнера ключа, указать уникальное имя ключевого контейнера в котором находится либо ключ ЭП, либо сертификат ключа проверки ЭП;

***pwd*** - Пароль ключевого контейнера, указать пароль от указанного контейнера;

***path*** - Путь до хранилища ключей, указать путь до файла хранилища ключевых контейнеров;

***pin*** – Пин от хранилища, указать пин-код от хранилища контейнеров ключей;

**</ESKeys>**

**Блок <ESServer>:**

**Вложенный блок<ESUrls>:**

**ConnectionHost -** Хост обработчика запросов ЕСИА, указывается ip-адрес сервера обработчика ЕСИА;

**ConnectionPort** - Порт обработчика запросов ЕСИА, указать значение, которое было задано в настройках обработчика ЕСИА;

**</ESUrls>:**

**Вложенный блок <ESLog>:**

**Log** - Путь к файлу журнала обмена с ИС, указать путь до каталога в который будет сохраняться журнал обмена;

**</ESLog>**

**ESKeyDir** – Настройка хранилища сертификатов и ключей;

***KeyContainerType*** - Тип хранилища сертификата;

***CryptoType*** - Тип провайдера;

**PermissionsFile** - Путь и наименование файла со списком разрешений, указать путь до json-файла в котором находятся разрешения;

**VerifySignature** – Проверка подписи в маркере доступа, значение true – проверка производится, false – проверка не производится;

**Блок <ESAccounts>:**

**ESAccount** - Учетная запись пользователя сервера, содержит атрибуты с данными необходимыми для авторизации на сервере Обработчика ИС;

***id*** - Идентификатор учетной записи, указать произвольное значение;

***login*** - Имя учетной записи, указать имя учетной для доступа;

***password*** - Пароль учетной записи, указать пароль от учетной записи в следующем формате:

Пароль должен быть зашифрован алгоритмом MD5, перед шифрованием добавить в начало пароля значение ESDPS933z.

**ПРИМЕР**:

Пароль: 123456

Перед шифрованием: ESDPS933z123456

После шифрования: 65b1cf10820a80a19db4e54762b39739

**</ESAccounts>**

**Блок <ESDB> - подключение к БД ИС:**

**address** - Адрес БД, указать подключение к базе данных в формате:

jdbc:firebirdsql:ip\_address/3050:alias?lc\_ctype=WIN1251

где

ip\_address - это IP-адрес сервера СУБД

alias - это псевдоним соответствующей БД указанный в файле «../rdb/aliases.conf» (databases.conf)

**login** - Логин БД, указать SYSDBA;

**password** - Пароль БД, указать пароль от SYSDBA;

**bd\_type** - Тип БД, указать «DB\_IS»;

**</ESDB>**

**ConnectionTimeout -** Таймаут подключени в секундах

**</ESServer>**

**</ESConfig>**

После внесения изменений в конфигурационный файл и его сохранения, необходимо произвести перезапуск сервера приложений Apache Tomcat.