

Инструкция по установке «ЕСП.начисления»

Согласовано			
Инв. № подл.	Подп. и дата	Взам. инв. №	

Москва 2021

Аннотация

Оглавление

Справочная информация.....	3
Описание системы	4
Архитектурная схема размещения.....	5
Состав дистрибутива	6
Конфигурационные файлы:	7
Список сторонних модулей и библиотек платформы ЕСП.начисления	7
Описание параметров конфигурационных файлов	8
Предпочитаемый порядок развертывания и запуска серверов	12
Детальное описание установки и настройки серверов системы	12

Согласовано				Взам. инв. №		Подп. и дата		Инв. № подл.					

Справочная информация

Сокращение	Обозначение
ЕСП.н	ЕСП.начисления
БД	База данных
ОС	Операционная система
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
СУБД	Система управления базой данных

Согласовано			

Взам. инв. №	
Подп. и дата	
Инв. № подл.	

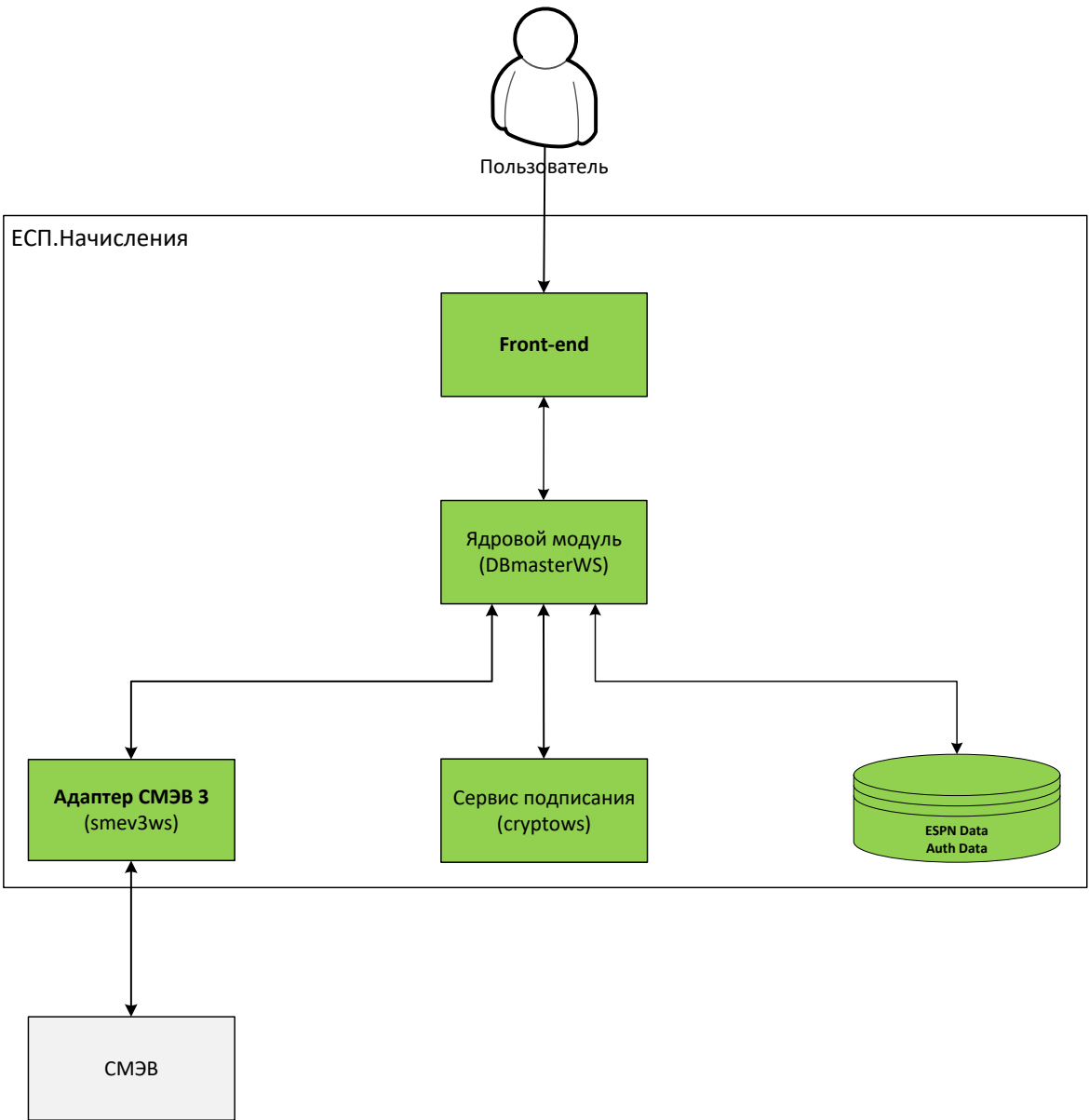
Изм.	Лист	№ документа	Подпись	Дата
Разраб.				
Проверил				
Н.контр.				
ГИП				
Утвердил				

Example			Стадия	Лист	Листов
			ТП	3	22
			Инструкция по развертыванию		

Описание системы

- Функциональная схема системы

Функциональная схема системы представлена на рисунке ниже.



Согласовано				

Взам. инв. №

Подп. и дата

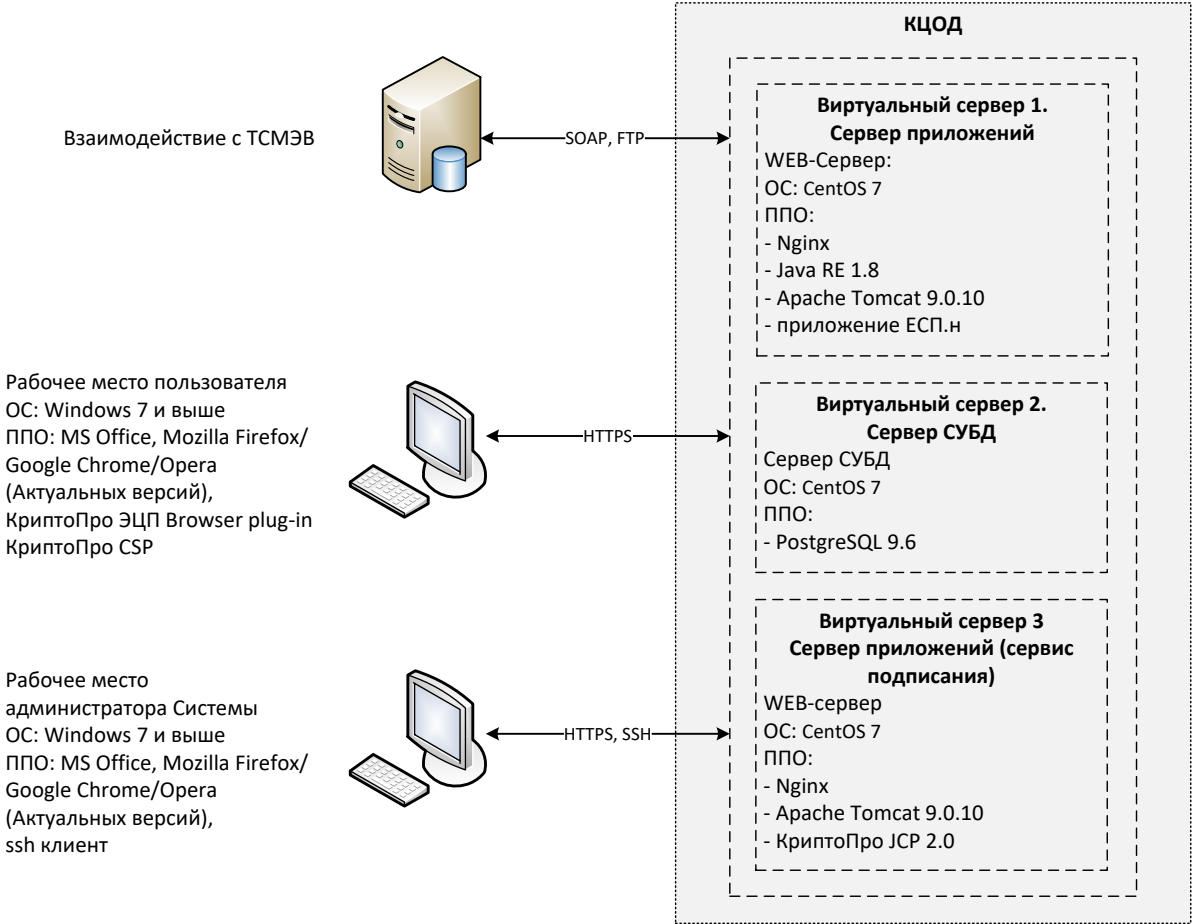
Инв. № подл.

Изм.	Лист	№ документа	Подпис	Дата
Разраб.				
Проверил				
Н.контр.				
ГИП				
Утвердил				

Example		
Инструкция по развертыванию		

Стадия	Лист	Листов
ТП	4	22

Архитектурная схема размещения



• Перечень ППО системы

№	Компоненты	Программное обеспечение
1.	Платформа ЕСП.н	Дистрибутив armp под управлением tomcat 9.0.10, Java RE 1.8
2.	Хранилище данных	PostgreSQL 9.6
3.	Сборщик приложения	Git, maven
4.	Сервер приложений	Apache tomcat 9.0.10
5.	Балансировщик	Nginx 1.12.2:
6.	Криптопровайдер	CryptoPro JCP 2.0 (ревизия 39014)

Согласовано					
Взам. инв. №					
Подп. и дата					
Инв. № подл.	Изм.	Лист	№ документа	Подпись	Дата
	Разраб.				
	Проверил				
	Н.контр.				
	ГИП				
Утвердил					

Example						Стадия	Лист	Листов
						ТП	5	22
						Инструкция по развертыванию		

	Инв. № подл.	Подп. и дата	Взам. инв. №	Согласовано			

Состав дистрибутива

- | | | | | | | | | |
|----------|------|-------------|---------|------|--|-----------|----------|-----------|
| | | | | | | | | |
| Изм. | Лист | № документа | Подпись | Дата | | | | |
| Разраб. | | | | | <div style="text-align: center;"> <p>Example</p> <p>Инструкция по разворачиванию</p> </div> | Стадия | Лист | Листов |
| Проверил | | | | | | ТП | 6 | 22 |
| Н.контр. | | | | | | | | |
| ГИП | | | | | | | | |
| Утвердил | | | | | | | | |

- smeV3ws.war
- front.war

Конфигурационные файлы:

- Сервер приложений **Apache tomcat** (файлы расположены по пути /opt/tomcat-9.0.10/conf)
 - a) server.xml – Основной конфигурационный файл сервера приложений Apache Tomcat.
 - b) tomcat-users.xml – Пользователи и роли для работы с административным интерфейсом сервера приложений.
 - c) logging.properties – Описание настройки логирования.
 - d) cryptows.properties – Конфигурационный файл сервиса подписания:
 - e) espn.properties – Конфигурационный файл ЕСП.начисления.
 - f) dbmasterws.yml – Конфигурационный файл сервиса предоставления АПИ для работы с БД.
 - g) log4j.properties – настройка логирования для веб-сервисов

Список сторонних модулей и библиотек платформы ЕСП.начисления

- Библиотеки для сборки клиента СМЭВ 3. Схема версии 1.2. (ФГБУ НИИ «Восход»)
 - \platform\smeV3ws-module\lib\
 - adminserv-1.2.jar
 - api-1.2.jar
 - commons-1.2.jar
 - factory-1.2.jar
 - ftp4j-1.7.2.jar
 - identification-1.2.jar
 - message-1.2.jar
 - messagetool-1.2.jar
 - server-api-1.2.jar
 - template-1.2.jar
 - transport-1.2.jar
 - util-1.2.jar
 - validation-1.2.jar
- Криптопровайдер CryptoPro JCP 2.0

Согласовано			

Взам. инв. №	
Подп. и дата	
Инв. № подл.	

Изм.	Лист	№ документа	Подпись	Дата					
Разраб.									
Проверил									
Н.контр.									
ГИП									
Утвердил									

Example

Инструкция по развертыванию

Стадия	Лист	Листов
ТП	7	22

Описание параметров конфигурационных файлов

В данном разделе описываются конфигурационные файлы дистрибутива и ключевые параметры данных файлов.

Например:

- cryptows.properties
- 1. **providerName** - Задаёт имя используемого криптографического провайдера. Значение по умолчанию – JCP.
- 2. **snevCertificateStorePath** - Путь до хранилища ключей с сертификатами. Значение по умолчанию - /var/opt/cproscsp/keys/.
- 3. **tsaAddress** - Адрес внешнего TSP-сервера для подписания с использованием метки времени.
- 4. **permittedAlgorithms** - Список разрешённых криптоалгоритмов при загрузке ключей(через запятую). Для использования любых доступных алгоритмов параметр необходимо закомментировать.
- 5. **trustedStorePath** – Путь доверенного хранилища сертификатов. Значение по умолчанию - /etc/pki/ca-trust/extracted/java/cacerts
- 6. **trustedStorePassword** – пароль к доверенному хранилищу сертификатов(по умолчанию *changeit*).
- 7. **keystoreName** – Имя хранилища сертификатов CryptoPro JCP. Значение по умолчанию - HDImageStore
- espn.properties
- 1. **db.dialect** – Диалект запросов к БД. (org.hibernate.dialect.PostgreSQL94Dialect)
- 2. **db.driver** – Драйвер для работы с БД. (org.postgresql.Driver)
- 3. **db.url** – URL, задающий подключение к базе данных и имя используемой базы. (jdbc:postgresql://localhost/newarmp)
- 4. **db.user** – Пользователь, под которым проходит подключение к БД.
- 5. **db.password** – Пароль для подключения к БД.
- 6. **hibernate.show_sql** – Включает логирование запросов к БД в консоль. (false)
- 7. **hibernate.hbm2ddl.auto** – Режим проверки и экспорта DDL схемы в БД. (none)
- 8. **hibernate.c3p0.min_size** – Минимальное количество подключений к БД в пуле.
- 9. **hibernate.c3p0.max_size** – Максимальное количество подключений к БД в пуле.

Согласовано			

Инов. № подл.	Взам. инв. №	
	Подп. и дата	

Изм.	Лист	№ документа	Подпись	Дата					
Разраб.					Example Инструкция по развертыванию				
Проверил									
Н.контр.									
ГИП									
Утвердил									
						Стадия	Лист	Листов	
						ТП	8	22	

10. **hibernate.c3p0.timeout** – Таймаут подключения к БД.
11. **hibernate.c3p0.acquire_increment** - Количество соединений, которые необходимо пытаться открыть при перегруженном пуле.
12. **hibernate.c3p0.max_statements** – Количество кэшируемых запросов к БД.
13. **service.nodeid** – Идентификатор текущей ноды сервера приложений(используется при интеграции со СМЭВ3)
14. **service.listener.response.period** – Интервал проверки очереди сообщений в СМЭВ3(в секундах).
15. **service.smev.testMode** – Добавлять ли в запросы к СМЭВ3 признак тестового запроса.
16. **service.smev.ackMissingRequest** - Подтверждать получение сообщений из очереди, даже если мы не являлись их отправителем.
17. **transport.list** - Идентификаторы используемых дополнительных серверов взаимодействия со СМЭВ3(через запятую)
18. **transport.<идентификатор>.timeout** – Таймаут до сервера СМЭВ3.
19. **transport.<идентификатор>.url** – URL, задающий адрес до сервера СМЭВ3.
20. **transport.main.url** - Адрес основного сервера взаимодействия со СМЭВ3.
(http://smev3-n0.test.gosuslugi.ru:7500/smev/v1.2/ws?wsdl)
21. **large.attachment.transport.address** – Адрес сервера СМЭВ3 для файлового обмена.
22. **signer.serviceUrl** - Адрес криптосервиса для подписания запросов при отправке в СМЭВ3(для межсервисного взаимодействия).
23. **signer.front.serviceUrl** – Адрес хоста, который предоставляет АПИ для загрузки ключевых контейнеров в криптосервис(должен быть доступен с машины клиента через браузер. Пример: http://<host>:<port>/front/crypto)
24. **template.log.output** - Необходимость логирования ответов СМЭВ3.
25. **template.log.input** - Необходимость логирования запросов СМЭВ3
26. **template.validate.output** - Необходимо ли проводить контрольную проверку ответов.
27. **template.validate.input** - Необходимо ли проводить контрольную проверку запросов.
28. **template.validate.smev.signature** - Контрольная проверки ЭП-СМЭВ (если =0, то проверка отключена; если =1, то проверка включена)

Согласовано			

Инв. № подл.	Взам. инв. №	
	Подп. и дата	

Изм.	Лист	№ документа	Подпись	Дата				
Разраб.					Example Инструкция по развертыванию	Стадия	Лист	Листов
Проверил						ТП	9	22
Н.контр.								
ГИП								
Утвердил								

29. **template.local.storage** - Путь сохранения файлов принимаемых вложений сообщений.
30. **service.listener.response.period** - Периодичность проверки ответов от СМЭВЗ(в секундах)
31. **service.listener.request.period** - Периодичность отправки сообщений СМЭВЗ из очереди(в секундах).
32. **service.listener.incoming_request.period** – Периодичность обращения к СМЭВЗ на предмет входящих сообщений(когда ИС выступает в роли поставщика данных)
33. **service.listener.request.grab_size** - Количество выбираемых сообщений из очереди для отправки.
34. **service.listener.request.max_error** - Количество неудачных попыток, после которых сообщение будет исключено из очереди на отправку в СМЭВЗ
35. **service.listener.request.max_time** - Срок жизни сообщения в очереди на отправку(В секундах).
36. **service.listener.request.max_repeat_time** - Игнорировать отправку запросов из журнала, у которых response_date старше чем max_repeat_time(в минутах)

- dbmasterws.yml

1. Параметры Spring

spring:

profiles:

active: development

2. Параметры подключения к БД:

datasource:

driver-class-name: org.postgresql.Driver

url: jdbc:postgresql://<host>:5432/newarmp?currentSchema=dev

username: postgres

password: postgres

3. # Параметры Hibernate (оставить значения по умолчанию):

jpa:

hibernate:

ddl-auto: validate

Согласовано				
Взам. инв. №				
Подп. и дата				
Инв. № подл.				

Изм.	Лист	№ документа	Подпись	Дата				
Разраб.					Example <			

Изм.	Лист	№ документа	Подпис	Дата				
Разраб.					Example Инструкция по разворачиванию	Стадия	Лист	Листов
Проверил						ТП	13	22
Н.контр.								
ГИП								
Утвердил								

6. Добавить автозапуск сервера приложений, создав файл:

```
# nano /etc/systemd/system/tomcat.service
```

С содержимым:

```
[Unit]
Description=Apache Tomcat 9
After=syslog.target network.target

[Service]
WorkingDirectory=/opt/tomcat/bin
User=tomcat
Group=tomcat
Type=forking
Environment=CATALINA_PID=/opt/tomcat/tomcat.pid
Environment=CATALINA_HOME=/opt/tomcat
Environment=CATALINA_BASE=/opt/tomcat
ExecStart=/opt/tomcat/bin/startup.sh
ExecStop=/opt/tomcat/bin/shutdown.sh
Restart=on-failure

[Install]
WantedBy=multi-user.target
```

7. Перезагрузить конфигурацию демона автозапуска и запустить сервер приложений, проверить статус запуска:

```
# systemctl daemon-reload
```

```
# systemctl start tomcat
```

```
# systemctl enable tomcat
```

```
# systemctl status tomcat
```

Настройка установленного Apache Tomcat 9

1. Создать учетную запись для административного входа в сервер приложений:

```
# nano /opt/tomcat/conf/tomcat-users.xml
```

Добавив содержимое:

```
<role rolename="admin-gui" />
<role rolename="manager-gui" />
<user username="admin" password="*****" roles="manager-gui,admin-gui"/>
```

1. Положить конфигурационные файлы дистрибутива ЕСП.начисления в каталог /opt/tomcat/conf и произвести настройку конфигурации путем редактирования файлов(учетная запись подключения к БД, уровень логирования и т.д)

- espn.properties, dbmasterws.yml - для платформы ЕСП.начисления;

Согласовано			

Инв. № подл.	Подп. и дата	Взам. инв. №	

Изм.	Лист	№ документа	Подпись	Дата					
Разраб.									
Проверил									
Н.контр.									
ГИП									
Утвердил									
Инструкция по развертыванию						Стадия	Лист	Листов	
						ТП	15	22	

- cryptows.properties – для сервера подписания;
- Установить сервисы платформы ЕСП.начисления, скопировав файлы в каталог /opt/tomcat/webapp/:
 - dbmasterws.war, smev3ws.war, front.war для платформы ЕСП.н;
 - cryptows.war для сервера подписания
 - Для настройки логирования сервера приложений Apache tomcat не через стандартный JULI(java.util.logging API), а через библиотеку log4j необходимо заменить файл из tomcat/bin/tomcat-juli.jar на библиотеку из сборки ЕСП.начисления, взяв её из armp/libs/tomcat-juli.jar. Так же необходимо подложить armp/libs/tomcat-juli-adapters.jar и armp/libs/log4j.properties в каталог дополнительных библиотек сервера приложений - /tomcat/lib/*.

Настройка сервера подписания

- Произвести установку КриптоПро JCP 2.0.39014 в соответствии с инструкцией производителя.
- Помимо библиотек, которые добавляет установка CryptoPro, необходимо наличие следующих библиотек в /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.171-8.b10.el7_5.x86_64/jre/lib/ext: xmlsec.jar, commons-logging.jar. Проверить и дополнить при отсутствии эти библиотеки из дистрибутива CryptoPro JCP. Убедиться, что все *.jar файлы из архива с дистрибутивом CryptoPro успешно скопировались в <путь до JAVA>/jre/lib/ext, в том числе файлы XAdES.jar и XMLDSigRI.jar.
- Настроить реквизиты используемого хранилища сертификатов в файле /opt/tomcat/conf/cryptows.properties
- В случае перехода на использование подписания по алгоритму ГОСТ-2012, необходимо отключить уведомление о попытке использования устаревшего криптоалгоритма ГОСТ-2001, выполнив:

```
/usr/lib/jvm/java-1.8.0-openjdk/jre/bin/java ru.CryptoPro.JCP.Util.SetPrefs -
system -node ru/CryptoPro/JCP/tools -key Gost2001Warning_class_default -value
true
```

После 01.01.2019 необходимо обновиться до КриптоПро JCP 2.0. R2*.

Согласовано									
	Взам. инв. №								
	Подп. и дата								
Инв. № подл.	Изм.	Лист	№ документа	Подпись	Дата	Example	Стадия	Лист	Листов
	Разраб.						ТП	16	22
	Проверил								
	Н.контр.								
	ГИП								
	Утвердил								
Инструкция по развертыванию									

В случае невозможности обновления до новой версии для переноса даты блокировки работы по ГОСТ Р 34.10-2001 с 1 января 2019 года в КриптоПро JCS 2.0.39014 необходимо:

- скачать патч [JCPGost2001DateProvider.jar](#) или взять из сборки в каталоге /libs/jcpghost2001dateprovider.jar
- скопировать JCPGost2001DateProvider.jar в <JRE>/lib/ext рядом с JCP.jar и другими файлами.
- Добавить в файле <JRE>/lib/security/java.security в самый конец (после JCP), соблюдая нумерацию строку **security.provider.<порядковый_номер>=ru.CryptoPro.JCP.Patch.Gost2001DateProvider** в список провайдеров.

- Убедиться, что у пользователя, под которым запускается Apache Tomcat есть права на файл `/usr/java/jdk1.8.0_181/jre/lib/security/cacerts` на запись.

6. В целях ограничения размера файла catalina.out сервера приложений, рекомендуется добавить периодическое задание для ротации логов:

Создать файл `/etc/logrotate.d/tomcat_armp_logrotate` с содержимым:

```
/opt/egov/tomcat/logs/catalina.out {  
    copytruncate  
    hourly  
    rotate 3  
    compress  
    missingok  
    create 0644 tomcat tomcat  
    size 100 M
```

7. Перезапустить сервер Apache Tomcat:

```
# systemctl restart tomcat
```

Установка и настройка балансировщика Nginx

1. Установить приложение:

Изм.	Лист	№ документа	Подпись	Дата				
Разраб.					Example Инструкция по разворачиванию	Стадия	Лист	Листов
Проверил						ТП	17	22
Н.контр.								
ГИП								
Утвердил								

```
# yum install nginx
```

- ## 2. Добавить Nginx в автозагрузку

```
# chkconfig nginx on
```

3. Сформировать конфигурационный файл `espn.conf` в каталоге `/etc/nginx/conf.d`. В конфигурационном файле необходимо указать адрес хоста в значении параметра `server_name`.

4. **Пример** конфигурационного файла на сервере приложений:

```
# cat /etc/nginx/conf.d/nginx.conf
```

```
log_format {{env.id}}_nlb_tracker '$remote_addr - $time_local - $status - $request_time
- $http_user_agent - "$request" - "$request_body";
```

```
upstream backend_espnapp_{env.id} {
    {{espnapp.nginx.servers}}
}
```

```
upstream backend_espnsign_{{env.id}} {
    {{espnsign.nginx.servers}}
}
```

server

$$\{$$

listen 80;

```
server_name {{dc.nlb.host}};
```

```
access_log {{rootpath}}/logs/access_{{env.id}}.log {{env.id}}_nlb_tracker;
error_log {{rootpath}}/logs/error_{{env.id}}.log;
```

```
error_page 411 = @my_411_error;
```

location /front

$$\{$$

```
proxy_pass http://backend_espnapp_{{env.id}}/front;
```

```
proxy_set_header    X-Real-IP $remote_addr;
```

Изм.	Лист	№ документа	Подпис	Дата				
Разраб.					Example Инструкция по разворачиванию	Стадия	Лист	Листов
Проверил						ТП	18	22
Н.контр.								
ГИП								
Утвердил								

Согласовано					
Взам. инв. №					
Подп. и дата					
Инв. № подл.	Изм.	Лист	№ документа	Подпись	Дата
	Разраб.				
	Проверил				
	Н.контр.				
	ГИП				
	Утвердил				

```

proxy_set_header  Host $host;
proxy_set_header  X-Forwarded-For $proxy_add_x_forwarded_for;
add_header Front-End-Https on;
proxy_buffering off;
}

```

```

location /smev3ws
{
    proxy_pass http://backend_espnapp_{{env.id}}/smev3ws;
    proxy_set_header  X-Real-IP $remote_addr;
    proxy_set_header  Host $host;
    proxy_set_header  X-Forwarded-For $proxy_add_x_forwarded_for;
    add_header Front-End-Https on;
    proxy_buffering off;
}

```

```

location /dbmasterws
{
    proxy_pass http://backend_espnapp_{{env.id}}/dbmasterws;
    proxy_set_header  X-Real-IP $remote_addr;
    proxy_set_header  Host $host;
    proxy_set_header  X-Forwarded-For $proxy_add_x_forwarded_for;
    add_header Front-End-Https on;
    proxy_buffering off;
}

```

```

location /cryptows
{
    proxy_pass http://backend_espnsign_{{env.id}}/cryptows;
    proxy_set_header  X-Real-IP $remote_addr;
    proxy_set_header  Host $host;
    proxy_set_header  X-Forwarded-For $proxy_add_x_forwarded_for;
    add_header Front-End-Https on;
}

```

Изм.	Лист	№ документа	Подпись	Дата	
Разраб.					Example Инструкция по развертыванию
Проверил					
Н.контр.					
ГИП					
Утвердил					
Стадия	Лист	Листов			
ТП	19	22			

```

        proxy_buffering off;
    }
}

```

5. **Пример** конфигурационного файла на сервере балансировки:

```

# cat /etc/nginx/conf.d/prod-ssl.conf

server {
    listen *:80;
    listen *:443 ssl;

    server_name espn.rtlabs.ru;

    ssl_certificate      /etc/nginx/ssl/2018_05_26.crt;
    ssl_certificate_key  /etc/nginx/ssl/tmp/private.key;

    return 301 https://espn.rtlabs.ru $request_uri;
}

server {
    listen 80;
    server_name espn.rtlabs.ru;
    return 301 https://espn.rtlabs.ru $request_uri;
#   allow 195.144.219.13; #lsr ip
#   deny all;
}

server {
    listen      *:443 ssl;
    listen      [::]:443 ssl;
    server_name espn.rtlabs.ru;
#   allow 195.144.219.13; #lsr ip
#   deny all;

    access_log /var/log/nginx/prod.access.log upstream;
    client_max_body_size 600m;

    ssl_certificate      /etc/nginx/ssl/2018_05_26.crt;
    ssl_certificate_key  /etc/nginx/ssl/tmp/private.key;

    ssl on;
    ssl_session_cache builtin:1000 shared:SSL:10m;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers HIGH:!aNULL:!eNULL:!EXPORT:!CAMELLIA:!DES:!MD5:!PSK:!RC4;
    ssl_prefer_server_ciphers on;

    location / {

```

Согласовано			

Взам. инв. №	
Подп. и дата	
Инв. № подл.	

Изм.	Лист	№ документа	Подпись	Дата
Разраб.				
Проверил				
Н.контр.				
ГИП				
Утвердил				

Example			Стадия	Лист	Листов
			ТП	20	22
Инструкция по развертыванию					

6. Создать папку `/var/log/nginx/espn`
7. Запустить Nginx

Более детальная инструкция доступна на сайте <http://nginx.org/>

- espn.rtlabs.ru/cryptows – Контекст сервиса подписания. К нему есть обращение по сети от сервиса smev3ws и сервиса dbmasterws.

- espn.rtlabs.ru/front – Основной сервис, к которому происходит обращение браузера пользователя.
- espn.rtlabs.ru/smev3ws – Сервис, предоставляющий АПИ по взаимодействию со СМЭВ3(К нему есть обращение по сети от сервиса dbmasterws).

Изм.	Лист	№ документа	Подпись	Дата				
Разраб.					Example Инструкция по разворачиванию	Стадия	Лист	Листов
Проверил						ТП	21	22
Н.контр.								
ГИП								
Утвердил								

- [illegible]