

**Контроль регламентных процедур службы оперативного  
планирования режимов исполнительного аппарата  
АО «СО ЕЭС»**

**ИНСТРУКЦИЯ ПО УСТАНОВКЕ  
И НАСТРОЙКЕ**

Москва  
2021

## СОДЕРЖАНИЕ

<b>1. ОСНОВНЫЕ ПОНЯТИЯ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ .....</b>	<b>3</b>
<b>2. НАЗНАЧЕНИЕ РУКОВОДСТВА .....</b>	<b>5</b>
<b>3. ТРЕБОВАНИЯ К ПРОГРАММНЫМ/АППАРАТНЫМ РЕСУРСАМ ...</b>	<b>6</b>
3.1. Требования к аппаратному обеспечению .....	6
3.2. Требования к программному обеспечению .....	6
3.3. Предварительная настройка окружения .....	7
3.4. Сетевой доступ .....	8
<b>4. УСТАНОВКА И НАСТРОЙКА КОМПОНЕНТОВ СИСТЕМЫ .....</b>	<b>11</b>
4.1. Настройка сервера приложений Системы .....	11
4.1.1. Предварительная настройка сервера приложений Системы .....	11
4.1.2. Установка и настройка СУБД.....	11
4.1.3. Настройка сервиса gr-control-web .....	13
4.1.4. Настройка Docker-engine.....	17
4.1.5. Настройка сервиса gr-control-service.....	18
4.2. Настройка сервера ИСЭИ проху .....	23
4.2.1. Установка и настройка сервиса isei-proxu-service .....	23

## 1. ОСНОВНЫЕ ПОНЯТИЯ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

<b>AD</b>	Служба каталогов, являющаяся единым хранилищем данных организации и контролирующая доступ для пользователей на основе политики безопасности каталога.
<b>API</b>	Описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой.
<b>CN</b>	Объект службы каталогов.
<b>CPU</b>	Центральное процессорное устройство
<b>DN</b>	Адрес объекта LDAP.
<b>Docker</b>	Программное обеспечение для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации.
<b>HDD</b>	Постоянное запоминающее устройство
<b>HTTP</b>	HyperText Transfer Protocol – протокол прикладного уровня передачи данных.
<b>HTTPS</b>	HyperText Transfer Protocol Secure – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности.
<b>IMAPS</b>	Протокол доступа к электронной почте
<b>Java</b>	Строго типизированный объектно-ориентированный язык программирования общего назначения.
<b>JavaScript</b>	Прототипно-ориентированный сценарный язык программирования.
<b>JSON</b>	Текстовый формат обмена данными, основанный на JavaScript.
<b>LDAP</b>	Протокол взаимодействия со службой каталогов (AD).
<b>LDAPS</b>	LDAP с поддержкой SSL.
<b>Nexus</b>	Менеджер репозитория предназначенный для проксирования репозитория и хранения ПО.
<b>OU</b>	Объект службы каталогов, представляющий из себя контейнер для хранения различных объектов AD.
<b>RAM</b>	Оперативное запоминающее устройство
<b>REST</b>	Архитектурный стиль взаимодействия компонентов распределённого приложения в сети. REST представляет

	собой согласованный набор ограничений, учитываемых при проектировании распределённой гипермедиа-системы.
<b>SNMP</b>	Протокол, используемый для управления сетевыми устройствами.
<b>SSH</b>	Сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой
<b>SSL</b>	Криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети.
<b>БД</b>	База данных.
<b>ИА</b>	Исполнительный аппарат АО «СО ЕЭС».
<b>ИУС</b>	Информационно-управляющая системы.
<b>ИУС СОИ</b>	Информационно-управляющая система «Система обмена информацией».
<b>КИТС</b>	Корпоративная интеграционно-транспортная система.
<b>ОИК СК-11</b>	Информационно-управляющая система «Оперативно информационный комплекс СК-11».
<b>ПАК</b>	Программно-аппаратный комплекс.
<b>ПАК ЕСМ</b>	ПАК «Единая система мониторинга».
<b>ПАК ИСП</b>	ПАК «Иерархическая система прогнозирования».
<b>ПАК ИСЭИ</b>	ПАК «Информационная система экспорта/импорта электроэнергии в зарубежные энергосистемы».
<b>ПАК ОпАМ</b>	ПАК «Оптимизация по активной мощности».
<b>ПАК ЭГ</b>	ПАК «Формирование прогнозных диспетчерских графиков операционных зон диспетчерских центров АО «СО ЕЭС».
<b>ПДГ</b>	Прогнозный диспетчерский график
<b>ПО</b>	Программное обеспечение
<b>ПШБР</b>	Предварительный план балансирующего рынка
<b>ПЭР</b>	Предварительный электроэнергетический режим
<b>СИБ</b>	Служба информационной безопасности
<b>СОПР</b>	Служба оперативного планирования режимов
<b>СУБД</b>	Система управления базами данных
<b>УЗ</b>	Учётная запись

## **2. НАЗНАЧЕНИЕ РУКОВОДСТВА**

Инструкция описывает действия администратора по установке и настройке программы для ЭВМ «Контроль регламентных процедур службы оперативного планирования режимов исполнительного аппарата АО «СО ЕЭС» (далее по тексту – Контроль РП, Система).

Перечисленные в инструкции команды выполняются с использованием SSH-клиента, например – PuTTY.

### 3. ТРЕБОВАНИЯ К ПРОГРАММНЫМ/АППАРАТНЫМ РЕСУРСАМ

#### 3.1. Требования к аппаратному обеспечению

Рекомендованные характеристики серверов указаны в таблице 1 (наименования серверов требуется запросить у ИА АО «СО ЕЭС»).

Таблица 1 – Рекомендуемая конфигурация серверов Системы

№	Серверы	Кол-во серверов	Рекомендованные характеристики серверов		
			CPU, core	RAM, Gb	HDD, Gb
1	<xxx-control-xxx>	1	8	16	120
2	<xxx-proxy-xxx>	1	4	8	120
	<b>Итого</b>	<b>2</b>	<b>12</b>	<b>24</b>	<b>240</b>

#### 3.2. Требования к программному обеспечению

На сервере <xxx-control-xxx> должно быть установлено следующее

ПО:

- Операционная система – Astra Linux Common Edition;
- Kaspersky Endpoint Security;
- ПО Docker Engine версии 19.03+;
- ПО Nginx версии 1.16.1+;
- СУБД – PostgreSQL версии 9.6.

На сервере <xxx-proxy-xxx> должно быть установлено следующее ПО:

- Операционная система – Astra Linux Common Edition;
- Kaspersky Endpoint Security;
- ПО Nginx версии 1.16.1+.

### 3.3. Предварительная настройка окружения

Для запуска Системы необходимо:

1. Выпустить SSL сертификат для сервера приложений Системы в PEM<sup>1</sup> формате.
2. Создать в AD сервисную УЗ для Системы (необходимо, чтобы сервисная УЗ имела одинаковые CommonName и sAMAccountName).
3. Запросить УЗ для доступа к ФПА с исходным кодом Системы, а также для получения конфигурационных файлов и артефактов сборки.
4. Запросить УЗ для доступа к артефактам Системы расположенным на Nexus сервере ФПА.
5. Создать в AD две группы пользователей (для администраторов и пользователей Системы).
6. Добавить УЗ пользователей Системы в AD группу пользователей Системы.
7. Добавить УЗ администраторов Системы в AD группу администраторов Системы.
8. Предоставить сервисной УЗ Системы право на чтение файлов с сервера, на котором хранятся квитанции КИТС (директории: XXX, XXXX, XXXXX на сервере xxx-cdu.cdu.so) *(предоставляются по запросу ИА АО «СО ЕЭС»)*.
9. Предоставить сервисной УЗ Системы права на чтение файлов с сервера, на котором хранится отчетная документация СОПР, (директории: XXX, XXXX, XXXXX на сервере xxxx-cdu.cdu.so) *(предоставляются по запросу ИА АО «СО ЕЭС»)*.
10. Предоставить сервисной УЗ Системы право отправлять почту от учетных записей, указанных технологом СОПР ИА.
11. Для сервисной УЗ предоставить право на запрос параметров из ОИК СК-11 через REST API.
12. Запросить УЗ для доступа к ПАК ИСЭИ.
13. Запросить УЗ для доступа к ИУС СОИ.
14. В список рассылки писем, содержащих статусы формирования электронных графиков и формируемых ПАК ЭГ, добавить сервисную УЗ, созданную в п.2, или получить данные УЗ, уже

---

<sup>1</sup> Необходима пара ключей (открытый и закрытый ключ), расширения по умолчанию данной пары - .csr и .key

подписанной на рассылку писем. Организовать доступ к почтовому ящику указанной УЗ по протоколу IMAPS.

15. В список рассылки писем, содержащих статусы акцепта ППБР и формируемых ПАК ОпАМ, добавить сервисную УЗ, созданную в п.2., или получить данные УЗ, уже подписанной на рассылку писем. Организовать доступ к почтовому ящику указанной УЗ по протоколу IMAPS.
16. Создать в АД сервисную УЗ для запуска сервиса интеграции с ИСЭИ. Добавить созданную УЗ на сервер <xxx-proxy-xxx>.

### 3.4. Сетевой доступ

Для обновления ПО и компонентов Системы серверам Системы необходим доступ в сеть Интернет. Список ресурсов, к которым необходим доступ, указан в таблице 2.

Таблица 2 – Список внешних ресурсов

Сервер	Сайт
Сервер приложений Системы	download.astralinux.ru download.docker.com

Необходимо обеспечить доступ к указанным сайтам напрямую, или через проху-сервер.

Для проверки доступности ресурсов можно выполнить следующие команды:

```
curl -Is https://download.astralinux.ru | head -n 1
curl -Is https://download.docker.com | head -n 1
```

Ожидаемый ответ:

```
HTTP/1.0 200 Connection established
```

Кроме этого, в таблице 3 представлен список сетевых взаимодействий Системы внутри корпоративной сети СО.

Таблица 3 – Сетевое взаимодействие Системы внутри корпоративной сети

Источник	Приёмник	Протокол/Порт
<b>Сервер приложений Системы (xxx-control-xxx)</b>		
Компьютер администратора Системы	Сервер приложений Системы (xxx-control-xxx)	TCP-22 (SSH), TCP-443 (HTTPS), TCP-8080 (HTTP), TCP-5432
Сервер ПАК ЕСМ	Сервер приложений Системы (xxx-control-xxx)	TCP-443 (HTTPS), TCP-8080 (HTTP),



Источник	Приёмник	Протокол/Порт
		TCP-5432, UDP-161
Сервер приложений Системы (xxx-control-xxx)	Сервер ПАК ЕСМ	UDP-162
Сервер приложений Системы (xxx-control-xxx)	Сервер с сервисом трансляции запросов из ПАК ИСЭИ (xxx-proxu-xxx)	TCP- 80 (HTTP)
Сервер приложений Системы (xxx-control-xxx)	Сервер AD (контроллер домена)	TCP-636 (LDAPS)
Сервер приложений Системы (xxx-control-xxx)	Почтовый сервер	TCP-25 (SMTP)
Сервер приложений Системы (xxx-control-xxx)	Файловые серверы (с файлами СОПР и квитанциями КИТС)	TCP-445 (SMB)
Компьютеры пользователей Системы	Сервер приложений Системы (xxx-control-xxx)	TCP-443 (HTTPS)
Сервер приложений Системы (xxx-control-xxx)	Сервер ФПА – хранилище конфигурации (xxx-xxx-gitlab.cdu.so)	TCP-443 (HTTPS)
Сервер приложений Системы (xxx-control-xxx)	Сервер ФПА – хранилище артефактов (xxx-xxx-nexus.cdu.so)	TCP-18181
Сервер приложений Системы (xxx-control-xxx)	Сервер ПАК ИСП	TCP-80 (HTTP) (порт API сервиса может отличаться, необходимо уточнение у администратора)
Сервер приложений Системы (xxx-control-xxx)	Почтовый сервер	TCP-993 (IMAPS)
Сервер приложений Системы (xxx-control-xxx)	Сервер ОИК СК-11	TCP-443 (HTTPS) (порт API сервиса может отличаться, необходимо уточнение у администратора)
Сервер приложений Системы (xxx-control-xxx)	Сервер ИУС СОИ	TCP-8010 (HTTPS) (порт API сервиса может отличаться, необходимо уточнение у администратора)
<b>Сервер с сервисом трансляции запросов из ПАК ИСЭИ (xxx-proxu-xxx)</b>		
Компьютер администратора Системы	Сервер с сервисом трансляции запросов из ПАК ИСЭИ (xxx-proxu-xxx)	TCP-3389 (RDP)
Сервер приложений Системы (xxx-control-xxx)	Сервер с сервисом трансляции запросов из ПАК ИСЭИ (xxx-proxu-xxx)	TCP-80
Сервер ПАК ЕСМ	Сервер с сервисом трансляции запросов из ПАК ИСЭИ (xxx-proxu-xxx)	TCP-80, UDP-161
Сервер с сервисом трансляции запросов из ПАК ИСЭИ (xxx-proxu-xxx)	Сервер ПАК ЕСМ	UDP-162

<b>Источник</b>	<b>Приёмник</b>	<b>Протокол/Порт</b>
Сервер с сервисом трансляции запросов из ПАК ИСЭИ (xxx-проху-xxx)	Сервер ПАК ИСЭИ	TCP-13080 (SOAP) (порт API сервиса может отличаться, необходимо уточнение у администратора)

Для проверки доступности сервисов можно воспользоваться клиентом Telnet.

## 4. УСТАНОВКА И НАСТРОЙКА КОМПОНЕНТОВ СИСТЕМЫ

### 4.1. Настройка сервера приложений Системы

#### 4.1.1. Предварительная настройка сервера приложений Системы

Для установки основного приложения необходимо подготовить сервер с операционной системой Astra Linux Common Edition в соответствии с данными, указанными в [разделе 3](#) настоящего руководства.

Для настройки Системы необходимо создать учетную запись пользователя на сервере и добавить данного пользователя в группу sudo.

Все дальнейшие настройки будут описаны для УЗ с именем **user**.

Для интеграции с ПАК ЕСМ необходимо установить пакет snmpd, используя команду:

```
sudo apt install snmpd
```

#### 4.1.2. Установка и настройка СУБД

Для установки PostgreSQL необходимо подключиться по SSH на сервер приложений Системы и выполнить следующие команды:

##### 1. устанавливаем СУБД PostgreSQL:

```
#Обновляем список пакетов с репозитория  
sudo apt update
```

```
#Устанавливаем пакет postgresql  
sudo apt install -y postgresql
```

##### 2. разрешаем подключение к PostgreSQL с внешних узлов:

```
#Повышаем привилегии пользователя  
sudo su
```

```
#Разрешаем авторизацию пользователей с любого ip адреса  
echo "host all all 0.0.0.0/0 md5" >>  
/etc/postgresql/9.6/main/pg_hba.conf
```

```
#Разрешаем подключения со всех сетевых интерфейсов  
echo "listen_addresses = '*'" >>  
/etc/postgresql/9.6/main/postgresql.conf
```

##### 3. Запускаем СУБД PostgreSQL:

```
#Добавление в автозапуск сервиса PostgreSQL  
sudo systemctl enable postgresql@9.6-main.service
```

```
#Перезапуск сервиса PostgreSQL  
sudo systemctl restart postgresql@9.6-main.service
```

Для информации:

```
#Удаление пакета postgresql
```

```
sudo apt purge postgresql
```

4. Создаем учетную запись и базу данных для сервиса **rp-control-service**, выполнив команды в соответствии с шаблоном и переменными, определёнными в таблице 4.

Таблица 4 – Параметры конфигурации БД

Переменные	Пример	Комментарии
<b>\$PG_PSWD</b>	PassWord	Пароль привилегированной учетной записи PostgreSQL
<b>\$RP_DB</b>	krp	Имя БД для сервиса <b>rp-control-service</b>
<b>\$RP_DB_LOGIN</b>	krp-user	УЗ для доступа к БД сервиса <b>rp-control-service</b>
<b>\$RP_DB_PSWD</b>	YR6m5BJ0	Пароль для УЗ <b>\$RP_DB_LOGIN</b>

#### Шаблон:

```
#Переключаемся в консоль привилегированного пользователя СУБД
sudo su postgres

#Входим в консоль СУБД
psql

#Изменяем пароль для входа в СУБД для пользователя postgres
ALTER USER postgres WITH PASSWORD '$PG_PSWD';

#Создаем УЗ для БД сервиса rp-control-service
CREATE USER "$RP_DB_LOGIN" WITH PASSWORD '$RP_DB_PSWD'
LOGIN;

#Создаем БД для сервиса rp-control-service
CREATE DATABASE "$RP_DB";

#Предоставляем права к БД для УЗ сервиса rp-control-service
GRANT ALL ON DATABASE "$RP_DB" TO "$RP_DB_LOGIN" WITH
GRANT OPTION;

#Выходим из консоли СУБД
\q
```

#### Пример:

```
sudo su postgres
psql
ALTER USER postgres WITH PASSWORD 'Fdpetjd5r';
CREATE USER "krp-user" WITH PASSWORD 'tjd5rfrt' LOGIN;
CREATE DATABASE "krp";
```

```
GRANT ALL ON DATABASE "krp" TO "krp-user" WITH GRANT  
OPTION;
```

Для проверки предоставления прав к БД необходимо выполнить в консоли `psql` команду:

```
select datname,datacl from pg_database;
```

в результате будет выведен список БД и УЗ, имеющих доступ к БД.

Для проверки работоспособности PostgreSQL необходимо выполнить команду:

```
systemctl status postgresql@9.6-main.service |grep active
```

Ожидаемый ответ:

```
Active: active (running)
```

### 4.1.3. Настройка сервиса `rp-control-web`

Для настройки сервиса на сервере приложений необходимо загрузить артефакт сервиса `rp-control-web` с ФПА, по ссылке: `https://hostname /krp/<...>` (ссылка может быть предоставлена по запросу у ИА АО «СО ЕЭС»).

После чего необходимо загрузить SSL сертификат и артефакт в домашнюю папку (`~/`), расположенную на сервере Системы.

Далее необходимо подключиться к серверу по SSH и выполнить следующую последовательность действий:

1. установить Nginx при помощи команды:

```
sudo apt install -y nginx
```

2. запустить файловый менеджер командой `sudo mc` и перенести SSL сертификат в директорию `/etc/nginx/conf.d/`

Если сертификаты предоставлены в формате PFX необходимо произвести конвертацию сертификата в PEM формат. Для конвертации рекомендуется использовать библиотеку `openssl`, документация на неё доступна по ссылке: <https://www.openssl.org/docs/manmaster/man1/openssl.html>

Пример конвертации сертификата с именем `my.pfx`:

```
sudo openssl pkcs12 -in ~/my.pfx/ -clcerts -nokeys -out  
/etc/nginx/conf.d/rp-control-web.crt  
sudo openssl pkcs12 -in ~/my.pfx/ -nocerts -out ~/my.key  
sudo openssl rsa -in ~/my.key -out /etc/nginx/conf.d/rp-  
control-web.key  
chmod -R +r /etc/nginx/conf.d/
```

3. предоставить права `user` на директорию с web-приложением `rp-control-web` используя команду:

```
sudo chown -R user:user /var/www/html
```

4. разархивировать артефакт сервиса командой:

```
unzip ./artifacts.zip
```

(необходимо заменить ./artifacts.zip на путь к артефакту сервиса)

5. очистить директорию web сайта командой:

```
rm -r /var/www/html/*
```

6. Переместить файлы сервиса в директорию web сайта командой:

```
cp -r ./build/* /var/www/html/
```

(необходимо заменить ./ на путь к разархивированному артефакту)

7. далее необходимо заполнить файл конфигурации, командой:

```
sudo nano /etc/nginx/sites-available/default
```

согласно нижеприведенному шаблону:

```
upstream backend {
    server 127.0.0.1:8080;
}

server {
    server_name $HOST-NAME;
    root    /var/www/html;
    gzip on;
    gzip_types text/css application/javascript
application/json image/svg+xml;
    gzip_comp_level 9;
    etag on;
    client_max_body_size 100m;
    proxy_connect_timeout      60;
    proxy_send_timeout        60;
    proxy_read_timeout        60;
    send_timeout              60;
    listen 443 ssl;
    ssl_certificate $CRT_PATH;
    ssl_certificate_key $KEY_PATH;
    error_log /var/log/nginx/error.log warn;
    access_log /var/log/nginx/access.log combined;
    location / {
        try_files $uri $uri/ /index.html =404;
    }
    location /backend/ {
        proxy_pass http://backend/;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For
$proxy_add_x_forwarded_for;
        proxy_set_header X-Real-IP $remote_addr;
    }
}
```

```

}
server {
    if ($host = $HOST-NAME) {
        return 301 https://$host$request_uri;
    }
    server_name $HOST-NAME;
    listen 80;
    return 404;
}

```

Список значений, которые необходимо изменить в шаблоне указан в таблице 5.

Таблица 5 – Список переменных в конфигурационном файле Nginx

<b>\$HOST-NAME</b>	DNS имя сервера Системы
<b>\$KEY_PATH</b>	Путь до файла, содержащего закрытый ключ
<b>\$CRT_PATH</b>	Путь до файла, содержащего открытый ключ

Пример:

```

upstream backend {
    server 127.0.0.1:8080;
}
server
{
    server_name xxx-xxx-cdu.so;
    root /var/www/html;
    gzip on;
    gzip_types text/css application/javascript
application/json image/svg+xml;
    gzip_comp_level 9;
    etag on;
    client_max_body_size 100m;
    proxy_connect_timeout 60;
    proxy_send_timeout 60;
    proxy_read_timeout 60;
    send_timeout 60;
    listen 443 ssl;
    ssl_certificate /etc/nginx/conf.d/rp-control-web.crt;
    ssl_certificate_key /etc/nginx/conf.d/rp-control-
web.key;
    error_log /var/log/nginx/error.log warn;
    access_log /var/log/nginx/access.log combined;
    location / {
        try_files $uri $uri/ /index.html =404;
    }
    location /backend/ {
        proxy_pass http://backend/;
        proxy_set_header Host $host;

```

```
        proxy_set_header X-Forwarded-For
$proxy_add_x_forwarded_for;
        proxy_set_header X-Real-IP $remote_addr;
    }
}
server {
    if ($host = xxx-xxx.cdu.so) {
        return 301 https://$host$request_uri;
    }
    server_name xxx-xxx.cdu.so;
    listen 80;
    return 404;
}
```

8. для применения настроек необходимо перезагрузить Nginx командой:

```
sudo systemctl restart nginx
sudo systemctl enable nginx
```

9. по умолчанию название Системы, отображаемое на вкладке браузера – RP CONTROL. Для редактирования названия Системы, необходимо выполнить нижеприведённую команду, заменив переменные \$NAME (текущее название) и \$NEW\_NAME (новое название).

Шаблон:

```
sudo sed -i 's/"a": "$NAME"/"a": "$NEW_NAME"/'
/var/www/html/static/js/*
```

Пример:

```
sudo sed -i 's/"a": "RP CONTROL"/"a": "Контроль РП"/'
/var/www/html/static/js/*
```

Установка и настройка сервиса **rp-control-web** закончена. Для проверки работоспособности Nginx необходимо выполнить команду:

```
systemctl status nginx |grep active
```

Ожидаемый ответ:

```
Active: active (running)
```

Для проверки работоспособности сервиса **rp-control-web** необходимо перейти на по web-ссылке, соответствующей имени сервера приложений Системы. Ожидаемый результат – отображение стартовой страницы сервиса **rp-control-web**.

В случае если стартовая страница приложения не загружается, рекомендуется обратиться к лог-файлам Nginx и устранить зафиксированную в них проблему. Для просмотра лог-файлов Nginx (если не менялись пути в



конфигурационном файле выше) необходимо воспользоваться следующими командами:

```
#Error лог
sudo cat /var/log/nginx/error.log
#Access лог
sudo cat /var/log/nginx/access.log
```

#### 4.1.4. Настройка Docker-engine

Подключиться к серверу по SSH и выполнить последовательно следующие команды для установки Docker-engine:

```
#Переходим в консоль root для повышения привилегий
sudo su

#Обновляем список доступных пакетов
apt-get update

#Устанавливаем пакеты необходимые для добавления репозитория Docker
apt-get install -y apt-transport-https ca-certificates
curl gnupg-agent software-properties-common

#Устанавливаем ПО для работы с git репозиторием ФПА
apt-get install -y git

#Загружаем ключ репозитория Docker
curl -fsSL https://download.docker.com/linux/debian/gpg |
sudo apt-key add

#Добавляем репозиторий Docker
add-apt-repository "deb [arch=amd64]
https://download.docker.com/linux/debian buster stable"

#Обновляем список доступных пакетов
apt-get update

#Устанавливаем Docker-engine
apt-get install -y docker-ce docker-ce-cli containerd.io

#Запускаем демон Docker-engine
systemctl start docker

#Включаем демон Docker-engine в автозагрузку
systemctl enable docker

#Включаем пользователя в группу docker для запуска контейнеров
usermod -aG docker user
```

Для доступа к репозиторию `xxx-xxx-nexus.cdu.so` добавляем открытый ключ корневого сертификата СО в доверенную зону.

```
#Переходим в консоль root для повышения привилегий
sudo su

#Скачиваем открытый ключ корневого сертификата
wget "http://ca.so-
ups.ru/system%20operator%20rsa%20cp%20ca%202019.cer"
(Ссылку на актуальный корневой сертификат можно запросить у СИБ)

#Конвертируем открытый ключ в формат PEM
openssl x509 -inform der -in ./system\ operator\ rsa\ cp\
ca\ 2019.cer -out ./ca.pem

#Создаем директории для хранения ключей
mkdir -p /etc/docker/certs.d/xxx-xxx-nexus.cdu.so:18181/
mkdir -p /etc/docker/certs.d/xxx-xxx-nexus.cdu.so:18180/

#Копируем открытый ключ в доверенную зону docker
cp ca.pem /etc/docker/certs.d/xxx-xxx-
nexus.cdu.so:18181/so-ca.crt
cp ca.pem /etc/docker/certs.d/xxx-xxx-
nexus.cdu.so:18180/so-ca.crt

#Копируем открытый ключ в хранилище ОС
cp ca.pem /usr/local/share/ca-certificates/so-ca.crt

#Обновляем
update-ca-certificates
```

Установка `docker-engine` закончена, для проверки установки необходимо выполнить команду:

```
systemctl status docker |grep active
```

Ожидаемый ответ:

```
Active: active (running)
```

#### 4.1.5. Настройка сервиса `rp-control-service`

Для настройки и запуска сервиса `rp-control-service` необходимо выполнять следующую последовательность действий:

1. Перейти в консоль **user**, для этого выполнив команду:

```
sudo su user
```

2. Загрузить репозиторий с шаблоном конфигурации запуска, используя команду:

```
git clone https://xxx-xxx-gitlab.cdu.so/krp/config.git
```

На запрос авторизации необходимо ввести данные УЗ, который предоставлен доступ к репозиторию проекта в ФПА.

3. Перейти в директорию с шаблоном запуска `cd ~/config/` и используя в качестве шаблона файл: `~/config/.env-example` создать новый файл: `~/config/.env/`. Он описывает переменные, которые необходимо заменить в файле `.env`.

Таблица 6 – Список переменных и параметров, используемых в `env-example`

Переменная	Пример	Описание
<b>JAVA_OPTS</b>	'-Xmx768M -Xms768M -XX:MaxMetaspaceSize=768m -XX:-UseCompressedOops'	Параметры запуска java ограничивающие размер оперативной памяти доступной сервису <b>rp-control-service</b> (значение не требует изменений)
<b>JWT_TOKEN_SECRET</b>	Fehtyd4hdyK	Закрытый ключ, используемый для создания токенов доступа к сервису <b>rp-control-service</b> . Данное значение необходимо заменить на случайный набор символов.
<b>ACCESS_TOKEN_TTL</b>	3600	Время жизни токенов доступа к сервису <b>rp-control-service</b> (значение не требует изменений)
<b>RP_SERVICE_LOG_PATH</b>	/var/log/RP	Директория для хранения журналов <b>rp-control-service</b>
<b>RP_PORT</b>	8080	Порт, по которому взаимодействует FE и BE (значение не требует изменений)
<b>LOG_LEVEL</b>	info	Уровень журналирования работы сервиса <b>rp-control-service</b> (по умолчанию <b>info</b> , доступны: <b>error</b> , <b>debug</b> )
<b>NEWSLETTER_CREATE_CRON</b>	"0 1 0 * * *" (каждый день в 00:01)	Расписание создания новых почтовых рассылок (значение не требует изменений)
<b>TASK_FOR_PROCESS_CREATE_CRON</b>	"0 31 0 * * *" (каждый день в 00:31)	Расписание создания новых процессов (значение не требует изменений)

Переменная	Пример	Описание
<b>CHECK_LINK_STATU S</b>	"0 */5 * ? * *" (каждые 5 минут)	Расписание проверки статуса соединения с внешними системами
<b>MAX_FILE_SIZE</b>	50MB	Максимальный размер обрабатываемого файла (значение не требует изменений)
<b>MAX_REQUEST_SIZE</b>	50MB	Максимальный размер запроса (значение не требует изменений)
<b>DB_IP</b>	***.*.*.*:5432	IP адрес и порт подключения к базе данных
<b>RP_DB</b>	krp	Имя базы данных сервиса <b>rp-control-service</b>
<b>RP_DB_USER</b>	krp-user	УЗ для БД сервиса <b>rp-control-service</b>
<b>RP_DB_PASS</b>	*****	Пароль для УЗ <b>\$RP_DB_USER</b>
<b>LDAP_URL_PORT</b>	ldaps://hostname:636	Адрес подключения к AD
<b>LDAP_BASE</b>	'dc=domain2,dc=domain1	Корневой DN службы каталога
<b>LDAP_MANAGER_LOGIN</b>	CN=ia-svc-krp, OU=Службы, OU=Служебные, DC= domain2,DC=domain1	DN для УЗ технического пользователя Системы
<b>LDAP_MANAGER_PAS S</b>	'*****'	Пароль для технической учетной записи
<b>LDAP_USER_SEARCH_FILTER</b>	LDAP_USER_SEARCH_FILTER='(&(sAMAccountName={0}) ((memberOf=CN=ia-krp-admins-test,OU=Группы,OU=Служебные,DC=domain2,DC=domain1)(memberOf=CN=ia-krp-users-test,OU=Группы,OU=Служебные,DC=domain2,DC=domain1))))'	Настройка фильтра, для поиска УЗ пользователей в AD (значение не требует изменений)
<b>LDAP_USER_DN_PAT TERNS</b>	'sAMAccountName={0}'	Настройка фильтра, для поиска УЗ пользователей в AD (значение не требует изменений)

Переменная	Пример	Описание
<b>LDAP_GROUP_SEARCH_BASE</b>	'ou=Группы,ou=Служебные'	DN OU содержащий технические группы (значение не требует изменений)
<b>LDAP_GROUP_SEARCH_FILTER</b>	'member={0}'	Настройка фильтра, для поиска групп в AD (значение не требует изменений)
<b>LDAP_ADMIN_GROUP_CN</b>	ia-krp-admins	Имя группы, в которой состоят администраторы Системы
<b>LDAP_TECHNOLOGIST_GROUP_CN</b>	ia-krp-users	Имя группы, в которой состоят пользователи Системы
<b>SMTP_HOST</b>	hostname.domain2. Domain1	DNS имя почтового сервера
<b>SMTP_PORT</b>	25	SMTP порт почтового сервера
<b>MAIL_SEND_TRY_NUM</b>	3	Количество попыток отправки сообщения по электронной почте (значение не требует изменений)
<b>MAIL_SEND_TRY_INTERVAL_SEC</b>	60	Интервал времени в секундах между неудачными попытками отправки сообщения по электронной почте (значение не требует изменений)
<b>CORS_URLS</b>	'https://hostname	Адрес веб-сайта Системы
<b>COOKIE_DOMAINS</b>	Hostname.domain2. Domain1'	Имя сайта Системы
<b>PASSWORD_CONFIG_KEY</b>	*****	Ключ шифрования для информации хранящейся в БД (16 случайных символов).
<b>rp_control_version</b>	poligon	Определяет версию контейнера с приложением (значение не требует изменений)

4. Для загрузки контейнера с сервисом необходимо авторизоваться в хранилище артефактов, для этого необходимо воспользоваться командой:

```
docker login xxx-xxx-nexus.cdu.so:18181
```

На запрос авторизации необходимо ввести данные УЗ, который предоставлен доступ к проекту в ФПА

Ожидаемый ответ:

```
Login Succeeded
```

5. Для запуска сервиса, необходимо использовать SH скрипт, выполнив команду:

```
./rp-control-service.sh
```

(SH скрипт расположен в директории с шаблоном конфигурации **.env**.)

Ожидаемый результат выполнения команд – запущен docker-контейнер, содержащий основное приложение Системы **rp-control-service**.

Для проверки корректного запуска docker-контейнера можно воспользоваться командой:

```
docker ps
```

Ожидаемый ответ – возвращен список с запущенными docker-контейнерами. Список содержит контейнер с именем (NAME) **rp-control-service** и имеет статус (STATUS) UP.

Если возвращаемый ответ не соответствует ожидаемому необходимо обратиться к docker логу и устранить зафиксированную в нём проблему. Команда для вывода записей из docker лога:

```
docker logs rp-control-service
```

Как правило, большинство проблем возникает в случае некорректного заполнения одной или нескольких переменных в файле **.env**. Рекомендуется проверить корректность их заполнения и при необходимости внести соответствующие правки. После внесения правок в файл **.env** необходимо остановить docker контейнер и выполнить его удаление командой:

```
docker stop rp-control-service && docker rm rp-control-service
```

После удаления необходимо повторно запустить SH скрипт:

```
./rp-control-service.sh
```

После получения ожидаемого ответа с успешно запущенным docker контейнером (STATUS UP) необходимо в браузере перейти на стартовую страницу сервиса **rp-control-web** для проверки его корректной связи с сервисом **rp-control-service**. Необходимо авторизоваться и выполнить тестовую отправку регламентной рассылки. В случае если попытка авторизации и отправки регламентной рассылки осуществлена успешно, то установка и настройка сервиса **rp-control-service** успешно завершена.

В противном случае необходимо обратиться к лог файлу сервиса **rp-control-service** и устранить зафиксированную в нем проблему. Для просмотра лог файла сервиса **rp-control-service** (путь указан по умолчанию, задается в файле **.env** переменной **\$RP\_SERVICE\_LOG\_PATH**) необходимо воспользоваться следующей командой:

```
sudo cat /var/log/RP/rp.log
```

После устранения проблем необходимо остановить, удалить и выполнить повторную загрузку и запуск docker контейнера с приложением **gp-control-service**. Необходимые команды приведены выше.

## 4.2. Настройка сервера ИСЭИ proxy

Для установки приложения необходимо подготовить сервер в соответствии с данными, указанными в [разделе 3](#) настоящего документа.

Для настройки Системы необходимо предоставить сервисной УЗ, созданной в п.16 раздела 3.3., административные права права на запись и изменение файлов в директории сайта. В руководстве в качестве сервисной УЗ будет использоваться УЗ **cdu\ia-svc-krp-proxy**.

Для интеграции с ПАК ЕСМ должна быть запущена служба «SNMP Service».

### 4.2.1. Установка и настройка сервиса **isei-proxy-service**

В данном разделе описана установка сервиса **isei-proxy-service** на веб-сервере.

Перед установкой сервиса необходимо загрузить архив с файлами сервиса **isei-proxy-service**.

После загрузки необходимо передать архив на веб-сервер, открыть архив и скопировать файлы, находящиеся в директории *isei-proxy-service/target*, в созданную директорию веб-сайта.

После копирования файлов приложения необходимо создать в директории файл *isei\_proxy\_service.log*.

После выдачи необходимых прав доступа сервисной УЗ необходимо перейти в оснастку Manager и выполнить следующие шаги:

1. Создать пул приложений.
2. В созданном пуле приложений необходимо перейти в дополнительные настройки и выставить следующие значения:

В поле «Identify» необходимо выбрать элемент «Custom account» и ввести данные сервисной УЗ.

В полях «Enable 32-Bit Applications» и «Load User Profile» необходимо установить значения «true».

На этом настройка пула приложений закончена. Далее необходимо создать веб-сайт и выполнить его настройку или выполнить настройку «Default Web Site».

В случае настройки «Default Web Site» необходимо ввести путь к директории с файлами сервиса (Physical path) и выбрать созданный на

предыдущем шаге пул приложений (Application pool). В случае необходимости можно обозначить Host name на вкладке Edit Site Binding.

Далее необходимо произвести конфигурацию сервиса **isei-proxy-service**, для этого в файле *Web.config*, расположенном в директории веб-сайта необходимо скорректировать адрес подключения к ПАК ИСЭИ, для этого в разделе «*endpoint address*» необходимо заменить «*localhost*» на *IP адрес:порт* сервера ПАК ИСЭИ.

Пример:

```
<endpoint
  address="http://***.**.*:13080/EIService.svc/ByUserName
  e" binding="wsHttpBinding"
  bindingConfiguration="UserNameEndpoint"
  contract="EIService.IEIService" name="UserNameEndpoint">
```

После изменения настроек, необходимо перезагрузить веб-сайт.

На этом установка и настройка веб-сервиса **isei-proxy-service** закончена. С результатами работы сервиса можно ознакомиться в лог файле *isei\_proxy\_service.log*, расположенном в директории с файлами сервиса.