

**АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА  
«ФОНД ПРОГРАММ И АЛГОРИТМОВ»  
(ФПА)**

**Инструкция по установке и настройке**

**Москва**

**2021 г.**

# ОГЛАВЛЕНИЕ

<b>1. ПОДГОТОВКА К УСТАНОВКЕ .....</b>	<b>5</b>
1.1. ОБЩИЕ СВЕДЕНИЯ .....	5
1.1. ТРЕБОВАНИЯ ПЕРЕД УСТАНОВКОЙ .....	6
1.1.1. Требования к техническим средствам .....	6
1.1.2. Требования к аппаратному обеспечению .....	6
1.1.3. Требования к операционной системе и дополнительному ПО .....	7
<b>2. УСТАНОВКА И НАСТРОЙКА КОМПОНЕНТОВ СИСТЕМЫ .....</b>	<b>8</b>
2.1. УСТАНОВКА КОМПОНЕНТА «ASDU-FPA-APP» .....	8
2.2. УСТАНОВКА КОМПОНЕНТА «ASDU-FPA-GIT» .....	9
2.3. УСТАНОВКА КОМПОНЕНТА «ASDU-FPA-FS» .....	10
2.4. УСТАНОВКА КОМПОНЕНТА «ASDU-FPA-W» .....	11
<b>3. УСТАНОВКА И НАСТРОЙКА СИСТЕМЫ ФПА .....</b>	<b>12</b>
3.1. ОБЩЕЕ ОПИСАНИЕ .....	12
3.2. ПОДГОТОВКА К УСТАНОВКЕ .....	12
3.2.1. База данных .....	12
3.2.2. Аутентификация .....	12
3.2.3. ЕСЭП .....	13
3.2.4. Требования к серверу .....	13
3.3. УСТАНОВКА BACK-END .....	13
3.4. УСТАНОВКА FRONT-END .....	14
<b>4. ПРИЛОЖЕНИЕ 1 ИНСТРУКЦИЯ ПО РАЗВОРАЧИВАНИЮ ЕСЭП .....</b>	<b>15</b>
1.1 УСТАНОВКА ОПЕРАЦИОННОЙ СИСТЕМЫ .....	15
1.2 УСТАНОВКА СУБД .....	16
1.2.1 Установка SQL БД .....	16
1.2.2 СУБД POSTGRESQL .....	18
1.3 ПЕРВИЧНОЕ РАЗВЕРТЫВАНИЕ БАЗ ДАННЫХ ЕСЭП .....	18
1.3.1 Установка pgAdmin .....	18
1.3.2 Установка дополнительного СПО и ППО .....	18
1.3.3 Редактирование и запуск скрипта генерации БД .....	18
1.4 УСТАНОВКА СЕРВЕРА ПРИЛОЖЕНИЙ С ПОМОЩЬЮ МАСТЕРА НАСТРОЙКИ СЕРВЕРА .....	19
1.5 УСТАНОВКА ПРИЛОЖЕНИЯ ЕСЭП .....	20
1.6 УСТАНОВКА КРИПТОПРО CSP 4.0 ДЛЯ ГОСТ Р 34.10-2012 .....	22
1.7 УСТАНОВКА GPL GHOSTSCRIPT .....	23
1.8 УСТАНОВКА СЕРВЕРНЫХ ДОПОЛНЕНИЙ КРИПТОКОМПОНЕНТА .....	24
1.9 УСТАНОВКА LIBREOFFICE .....	24
1.10 УСТАНОВКА КЛИЕНТСКОГО КОРНЕВОГО СЕРТИФИКАТА .....	24
1.11 НАСТРОЙКА СИСТЕМЫ ЕСЭП .....	25
1.13 УСТАНОВКА СЛУЖБЫ «СТОРОЖ ОЧЕРЕДИ СООБЩЕНИЙ ПОРТАЛА ЕСЭП» .....	29
1.14 НАСТРОЙКА БРАУЗЕРА .....	30

## ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

Сокращение	Определение
HTTP	HyperText Transfer Protocol — протокол прикладного уровня передачи данных
АО «СО ЕЭС», СО, СО ЕЭС	Акционерное общество «Системный оператор Единой энергетической системы»
БД	База данных
ЕСЭП	Единая система электронной подписи
ИУС	Информационно-управляющая система
ПО	Программное обеспечение
Репозиторий	Распределенная система управления версиями файлов
СУБД	Система управления базы данных

## **АННОТАЦИЯ**

Настоящий документ разработан в рамках выполнения работ по созданию автоматизированной информационной системы «Фонд программ и алгоритмов» (далее – Система).

Пошаговая инструкция по установке и настройке Системы предназначена для определения действий администратора для полного развертывания Системы на рабочем серверном оборудовании АО «СО ЕЭС», и приведении Системы в состояние штатной эксплуатации.

# 1. ПОДГОТОВКА К УСТАНОВКЕ

## 1.1. Общие сведения

Архитектура Системы выполнена на компонентной модели, элементами которой являются виртуальные машины. Взаимосвязь между компонентами осуществляется по протоколу HTTP. Процесс установки Системы происходит поэтапно для каждого компонента с помощью соответствующих консольных команд.

В составе Системы имеются компоненты, перечень и описание которых приведены ниже (Таблица 1):

Таблица 1. Перечень компонентов Системы

Название VM	asdu-fpa-git	asdu-fpa-app	asdu-fpa-w	asdu-fpa-fs
Операционная система	CentOS Linux release 7.5	CentOS Linux release 7.5	Server 2016 Standard	CentOS Linux release 7.5
Назначение	<ul style="list-style-type: none"><li>- БД перечня ИУС</li><li>- БД GitLab</li><li>- БД ЕСЭП</li></ul>	<ul style="list-style-type: none"><li>- Управление исходным кодом</li><li>- Управление релизами</li><li>- Сборка исходного кода пол платформу Linux, запуск тестов</li><li>- Рассылка уведомлений</li><li>- Настройка полномочий</li><li>- Ведение реестра ИУС</li><li>- Распределение доступа к сведениям ИУС</li><li>- Ведение проектной документации по ИУС</li></ul>	<ul style="list-style-type: none"><li>- Сборка исходного кода , запуск тестов</li><li>- Визуализация содержания электронных документов</li><li>- Наложение электронной подписи для электронных документов</li><li>- Проверка электронных подписей</li></ul>	<ul style="list-style-type: none"><li>- Хранение артефактов сборки исходного кода</li><li>- Статический анализ кода</li><li>- Настройка правил анализа</li><li>- Создание отчетов качества исходных кодов</li></ul>
Программное обеспечение	PostgreSQL 9.6	<ul style="list-style-type: none"><li>- GitLab 11.4</li><li>- OpenJDK 8</li></ul>	<ul style="list-style-type: none"><li>-SQL</li><li>- ЕСЭП</li></ul>	<ul style="list-style-type: none"><li>- SonarQube 7.3</li><li>- Sonatype Nexus</li></ul>

Название ВМ	asdu-fpa-git	asdu-fpa-app	asdu-fpa-w	asdu-fpa-fs
			<ul style="list-style-type: none"> <li>- КриптоПРО CSP 4.0</li> <li>- Libre Office 5.4.1</li> <li>- GhostScript 9.0.6</li> <li>- GitLab Runner 11.4</li> </ul>	Repository OSS 3.14

## 1.1. Требования перед установкой

### 1.1.1. Требования к техническим средствам

Для обеспечения работы пользователя с Системой необходимо соблюдение следующих требований к техническим средствам:

- рабочее место пользователя должно состоять из следующих технических средств:

- системный блок;
- монитор;
- клавиатура;
- мышь.

**Примечание:** допускается использование других технических средств, обладающих аналогичным функционалом (ноутбуки, нетбуки и прочее).

- технические средства рабочего места пользователя должны быть исправны;
- рабочее место администратора должно быть подключено к электросети;
- рабочее место администратора должно быть подключено к локальной сети АО «СО ЕЭС» и к сети Интернет;
- сетевое оборудование рабочего места должно быть исправно.

### 1.1.2. Требования к аппаратному обеспечению

Требования к аппаратному обеспечению для установки Системы приведены ниже (Таблица 2):

**Таблица 2. Требования к аппаратному обеспечению**

<b>Название VM</b>	<b>asdu-fpa-git</b>	<b>asdu-fpa-app</b>	<b>asdu-fpa-w</b>	<b>asdu-fpa-fs</b>
<b>Частота процессора</b>	2.3 ГГц	2.3 ГГц	2.3 ГГц	2.3 ГГц
<b>Количество ядер процессора</b>	4	4	4	4
<b>Объем оперативной памяти (RAM)</b>	16 ГБ	16 ГБ	16 ГБ	16 ГБ
<b>Объем накопителя данных (HDD)</b>	100 ГБ	100 ГБ	100 ГБ	100 ГБ

### **1.1.3. Требования к операционной системе и дополнительному ПО**

Для обеспечения процесса установки Системы должны быть соблюдены следующие требования к общесистемному и специальному программному обеспечению:

- должна быть осуществлена корректная загрузка общего программного обеспечения: CentOS Linux release 7.5 для соответствующих компонентов Системы (Таблица 1).

## 2. УСТАНОВКА И НАСТРОЙКА КОМПОНЕНТОВ СИСТЕМЫ

### 2.1. Установка компонента «asdu-fpa-app»

Для начала процесса установки необходимо произвести обновление:

```
yum update
```

После обновления, необходимо загрузить пакет GitLab:

```
wget --content-  
disposition https://packages.gitlab.com/gitlab/gitlab-  
ce/packages/el/7/gitlab-ce-11.2.8-  
ce.0.el7.x86_64.rpm/download.rpm
```

Установить GitLab:

```
yum localinstall gitlab-ce-11.2.8-ce.0.el7.x86_64.rpm
```

Установить Java OpenJDK:

```
yum install java-1.8.0-openjdk
```

Произвести настройку GitLab:

```
vim /etc/gitlab/gitlab.rb  
  
gitlab_rails['db_adapter'] = "postgresql"  
gitlab_rails['db_encoding'] = "utf8"  
#gitlab_rails['db_collation'] = nil  
gitlab_rails['db_database'] = "gitlabhq_production"  
#gitlab_rails['db_pool'] = 10  
gitlab_rails['db_username'] = "gitlab"  
gitlab_rails['db_password'] = "gitlab123"  
gitlab_rails['db_host'] = "asdu-fpa-git.cdu.so"  
gitlab_rails['db_port'] = 5432
```

Применить конфигурацию:



```
sudo gitlab-ctl reconfigure
```

Установка и настройка компонента завершена.

## 2.2. Установка компонента «asdu-fpa-git»

Для начала процесса установки необходимо произвести обновление:

```
yum update
```

После обновления, необходимо установить пакет PostgreSQL:

```
yum install -y postgresql96-contrib-9.6.11-1PGDG.rhel7.x86_64
```

Произвести инициализацию БД:

```
/usr/pgsql-9.6/bin/postgresql96-setup initdb
```

Произвести настройку PostgreSQL:

```
vim /var/lib/pgsql/9.6/data/postgresql.conf
```

```
listen_addresses = 'asdu-fpa-git.cdu.so'
```

Произвести настройку соединения к PostgreSQL:

```
vim /var/lib/pgsql/9.6/data/pg_hba.conf
```

```
local all all peer
#IPv4 local connections:
host all all 127.0.0.1/32 password
#Allow Gitlab server to connect via md5
host all all 172.16.11.57/24 md5
#IPv6 local connections:
host all all ::1/128 ident
```

Запуск PostgreSQL:

```
sudo -u postgres pg_ctl start -D /var/lib/pgsql/9.6/data/
```

Установка и настройка компонента завершена.

### **2.3. Установка компонента «asdu-fpa-fs»**

Для начала процесса установки необходимо произвести обновление:

```
yum update
```

После обновления, необходимо скачать архив SonarQube:

```
wget  
https://binaries.sonarsource.com/Distribution/sonarqube/sonarqube-7.3.zip
```

Произвести распаковку архива:

```
unzip sonarqube-7.3.zip
```

Запустить SonarQube:

```
cd sonarqube-7.3/  
bin/linux-x86-64/sonar.sh start
```

Скачать репозитории Sonatype Nexus:

```
wget 'https://www.sonatype.com/oss-thank-you-tar.gz'
```

Распаковать архив:

```
gunzip nexus-3.14.0-04-unix.tar.gz  
tar -xvf nexus-3.14.0-04-unix.tar
```

Произвести настройке Sonatype Nexus:

```
cd nexus-3.14.0-04/  
nano nexus.conf  
  
upstream fpa-nexus {  
server XXX.X.X.X:XXXX;  
}  
  
server {  
  
listen 80;  
server_name asdu-fpa-nexus asdu-fpa-nexus.cdu.so;
```

Запустить сервер Nginx:

```
systemctl start nginx  
systemctl enable nginx
```

Установка и настройка компонента завершена.

#### **2.4. Установка компонента «asdu-fpa-w»**

На компоненте asdu-fpa-w должно быть установлены следующее СПО и ППО:

- ЕСЭП - установка проводится согласно Инструкции по разворачиванию ЕСЭП 91561945.ССПЗ.122.И4.01.
- GitLab Runner
  - JavaScript Language Service 2.0
  - JavaScript Project System 2.0
  - Node.js Tools
  - ProjectServicesPackage Extension 1.0
  - ResourcePackage Extension 1.0
  - SQL Server.
  - TypeScript Tools 15.9.20918.2001

## 3. УСТАНОВКА И НАСТРОЙКА СИСТЕМЫ ФПА

### 3.1. Общее описание

Система «ФПА» состоит из клиентской части программного интерфейса (front-end) и программно-аппаратной части сервиса (back-end).

Back-end представляет из себя Java-приложение (Java 11, SpringBoot 2.1), которое реализует REST API, обеспечивающее работу клиентской части. Устанавливается в CentOS Linux release 7.5 в виде systemd сервиса.

Конфигурация back-end части описывается в файле application.properties, размещаемом в одной директории с файлом приложения (fra-backend.jar).

Клиентская часть представляет собой набор статических js, css и html файлов, формирующих пользовательский интерфейс. Разработана с использованием библиотеки ReactJS, поставляется в собранном (компилированном) виде.

В состав дистрибутива входит:

- приложение back-end (jar-файл) fra-backend.jar;
- приложение front-end (zip-архив с файлами) fra-frontend.zip;
- примеры конфигурационных файлов:
  - config.js – для front-end;
  - application.properties – для back-end;
  - fra.conf – веб-сервер Nginx;
  - fra-backend.service – system сервис для back-end (для установки на CentOS Linux release 7.5 и другие дистрибутивы, поддерживающие system).

### 3.2. Подготовка к установке

#### 3.2.1. База данных

Для работы приложения необходимо заранее создать пользователя PostgreSQL (не ниже версии 9.6) и БД для него, доступную приложению по TCP/IP.

В конфигурации back-end (application.properties) понадобится указать:

- JDBC URL созданной БД;
- логин пользователя;
- пароль пользователя.

#### 3.2.2. Аутентификация

Приложение использует внешнюю аутентификацию через GitLab. Для настройки этой функции необходимо создать в GitLab под административным аккаунтом приложение ФПА.

В конфигурации back-end (application.properties) понадобится указать:

- URL GitLab;
- внешний адрес приложения (как его видят пользователи).

В конфигурации front-end (config.js) понадобится указать:

- URL GitLab;
- id и secret приложения, созданного в GitLab;
- URL бэкенда;
- внешний адрес приложения (как его видят пользователи).

### 3.2.3. ЕСЭП

Для работы подписания документов и проверки подписи необходимо создать в ЕСЭП внешнюю систему.

В конфигурации back-end (application.properties) понадобится указать:

- адрес файлового и основного веб-сервисов ЕСЭП;
- логин внешней системы;
- пароль внешней системы.

### 3.2.4. Требования к серверу

Для установки Системы на компоненте asdu-fra-app должны быть выполнены следующие условия:

- Установлен веб-сервер Nginx, открыты его порты (80, 433)
- Установлен Java Development Kit версии не ниже 11. В прилагаемом файле systemd сервиса предполагается, что он установлен в директории /usr/java/jdk-11.0.1
- Создан пользователь для запуска приложения. В прилагаемом файле systemd сервиса предполагается, что он называется asdu
- С компонента возможен TCP/IP доступ к БД, GitLab и ЕСЭП по адресам, указанным в конфигурационном файле бэкенда.

## 3.3. Установка back-end

Создать директорию /opt/fra-backend, разместить в ней файл приложения back-end (fra-backend.jar) и файл настроек (application.properties).

При необходимости отредактировать настройки.

Поместить файл fra-backend.service в директорию /etc/systemd/system. При необходимости внести правки в файл (имя пользователя, расположение jdk, рабочая директория).

Запустить back-end командой

```
service fpa-backend start
```

Убедиться что приложение принимает на указанном в `application.properties` порту и в логах нет ошибок.

### 3.4. Установка front-end

Создать директории:

```
- /srv/www/asdu-fpa-app/www  
- /srv/www/asdu-fpa-app/logs
```

Поместить файлы front-end в директорию `/srv/www/asdu-fpa-app/www`

При необходимости: отредактировать настройки front-end в файле `config.js`

Поместить файл конфигурации приложения `fpa.conf` в директорию `/etc/nginx/conf.d`, при необходимости изменить имя сервера, адрес back-end (секция `fpa-upstream`), место расположения SSL сертификата и ключа (если используется SSL).

Проверить правильность конфигурации Nginx командой:

```
nginx -t
```

Выполнить перезапуск сервиса Nginx командой:

```
service nginx restart
```

После этого появится возможность зайти в приложение по адресу и порту, которые указаны в конфиге Nginx (`fpa.conf`).

## **4. ПРИЛОЖЕНИЕ 1**

### **ИНСТРУКЦИЯ ПО РАЗВОРАЧИВАНИЮ ЕСЭП**

#### **1.1 Установка операционной системы**

Для установки необходим установочный диск с дистрибутивом ОС.

1. Загрузка установщика с диска.
2. Выбор настройки.
3. Выбор нужного диска для инсталляции.
4. После перезагрузки система будет установлена.

## 1.2 Установка СУБД

### 1.2.1 Установка SQL БД.

Для установки необходим установочный диск.

1. Вставьте установочный диск в CD привод. В корневой папке запустите файл Setup.exe. В случае, если не установлены обязательные компоненты, мастер установки предложит их установить.

2. После того, как все обязательные компоненты будут установлены, откроется Центр установки SQL БД.

3. В приветственном диалоге выберите пункт Installation (Установка) → New installation or add features to an existing installation (Новая установка или добавление компонентов к существующей установке). После этого будет осуществлена проверка совместимости операционной системы, прав пользователя, а также других условий.

4. Если все проверки пройдены, нажмите кнопку **ОК**. Будут осуществлены распаковка файлов, необходимых для установки, и еще один этап проверки условий.

5. Если все обязательные условия выполнены откроется форма конфигурации установки, первым этапом которой будет ввод лицензионного ключа продукта.

6. Введите лицензионный ключ.

7. Установите галочку напротив опции «Я принимаю условия лицензионного соглашения» («I accept the license terms») и нажмите кнопку **Далее (Next)**. Будет произведена установка файлов и откроется форма выбора формата и настройки установки.

8. Выберите опцию «SQL Server Feature» и нажмите кнопку **Далее (Next)**. Откроется форма выбора компонент SQL Server, которые необходимо установить.

9. Нажмите на кнопку **Выбрать все (Select All)** для установки все компонентов или выберите те, что необходимы (минимальные требования: **Database Engine Services** с подпунктами, **Management Tools** с подпунктами; дальнейшие инструкции даны для варианта полной установки), и нажмите кнопку **Далее (Next)**.

10. Если все обязательные условия выполнены, нажмите кнопку **Далее (Next)**. Откроется форма настройки экземпляра SQL Server.

11. Выберите тип экземпляра «Default Instance» и нажмите кнопку **Далее (Next)**. Будет осуществлена проверка места на жестком диске и откроется следующий шаг мастера установки «Server Configuration».

12. Здесь необходимо указать учетные записи, под которыми будут запускаться службы SQL Server и тип запуска службы (автоматически, вручную или вообще не



запускать). Рекомендуется создать под каждую службу свою учетную запись и предоставлять ей права по мере необходимости.

13. Перейдите на вкладку Collation и по кнопке Customize в полях «Database engine» и «Analysis Services» выберите «**Cyrillic\_General\_CI\_AS**»

14. Нажмите кнопку **Далее (Next)**. Откроется форма настройки доступа к SQL Server.

15. Задайте тип аутентификации «Mixed Mode (SQL Server authentication)» и административные учетные записи (как минимум одну). Задайте пароль в поле Enter password и подтвердите его в поле Confirm password. Этот пароль будет паролем учетной записи sa. Перейдите на вкладку Data Directories.

16. Здесь можно задать директории для размещения пользовательских баз данных. Перейдите на вкладку FILESTREAM.

17. Установите опции «Enable FILESTREAM for Transact-SQL access», «Enable FILESTREAM for file I/O streaming access». Нажмите кнопку **Далее (Next)**. Откроется форма выбора административной учетной записи и папок для хранилища Analysis Services.

18. Укажите учетную запись на вкладке Account Provisioning и папку хранилища Analysis Services на вкладке Data Directories. Нажмите кнопку **Далее (Next)**. Откроется форма конфигурации Reporting Services.

19. Выберите опцию «Install the native mode default configuration» и нажмите кнопку **Далее (Next)**. Откроется форма настройки отправки отчетов.

20. При необходимости установите соответствующую опцию и нажмите кнопку **Далее (Next)**. Откроется форма отображения конфигурации установки.

21. Сохраните в надежном месте расположение конфигурационного файла, указанного в поле Configuration file path. В дальнейшем им можно воспользоваться для установки SQL Server в одинаковой конфигурации на нескольких серверах при необходимости создания отказоустойчивого кластера БД. Если использование кластера не предполагается, конфигурационный файл можно не создавать. Файл конфигурации можно использовать только при установке из командной строки. Поэтому для такого способа установки необходимо запустить Setup.exe с указанием файла конфигурации (Setup.exe /ConfigurationFile=<путь\_к\_ConfigurationFile.ini>)

22. Нажмите кнопку Install. Начнется процесс установки SQL Server.

23. Нажмите кнопку **Закреть (Close)**. Установка SQL Server завершена.

24. Запустите любой SQL Manager и создайте пользователя с логином «eser» и паролем «1q2w3e4r+». Пользователю необходимо дать права, достаточные для создания баз данных, а также запуска процедуры [db].[dbo].[sp\_delete\_database\_backuphistory], например права администратора.

### 1.2.2 СУБД POSTGRESQL

Место установки: VM hostname

Необходимо отредактировать файл /var/lib/pgsql/9.6/data/pg\_hba.conf добавления разрешения к подключению хоста с приложением ЕСЭП (host all all \*.\*.\*.\*\*/24 trust)

## 1.3 Первичное развертывание баз данных ЕСЭП

### 1.3.1 Установка pgAdmin

pgAdmin 4 - это свободное кроссплатформенное программное обеспечение, предоставляющее графический интерфейс для работы с базой данных.

Ссылка для скачивания <https://www.pgadmin.org/download/>

Ссылка на документацию <https://www.pgadmin.org/docs/pgadmin4/3.x/>

Учётные данные для соединения:

Host: \*.\*.\*.\*

Port: 5432

Main base: postgres

Username: postgres

### 1.3.2 Установка дополнительного СПО и ППО

На компоненте asdu-fra-w должно быть такое установлено дополнительное ПО:

- CryptoPro CSP v4.0 R4
- GhostScript v9.25
- TSP UC.EM Certificates
- Серверный криптокомпонент

### 1.3.3 Редактирование и запуск скрипта генерации БД

Для конфигурационных файлов:

ЕСЭП\_27.11.2018\ESEP.DB\ESEP.DB\Configs\Ppnp.NHibernate.config

ЕСЭП\_27.11.2018\ESEP.DB\ESEP.DB\Configs\Pvruc.NHibernate.config

ЕСЭП\_27.11.2018\ESEP.DB\ESEP.DB\Configs\Pzkhd.NHibernate.config

ЕСЭП\_27.11.2018\ESEP.DB\ESEP.DB\Configs\Vkhd.NHibernate.config

Необходимо изменение атрибутов доступа к серверу БД:

```
<property name="connection.connection_string">Server=***.**.**.*;
```

Далее запуск: ЕСЭП\_27.11.2018\ESEP.DB\ESEP.DB\Deploy all databases.bat.

Результатом должно быть следующее:

## 1.4 Установка сервера приложений с помощью мастера настройки сервера

**Сервер приложений** — проприетарный набор серверов распространяемый с операционными системами unix. Основным компонентом является веб-сервер, который позволяет размещать в Интернете сайты. Поддерживает протоколы HTTP, HTTPS, FTP, POP3, SMTP, NNTP.

Для выполнения описанных ниже процедур необходимо входить в группу "Администраторы" на локальном компьютере.

1. Запустите Server Manager. Выберите раздел Roles и нажмите кнопку **Add Roles**.
2. Нажмите кнопку **Далее (Next)**.
3. Выберите следующие сервисы и нажмите кнопку **Далее (Next)**:

Static Content;

Default Document;

Directory browsing;

HTTP Errors;

HTTP Redirection;

HTTP Logging;

Logging Tools;

Request Monitor;

Request Filtering;

Static Content Compression;

Dynamic Content Compression;

4. При выборе сервисов могут открываться предупреждения об установке дополнительных сервисов, необходимых для выбранных вами, если эти сервисы еще не установлены.

5. В таких окнах нажмите кнопку **Add Required Role Services**. После выбора нужных сервисов нажмите кнопку **Далее (Next)** и затем на форме отображения параметров установки нажмите на кнопку **Установить (Install)**.

Нажмите кнопку **Заккрыть (Close)**.

6. Выберите раздел Features и нажмите кнопку **Add Features**. Откроется форма выбора компонентов для установки на сервер. Выберите все компоненты. Нажмите install. Установка Сервера приложений завершена.

## 1.5 Установка приложения ЕСЭП

Для установки приложения необходим дистрибутив приложения ЕСЭП.

Файлы дистрибутива находятся на установочном диске Приложения в папке ESEP.Web.rar и включают в себя следующие компоненты:

Esep-Admin - интерфейс администратора;

Esep-WebApp - интерфейс пользователя (интерфейс для подписания);

Esep-Services - веб-сервисы, к которым обращается внешняя система;

Esep-ExternalSystem – Пример внешней системы (в том числе для тестирования).

1. Скопируйте папки дистрибутива приложения на компьютер в папку C:\inetpub\wwwroot.

2. При необходимости можно задать строки подключения к БД в конфигурационных файлах Ppnp.NHibernate.config, Pvruc.NHibernate.config, Pzkhd.NHibernate.config, Vkhd.NHibernate.config. Конфигурационные файлы каждого из четырех web-приложений находятся в подпапках «bin».

3. В случае использования СУБД Oracle следует задать актуальные пароли для каждой из созданных схем ESEP\_PPNP, ESEP\_PVRUC, ESEP\_VKHD, ESEP\_PZKHD. Параметры подключения к СУБД Oracle настраиваются в файле tnsnames.ora, находящемся в корне каждого из web-приложений.

4. Для Esep-ExternalSystem в конфигурационных файлах Esep-ExternalSystem\bin\WcfConfigs\Client.config и Esep-ExternalSystem\bin\WcfConfigs\Behaviors.config вместо localhost необходимо указать реальные внешние адреса сервисов Esep.

5. Для Esep-Services в конфигурационных файлах Esep-Services\WcfConfigs\Client.config и Esep-Services\bin\WcfConfigs\Behaviors.config вместо localhost необходимо указать реальные внешние адреса сервисов Esep.

6. Для Esep-Services в файлах метаданных сервисов Esep-WebApp\fileservice.wsdl и Esep-WebApp\esepservice.wsdl вместо localhost необходимо указать реальные внешние адреса сервисов Esep.

7. Для Esep-WebApp в конфигурационных файлах Esep-WebApp\bin\WcfConfigs\Client.config и Esep-WebApp\bin\WcfConfigs\Behaviors.config вместо localhost необходимо указать реальные внешние адреса сервисов Esep.

8. Указанный в пунктах 4 и 7 хост (и, при наличии, номер порта) должен соответствовать тому внешнему адресу, по которому будет происходить обращение к сервису. Однако допустимо оставить хост по умолчанию «localhost», если обращение к сервису будет происходить с этого же сервера. Например, при мультисерверной конфигурации, если запрос пользователя к приложению Esep-WebApp поступил с балансировщика на сервер номер 1, будет оптимальным, чтобы дальнейшее внутреннее взаимодействие Esep-WebApp с приложением Esep-Services происходило на том же сервере номер 1 – в этом случае в настройках Esep-WebApp следует оставить хост по умолчанию. Данная рекомендация неприменима к пунктам 5 и 6.

9. Для Esep-WebApp в конфигурационном файле Esep-WebApp\Web.config в ключах «CryptoPluginUrl» и «CryptoXmlUrl» вместо localhost необходимо указать реальные внешние адреса сервисов Esep.

10. Для Esep-WebApp в файле Esep-WebApp\update\_info.xml вместо localhost необходимо указать реальный внешний адрес сервисов Esep.

11. Для всех web-приложений в файлах web.config необходимо настроить путь сохранения логов приложения, который указан в секции настроек log4.

12. В меню Connections выберите раздел Application Pools и нажмите на кнопку **Add Application pool**.

13. Заполните форму в соответствии с данными и нажмите кнопку **ОК**. В списке Application pool будет добавлена новая запись. Вызовите контекстное меню на данной записи и выберите пункт Advanced Settings.

14. Создайте серверного пользователя, от имени которого будут запускаться приложения ЕСЭП, например «esep». Пользователь должен обладать привилегиями, достаточными для запуска web-приложений, запуска методов com-библиотек (включая http-запросы к внешним сервисам из com-библиотеки), запись временных файлов на жесткий диск.

15. В поле Start Automatically установите значение «OnDemand» или «True», в поле Identity укажите «esep» и введите пароль этого пользователя, в поле «Load User profile» установите значение «True». Нажмите кнопку **OK**.

16. Теперь необходимо настроить web-приложения. Допустимо 2 способа: на каждое из приложений ЕСЭП создать собственный сайт или добавить виртуальные приложения как подчинённые конкретному сайту (например, «Default Web Site»). Ниже будет рассмотрено создание отдельного сайта для каждого из web-приложений ЕСЭП.

17. В меню Connections выберите раздел Sites и нажмите на кнопку **Add Web Site**.

18. Заполните форму, в разделе Binding укажите данные подключения. В поле Physical path укажите папку, в которую на шаге 1 был скопирован соответствующий дистрибутив приложения. Проверьте возможность подключения по кнопке **Test Settings**. В случае сбоя подключения по кнопке **Connect as** укажите учетную запись локального администратора. Нажмите кнопку **OK**.

19. В меню Connections в разделе Sites выберите только что добавленную запись.

20. Нажмите на ссылку Advanced Settings в меню Browse Web Site.

21. Укажите в одноименном поле Application Pool «ESEP», созданный в пункте 5. Нажмите кнопку **OK**.

22. Выполните аналогичные действия, начиная с пункта 18 для других 3 сайтов.

23. После установки добавить и проверить Bindings. Добавить SSL сертификат для данного Хоста (hostname)

## **1.6 Установка КриптоПРО CSP 4.0 для ГОСТ Р 34.10-2012**

**КриптоПро** — линейка криптографических утилит (вспомогательных программ) — так называемых криптопровайдеров. Они используются во многих программах российских разработчиков для генерации ЭЦП, работы с сертификатами, организации структуры РКІ и т.д.

Дополнительная настройка приложения после установки не требуется.

Для установки необходим дистрибутив КриптоПро CSP 4.0 с поддержкой ГОСТ Р 34.10-2012, который находится на установочном диске Приложения в папке «ESEP.Soft.rar\CryptoPro CSP v4.0» (также можно скачать на оф. сайте КриптоПро).

**Внимание!** Для сохранения полного функционала КристоПро CSP и во избежание появления ошибок подписания по окончании испытательного периода (3 месяца) потребуется приобретение у оф. разработчика и последующая регистрация серверной лицензии.

1. Запустите дистрибутив КристоПро CSP 4.0
2. Нажмите кнопку **Далее (Next)**.
3. Установите галочку напротив опции «Я принимаю условия лицензионного соглашения» («I accept the terms in the License Agreement») и нажмите кнопку **Далее (Next)**.
4. Введите данные, укажите серийный номер и нажмите кнопку **Далее (Next)**.
5. После окончания установки откроется информирующая об этом форма.
6. Нажмите кнопку **Готово (Finish)**.

Нажмите кнопку **Да**. Будет произведена перезагрузка компьютера.

7. После перезагрузки установка КристоПро CSP 4.0 будет завершена.

Обратите внимание, что срок действия тестовой лицензии составляет 3 месяца. По истечению этого срока для дальнейшей корректной работы ЕСЭП необходимо приобрести официальную лицензию.

## 1.7 Установка GPL GhostScript

Для установки необходим дистрибутив GPL GhostScript, который находится на установочном диске Приложения в папке «ESEP\_Soft.rar\GhostScript» (наиболее свежую версию также можно скачать по адресу <http://www.ghostscript.com/download/gsdnld.html>).

1. Запустите дистрибутив.
2. Нажмите кнопку «Далее» (Next).
3. Нажмите кнопку «I Agree».
4. Путь установки рекомендуется выбрать за пределами предлагаемой по умолчанию папки.
5. Для завершения установки GPL GhostScript нажмите кнопку «Finish».
6. Установить необходимо версию GhostScript x64.
7. После установки GhostScript следует перезагрузить систему. Установка завершена.

## **1.8 Установка серверных дополнений криптокомпонента**

1. Перед установкой дополнений криптокомпонента необходимо установить Redistributable Package обеих разрядностей, x86 и x64, дистрибутивы находятся в папке «ESEP.Soft\2010 Redistributable».
2. Для установки необходим комплект файлов, расположенный на установочном диске Приложения в папке «Серверный криптокомпонент (COM)».
3. Запустите исполняемый файл RegTopCase.bat в обеих подпапках с правами администратора, При необходимости целевую папку можно изменить, отредактировав исполняемый файл.
4. Сертификат «Thawte Code Signing CA.cer» следует установить в «Промежуточные центры сертификации – физ. хранилища Локальный компьютер и текущий пользователь».

## **1.9 Установка LibreOffice**

Для установки необходим дистрибутив LibreOffice 6.1.2 x64, который находится на установочном диске Приложения в папке «ESEP.Soft.rar\LibreOffice v6.1.2».

1. Запустите дистрибутив. Нажмите на кнопку «Далее».
2. Нажмите на кнопку «Далее». Откроется окно выбора типа установки, выберите значение «Обычная».
3. Нажмите кнопку «Далее». В открывшемся окне установите флажок в опции «Загрузка LibreOffice 6.1.2.1 при старте системы».
4. Нажмите кнопку «Установить». Запустится процесс установки Libre Office.
5. По окончании процесса инсталляции появится окно «Работа мастера установки завершена». Нажмите кнопку «Готово». Процесс установки завершен
6. По завершении установки следует запустить LibreOffice и проверить корректность запуска.

## **1.10 Установка клиентского корневого сертификата**

1. Выберите оснастку Сертификаты (Certificates).
2. В меню разверните раздел Сертификаты (локальный компьютер) – Доверенные корневые центры сертификации (Trusted Root Certification Authorities) – Реестр (Registry) – Сертификаты (Certificates). Вызовите на папке Сертификаты (Certificates) контекстное меню и выберите пункт Все задачи (All tasks) – Импорт (Import).
3. Импортируйте нужный сертификат



4. Нажмите кнопку **Готово**.
5. Нажмите кнопку **ОК**.
6. При необходимости установите аналогичным образом соответствующий сертификат в «Промежуточные центры сертификации\локальный компьютер», а также в аналогичные хранилища текущего пользователя (того пользователя, от имени которого запущен пул приложений ЕСЭП).

## 1.11 Настройка системы ЕСЭП

1. Запустите портал администратора системы ЕСЭП. Учетные данные администратора по умолчанию: admin / 123456.

2. Перейдите в раздел Настройки ЕСЭП и нажмите кнопку **Редактировать** в пункте «Корневой url клиентского интерфейса ППНП».

3. Укажите корневой адрес клиентского интерфейса ППНП (например, <http://dis3.internal.granit.ru:12777/ESEP-WebApp/>), данный адрес должен быть внешним, так как оп нему будут открываться у пользователей страницы подписания. Также укажите путь к временному файловому хранилищу. Дайте пользователю, под которым работают приложения ЕСЭП, права на чтение и запись в эту папку. Значения остальных пунктов можно оставить по умолчанию. Нажмите кнопку **Сохранить**.

4. Перейдите в раздел «Реестр удостоверяющих центров» и нажмите на кнопку **Добавить** для добавления Удостоверяющего центра.

5. Укажите необходимые данные и нажмите на кнопку **Добавить**. Откроется форма добавления сертификата.

6. Выберите файл корневого сертификата УЦ или укажите ссылку на него и нажмите кнопку **Сохранить**. При необходимости можно добавить ещё несколько корневых сертификатов, если данный УЦ их также использует. Затем на форме редактирования данных УЦ нажмите кнопку **Сохранить**.

7. Перейдите в раздел «Реестр сервисов проверки».

При необходимости можно настроить один из существующих в примере сервисов проверки или добавить новый нажатием на кнопку «+»

Если выбран тип сервиса «Rostelecom», то необходимо заполнить следующие поля:

- Название сервиса проверки подписей и сертификатов;
- Адрес сервиса проверки;

Опция «Использовать ТЭП» должна быть отключена.

Если выбран тип сервиса «Esped», то необходимо дополнительно заполнить следующие поля:

- XPath пути элементов для включения в ТЭП;
- Id элементов для включения в ТЭП;
- Actor (ТЭП).

Типичные значения этих полей уже установлены для сервиса, добавленного при первичном разворачивании баз данных ЕСЭП.

Опция «Использовать ТЭП» должна быть включена.

Далее нажмите кнопку «Сохранить».

8. Перейдите в раздел «Реестр внешних систем»
9. Нажмите кнопку **Редактировать** для изменения параметров Тестовой внешней системы.

В поле «Адрес TSP службы» следует ввести актуальный адрес службы штампов времени, предоставляемый настроенным УЦ.

В поле «Проверка подписей и сертификатов» следует выбрать способ проверки сертификатов и ЭП, который будет использоваться при наложении подписи на документ.

Если выбран сервис внешней проверки типа «ЕСПЭД» (с включенной опцией «Использовать ТЭП»), требуется указать параметры чтения серверного сертификата для наложения ТЭП в следующих полях:

- Отпечаток сертификата;
- Место хранения сертификата;
- Физическое хранилище сертификата;
- Пин-код контейнера.

Соответствующий сертификат должен быть установлен (включая контейнер закрытого ключа) средствами CryptoPro CSP в указанное хранилище сервера под тем пользователем, от имени которого запущен пул приложений ESEP (в примере – пользователь «esep»).

10. Для указанной TSP службы необходимо соответствующий корневой сертификат УЦ, предоставившего TSP службу, установить в доверенные корневые центры сертификации хранилища «локальный компьютер».

11. Проверку полномочий РУЛ следует отключить (за исключением конкретных ИС, использующих эту службу).

12. Значения остальных параметров внешней системы можно оставить по умолчанию. Нажмите кнопку **Сохранить**.

*Примечание: Внешняя проверка используется в том случае, если используется любой формат подписи, кроме CAAdES X Long Type 1.*

**1.12** При необходимости настройки пользователей, имеющих доступ к административному интерфейсу, можно произвести в разделе «Пользователи Установка службы «Очередь сообщений портала ЕСЭП»

Для установки службы необходим дистрибутив приложения «Очередь сообщений портала ЕСЭП» EsepDemon.

Файлы дистрибутива находятся на установочном диске Приложения в архиве ESEP.MD.rar.

Распакуйте дистрибутив приложения EsepDemon в соответствующую папку, находящуюся в корне диска C:\. После установки службы нельзя перемещать папку с распакованным приложением.

1. Для установки службы EsepDemon запустите исполняемый файл install.bat, находящийся в распакованной папке, и дождитесь сообщения об успешном завершении операции.

2. Войдите в Администрирование (Administrative Tools) – Службы

3. В списке служб найдите службу EsepDemon. Вызовите на ней контекстное меню и выберите пункт Свойства (Properties).

4. Установите тип запуска службы «Автоматически (отложенный запуск)»

5. Перейдите на вкладку Вход в систему (Log on)

6. Установите опцию «С учетной записью (This account)» и укажите учетную запись и пароль, под которыми будет осуществляться запуск службы (в примере: «esep»), необходимо указать учётную запись и пароль того же пользователя, под которым работает пул приложений ЕСЭП.

7. Нажмите кнопку **ОК**.

8. При необходимости можно задать строку подключения к БД в файлах Ppnp.NHibernate.config, Pvruc.NHibernate.config, Pzkhd.NHibernate.config и Vkhd.NHibernate.config в папках обоих распакованных приложений.

9. В случае использования СУБД Oracle следует задать актуальные пароли для каждой из созданных схем ESEP\_PPNP, ESEP\_PVRUC, ESEP\_VKHD, ESEP\_PZKHD. Параметры подключения к СУБД Oracle настраиваются в файле tnsnames.ora, находящемся в папке службы.

10. Перед запуском необходимо произвести настройку службы. Откройте конфигурационный файл MailingDemon.exe.config.

10.1. Найдите в нем группу настроек периодических задач, находящуюся в секции:

```
<preset key="debug" base="general">
```

```
<tasks xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

10.2. Настройте периодические задачи согласно требованиям в соответствии с комментариями в конфигурационном файле.

10.2.1. Список возможных типов задач для 64-разрядной службы EsepDemon:

- Удаление временных файлов из хранилища;
- Удаление просроченных операций;
- Удаление «потерянных» папок с изображениями;
- Удаление временных файлов конвертации;
- Загрузка информации по электронным подписям файлов на внешний сервис (используется по необходимости для специализированных ИС);
- Повторная загрузка информации по электронным подписям файлов на внешний сервис (используется по необходимости для специализированных ИС).
- Конвертирование файлов в формат JPEG с настройкой типа, размера, длины обрабатываемой очереди и т.п.;
- Повторное конвертирование файлов в формат JPEG, в случае ошибки при первичном конвертировании;
- Сброс статуса «зависших» задач конвертирования при запуске службы.

10.3. Найдите настройки, находящиеся в секции:

```
<appSettings>
```

```
<add key="LockOwner" value="Web-01" />
```

```
</appSettings>
```

Для ключа LockOwner установите уникальное значение для настраиваемого сервера (в примере для односерверной конфигурации – «Web-01»).

В случае установки службы на нескольких серверах это значение должно быть уникальным для каждого из них.

Зайдите в административный интерфейс ESEP в раздел «Настройки ЕСЭП» и укажите уникальные идентификаторы служб для всех серверов в поле «Список имён нод с установленными приложениями ЕСЭП», разделяя их символом «;» (например, для конфигурации из трёх параллельно работающих серверов – «Web-01;Web-02;Web-03;»).

В списке служб найдите службу EsepDemon. Вызовите на ней контекстное меню и выберите пункт Restart (в случае, если служба уже запущена), либо пункт Start (если она еще не была запущена).

### **1.13 Установка службы «Сторож очереди сообщений портала ЕСЭП»**

Для установки службы необходим дистрибутив приложения «Сторож очереди сообщений портала ЕСЭП» EsepDemonGuard.

Файлы дистрибутива находятся на установочном диске Приложения в архиве ESEP.MD.Guard.rar.

Распакуйте дистрибутив приложения EsepDemonGuard в новую папку, находящуюся в корне диска C:\. После установки службы нельзя перемещать папку с дистрибутивом.

1. Для установки службы перейдите в эту папку и запустите командный файл Install.bat с правами Администратора.

2. Начнется установка службы «Сторож очереди сообщений портала ЕСЭП». Дождитесь отображения сообщения «Групповая операция установки выполнена» и закройте командную строку.

3. В списке служб найдите службу EsepDemonGuard. Вызовите на ней контекстное меню и выберите пункт Свойства (Properties).

4. Установите тип запуска службы «Автоматически (отложенный запуск)».

5. Перейдите на вкладку Вход в систему (Log on).

6. Установите опцию «С учетной записью (This account)» и укажите учетную запись и пароль, под которыми будет осуществляться запуск службы (в примере: «esep»).

7. Нажмите кнопку **ОК**.

8. При необходимости можно задать строку подключения к БД в файлах Ppnp.NHibernate.config, Pvruc.NHibernate.config, Pzkhd.NHibernate.config и Vkhd.NHibernate.config.

9. В случае использования СУБД Oracle следует задать актуальные пароли для каждой из созданных схем ESEP\_PPNP, ESEP\_PVRUC, ESEP\_VKHD, ESEP\_PZKHD. Параметры подключения к СУБД Oracle настраиваются в файле tnsnames.ora, находящемся в папке службы.

10. Перед запуском необходимо произвести настройку службы. Откройте конфигурационный файл MailingDemonGuard.exe.config.

Найдите настройки, находящиеся в секции:

```
<appSettings>  
<add key="LockOwner" value="Web-01" />  
</appSettings>
```

Для ключа LockOwner установите то же значение, которое указывали в настройке службы очереди сообщений (в примере для односерверной конфигурации – «Web-01»).

11. В списке служб найдите службу EsepDemonGuard. Вызовите на ней контекстное меню и выберите пункт Restart (в случае, если служба уже запущена), либо пункт Start (если она еще не была запущена).

## 1.14 Настройка браузера.

Для работы в Системе массовой выдачи сертификатов ключей подписи необходимо провести следующие настройки браузера.

1. Выберите раздел Сервис – Параметры режима представления совместимости.
2. Откроется форма настройки параметров.
3. Удалите веб-узел Esep-WebApp из списка «Веб-узлы, добавленные к просмотру в режиме совместимости» (только в случае, если он там присутствует).
4. Снимите галочки «Отображать узлы интрасети в режиме представления совместимости» и «Отображать все веб-узлы в режиме представления совместимости» (только в случае, если он стоят).
5. Выберите раздел Сервис – Свойства обозревателя.
6. Перейдите на закладку Безопасность и выберите зону «Надежные узлы» для настройки ее параметров.

7. Нажмите кнопку **Узлы**.
8. Введите реальный внешний адрес приложения Eser-WebApp в пункте «Добавить в зону следующий узел», снимите галочку «Для всех узлов этой зоны требуется проверка серверов (https:)» и нажмите кнопку **Добавить**. Адрес портала будет добавлен в список надежных узлов.
9. Установите уровень безопасности для зоны надежных узлов в положение «Низкий».
10. Нажмите кнопку **Другой** и в открывшемся окне «Параметры безопасности» и установите в разделе «Включить фильтрацию» переключатель в положение «Отключить», а в разделе «Загрузка неподписанных элементов» переключатель в положение «Включить» и нажать кнопку **ОК**.

Для сохранения сделанных настроек в окне «Свойства обозревателя» нажмите кнопку **ОК**.