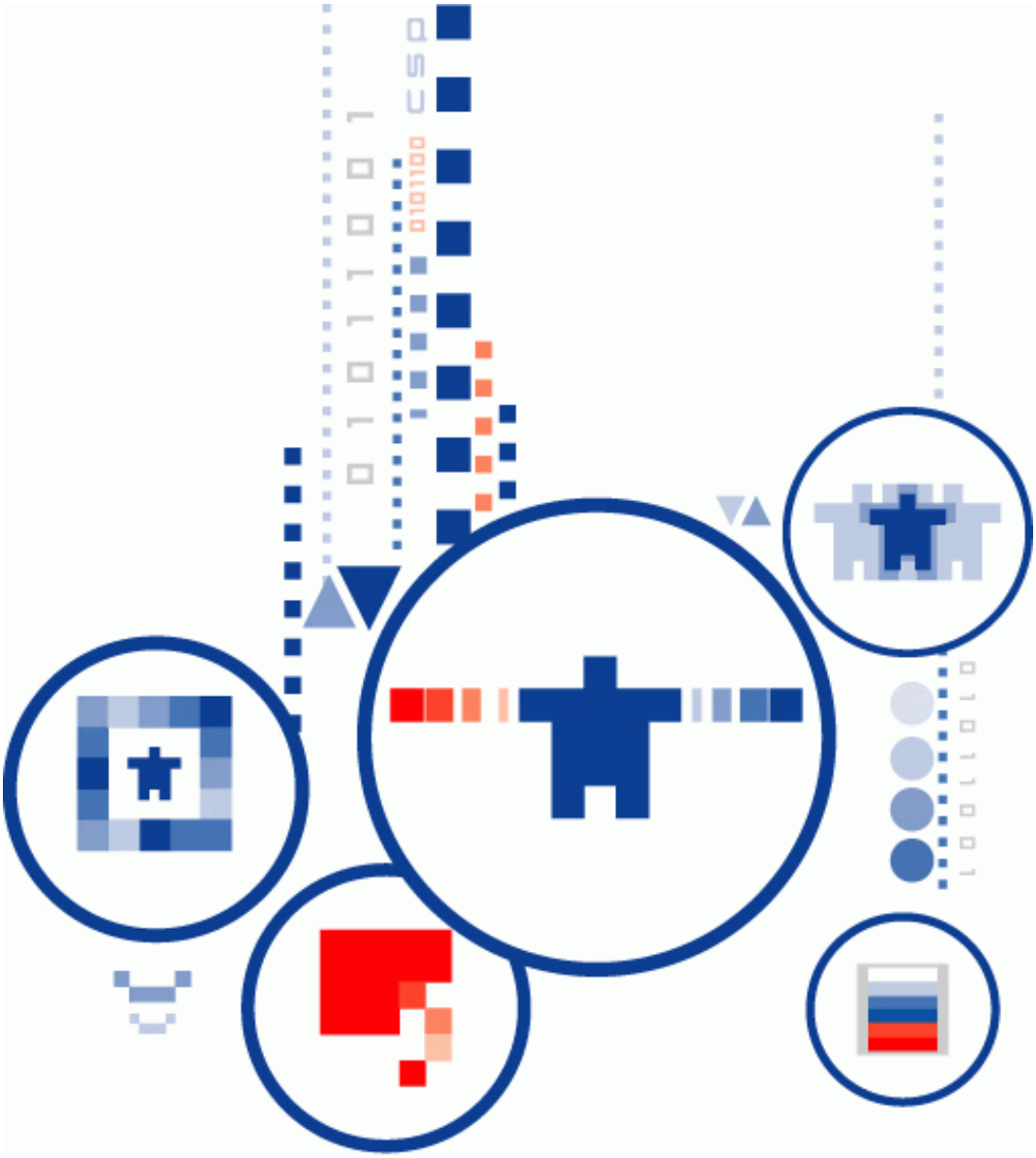

КриптоПро PKI-Кластер

Сервис обеспечения работы Операторов

Руководство администратора

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

CSP	—	Криптопровайдер (Cryptographic Service Provider)
SSL	—	Протокол защиты сокетов (Secure Sockets Layer)
TLS	—	Протокол защиты транспортного уровня (Transport Layer Security)
URL	—	Единый указатель ресурсов (Uniform Resource Locator)
АПМЗ	—	Аппаратный модуль доверенной загрузки
БД	—	База данных
ЗПС	—	Замкнутая программная среда
ИС	—	Информационная система
НСД	—	Несанкционированный доступ
СУБД	—	Система управления базой данных
ОС	—	Операционная система
ПО	—	Программное обеспечение
СЗИ	—	Средство защиты информации
СКЗИ	—	Средство криптографической защиты информации
ЭП	—	Электронная подпись
ПАК	—	Программно-аппаратный комплекс
УЦ	—	Удостоверяющий Центр

СОДЕРЖАНИЕ

1. Аннотация

Настоящий документ содержит Руководство администратора Сервиса обеспечения работы Операторов ПК «КриптоПро PKI-Кластер» (Далее – Сервис обеспечения работы Операторов).

Документ включает в себя сведения описание процесса разворачивания и настройки основных технических и программных решений и предназначен для системных администраторов и Администраторов PKI-Кластер как руководство по установке и конфигурированию PKI-Кластер.

2. Системные требования

2.1. Требования к аппаратному обеспечению

Аппаратные требования к техническим средствам, на которых размещаются программные компоненты Сервиса обеспечения работы Операторов, зависят от требований по производительности всего комплекса.

Таблица 1. Требования к аппаратному обеспечению

Оборудование	Минимальные требования
Центральный процессор	64-разрядный двухъядерный процессор с тактовой частотой 1,86 ГГц
Оперативная память	4 ГБ ОЗУ
Жесткий диск	4 ГБ свободного места
Сетевые адаптеры	Один сетевой адаптер, совместимый с операционной системой компьютера, для взаимодействия с внутренней сетью
СЗИ от НСД	АПМЗ в соответствии с эксплуатационной документацией на СКЗИ

2.2. Требования к программному обеспечению

В Таблица 2 указаны предъявляемые к программному обеспечению требования.

Таблица 2. Требования к программному обеспечению

Компонент	Наименование
Операционная система	Astra Linux Special Edition в режиме ЗПС
Веб-сервер	➢ Nginx с патчем ng-nginx.1.18.0.patch, ➢ Apache с модулем СКЗИ. Применение допустимо в соответствии с эксплуатационной документацией на СКЗИ
Антивирусное ПО	В соответствии с эксплуатационной документацией на СКЗИ
СКЗИ	КриптоПро CSP 5.0 R2

3. Развертывание Сервиса обеспечения работы Операторов

В данном разделе описывается развертывание Сервиса обеспечения работы Операторов. Для выполнения развертывания Сервиса обеспечения работы Операторов «с нуля» необходимо выполнить следующие шаги:

1. Установка ОС.
2. Установка КриптоПро CSP.
3. Установка веб-сервера.
4. Установка ПО Сервиса обеспечения работы Операторов и дополнительного ПО.

3.1. Установка ОС

Дистрибутив Astra Linux Special Edition необходимо получить самостоятельно. Установка выполняется согласно эксплуатационной документации на ОС СН Astra Linux SE Смоленск.

Для отображения печатных форм в Сервисе обеспечения работы Операторов необходимо установить пакет **libgdiplus**.

3.2. Установка КриптоПро CSP

Дистрибутив необходимо получить самостоятельно. Установка выполняется согласно эксплуатационной документации на КриптоПро CSP 5.0 КС3.

3.3. Развертывание веб-сервера

Необходимо выполнить настройку веб-серверов nginx или Apache согласно эксплуатационной документации на КриптоПро CSP 5.0 КС3.

3.3.1. Пример развертывания и настройки веб-сервера nginx

Для настройки работы веб-сервера необходимо установить **nginx с патчем ng-nginx.1.18.0.patch** из состава дистрибутива КриптоПро CSP.

ППО nginx не входит в комплект поставки СКЗИ. Исходные тексты nginx 1.18.0 скачиваются с официального сайта с последующей проверкой контрольной суммы, указанной в документации на СКЗИ.

После применения патча осуществляется сборка «пропатченных» исходных текстов сервера nginx с последующим вычислением ЭП (в соответствии с эксплуатационной документацией на ОС Astra Linux SE) для возможности их использования в замкнутой программной среде (ЗПС) ОС Astra Linux SE.

Перед установкой nginx на сервер необходимо загрузить патч **ng-nginx.1.18.0. patch** и init-скрипт **nginx.init**.

Пример разворачивания веб-сервера nginx:

- Установка дополнительных пакетов:

```
sudo apt-get install build-essential patch
```

- Применение модуля СКЗИ для nginx:

```
wget https://nginx.org/download/nginx-1.18.0.tar.gz
tar -xvf ./nginx-1.18.0.tar.gz
cp ./ng-nginx.1.18.0.patch ./nginx-1.18.0 && cd ./nginx-1.18.0/
patch -p1 < ./ng-nginx.1.18.0.patch
```

- Получение дополнительных исходных текстов:

```
wget https://ftp.pcre.org/pub/pcre/pcre-8.44.tar.gz
tar -xvf ./pcre-8.44.tar.gz && cd ./pcre-8.44
wget https://zlib.net/zlib-1.2.11.tar.gz
tar -xvf ./zlib-1.2.11.tar.gz
wget https://www.openssl.org/source/openssl-1.1.1h.tar.gz
tar -xvf ./openssl-1.1.1h.tar.gz
```

- Сборка:

```
cd ./nginx-1.18.0
./configure \
--user=nginx \
--group=nginx \
--with-cc-opt='-fstack-protector -fstack-protector-strong --param=ssp-buffer-
size=4 -Wformat -Werror=format-security -Werror=implicit-function-declaration
-Winit-self -Wp,-D_FORTIFY_SOURCE=2 -fPIC' \
--with-ld-opt='-Wl,-z,relro -Wl,-z,now -Wl,--as-needed -pie -
L/opt/cprocsp/lib/amd64 -lrdrsup -lssp -lcapi10 -lcapi20' \
--prefix=/opt/nginx \
--conf-path=/etc/nginx/nginx.conf \
--error-log-path=/var/log/nginx/error.log \
--http-log-path=/var/log/nginx/access.log \
--lock-path=/var/run/lock/nginx.lock \
--pid-path=/var/run/nginx.pid \
--with-pcre=/home/test/src/pcre-8.44/ \
--with-pcre-jit \
--with-zlib=/home/test/src/zlib-1.2.11/ \
--with-http_ssl_module \
--with-http_sspi_module \
--with-http_stub_status_module \
--with-openssl=/home/test/src/openssl-1.1.1h/ \
--with-openssl-opt='no-gost no-comp no-dtls no-deprecated no-dynamic-engine
no-engine no-hw-padlock no-nextprotoneg no-psk no-tests no-ts no-ui-console'
\
--with-stream \
--with-stream_ssl_module \
--with-stream_sspi_module \
--with-http_v2_module
```

- Запуск сборки:

```
make
```

- Копирование базовой конфигурации (пример конфигурации приведён в **3.3.3):**

```
sudo cp ./nginx.conf.sample ./nginx-1.18.0/conf/nginx.conf
sudo make install
```

- Создание системного пользователя:

```
sudo adduser --system --no-create-home --group nginx
sudo chown -R nginx:nginx /var/log/nginx/
```

- Перенос init-скрипта:

```
sudo cp ./nginx.init /etc/init.d/nginx
```

3.3.2. Работа с ключами и сертификатами

В рамках задач Сервиса обеспечения работы Операторов для nginx необходимо подготовить сертификат веб-сервера TLS. Требования к нему такие же, как к серверным сертификатам — наличие в субъекте или расширении “Дополнительное имя субъекта” (SAN) имени хоста и наличие Проверка подлинности сервера (1.3.6.1.5.5.7.3.1) в расширении “Улучшенный ключ”. Ниже описан пример установки сертификата из pfx. В этом варианте, сертификат веб-сервера должен быть получен заранее на ЦС и скопирован на сервер с компонентами Сервиса обеспечения работы Операторов в виде pfx файла.

```
sudo -u nginx /opt/cprocsp/bin/amd64/certmgr -install -pfx -store uMy -file
/<path>/certificate.pfx -pin <пароль от файла pfx>
```

Для успешной проверки серверных и клиентских сертификатов необходимо установить сертификаты всех вышестоящих УЦ. Ниже пример установки корневых и промежуточных сертификатов УЦ. (где uRoot – хранилище корневых сертификатов, uCa – хранилище промежуточных сертификатов)

```
sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mRoot -file /<path>/root.cer
sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mCa -file /<path>/to/ca.cer
```

3.3.3. Конфигурация nginx для Сервиса обеспечения работы Операторов

Для обеспечения работоспособности Сервиса обеспечения работы Операторов nginx необходимо настроить в режимах двусторонней аутентификации по сертификату (Mutual TLS) и обратного прокси-сервера (reverse-proxy). Ниже приведен пример конфигурации nginx.

```
server {
 listen 443;
 server_name ecpserver; # DNS – имя сервера
 proxy_set_header Host $host;
 proxy_set_header X-Real-IP $remote_addr;
 proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
```

```
 proxy_set_header X-Forwarded-Proto $scheme;
 proxy_set_header X-SSL-CERT $sspi_client_escaped_cert;

 # ECP Web
 location / {
 proxy_pass http://localhost:5000;
 proxy_buffer_size 64k;
 proxy_buffers 4 64k;
 proxy_busy_buffers_size 64k;
 }

 # ECP API
 location /api/ca {
 proxy_pass http://localhost:5000;
 }

 # SMEV API
 location /api/smev {
 proxy_pass http://localhost:5001;
 }
 sspi on;
 sspi_certificate 0x4ACAE00070AC82A84C2660BBDC1DD3A1; # Серийный номер
сертификата веб-сервера
 sspi_protocols TLSv1 TLSv1.1 TLSv1.2;
 sspi_verify_client on;
 sspi_client_certificate root;
 }
```

После изменения конфигурации nginx необходимо перезапустить:

```
sudo systemctl stop nginx && sudo systemctl start nginx
```

3.4. Установка ПО Сервиса обеспечения работы Операторов

3.4.1. Подготовка дистрибутива Сервиса обеспечения работы Операторов

Дистрибутив Сервиса обеспечения работы Операторов необходимо скопировать на сервер в директорию «/opt/ecp/version_ecp/» (**допустимо указание другого пути**) и дать права на исполнение следующим файлам:

```
chmod u+x "/opt/ecp/version_ecp/CryptoPro.Ecp.Web/CryptoPro.Ecp.Web"
chmod u+x
"/opt/ecp/version_ecp/CryptoPro.SmevArchive.Web/CryptoPro.SmevArchive.Web"
```

Компонент nats-server необходимо скопировать в директорию /opt/ecp/ (**допустимо указание другого пути**)

```
chmod u+x "/opt/ecp/nats-server/nats-server"
```

В директории каждого приложения располагается конфигурационный файл **appsettings.json**. Для каждого приложения в файле **appsettings.json** необходимо указать путь (path) для сохранения логов приложений. Ниже указан пример для приложения CryptoPro.SmevArchive.Web.

```
"path": "/opt/ecp/log/CryptoPro.SmevArchive.Web_.log",
```

3.4.2. Подготовка сервисных сертификатов

Для обеспечения функционирования Сервиса обеспечения работы Операторов необходимо подготовить следующие сервисные сертификаты:

1. Сертификат веб-сервера (см. 3.3.2);
2. Сертификат nats-server (см. 6.1);
3. Сертификаты веб-сервиса обеспечения работы Операторов (см. 6.2).

3.4.3. Запуск сервиса NATS Server

Для запуска сервиса NATS Server необходимо запустить сервис nats-server, выполнив следующую команду:

```
cd /opt/ecp/nats-server/ && ./nats-server -c nats.conf
```

3.4.4. Запуск веб-сервиса обеспечения работы Операторов (CryptoPro.SmevArchive.Web)

Для запуска Сервис обеспечения работы Операторов в файле **appsettings.json** приложения CryptoPro.SmevArchive.Web необходимо:

- для секции ArchiveWebOptions указать:

```
"ArchiveWebOptions": {
    "UseEcpNatsProxyHandlers": true
  },
```

- убрать секции Database и Stan;
- указать порт веб-службы:

```
    "Urls": http://localhost:5001, # добавить новую строку
```

- выполнить следующую команду:

```
cd /opt/ecp/version_ecp/CryptoPro.SmevArchive.Service &&
./CryptoPro.SmevArchive.Service
```

3.4.5. Запуск веб-сервиса Сервиса обеспечения работы Операторов (CryptoPro.Ecp.Web)

Для запуска веб-сервиса Сервис обеспечения работы Операторов в файле **appsettings.json** приложения CryptoPro.Ecp.Web необходимо:

- для секции EcpWebOptions указать:

```
"EcpWebOptions": {
    "UseEcpNatsProxyHandlers": true
  },
```

- убрать секции Database и Stan;
- выполнить следующую команду:

```
cd /opt/ecp/version_ecp/CryptoPro.Ecp.Web && ./CryptoPro.Ecp.Web
```

4. Настройка Сервиса обеспечения работы Операторов

4.1. Регистрация сервисов

В данном разделе описан процесс создания юнитов в systemd для сервисов для обеспечения их автоматического управления. Для этого необходимо выполнить следующие действия.

- Создать для сервиса файл в следующей директории:

```
/etc/systemd/system/<имя сервиса>.service
```

- Применить изменения:

```
sudo systemctl daemon-reload
```

- Разрешить автозагрузку:

```
sudo systemctl enable <имя юнит-сервиса>
```

- Запустить сервис:

```
sudo systemctl start <имя юнит-сервиса>
```

- Пример файла <имя сервиса>:

```
[Unit]
Description=nats-server
[Service]
WorkingDirectory=/opt/ecp/nats-server
ExecStart=/opt/ecp/nats-server/nats-server -c /opt/ecp/nats-server/nats.conf
Restart=always
# Restart service after 10 seconds if the dotnet service crashes:
RestartSec=10
KillSignal=SIGINT
SyslogIdentifier=nats-server
User=cp
[Install]
WantedBy=multi-user.target
```

- Посмотреть информацию о работе сервисов можно при помощи следующих команд:

```
sudo systemctl status <имя приложения>
sudo journalctl -u <имя приложения>
```

5. Обновление Сервиса обеспечения работы Операторов

Для обновления Сервиса обеспечения работы Операторов необходимо скопировать новый дистрибутив и выполнить поочередно следующие действия:

1. Подготовить дистрибутив Сервиса обеспечения работы Операторов (см. 3.4.1).

2. Остановить службы приложений предыдущей версии Сервиса обеспечения работы Операторов.

3. Запустить службы приложений новой версии Сервиса обеспечения работы Операторов (см. 3.4.3-3.4.5).

6. Управление сервисными сертификатами

6.1. Пример назначения сертификата NATS Server

Для NATS Server необходим серверный сертификат. Требования к нему такие же, как к серверным сертификатам для веб-серверов - наличие в субъекте или расширении “Дополнительное имя субъекта” (SAN) имени хоста и наличие Проверка подлинности сервера (1.3.6.1.5.5.7.3.1) в расширении “Улучшенный ключ”. Возможный способ выпуска такого сертификата - использование соответствующего мастера из Диспетчера УЦ 2.0. Действия по установке: 1. Выпустить серверный сертификат. Если серверный сертификат был выпущен сразу в формате PEM, то сразу перейти к шагу 4. 2. Выгрузить сертификат в pfx. 3. Сконвертировать полученный pfx в формат PEM с помощью утилиты openssl. Команды для конвертации:

```
openssl pkcs12 -in <сервер>.pfx  -nocerts -nodes -out <ключ сервера>.pem
openssl pkcs12 -in <сервер>.pfx  -nokeys -clcerts -out <сертификат
сервера>.pem
```

- Добавить путь к полученным файлам ключа и сертификата в файл конфигурации NATS в разделы **tls:**

```
...
tls: {
# серверный сертификат NATS
  cert_file: "путь к <сертификат сервера>.pem"
  key_file:  "путь к <ключ сервера>.pem"
  verify_and_map: true
}
```

Сертификат необходимо установить в хранилище **umy** от имени пользователя, под которым будут запущены сервисы.

6.2. Пример назначения сервисных сертификатов Сервиса обеспечения работы Операторов

В Сервисе Обеспечения работы Операторов сервисы NATS используют CryptoPro.Ecp.Web и CryptoPro.SmevArchive.Web. Для всех них настройка защищенного подключения к NATS производится аналогичным образом, путем редактирования файла **appsettings.json**. Сертификат для подключения является обычным клиентским TLS сертификатом с Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) в расширении “Улучшенный ключ”, поэтому для его выпуска возможно использовать мастер выпуска клиентского сертификата ЦР из Диспетчера УЦ 2.0. Действия по настройке: 1. Выпустить клиентский сертификат. Так как для каждого компонента сертификат настраивается отдельно, то необходимо, чтобы сертификат содержал отличительный признак того, какой компонент этот сертификат будет использовать. Этим признаком может быть уникальной значение DNS имени или email в расширении “Дополнительное имя субъекта” (SAN), либо субъект сертификата целиком. 2. Если сертификат был получен в формате PEM, то сконвертировать его в PFX с помощью openssl:

```
openssl pkcs12 -inkey <ключ>.pem -in <сертификат>.pem -export -out
<сертификат>.pfx
```

- Установить сертификат в хранилище “Личное”. Можно воспользоваться утилитой certmgr:

```
certmgr -install -store umy -file <файл сертификата>.cer -provtype 80 -
container <имя контейнера>
```

Сертификаты необходимо установить в хранилище **umy** от имени пользователя, под которым будут запущены сервисы.

- В конфигурационном файле **appsettings.json** компонента включить защищенное соединение "Secure": true и добавить отпечаток сертификата в существующие разделы Nats и Stan:

```
...
"Nats": {
  "Url": "nats://localhost:4222",
  "Secure": true,
  "Thumbprint": "<отпечаток клиентского сертификата>"
},
```

- В конфигурационном файле NATS Server добавить уникальный признак сертификата в раздел сопоставления authorization.users для соответствующего компонента. Если в качестве уникального признака используется субъект целиком, то в конфигурационный файл он прописывается в виде текстовой строки с компонентами, разделенными запятыми без пробелов. Порядок компонент обратный (как в окне просмотра сертификата). Если в субъекте есть повторяющиеся компоненты, то используется только первый. Пример для CryptoPro.SmevArchive.Web:

```
authorization: {
...
  users = [
  ...
     {user: "<уникальный признак сертификата>", permissions: $ECP_WEB} #
сопоставление сертификата для CryptoPro.SmevArchive.Web
  ...
  ]
}
```

- После настройки защищенного соединения для всех компонентов для применения настроек необходимо перезапустить NATS Server.

7. Дополнительные настройки компонент сервиса обеспечения работы Операторов

7.1. Настройки веб-сервиса Сервиса обеспечения работы Операторов (CryptoPro.Ecp.Web)

Конфигурация (настройки) сервиса обеспечения работы Операторов определяются параметрами в файле appsettings.json приложения CryptoPro.Ecp.Web.

Таблица 3. Параметры приложения CryptoPro.Ecp.Web

Блок	Параметр	Возможные значения	Описание
Nats	Url	"nats://<DNS>:4222"	Адрес подключения к NATS
EcpWebOptions	SmevArchiveUri	"https://<DNS>"	Адрес для получения содержимого ответов из СМЭВ
	UseCertificateForwarding	"true"	Значение д.б. указано как true
	IsNewCertRequestOnSeparatedPage	"false | true"	Отображение запросов на сертификат на отдельной странице
	UseEcpNatsProxyHandlers	"true"	Для Сервиса обеспечения операторов значение должно быть выставлено в true
	EnabledCarrierUniqueFilter	["pkcs11_", "rutoken_", "jacarta_", "esmart_", "mskey_", "smartpark_", "magistra_", "ic_fkc", "ic_vpn"]	Перечень разрешенных носителей в веб-интерфейсе Оператора
	UseSystemOperatorMessage	"false|true"	Отображение сообщения от администратора в интерфейсе оператора
	SystemOperatorMessage	"Отсутствует подключение к СМЭВ. Необходимо обратиться к оператору ЕЦП"	Текст сообщения от администратора
	"RevokeValidCertificateAfter"	"01.00:00:00"	По умолчанию (без параметра) формируется отложенный отзыв, и он равен 5 дням. Чтобы указать параметр периода времени, через который будет отозван сертификат по-другому, нужно добавить параметр
	"SignCertRequest"	true | false	Подпись запроса при создании и одобрении запроса на сертификат в пользовательском интерфейсе оператора
	UseDocAttachmentUI	true | false	Включение/отключение пользовательского интерфейса прикрепления документов
	UseIdScanningUI	true | false	Включение/отключение пользовательского интерфейса сканирования УЛ заявителя
	UseDssCertRequestCreationUI	true | false	Включение/отключение пользовательского интерфейса создания ключа в СДЭП
	DataProtectionKeysFolder	“/etc/sharefolder”	Путь до общей папки для хранения ключа, используемого при создании токенов проверки подлинности веб-сайта
	DocAttachmentMaxSize	5	максимальный размер загружаемого файла, значение указывается в мегабайтах
	EnabledDocAttachmentExtensions	[".pdf", ".jpg", ".jpeg", ".png", ".tiff", ".docx", ".doc", ".xlsx", ".xls", ".csv"]	разрешённые расширения загружаемых документов
	UserTemplateOid	"<OID шаблона сертификата пользователя>",	OID шаблона сертификата пользователя
	OperatorTemplateOid	"<OID шаблона сертификата оператора>"	OID шаблона сертификата оператора (шаблон, по которому будет создаваться запрос оператора)

Блок	Параметр	Возможные значения	Описание
Serilog	Default	"Warning|Error|Information|Debug"	Уровень журналирования
	Microsoft		
	Microsoft.Hosting.Lifetime		
WriteTo	path	"/home/cryptopro/ecp/log/CryptoPro.Ecp.Web_.log"	Путь для сохранения журналов
	rollingInterval	"Day"	Создание нового журнала в указанный период времени
	retainedFileCountLimit	"7"	Сохранение последних журналов согласно указанному количеству
	fileSizeLimitBytes	"1024"	Ограничение размера файла журналов. По умолчанию: 1 Гб

7.2. Настройки веб-сервиса Сервиса обеспечения работы Операторов (CryptoPro.SmevArchive.Web)

Конфигурация (настройки) сервиса обеспечения работы Операторов определяются параметрами в файле appsettings.json приложения CryptoPro. SmevArchive.Web.

Таблица 4. Параметры приложения CryptoPro.SmevArchive.Web

Блок	Параметр	Возможные значения	Описание
Сетевые настройки приложения	Urls	http://localhost:5001	Адрес приложения. Если параметр не задан, по умолчанию приложение будет запущено с адресом http://localhost:5001
Nats	Url	"nats://<DNS>:4222"	Адрес подключения к NATS
ArchiveWebOptions	UseCertificateForwarding	"true"	Значение должно быть указано как true
	UseEcpNatsProxyHandlers	"true"	Для Сервиса обеспечения операторов значение должно быть выставлено в true
Serilog	Default	"Warning|Error|Information|Debug"	Уровень журналирования
	Microsoft		
	Microsoft.Hosting.Lifetime		
WriteTo	path	"/home/cryptopro/ecp/log/CryptoPro.SmevArchive.Web_.log"	Путь для сохранения журналов
	rollingInterval	"Day"	Создание нового журнала в указанный период времени
	retainedFileCountLimit	"7"	Сохранение последних журналов согласно указанному количеству
	fileSizeLimitBytes	"1024"	Ограничение размера журналов. По умолчанию: 1 Гб

7.3. Настройки сервиса NATS

Конфигурация (настройки) сервиса NATS определяются параметрами в файле nats.conf приложения nats-server

Таблица 5. Параметры приложения NATS

Блок	Параметр	Возможные значения	Описание
# NATS	listen	"<DNS>:4222"	Адрес подключения к NATS
	http_port	"8222"	Адрес сервера мониторинга NATS. Без указания параметра сервер мониторинга будет выключен. Пример адреса: • NATS http://server:port/varz
tls			Настройка TLS между клиентом и серверов NATS Если параметр не указан, TLS не требуется