Руководство по установке Программа для ЭВМ «Internet of Things Security Module Сервер управления (IT SM Сервер управления)»

1 УСТАНОВКА И НАСТРОЙКА

1.1 НЕОБХОДИМЫЕ ПОДГОТОВИТЕЛЬНЫЕ МЕРОПРИЯТИЯ

Для установки, настройки, запуска и локального тестирования ПО IT SM Сервер управления необходимы:

1) Физический сервер с установленной платой PCI-E из состава ПАК «Соболь» Версии 3.2, сертифицированной ФСБ России.

2) Установленная на сервере операционная система Oracle Linux Server 7.9 (вариант установки Minimal Install), соответствующая следующим требованиям:

− статический IPv4-адрес;

− заданное FQDN-имя сервера;

− подключение к сети Интернет, включая доступ к стандартным Интернет-репозиториям Oracle Linux 7 Server Latest (x86_64);

− права пользователя root с возможностью запуска консоли.

Кроме того, в целях обеспечения контроля целостности с помощью ПАК «Соболь» Версии 3.2 необходимо обеспечить (см. полный список требований в документации ПАК «Соболь» Версии 3.2):

− отсутствие использования логических томов LVM;

− использование файловой системы EXT4 на контролируемых разделах.

Примечание 1: Вариант установки ОС Minimal Install необходим для корректного выполнения действий, описанных в нижеследующих разделах. В противном случае корректность действий, выполняемых по настоящей инструкции, не гарантируется.

Примечание 2: Указанный сервер должен быть предназначен исключительно для целей эксплуатации компонентов ПО IT SM Сервер управления. Одновременное использование сервера для других целей не рекомендуется и корректность работы в этом случае не гарантируется.

3) Дистрибутив ПО Версии 3.0.9-5 для ОС семейства Linux, входящий в состав ПАК «Соболь» Версии 3.2, сертифицированной ФСБ России.

4) Дистрибутив сертифицированной ФСБ России версии СКЗИ КриптоПро CSP 5.0.11455 (Fury) от 8.05.2019 для Linux (x64, rpm).

5) Серверная лицензия КриптоПро CSP 5.0 (ключ активации).

6) Параметры подключения к Крипто-Про УЦ версии 2.0 по HTTP API, включая:

− FQDN/IP-адрес Крипто-Про УЦ ЦР 2.0;

− сертификат/ключ API-клиента Крипто-Про УЦ (контейнер PKCS#12 с паролем или ключевой контейнер Крипто-Про CSP, сертификат клиента, цепочка сертификатов ЦС);

− идентификатор папки folderId (GUID), для которой у API-клиента есть право «Запроса регистрации»;

− наименование шаблона (template), зарегистрированного на Крипто-Про УЦ, в рамках которого будут издаваться сертификаты для устройств (СКЗИ IT SM).

7) Сертификат/ключ сервера, в котором CN=[FQDN сервера] (контейнер PKCS#12 с паролем или ключевой контейнер Крипто-Про CSP, сертификат сервера, цепочка сертификатов ЦС).

Примечание: В состав предоставляемого комплекта материалов включен ключевой контейнер (plmbServ) и тестовый сертификат (CN=plumba), изданный локальным тестовым ЦС (CN=testCA01).

Примечание: Предполагается, что все сторонние дистрибутивы (за исключением тех, что загружаются в процессе установки из Интернет) предварительно загружены и размещены в директории:

```
/opt/distrib/third-party-distrib/
```

1.2 ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА И УСТАНОВКА СИСТЕМНЫХ КОМПОНЕНТОВ

Примечания:

1) Все описанные команды, если не оговорено иное, выполняются пользователем root.

2) При копировании команд, приведенных в данном руководстве, необходимо убедиться, что символы не претерпели изменений. Например, символ дефиса “-” может принять форму тире “–” и тогда команда не будет выполнена корректно. Оптимальным вариантом является предварительное копирование команд в простой текстовый редактор типа Notepad из состава ОС Microsoft Windows.

Для выполнения предварительной настройки и установки системных компонентов, а также окружения для сборки необходимо:

1) Выполнить обновление компонентов ОС до актуальных версий:

```
yum -y update
```

2) Выполнить отключение технологии SELinux. Для этого необходимо отредактировать файл:

```
/etc/selinux/config
```

изменив значение следующего параметра (штатно установлено "enforcing"):

```
SELINUX=disabled
```

3) Выполнить изменение версии ядра, загружаемого по умолчанию:

```
grub2-set-default \
'Oracle Linux Server 7.9, with Linux 3.10.0-1160.el7.x86_64'
grub2-mkconfig -o /boot/grub2/grub.cfg
```

4) Перезагрузить сервер:

```
reboot
```

после чего проверить текущую версию ядра:

```
uname -r
```

Примечание: Указанная версия ядра (3.10.0-1160.el7.x86_64) актуальная на момент написания документа. При необходимости, в командах, приведенных выше, нужно указать актуальную доступную версию ядра. При этом необходимо

использовать версии ядра 3.10.0-***, которые совместимы в модулем ядра sobol.ko из состава ПАК «Соболь» Версии 3.2, сертифицированного ФСБ России, которое входит в состав ПО IT SM Сервер управления.

5) Выполнить отключение встроенного МЭ:

```
systemctl stop firewalld
systemctl disable firewalld
```

6) Выполнить установку необходимых системных утилит:

```
yum -y install zip unzip wget
```

7) Выполнить установку дополнительных системных утилит для диагностики сетевых соединений:

```
yum -y install telnet net-tools
```

8) Выполнить установку сервиса rngd, обеспечивающего доступ системного датчика случайных чисел ОС к аппаратному обеспечению сервера:

```
yum -y install rng-tools
```

9) Выполнить активацию и запуск сервиса rngd:

```
systemctl enable rngd
systemctl start rngd
```

10) Выполнить установку сервиса ntpd, обеспечивающего синхронизацию времени:

```
yum -y install ntp
```

При необходимости, отредактировать файл конфигурации сервиса ntpd, указав необходимые сервера:

```
vi /etc/ntp.conf
```

11) Выполнить активацию и запуск сервиса ntpd:

```
systemctl enable ntpd
systemctl start ntpd
```

12) Выполнить установку пакета, включающего в себя утилиту xxd, необходимую для работы скрипта randomer.sh:

```
yum -y install vim-common
```

13) Выполнить установку окружения Java JRE 11, необходимого для запуска и функционирования Java-приложений:

```
yum -y install java-11-openjdk-headless
```

14) Выполнить установку системного пакета, необходимого для функционирования КриптоПро CSP из состава СКЗИ:

```
yum -y install redhat-lsb-core
```

15) Выполнить установку компонентов, необходимых для работы ПО из состава ПАК «Соболь» Версии 3.2:

```
yum -y install gtk2 libglade2
```

16) Выполнить установку компонентов, необходимых для сборки Web-сервера NGINX 1.18.0:

```
yum -y install gcc pcre-devel zlib-devel
```

17) Выполнить установку Python3 и модулей Python, необходимых для работы скрипта issue-cpro.py:

```
yum -y install python3
pip3 install requests
```

1.3 УСТАНОВКА ПО ПАК «СОБОЛЬ» ВЕРСИИ 3.2

Для установки программных компонент ПАК «Соболь» Версии 3.2 на ОС Oracle Linux 7.9 с версией ядра 3.10.0-1160.el7.x86_64 необходимо:

1) Выполнить установку пакета версии 3.0.9-5 из состава ПАК «Соболь» Версии 3.2:

```
cd /opt/distrib/third-party-distrib/sobol/
rpm -ivh sobol-3.0.9-5.el7.0.x86_64.rpm
```

при этом в процессе установки будет выдано следующее сообщение:

```
Loading sobol device driver...
modprobe: FATAL: Module sobol not found.
Device is present
```

Данное сообщение является ожидаемым и связано с тем, что модуль ядра sobol.ko по умолчанию устанавливается в директорию, соответствующую другой версии ядра (3.10.0-123.el7).

2) Выполнить создание символической ссылки, которая обеспечит доступность модуля ядра sobol.ko для системы управления модулями ядра modprobe с учетом текущей используемой версии ядра (3.10.0-1160.el7.x86_64):

```
ln -s \
/usr/lib/modules/3.10.0-123.el7.x86_64/kernel/drivers/char/sobol.ko
/usr/lib/modules/3.10.0-1160.el7.x86_64/kernel/drivers/char/sobol.ko
```

3) Выполнить обновление конфигурации системы управления модулями ядра modprobe:

```
depmod
```

4) Перезапустить службу, обеспечивающую загрузку драйвера устройства из состава ПАК «Соболь» Версии 3.2:

```
systemctl restart sobol
```

после чего проверить статус выполнения загрузки драйвера:

```
systemctl status sobol
```

5) Выполнить команду проверки статуса устройства из состава ПАК «Соболь» Версии 3.2:

```
sobol -vt
```

В выводе команды должно отобразиться:

```
Checking device availability...
Device is ready
```

6) Выполнить проверку датчика случайных чисел ПАК «Соболь» Версии 3.2:

```
sobol -vG
```

В выводе команды должно отобразиться:

```
Waiting...

Test random success
```

1.4 УСТАНОВКА И НАСТРОЙКА СУБД POSTGRESQL

Для выполнения установки и настройки СУБД PostgreSQL необходимо:

1) Выполнить установку СУБД PostgreSQL из штатного репозитория:

```
yum -y install postgresql-server
```

2) Выполнить инициализацию СУБД PostgreSQL:

```
/usr/bin/postgresql-setup initdb
```

3) Выполнить активацию и запуск сервиса СУБД:

```
systemctl enable postgresql
systemctl start postgresql
```

а также убедиться, что сервис СУБД корректно запустился, выполнив команду:

```
systemctl status postgresql
```

4) Выполнить создание пользователя БД (plumba) и БД (plumba):

```
sudo -iu postgres createuser --createdb plumba
sudo -iu postgres createdb --owner plumba plumba
```

5) Выполнить редактирование конфигурации СУБД с целью разрешения доступа пользователю plumba к БД plumba без аутентификации. Для этого открыть на редактирование файл:

```
vi /var/lib/pgsql/data/pg_hba.conf
```

перейти в следующий раздел (строка 81):

```
# IPv4 local connections:
```

в начало раздела добавить строку:

```
host    plumba          plumba          127.0.0.1/32            trust
```

чтобы раздел выглядел следующим образом:

```
# IPv4 local connections:
host    plumba          plumba          127.0.0.1/32            trust
host    all             all             127.0.0.1/32            ident
```

и сохранить изменения в файле.

6) Выполнить перезапуск сервиса СУБД:

```
systemctl restart postgresql
```

1.5 УСТАНОВКА И НАСТРОЙКА КРИПТО-ПРО CSP

Для функционирования и сборки приложения необходимо выполнить установку и настройку СКЗИ КриптоПро CSP из состава ПО IT SM Сервер управления следующим образом:

1) Выполнить установку базовых компонентов КриптоПро CSP из состава ПО:

```
cd /opt/distrib/third-party-distrib/cryptopro/
tar -xf linux-amd64.tgz
cd linux-amd64
./install.sh kc2
```

2) Выполнить установку модуля поддержки ПАК «Соболь»:

```
rpm -ivh lsb-cprocsp-rdr-sobol-64-5.0.11455-5.x86_64.rpm
```

3) Выполнить отображение списка датчиков случайных чисел:

```
/opt/cprocsp/sbin/amd64/cpconfig -hardware rndm -view
```

В выводе команды должен присутствовать ПАК «Соболь» (Sable):

```
Nick name: Sable
Connect name:
Rndm name: Sobol
Rndm level: 2
...
```

4) Выполнить установку дополнительных компонентов КриптоПро CSP из состава ПО, реализующих интерфейс OpenSSL 1.1.0:

```
rpm -ivh cprocsp-cpopenssl-110-base-5.0.11455-5.noarch.rpm
rpm -ivh cprocsp-cpopenssl-110-64-5.0.11455-5.x86_64.rpm
rpm -ivh cprocsp-cpopenssl-110-gost-64-5.0.11455-5.x86_64.rpm
```

а также библиотек и заголовочных файлов OpenSSL 1.1.0, необходимых для сборки NGINX 1.18.0 и модуля подписи PKCS#10-запросов перед отправкой в Крипто-Про УЦ 2.0 через HTTP API:

```
rpm -ivh cprocsp-cpopenssl-110-devel-5.0.11455-5.noarch.rpm
```

5) Выполнить установку серверной лицензии КриптоПро CSP 5.0:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -set [ключ активации]
```

1.6 УСТАНОВКА СКРИПТОВ И КОНФИГУРАЦИОННЫХ ФАЙЛОВ ПРИЛОЖЕНИЯ

Для установки комплекта структуры каталогов, скриптов и конфигурационных файлов, необходимых для работы Java-приложений, реализующих Web-сервис и командный интерпретатор, а также других компонентов системы необходимо:

1) Выполнить распаковку дистрибутива:

```
cd /opt/distrib/
unzip plumba-distrib-0.3.zip
cd plumba-distrib-0.3
```

2) Запустить скрипт установки:

```
./plumba-install.sh
```

В результате работы скрипта будет создан общий рабочий каталог для всех компонентов приложения (/opt/plumba).

1.7 СБОРКА И НАСТРОЙКА NGINX 1.18.0

Для выполнения сборки и настройки NGINX 1.18.0 с целью обеспечения его работы с модулем Крипто-Про cp-openssl-1.1.0 необходимо:

1) Выполнить загрузку и распаковку исходных кодов NGINX 1.18.0:

```
cd /opt/distrib/
wget https://nginx.org/download/nginx-1.18.0.tar.gz
tar -xf nginx-1.18.0.tar.gz
cd nginx-1.18.0
```

2) Заменить файл конфигурации сборки OpenSSL:

```
cp /opt/plumba/nginx-1.18.0-confs/conf auto/lib/openssl/
```

Изменения затрагивают пути к библиотекам и заголовочным файлам модуля Крипто-Про cp-openssl-1.1.0:

```
...
   CORE_INCS="$CORE_INCS $OPENSSL/include"
   CORE_DEPS="$CORE_DEPS $OPENSSL/include/openssl/ssl.h"
   CORE_LIBS="$CORE_LIBS $OPENSSL/lib/amd64/libssl.a"
   CORE_LIBS="$CORE_LIBS $OPENSSL/lib/amd64/libcrypto.a"
...
```

3) Выполнить создание системного пользователя и группы NGINX:

```
useradd -c "Nginx Web Server" -m -b /var/lib \
```

```
-s /sbin/nologin nginx
```

4) Выполнить конфигурацию сборщика NGINX:

```
./configure --prefix=/etc/nginx \
--user=nginx --group=nginx \
--sbin-path=/usr/sbin/nginx \
--conf-path=/etc/nginx/nginx.conf \
--error-log-path=/var/log/nginx/error.log \
--http-log-path=/var/log/nginx/access.log \
--pid-path=/var/run/nginx.pid \
--lock-path=/var/run/nginx.lock \
--http-client-body-temp-path=/var/lib/nginx/client_temp \
--http-proxy-temp-path=/var/lib/nginx/proxy_temp \
--http-fastcgi-temp-path=/var/lib/nginx/fastcgi_temp \
--without-http_autoindex_module \
--without-http_ssi_module \
--without-http_scgi_module \
--without-http_uwsgi_module \
--without-http_geo_module \
--without-http_split_clients_module \
--without-http_memcached_module \
--without-http_empty_gif_module \
--without-http_browser_module \
--with-http_auth_request_module \
--with-http_stub_status_module \
--with-http_ssl_module \
--with-openssl=/opt/cprocsp/cp-openssl-1.1.0/
```

5) Выполнить сборку и установку NGINX:

```
make
make install
```

6) Скопировать предоставляемый ключевой контейнер сервера в директорию ключевых контейнеров пользователя root Крипто-Про CSP:

```
cp -rp /opt/plumba/testCA/private/plmbServ.000/ \
/var/opt/cprocsp/keys/root/
```

после чего выполнить визуальную проверку параметров контейнера:

```
/opt/cprocsp/bin/amd64/csptest -keyset -info -container \
'\\.\HDIMAGE\plmbServ'
```

7) Скопировать сертификат сервера в директорию конфигурации NGINX:

```
cp /opt/plumba/testCA/certs/plmbServ.cert.pem /etc/nginx/
```

8) Скопировать предоставляемый конфигурационный файл nginx.conf, заменив существующий:

```
cp /opt/plumba/nginx-1.18.0-confs/nginx.conf /etc/nginx/
```

При необходимости отредактировать конфигурационный файл nginx.conf, указав корректные имена контейнера Крипто-Про CSP и пути к сертификату в разделе # Proxy to main Java Web Service (по умолчанию этого не требуется):

```
...
        ssl_certificate /etc/nginx/plmbServ.cert.pem;
        ssl_certificate_key engine:gostengy:c:plmbServ;
...
```

9) Ограничить количество соединений, одновременно обрабатываемых сервером, добавив следующие конфигурационные параметры в соответствующие разделы:

```
...
http {
    limit_conn_zone $server_name zone=perserver:10m;
...
    server {
        limit_conn perserver 100;
    }
}
```

10) Выполнить активацию сервиса systemd nginx в соответствии с предоставляемым конфигурационным файлом:

```
systemctl enable /opt/plumba/nginx-1.18.0-confs/nginx.service
```

11) Выполнить запуск NGINX и контроль статуса сервиса:

```
systemctl start nginx
systemctl status nginx
```

1.8 НАСТРОЙКА И ЗАПУСК WEB-СЕРВИСА

Для настройки и запуска Web-сервиса, предоставляющего HTTP API для компонентов системы в Исполнениях 1 и 2, необходимо:

1) Выполнить ревизию и, при необходимости, корректировку параметров работы приложения в конфигурационном файле (пути к файлам, время жизни токенов доступа и т.п.):

```
vi /opt/plumba/application.yml
```

Файл конфигурации приложения содержит следующие параметры (см. описание конфигурационного файла в Руководстве программиста), непосредственно влияющие на работу приложения (в разделе plumba):

```
plumba:
#  issuer: /opt/plumba/issue-cpro.py
#  CA: /opt/plumba/cdp-aia/cpro-ca.crt
#  CRL: /opt/plumba/cdp-aia/cpro-ca.crl
#  randomer: /opt/plumba/soboler.sh
  randomer: /opt/plumba/randomer.sh
  issuer: /opt/plumba/issue-localtest.sh
  CA : /opt/plumba/testCA/certs/testCA01.cert.pem
  CRL : /opt/plumba/testCA/crl/testCA01.crl.pem
  csrout: /opt/plumba/csr
  crtin: /opt/plumba/crt
  ivsize: 32
  tokenttl: 600
  gettimeout: 5
  serviceCrtMask: '^[0-9A-Z-]*-service[0-9]$'
...
```

Для активации скрипта, обеспечивающего получение гаммы с датчика случайных чисел ПАК «Соболь» (soboler.sh), необходимо отредактировать конфигурационный файл следующим образом:

```
plumba:
#  issuer: /opt/plumba/issue-cpro.py
#  CA: /opt/plumba/cdp-aia/cpro-ca.crt
#  CRL: /opt/plumba/cdp-aia/cpro-ca.crl
  randomer: /opt/plumba/soboler.sh
#  randomer: /opt/plumba/randomer.sh
  issuer: /opt/plumba/issue-localtest.sh
  CA : /opt/plumba/testCA/certs/testCA01.cert.pem
  CRL : /opt/plumba/testCA/crl/testCA01.crl.pem
  csrout: /opt/plumba/csr
  crtin: /opt/plumba/crt
```

```
  ivsize: 32
  tokenttl: 600
  gettimeout: 5
  serviceCrtMask: '^[0-9A-Z-]*-service[0-9]$'
...
```

Примечание 1: При редактировании конфигурационного файла необходимо сохранять форматирование и, в частности, отступы для строк.

Примечание 2: По умолчанию приложение настроено на издание сертификатов с использованием локального тестового ЦС (см. раздел 3) без обращения в Крипто-Про УЦ 2.0 – соответствующие строки конфигурации скрыты в качестве комментариев.

Примечание 3: По умолчанию приложение настроено работу с системным датчиком случайных чисел /dev/urandom без обращения к ПАК «Соболь» Версии 3.2 – соответствующая строка конфигурации (randomer) скрыта в качестве комментария. Программный ДСЧ допустимо использовать только в тестовых целях – в соответствии с Правилами пользования ПО IT SM Сервер управления при эксплуатации запрещено использовать программные ДСЧ и длину IV ниже заявленной.

2) Выполнить активацию сервиса systemd plumba в соответствии с предоставляемым конфигурационным файлом:

```
systemctl enable /opt/plumba/plumba.service
```

3) Выполнить запуск Web-ссервиса:

```
systemctl start plumba
```

и через 10-15 секунд контроль статуса Web-сервиса:

```
systemctl status plumba
```

Примечание: При первом запуске Web-сервиса в БД будут созданы необходимые таблицы, о чём в системном журнале будут выданы соответствующие предупреждения WARN (SQL Warning Code: 0).

Успешный запуск Web-сервиса (занимает 10-15 секунд) завершится информацией о запуске сервера Tomcat на соответствующем порту (указывается в конфигурации приложения) и отображением времени, затраченного на запуск:

```
...
o.s.b.w.embedded.tomcat.TomcatWebServer : Tomcat started on port(s): 8888
(http) with context path ''
ru.rawlab.plumba.BackendService : Started BackendService in 13.458 seconds
(JVM running for 15.41)
```

1.9 НАСТРОЙКА КОНТРОЛЯ ЦЕЛОСТНОСТИ С ИСПОЛЬЗОВАНИЕМ ПАК «СОБОЛЬ» ВЕРСИИ 3.2

Для настройки контроля целостности файлов ПО IT SM Сервер управления с помощью ПАК «Соболь» Версии 3.2 необходимо:

1) Добавить файлы в список контролируемых:

```
scheck --add-ls-files /opt/plumba/sobol-controlled.txt
```

Контролю целостности с помощью ПАК «Соболь» Версии 3.2 подвергаются следующие файлы ПО IT SM Сервер управления:

```
/opt/plumba/cpro-signer
/opt/plumba/plumba-jvm-interactive-shell.jar
/opt/plumba/plumba-jvm-backend.jar

/opt/plumba/issue-cpro.py
/opt/plumba/plumba-cli.sh
/opt/plumba/soboler.sh

/opt/plumba/plumba.service
/opt/plumba/nginx-1.18.0-confs/nginx.service
```

2) Перезагрузить сервер и на этапе загрузки, после передачи управления ПАК «Соболь» Версии 3.2, выполнить расчет эталонных значений контрольных сумм в соответствии Руководством администратора на ПАК «Соболь» Версии 3.2 из состава ПО.

2 ЛОКАЛЬНОЕ ТЕСТИРОВАНИЕ ИНСТАЛЛЯЦИИ

Примечание 1: Локальное тестирование предполагает реализацию основного сценария работы системы с использованием утилиты curl из состава Крипто-Про CSP, что позволяет проверить корректность работы созданной инсталляции ПО IT SM Сервер управления.

Примечание 2: При локальном тестировании сертификаты Криптомодулям издаются локальным тестовым ЦС (CN=testCA01) на базе на базе cp-openssl-1.1.0 без обращения в Крипто-Про УЦ 2.0.

2.1 НАСТРОЙКА ЛОКАЛЬНОГО ТЕСТОВОГО ОКРУЖЕНИЯ

Для настройки локального тестового окружения необходимо:

1) Отредактировать системный файл /etc/hosts, добавив запись для локального сервера в целях соответствия имени в Common Name тестового сертификата:

```
...
127.0.0.1 plumba
...
```

2) Скопировать предоставляемый ключевой контейнер тестового ЦС в директорию ключевых контейнеров пользователя root Крипто-Про CSP:

```
cp -rp /opt/plumba/testCA/private/testCA01.000/ \
/var/opt/cprocsp/keys/root/
```

после чего выполнить визуальную проверку параметров контейнера:

```
/opt/cprocsp/bin/amd64/csptest -keyset -info -container \
'\\.\HDIMAGE\testCA01'
```

3) Выполнить установку сертификата тестового ЦС (CN=testCA01) в локальное корневое хранилище Крипто-Про CSP:

```
/opt/cprocsp/bin/amd64/certmgr -install -store uRoot -file \
/opt/plumba/testCA/certs/testCA01.cert.pem
```

При выполнении команды подтвердить установку сертификата в хранилище доверенных корневых центров сертификации, нажав соответствующую клавишу:

```
...
CPCSP: Warning: installing a root certificate with an unconfirmed
thumbprint is a security risk. Do you want to install this certificate?
Subject: testCA01
Thumbprint (sha1): A2ED1D4895F61AF105582055E290068A2D71D5B8
```

```
(o)OK, (c)Cancel
...
```

4) Выполнить установку CRL тестового ЦС (CN=testCA01) в локальное корневое хранилище Крипто-Про CSP:

```
/opt/cprocsp/bin/amd64/certmgr -install -crl -store uRoot -file \
/opt/plumba/testCA/crl/testCA01.crl.pem
```

5) Скопировать предоставляемый ключевой контейнер тестового оператора в директорию ключевых контейнеров пользователя root Крипто-Про CSP:

```
cp -rp /opt/plumba/testCA/private/plmbOper.000/ \
/var/opt/cprocsp/keys/root/
```

6) Выполнить установку предоставляемого сертификата тестового оператора в локальное хранилище персональных сертификатов Крипто-Про CSP с привязкой к контейнеру:

```
/opt/cprocsp/bin/amd64/certmgr -install -container \
'\\.\HDIMAGE\plmbOper' \
-file /opt/plumba/testCA/certs/plmbOper.cert.pem
```

7) Выполнить отображение списка локальных персональных сертификатов:

```
/opt/cprocsp/bin/amd64/certmgr -list
```

В выводе команды зафиксировать идентификатор (SHA1 Hash) сертификата тестового оператора (CN=plumba-operator) и убедиться в наличии привязки к ключу (PrivateKey Link : Yes):

```
...
Issuer             : CN=testCA01
Subject            : CN=plumba-operator
Serial             : 0x02
SHA1 Hash          : 1f4e4b4c0af7ad37c5d3aa6361656e7f4c60f30d
SubjKeyID          : 3f442481dd5475e4dcc1e9b8e4867c7150d30b45
Signature Algorithm : ГОСТ Р 34.11-2012/34.10-2012 256 бит
PublicKey Algorithm : ГОСТ Р 34.10-2012 (512 bits)
Not valid before   : 18/03/2021  16:53:23 UTC
Not valid after    : 18/03/2022  16:53:23 UTC
PrivateKey Link    : Yes
Container          : HDIMAGE\\plmbOper.000\EDED
Provider Name      : Crypto-Pro GOST R 34.10-2012 KC2 CSP
Provider Info      : ProvType: 80, KeySpec: 1, Flags: 0x0
```

```
Extended Key Usage  : 1.3.6.1.5.5.7.3.2
...
[ErrorCode: 0x00000000]
```

8) Запустить командный интерпретатор приложения:

```
/opt/plumba/plumba-cli.sh
```

Запуск командного интерпретатора (занимает 5-10 секунд) завершится отображением приглашения для ввода команд:

```
shell:>
```

9) Выполнить команду создания УЗ с ролью OPERATOR:

```
add-user --role OPERATOR
```

после чего необходимо скопировать в буфер обмена сертификат тестового оператора в текстовом виде (файл plmbOper.cert.pem из дополнительной директории test-certs) и вставить текст сертификата в окно терминала:

```
Type certificate(end input with empty string):
-----BEGIN CERTIFICATE-----
MIIBmDCCAUOgAwIBAgIBAjAMBggqhQMHAQEDAgUAMBMxETAPBgNVBAMTCHRlc3RD
QTAxMB4XDTIxMDMxODE2NTMyM1oXDTIyMDMxODE2NTMyM1owGjEYMBYGA1UEAwwP
cGx1bWJhLW9wZXJhdG9yMGYwHwYIKoUDBwEBAQEwEwYHKoUDAgIkAAYIKoUDBwEB
AgIDQwAEQGS8xOzY09cLWHvH1GCnwfdlD1LPrOX5ObWDLqrmoeS9v7cXy9hNNLxJ
wAbIWQLXXBTzDkkA+tmwwixd8Y62aCujcjBwMAkGA1UdEwQCMAAwHQYDVR0OBBYE
FD9EJIHdVHXk3MHpuOSGfHFQ0wtFMB8GA1UdIwQYMBaAFHU+o4RLNO9O7mY7Aowf
/TsfZG24MA4GA1UdDwEB/wQEAwIFoDATBgNVHSUEDDAKBggrBgEFBQcDAjAMBggq
hQMHAQEDAgUAA0EAzJxI2uZ6nEQNZvOCJsBZGYLsEP5pq7elTvTNU2Y2NKEy9WrA
kOT6BRfTEwElX401pjJ7/cwAB6tl//WSkxYwqQ==
-----END CERTIFICATE-----

Add user with subject CN=plumba-operator and role OPERATOR? (y/n)
y
User added
```

После вставки текста сертификата необходимо дважды нажать Enter до появления подтверждения создания УЗ после чего нажать «y» для подтверждения.

10) Выполнить команду отображения списка УЗ:

```
show-accounts
```

В списке должна отобразиться созданная УЗ, после чего осуществить выход из командного интерпретатора:

```
exit
```

2.2 ВЫПОЛНЕНИЕ ЛОКАЛЬНЫХ ТЕСТОВЫХ ЗАПРОСОВ

Для выполнения локальных тестовых запросов необходимо:

1) Отправить запрос базовой информации:

```
/opt/cprocsp/bin/amd64/curl --verbose \
--request POST \
--header "Accept: application/json" \
--header "Content-type: application/json" \
https://plumba/common/info
```

В ответе сервера должен присутствовать сертификат ЦС (ca) и CRL (crl):

```
...
< HTTP/1.1 200
< Server: nginx/1.18.0
< Date: Fri, 09 Apr 2021 22:41:35 GMT
< Content-Type: application/json
< Transfer-Encoding: chunked
< Connection: keep-alive
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Cache-Control: no-cache, no-store, max-age=0, must-revalidate
< Pragma: no-cache
< Expires: 0
< X-Frame-Options: DENY
<
* Connection #0 to host plumba left intact
* Closing connection #0
{"ca":"-----BEGIN CERTIFICATE-----
\nMIIBrTCCAVqgAwIBAgIIFC+Q2QDPMiowCgYIKoUDBwEBAwIwEzERMA8GA1UEAxMI\ndGVzdE
NBMDEwHhcNMjEwMzEwMTkxNTU5WhcNMjIwOTAxMTkyNTU5WjATMREwDwYD\nVQQDEwh0ZXN0Q0
EwMTBmMB8GCCqFAwcBAQEBMBMGByqFAwICJAAGCCqFAwcBAQIC\nA0MABEDt6MxynOwYi6/X30
sFuYA96KcgRLIW+GrDJ++Fx70NOs/TdRjG+Wk02mvH\n0skTdWhSii6rFmCZe09ka9gd8H7mo4
GKMIGHMB0GA1UdDgQWBBR1PqOESzTvTu5m\nOwKMH/07H2RtuDAOBgNVHQ8BAf8EBAMCAf4wEg
YDVR0TAQH/BAgwBgEB/wIBATBC\nBgNVHSMEOzA5gBR1PqOESzTvTu5mOwKMH/07H2RtuKEXpB
UwEzERMA8GA1UEAxMI\ndGVzdENBMDGCCBQvkNkAzzIqMAoGCCqFAwcBAQMCA0EAT/4pXXWX3c
```

```
Q4Trv3OYzl\nD+M5PufqLId6kVyVOgPGChMUHnjdmnAw4EVX/UaP8E4kp7mMZ6fcKSDygWUO23
Ry\n8g==\n-----END CERTIFICATE-----\n","crl":"-----BEGIN X509 CRL-----
\nMIHJMHYCAQEwDAYIKoUDBwEBAwIFADATMREwDwYDVQQDEwh0ZXN0Q0EwMRcNMjEw\nMzEwMj
I0MjMzWhcNMjIwMzEwMjI0MjMzWqAwMC4wHwYDVR0jBBgwFoAUdT6jhEs0\n707uZjsCjB/9Ox
9kbbgwCwYDVR0UBAQCAhACMAwGCCqFAwcBAQMCBQADQQD5N47u\nbZZCUQpg+0uynYVeQeuDT1
UbZy/4Dxzt5aKK6o32H/hzQ/g7eA40ZCQF2UcqsnQK\nrUpR8Yi5oOFw5k9R\n-----END
X509 CRL-----\n"}
```

2) Отправить запрос токена с аутентификацией по сертификату тестового оператора (в параметре --cert указан идентификатор, зафиксированный на шаге 7 инструкции из Раздела 3.1):

```
/opt/cprocsp/bin/amd64/curl --verbose \
--request POST \
--header "Accept: application/json" \
--header "Content-type: application/json" \
--cert 1f4e4b4c0af7ad37c5d3aa6361656e7f4c60f30d \
--data '{"deviceid":"SCM-100-001-000000001"}' \
https://plumba/operator/token
```

В ответе сервера должен присутствовать токен доступа (token) и время жизни токена в секундах (tokenttl):

```
...
< HTTP/1.1 200
< Server: nginx/1.18.0
< Date: Fri, 09 Apr 2021 22:46:45 GMT
< Content-Type: application/json
< Transfer-Encoding: chunked
< Connection: keep-alive
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Cache-Control: no-cache, no-store, max-age=0, must-revalidate
< Pragma: no-cache
< Expires: 0
< X-Frame-Options: DENY
<
* Connection #0 to host plumba left intact
* Closing connection #0
{"token":"c76926d9-c5db-434b-b5a7-4c0de6979b87","tokenttl":600}
```

Зафиксировать значение токена из ответа сервера.

3) Отправить запрос вектора инициализации с аутентификацией по токену, полученному на предыдущем шаге (необходимо изменить значение X-Token в параметрах команды):

```
/opt/cprocsp/bin/amd64/curl --verbose \
--request POST \
--header "Accept: application/json" \
--header "Content-type: application/json" \
--header "X-Token: c76926d9-c5db-434b-b5a7-4c0de6979b87" \
https://plumba/device/init
```

Примечание: Перед отправкой команды в параметре --header необходимо указать действительное значение токена, полученного на шаге 2 настоящей инструкции. При этом необходимо учитывать и время жизни токена, по истечении которого токен удалится из БД и необходимо будет запрашивать новый. В случае, если время жизни токена истекло, и он удалился из БД, в ответ на запрос будет выдана ошибка авторизации 403:

```
...
< HTTP/1.1 403
< Server: nginx/1.18.0
< Date: Fri, 09 Apr 2021 22:57:45 GMT
< Content-Length: 0
< Connection: keep-alive
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Cache-Control: no-cache, no-store, max-age=0, must-revalidate
< Pragma: no-cache
< Expires: 0
< X-Frame-Options: DENY
<
* Connection #0 to host plumba left intact
* Closing connection #0
```

В ответе сервера должно присутствовать текущее время (time) и вектор инициализации (iv) длиной 32 (значение по умолчанию, заданное в конфигурации приложения):

```
...
< HTTP/1.1 200
< Server: nginx/1.18.0
```

```
< Date: Fri, 09 Apr 2021 22:59:47 GMT
< Content-Type: application/json
< Transfer-Encoding: chunked
< Connection: keep-alive
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Cache-Control: no-cache, no-store, max-age=0, must-revalidate
< Pragma: no-cache
< Expires: 0
< X-Frame-Options: DENY
<
* Connection #0 to host plumba left intact
* Closing connection #0
{"time":"2021-04-
10T01:59:47+03:00","iv":"12d588ce146e1f2676e259f5e31fc4477cce3c9eededa31e5
eb496840c64d4e0"}
```

Дополнительно можно отправить запрос вектора инициализации с указанием требуемого размера (ivsize) и аутентификацией по токену, полученному на шаге 2 настоящей инструкции:

```
/opt/cprocsp/bin/amd64/curl --verbose \
--request POST \
--header "Accept: application/json" \
--header "Content-type: application/json" \
--header "X-Token: c76926d9-c5db-434b-b5a7-4c0de6979b87" \
--data '{"ivsize":"128"}' \
https://plumba/device/init
```

В ответе сервера должно присутствовать текущее время (time) и вектор инициализации (iv) соответствующей длины:

```
...
< HTTP/1.1 200
< Server: nginx/1.18.0
< Date: Fri, 09 Apr 2021 23:02:02 GMT
< Content-Type: application/json
< Transfer-Encoding: chunked
< Connection: keep-alive
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Cache-Control: no-cache, no-store, max-age=0, must-revalidate
< Pragma: no-cache
```

```
< Expires: 0
< X-Frame-Options: DENY
<
* Connection #0 to host plumba left intact
* Closing connection #0
{"time":"2021-04-
10T02:02:02+03:00","iv":"4fae315bf5baed2cd67b77c1491952a380fbef75e9beaddb1
281804bfba8c816ee1d891b698e6dd9b17883df63752cdbefbadd6d9f4d0715669f507ac76
5207349cb2317ac58103a313a11d8111bd52ce451afca882551f654dc92bf7ef8da2f1b3a3
e36ba2b0f0b1054935f8664d1dc8b994b7b39c6b1ee439b1847059008c8"}
```

4) Отправить запрос на сертификат с аутентификацией по токену, полученному на шаге 2 настоящей инструкции:

```
/opt/cprocsp/bin/amd64/curl --verbose \
--request POST \
--header "Accept: application/json" \
--header "Content-type: application/json" \
--header "X-Token: c76926d9-c5db-434b-b5a7-4c0de6979b87" \
--data '{"csr":"-----BEGIN CERTIFICATE REQUEST-----
\nMIICQjCCAe8CAQAwNjELMAkGA1UEBhMCUlUxJzAlBgNVBAMMHlNDTS0xMDAtMDAx\nLTAwMD
AwMDAwMS1zZXJ2aWNlMDBmMB8GCCqFAwcBAQEBMBMGByqFAwICJAAGCCqF\nAwcBAQICA0MABE
CRQp7y6x35PyQBxdQfTNILa8UbMyZfAlnYMmQ2ur8pK+FslhIK\nrCdZWR50QePd7Py1AlsJBJ
5jIrAEdHiw40hAoIIBSDAaBgorBgEEAYI3DQIDMQwW\nCjYuMi45MjAwLjIwQwYJKwYBBAGCNx
UUMTYwNAIBBQwMbWFvUG93ZXJib29rDBBN\nQU9QT1dFUkJPT0tcbWFvDA9jcnlwdGNwLng2NC
5leGUwUwYJKoZIhvcNAQkOMUYw\nRDATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBA
MCBPAwHQYDVR0OBBYE\nFGUwDcOcb9qiOww0zvWEYC+9AA5EMIGPBgorBgEEAYI3DQICMYGAMH
4CAQEedgBD\nAHIAeQBwAHQAbwAtAFAAcgBvACAARwBPAFMAVAAgAFIAIAAzADQALgAxADAALQ
Ay\nADAAMQAyACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFMAZQByAHYAaQBj\nAGUA
IABQAHIAbwB2AGkAZABlAHIDAQAwCgYIKoUDBwEBAwIDQQABp+eGLgvmVyli\nQDm7f2xhPOqP
oUwHMkMcBm/UGI/saMim8mguMwFG09illaPFbCyCxV4lKL95vCSD\nVIB4t+da\n-----END
CERTIFICATE REQUEST-----"}' \
https://plumba/device/request
```

В ответе сервера должен присутствовать присвоенный идентификатор запроса (csrid) и минимальное время в секундах, через которое необходимо обращаться за изданным сертификатом (gettimeout):

```
...
< HTTP/1.1 200
< Server: nginx/1.18.0
< Date: Fri, 09 Apr 2021 23:14:13 GMT
< Content-Type: application/json
```

```
< Transfer-Encoding: chunked
< Connection: keep-alive
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Cache-Control: no-cache, no-store, max-age=0, must-revalidate
< Pragma: no-cache
< Expires: 0
< X-Frame-Options: DENY
<
* Connection #0 to host plumba left intact
* Closing connection #0
{"csrid":"d7dfa9b3-d088-4101-85a3-686cc4f58e1d","gettimeout":5}
```

Зафиксировать значение идентификатора из ответа сервера.

5) Отправить запрос на получение изданного сертификата с аутентификацией по токену, полученному на шаге 2 настоящей инструкции, и указанием идентификатора, полученного на предыдущем шаге:

```
/opt/cprocsp/bin/amd64/curl --verbose \
--request POST \
--header "Accept: application/json" \
--header "Content-type: application/json" \
--header "X-Token: c76926d9-c5db-434b-b5a7-4c0de6979b87" \
--data '{"csrid":"d7dfa9b3-d088-4101-85a3-686cc4f58e1d"}' \
https://plumba/device/get
```

В ответе сервера должен присутствовать изданный сертификат (crt):

```
...
< HTTP/1.1 200
< Server: nginx/1.18.0
< Date: Fri, 09 Apr 2021 23:17:37 GMT
< Content-Type: application/json
< Transfer-Encoding: chunked
< Connection: keep-alive
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Cache-Control: no-cache, no-store, max-age=0, must-revalidate
< Pragma: no-cache
< Expires: 0
< X-Frame-Options: DENY
<
```

```
* Connection #0 to host plumba left intact
* Closing connection #0
{"crt":"-----BEGIN CERTIFICATE-----
\nMIIBvjCCAWmgAwIBAgIBAzAMBggqhQMHAQEDAgUAMBMxETAPBgNVBAMTCHRlc3RD\nQTAxMB
4XDTIxMDQwOTIzMTQxNloXDTIyMDQwOTIzMTQxNlowNjELMAkGA1UEBhMC\nUlUxJzAlBgNVBA
MMHlNDTS0xMDAtMDAxLTAwMDAwMDAwMS1zZXJ2aWNlMDBmMB8G\nCCqFAwcBAQEBMBMGByqFAw
ICJAAGCCqFAwcBAQICA0MABECRQp7y6x35PyQBxdQf\nTNILa8UbMyZfAlnYMmQ2ur8pK+Fslh
IKrCdZWR50QePd7Py1AlsJBJ5jIrAEdHiw\n40hAo3wwejAJBgNVHRMEAjAAMB0GA1UdDgQWBB
RlMA3DnG/aojsMNM71hGAvvQAO\nRDAfBgNVHSMEGDAWgBR1PqOESzTvTu5mOwKMH/07H2RtuD
AOBgNVHQ8BAf8EBAMC\nA6gwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMBMAwGCCqFAw
cBAQMCBQAD\nQQCbT4oUSP1iq24EtYDFmK0EVcvwPTOSVVWuR51tuy3ZBa8qWxj1Q5LZfeFpHi
hb\npZuZjgs0nufnCjU0fXQU4CL8\n-----END CERTIFICATE-----\n"}
```

3 НАСТРОЙКА ПОДКЛЮЧЕНИЯ К КРИПТО-ПРО УЦ

Для настройки подключения к Крипто-Про УЦ и переключения приложения на издание сертификатов с его использованием необходимо:

1) Отредактировать системный файл /etc/hosts, добавив запись для Крипто-Про УЦ ЦР, к которому будет производиться подключение с использованием HTTP API:

```
…
[IP-Address] cpro-ra
```

2) Проверить доступность узла по портам 80 (CDP/AIA) и 443 (HTTP API):

```
telnet cpro-ra 80
telnet cpro-ra 443
```

3) Отредактировать и выполнить скрипт загрузки сертификата ЦС по ссылке AIA, указав в скрипте действительные значения:

```
/opt/plumba/cdp-aia/get-cert.sh
```

в результате должен появиться файл с сертификатом ЦС:

```
/opt/plumba/cdp-aia/cpro-ca.crt
```

4) Отредактировать и выполнить скрипт загрузки CRL ЦС по ссылке CDP, указав в скрипте действительные значения:

```
/opt/plumba/cdp-aia/get-crl.sh
```

в результате должен появиться файл с CRL ЦС:

```
/opt/plumba/cdp-aia/cpro-ca.crl
```

5) Распаковать ключевой контейнер API-клиента Крипто-Про УЦ в директорию ключевых контейнеров пользователя root Крипто-Про CSP:

```
unzip -d /var/opt/cprocsp/keys/root/ \
/opt/distrib/test-certs/apiuser.key.zip
```

после чего выполнить визуальную проверку параметров контейнера:

```
/opt/cprocsp/bin/amd64/csptest -keyset -info -container \
'\\.\HDIMAGE\CAUser'
```

6) Скопировать сертификат API-клиента в директорию конфигурации NGINX:

```
cp /opt/distrib/test-certs/apiuser.cert.pem /etc/nginx/
```

7) Отредактировать файл конфигурации NGINX:

```
vi /etc/nginx/nginx.conf
```

удалив знаки комментария # в начале соответствующих строк:

```
...
# Proxy to Crypto-Pro RA
#    server {
#        listen       488 default_server;
#        listen       [::]:488 default_server;
#        server_name  _;
#        location /CA/ {
#            proxy_pass https://cpro-ra/;
#            proxy_ssl_verify off;
#            proxy_ssl_certificate /etc/nginx/apiuser.cert.pem;
#            proxy_ssl_certificate_key engine:gostengy:c:CAUser;
#        }
#        location / {
#            proxy_pass http://[::1]:8888/;
#        }
#    }
```

8) Выполнить перезапуск сервиса NGINX:

```
systemctl restart nginx
```

9) Выполнить ревизию и при необходимости корректировку параметров работы модуля взаимодействия с Крипто-Про УЦ:

```
vi /opt/plumba/issue_cpro_config.py
```

в целях соответствия текущим параметрам подключения к Крипто-Про УЦ 2.0 через HTTP API (значения folderid и template):

```
container_name = "c:CAUser"
certificate = "/etc/nginx/apiuser.cert.pem"
folderid = "0867e43b-0bff-4255-bb39-ac1b00d6aca8"
template = "User"
csigner = "/opt/plumba/cpro-signer"

endpoint = "http://localhost:488/CA//RA/RegAuthLegacyService.svc"
num_retry = 5
```

10) Отредактировать файл конфигурации приложения:

```
vi /opt/plumba/application.yml
```

скрыв комментариями строки, соответствующие изданию сертификатов с использованием локального тестового ЦС и открыв ранее скрытые строки, соответствующие изданию сертификатов с использованием Крипто-Про УЦ:

```
plumba:
  issuer: /opt/plumba/issue-cpro.py
  CA: /opt/plumba/cdp-aia/cpro-ca.crt
  CRL: /opt/plumba/cdp-aia/cpro-ca.crl
  randomer: /opt/plumba/soboler.sh
#  randomer: /opt/plumba/randomer.sh
#  issuer: /opt/plumba/issue-localtest.sh
#  CA : /opt/plumba/testCA/certs/testCA01.cert.pem
#  CRL : /opt/plumba/testCA/crl/testCA01.crl.pem
  csrout: /opt/plumba/csr
  crtin: /opt/plumba/crt
  ivsize: 32
  tokenttl: 600
  gettimeout: 5
  serviceCrtMask: '^[0-9A-Z-]*-service[0-9]$'
...
```

11) Выполнить перезапуск Web-сервиса:

```
systemctl restart plumba
```

4 ПОРЯДОК ЭКСПЛУАТАЦИИ

При штатной эксплуатации ПО IT SM Сервер управления работает в автоматическом режиме.

При обнаружении последствий возможного несанкционированного доступа к ПО IT SM Сервер управления следует руководствоваться пунктом 3.7 настоящих правил.

5 ЗАПРЕЩЕННЫЕ ДЕЙСТВИЯ

При эксплуатации ПО IT SM Сервер управления, запрещается:

- использовать ПО IT SM Сервер управления, если выявлено нарушение целостности хотя бы одного из его компонентов;
- вносить какие-либо изменения в ПО;
- использовать криптографические ключи за пределами сроков действия;
- передавать ПО лицам, не допущенным к его использованию.

6 ВЫВОД ИЗ ЭКСПЛУАТАЦИИ

При выводе из эксплуатации ПО IT SM Сервер управления, следует выполнить полное форматирование жесткого диска ЭВМ-сервера.