

УТВЕРЖДЕН
РБ.МЕЯШ.11020-01 34 01-ЛУ

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

Приложение itTLSCln
РУКОВОДСТВО ОПЕРАТОРА

РБ.МЕЯШ.11020-01 34 01

(компакт-диск)

Листов 23

Минск 2023

Литера

АННОТАЦИЯ

Настоящий документ содержит руководство оператора приложения itTLSCln (РБ.МЕЯШ.11020-01), являющегося TLS-клиентом согласно СТБ 34.101.65. В документе приводится информация о назначении средства защиты транспортного уровня itTLSCln, установке, настройке и запуске itTLSCln, условиях выполнения сервисов и настройках среды, а также об ошибках, возникающих в процессе выполнения программы.

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ИОК – инфраструктура открытых ключей;

ОС – операционная система;

ПК – персональный компьютер;

ПО – программное обеспечение;

ПЭВМ – персональная электронно-вычислительная машина;

СКЗИ – средство криптографической защиты информации;

СОК – сертификат открытого ключа;

СОК – список отозванных сертификатов;

УЦ – удостоверяющий центр

СОДЕРЖАНИЕ

1	НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ	5
1.1	Функции.....	5
1.2	Уровень подготовки оператора	6
2	ПОДГОТОВКА К РАБОТЕ	7
2.1	Общее описание	7
2.2	Состав и содержание дистрибутивного носителя	7
2.3	Установка приложения itTLSCln	8
2.3.1	Установка приложения itTLSCln	8
2.3.2	Шаг 1: Распаковка файла-архива itTLSCln.....	8
2.3.3	Шаг 2: Настройка безопасности itTLSCln	9
2.4	Настройка системного прокси-сервера	13
2.4.1	Настройка системного прокси-сервера в ОС Windows	13
2.4.2	Настройка системного прокси-сервера в ОС Linux.....	14
3	ЗАПУСК ПРИЛОЖЕНИЯ itTLSCln.....	15
3.1	Запуск приложения itTLSCln на ОС Windows.....	15
3.2	Запуск приложения itTLSCln на ОС Linux	16
3.3	Самотестирование itTLSCln	17
4	УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ	19
5	НАСТРОЙКА СРЕДЫ	20
6	СООБЩЕНИЯ ОПЕРАТОРУ	22

1 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

Наименование программы: приложение itTLSCln (РБ.МЕЯШ.11020-01).

Обозначение программы: itTLSCln

Разработчик программы: ООО «ИТТАС».

Назначение программы: приложение itTLSCln предназначено для функционирования на персональном компьютере (ПК) с целью защиты соединений, устанавливаемых с серверными приложениями (серверами) на транспортном (коммуникационном) уровне по протоколу TLS согласно СТБ 34.101.65 с односторонней аутентификацией сервера перед клиентом (режим односторонней аутентификации). Приложение itTLSCln обеспечивает выполнение криптографических операций с использованием криптографического набора TLS_DHE_BIGN_WITH_BELT_CTR_MAC_HBELT, определенного в приложении В СТБ 34.101.65.

1.1 Функции

Применительно к созданию защищенного TLS-соединения между клиентом (приложение itTLSCln) и сервером (приложение itTLSCln), средство itTLSCln реализует следующие основные функциональные возможности:

- аутентификацию сервера перед клиентами с использованием сертификатов открытых ключей;
- шифрование и имитозащиту передаваемых между сервером и клиентами данных;
- контроль объема зашифрованных данных соединения с целью соблюдения квот ключей шифрования;
- контроль целостности файлов настроек и программ СКЗИ.

1.2 Уровень подготовки оператора

Оператор средства itTLSCln должен иметь опыт работы с персональным компьютером (далее - ПК) на базе операционных систем семейств Linux, Windows на уровне квалифицированного пользователя, а также иметь опыт работы с консольными приложениями.

Оператор должен ознакомиться с настоящим руководством и выполнить стандартные операции, описанные в разделе 2, а также обладать достаточным уровнем знаний в области технологии инфраструктуры открытых ключей.

2 ПОДГОТОВКА К РАБОТЕ

2.1 Общее описание

Вне зависимости от используемой операционной системы, процесс установки и запуска приложения itTLSCln включает в себя:

- установку приложения (п. 2.3.1);
- настройка системного прокси-сервера (п. 2.4);
- запуск приложения itTLSCln (п. 3).

2.2 Состав и содержание дистрибутивного носителя

Установочный пакет приложения itTLSCln включает в себя

`itTLSCln_x86_Ubuntu_Debian64.tar.gz`

Файл-архив: Содержит установочный комплект приложения itTLSCln для 64-х разрядной ОС Ubuntu 16 и выше и Debian 8 и выше и процессоров с архитектурой x86

`itTLSCln_x86_CentOS64.tar.gz`

Файл-архив: Содержит установочный комплект приложения itTLSCln для 64-х разрядной ОС CentOS версии 6 и выше и процессоров с архитектурой x86

`itTLSCln_windows.zip`

Файл-архив: Содержит установочный комплект приложения itTLSCln для 64-х разрядной Windows 10 и выше и процессоров с архитектурой x86

2.3 Установка приложения itTLSCln

2.3.1 Установка приложения itTLSCln

Процесс установки приложения itTLSCln на хост включает в себя следующие шаги:

Шаг 1: Распаковка файла-архива с itTLSCln;

Шаг 2: Настройка безопасности itTLSCln.

2.3.2 Шаг 1: Распаковка файла-архива itTLSCln

Пользователям ОС Windows после получения файла архива с itTLSCln необходимо скопировать данный файл на рабочее место пользователя и разархивировать его в любую директорию. Для разархивирования файла-архива с itTLSCln может быть использовано любое программное обеспечение, работающее с zip-архивом.

Пользователям ОС Linux необходимо создать директории:

```
mkdir /etc/ittlscli/  
mkdir /var/log/ittlscli/
```

Разархивировать архив с itTLSCln в директорию /etc/ittlscli/.

В директории /var/log/ittlscli/ создать файлы access.log и cache.log, дать все права доступа к этим файлам.

```
cd /var/log/ittlscli/  
touch access.log cache.log  
chmod 777 ./*
```

В директории /etc/ittlscli/ дать все права доступа к файлам ittlscli, log_file_daemon, security_file_certgen.


```
cd /etc/ittlscli/
touch ittlscli log_file_daemon security_file_certgen
```

В системах Red Hat Enterprise Linux необходимо создать пользователя proxy.

```
adduser proxy
```

2.3.3 Шаг 2: Настройка безопасности itTLSCln

Для работы приложения itTLSCln необходимо осуществить настройку безопасности itTLSCln, которая включает в себя установку и подключение атрибутов, необходимых для создания безопасного (шифрованного) соединения между itTLSSrv и itTLSCln. К таким атрибутам безопасности относятся:

- **СОК информационного ресурса:** файл технологического сертификата открытого ключа;

- **СОК УЦ:** сертификат открытого ключа удостоверяющего центра, выпустившего СОК информационного ресурса.

2.3.3.1 В рамках настройки безопасности itTLSCln, для ОС Windows, необходимо скопировать файл сертификата удостоверяющего центра, сгенерированного на этапе установки itTLSSrv (hash.0), по следующему пути относительно папки установки: usr/local/ssl/certs.

компьютер > Локальный диск (D:) > my_squid > usr > local > ssl > certs		
Имя	Дата изменения	Тип
8d2935e7.0	31.01.2023 18:17	Файл "0"
ca-bundle	02.04.2021 0:37	Сертификат безо...
ca-bundle.trust	02.04.2021 0:37	Сертификат безо...

Рисунок 2.1: Директория с сертификатами itTLSCln

Для ОС Linux необходимо скопировать файл сертификата удостоверяющего центра, сгенерированного на этапе установки itTLSSrv (hash.0), по следующему пути: /etc/ittlscli/certs/.

2.3.3.2 Указать список доменов, для которых itTLSCln должен генерировать сертификаты. Для этого заходим в папку etc/squid (относительный путь от папки распаковки для ОС Windows).

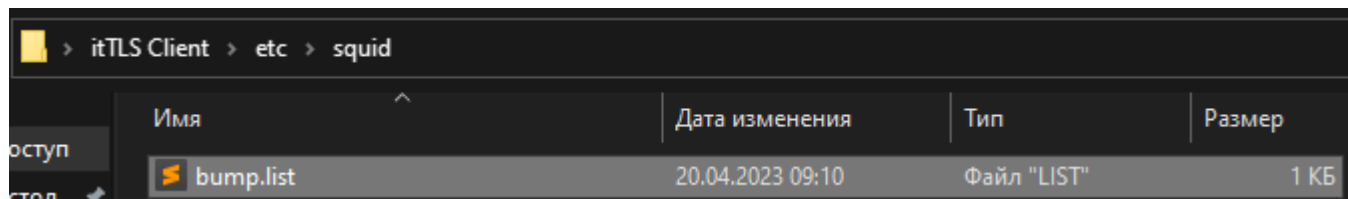
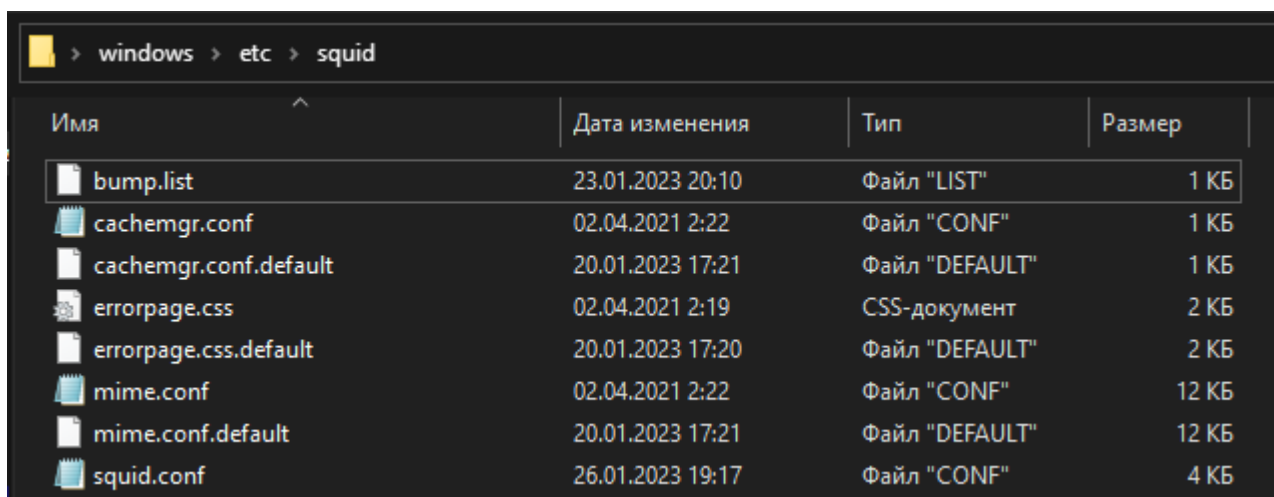


Рисунок 2.2: Директория с конфигурационными файлами

Для ОС Linux необходимо перейти в директорию /etc/ittlscli/certs.

Открываем файл «bump.list» для редактирования и добавляем доменные имена нужных ресурсов.

2.3.3.3 Настроить конфигурационный файл itTLSCln. По умолчанию itTLSCln работает в виде шлюза. В этом случае, устройства, находящиеся в одной подсети с хостом itTLSCln, могут использовать хост itTLSCln в качестве прокси сервера. Если необходимо, чтобы другие устройства не могли использовать itTLSCln в качестве шлюза, необходимо изменить конфигурационный файл. Для этого заходим в папку etc/squid (относительный путь от папки распаковки для ОС Windows). Пользователям ОС Linux необходимо перейти в директорию /etc/ittlscli/.



Имя	Дата изменения	Тип	Размер
bump.list	23.01.2023 20:10	Файл "LIST"	1 КБ
cachemgr.conf	02.04.2021 2:22	Файл "CONF"	1 КБ
cachemgr.conf.default	20.01.2023 17:21	Файл "DEFAULT"	1 КБ
errorpage.css	02.04.2021 2:19	CSS-документ	2 КБ
errorpage.css.default	20.01.2023 17:20	Файл "DEFAULT"	2 КБ
mime.conf	02.04.2021 2:22	Файл "CONF"	12 КБ
mime.conf.default	20.01.2023 17:21	Файл "DEFAULT"	12 КБ
squid.conf	26.01.2023 19:17	Файл "CONF"	4 КБ

Рисунок 2.3: Директория с конфигурационными файлами

Используя любой текстовый редактор, открываем конфигурационный файл «squid.conf», изменяем параметр порт (3128) на локальный IP-адрес:порт (127.0.0.1:3128).

```
http_port 127.0.0.1:3128 ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=8MB cert=/usr/local/ssl/squidCA.pem
sslcrtd_program /bin/security_file_certgen.exe -s /var/cache/squid/ssldb -M 8MB
#tls_outgoing_options flags=DONT_VERIFY_DOMAIN
```

Рисунок 2.4: Часть конфигурационного файла

Для настройки используемого DNS сервера, необходимо открыть конфигурационный файл «squid.conf» и изменить строку dns_nameservers.

```
dns_nameservers 8.8.8.8
```

Рисунок 2.5: Часть конфигурационного файла

2.3.3.4 Пользователям ОС Windows и Linux необходимо произвести импорт сертификата удостоверяющего центра, сгенерированного на хосте с установленным **squid** (самоподписанный), в браузер клиента. Пользователю ОС Windows необходимо зайти в папку `usr/local/ssl` (относительный путь от папки распаковки). Пользователю ОС Linux необходимо зайти в директорию `/etc/ittlscli/certs`. Далее необходимо найти файл «squidCA.pem» и сделать его копию.

Этот компьютер > Локальный диск (D:) > my_squid > usr > local > ssl			
Имя	Дата изменения	Тип	Размер
certs	31.01.2023 19:14	Папка с файлами	
cert.pem	02.04.2021 0:37	Файл "PEM"	215 КБ
openssl.cnf	31.01.2023 15:30	Файл "CNF"	1 КБ
squidCA.pem	11.01.2023 17:18	Файл "PEM"	4 КБ

Рисунок 2.6: Директория с сертификатом для браузера

Открываем копию файла сертификата браузера на редактирование (при помощи блокнота) и удаляем блок данных, относящийся к «PRIVATE KEY», и сохраняем файл под именем «squid-ca.crt».

Этот компьютер > Локальный диск (D:) > my_squid > usr > local > ssl			
Имя	Дата изменения	Тип	Размер
certs	31.01.2023 19:14	Папка с файлами	
cert	02.04.2021 0:37	Файл "PEM"	215 КБ
openssl.cnf	31.01.2023 15:30	Файл "CNF"	1 КБ
<u>squid-ca</u>	30.01.2023 17:58	Сертификат безо...	2 КБ
squidCA	11.01.2023 17:18	Файл "PEM"	4 КБ

Рисунок 2.7: Сертификат для браузера

Данный файл необходимо импортировать в систему на стороне клиента, иначе, при вводе url (в данном примере <https://www.ittas.by>) в адресной строке браузера, будет отображаться сообщение «Ошибка нарушения конфиденциальности». Импорт сертификата разберем на примере браузера Google Chrome.

Откройте настройки браузера, перейдите в раздел Конфиденциальность и безопасность, пункт Безопасность, Настроить сертификаты.

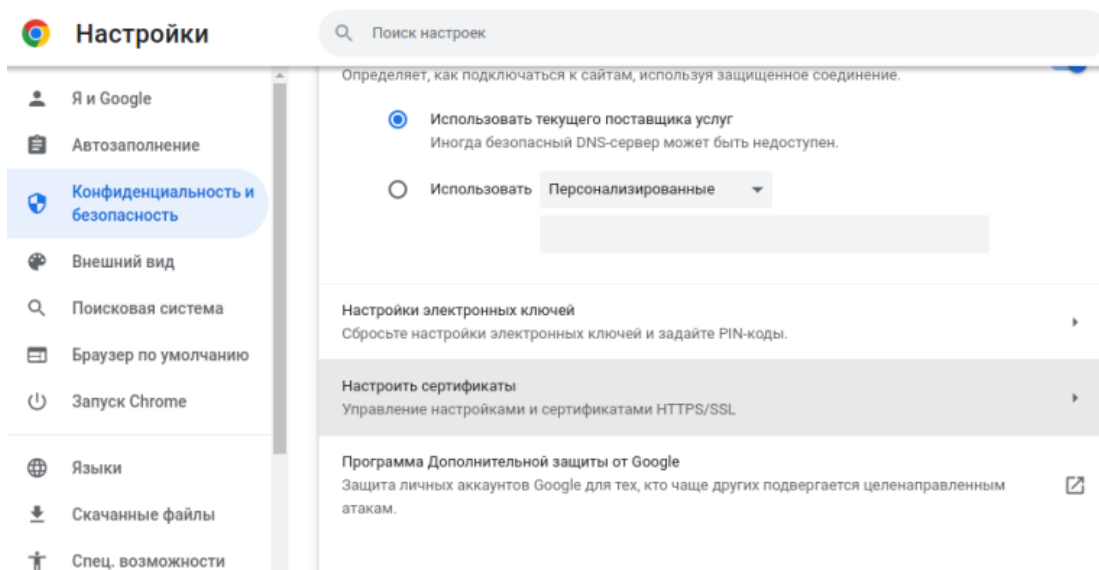


Рисунок 2.8: Управление сертификатами

Перейдите во вкладку Центры сертификации, нажмите кнопку Импорт и выберите сертификат `squid-ca.crt`. После этого появится окно, в котором необходимо выбрать 1 пункт.

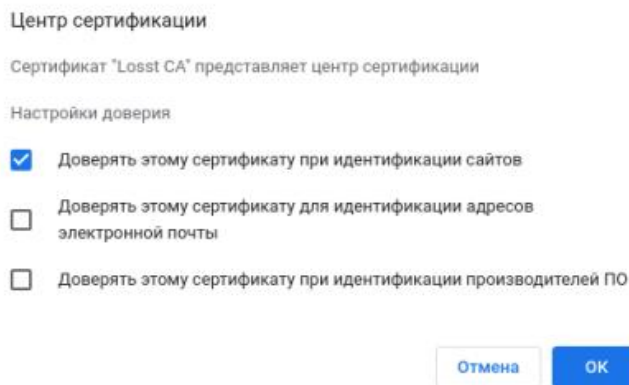


Рисунок 2.9: Настройки доверия

После этого сертификат добавится в хранилище данного браузера.

2.4 Настройка системного прокси-сервера

2.4.1 Настройка системного прокси-сервера в ОС Windows

2.4.1.1 Нажмите кнопку Пуск, затем выберите Параметры > Сеть и Интернет > Proxy.

2.4.1.2 В разделе Настройка прокси-сервера вручную включите функцию «Использовать прокси-сервер» и отключите «Автоматическое определение параметров».

2.4.1.3 В полях Адрес и Порт введите имя localhost и порт 3128 соответственно и нажмите Сохранить.

ВНИМАНИЕ:



Firefox умеет использовать как глобальные настройки, так и свои собственные. Для того чтобы назначить ему прокси, откройте его окно настроек, перейдите на вкладку «Дополнительно», далее на вкладку «Сеть» и нажмите на кнопку «Настроить» напротив надписи «Настройка параметров соединения Firefox с Интернетом».

2.4.2 *Настройка системного прокси-сервера в ОС Linux*

2.4.2.1 Для того чтобы настроить прокси в ОС Linux с графическим интерфейсом откройте «Системные параметры», перейдите в пункт «Сеть». Выберите пункт «Сетевая прокси-служба». Смените метод на «вручную» и введите настройки прокси: имя localhost и порт 3128.

3 ЗАПУСК ПРИЛОЖЕНИЯ itTLSCln

3.1 Запуск приложения itTLSCln на ОС Windows

1. Для запуска приложения itTLSCln необходимо открыть командную строку в рабочей директории приложения.

2. Перейти в директорию bin/:

```
cd bin/
```

3. Выполнить команду:

```
ittlscli.exe -N -d1
```

где:

N: Запуск основного процесса;

d1: Уровень детализации журнала событий.

4. Параметры запуска приложения itTLSCln можно посмотреть путем вывода команды:

```
ittlscli.exe -h
```

```
-h | --help      Print help message.
-v | --version   Print version details.

-a port    Specify HTTP port number (default: 3128).
-d level   Write debugging to stderr also.
-f file     Use given config-file instead of
            /etc/squid/squid.conf
-k reconfigure|rotate|shutdown|restart|interrupt|kill|debug|check|parse
            Parse configuration file, then send signal to
            running copy (except -k parse) and exit.
-n name     Specify service name to use for service operations
            default is: squid.
-s | -l facility
            Enable logging to syslog.
-u port     Specify ICP port number (default: 3130), disable with 0.
-z          Create missing swap directories and then exit.
-C          Do not catch fatal signals.
-D          OBSOLETE. Scheduled for removal.
-F          Don't serve any requests until store is rebuilt.
-N          Master process runs in foreground and is a worker. No kids.
--foreground
            Master process runs in foreground and creates worker kids.
--self-test
            Run self-test.
--kid role-ID
            Play a given SMP kid process role, with a given ID. Do not use
            this option. It is meant for the master process use only.
-R          Do not set REUSEADDR on port.
-S          Double-check swap during rebuild.
-X          Force full debugging.
-Y          Only return UDP_HIT or UDP_MISS_NOFETCH during fast reload.
```

Рисунок 3.1: Перечень команд запуска приложения itTLSCln

3.2 Запуск приложения itTLSCln на ОС Linux

1. Для запуска приложения itTLSCln необходимо открыть терминал в рабочей директории приложения.
2. Перейти в директорию /etc/ittlscli/:

```
cd /etc/ittlscli/
```

3. Выполнить команду:

```
./ittlscli -N -d1
```

где:

N: Запуск основного процесса;

d1: Уровень детализации журнала событий.

4. Параметры запуска приложения itTLSCln можно посмотреть путем вывода команды:

```
./ittlscli -h
```

```
-h | --help      Print help message.
-v | --version   Print version details.

-a port        Specify HTTP port number (default: 3128).
-d level       Write debugging to stderr also.
-f file        Use given config-file instead of
               /etc/squid/squid.conf
-k reconfigure|rotate|shutdown|restart|interrupt|kill|debug|check|parse
               Parse configuration file, then send signal to
               running copy (except -k parse) and exit.
-n name        Specify service name to use for service operations
               default is: squid.
-s | -l facility
               Enable logging to syslog.
-u port        Specify ICP port number (default: 3130), disable with 0.
-z            Create missing swap directories and then exit.
-C            Do not catch fatal signals.
-D            OBSOLETE. Scheduled for removal.
-F            Don't serve any requests until store is rebuilt.
-N            Master process runs in foreground and is a worker. No kids.
--foreground   Master process runs in foreground and creates worker kids.
--self-test    Run self-test.
--kid role-ID  Play a given SMP kid process role, with a given ID. Do not use
               this option. It is meant for the master process use only.
-R            Do not set REUSEADDR on port.
-S            Double-check swap during rebuild.
-X            Force full debugging.
-Y            Only return UDP_HIT or UDP_MISS_NOFETCH during fast reload.
```

Рисунок 3.2: Перечень команд запуска приложения itTLSCln

3.3 Самотестирование itTLSCln

При каждом запуске itTLSCln выполняется самотестирование, включающее:

- контроль целостности файлов программ, настроек и долговременных системных объектов;
- тесты криптографических алгоритмов, основанные на сравнении результата криптографического преобразования с эталонным значением, а также на выполнении прямого и обратного криптографического преобразования;
- статистическое тестирование источников случайности.

Дополнительно, при тестировании itTLSCln по команде оператора, Оператору отображаются имена файлов программ itTLSCln, для которых выполняется контроль целостности, вместе с их контрольными характеристиками (хэш-значениями согласно СТБ 34.101.31).

При обнаружении нарушения контроля целостности программ и при ошибках тестирования криптографических алгоритмов производится завершение работы itTLSCln с выводом соответствующего сообщения об ошибке.

Для проведения самотестирования приложения в ручном режиме на ОС Linux, в рабочей директории приложения itTLSCln /etc/ittlscli/ выполнить команду:

```
./ittlscli --self-test
```

Для проведения самотестирования приложения в ручном режиме на ОС Windows, в рабочей директории приложения itTLSCln выполнить команду:

```
ittlscli.exe --self-test
```

4 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

Приложение itTLSCln функционирует под управлением 64-разрядной ОС семейства Linux: Ubuntu версии 16 и выше, Debian 8 и выше, CentOS 6 и выше, а так же под управлением ОС семейства Windows версии 10 и выше.

Клиенты должны иметь сертификаты открытого ключа (СОК), а также иметь доступ к актуальному списку отозванных сертификатов, издаваемому удостоверяющим центром (УЦ) инфраструктуры открытых ключей (ИОК) для проверки действительности сертификатов клиента.

Все клиенты должны быть участниками одной ИОК или разных ИОК, доверие к сертификатам которых поддерживается в ИОК сервера. При этом должна быть обеспечена совместимость ИОК по форматам и содержимому СОК и СОС, а также доступность актуальных СОС внешних ИОК для сервера.

Технические характеристики ПЭВМ должны соответствовать требованиям используемой ОС. Кроме того, рекомендуется иметь в наличии не менее 60 мегабайт свободного места на жёстком диске для установки и использования itTLSCln.

5 НАСТРОЙКА СРЕДЫ

Перед установкой программ itTLSCln системный администратор настраивает специальную группу операционной системы, соответствующую роли администратора itTLSCln. Настройка осуществляется таким образом, что установка программ itTLSCln и полный доступ (доступ на чтение, запись, удаление файлов/папок и выполнение программ) к папкам с программами и данными itTLSCln разрешена только членам этой группы и системному администратору.

Системный администратор должен убедиться, что для остальных групп операционной системы (не соответствующих роли администратора itTLSCln) любой доступ к папкам с программами и данными itTLSCln запрещен.

Системный администратор настраивает политику управления паролями и политику блокировки учетных записей пользователей компьютера. Дополнительно системный администратор настраивает, средства защиты рабочего места администратора, включая средства защиты от вредоносных программ.

Для защиты рабочего места администратора применяются следующие средства:

- Средства и методы безопасности, встроенные в саму операционную систему. В качестве реализации данного метода можно предложить использовать принцип предоставления наименьших полномочий в системе.
- Антивирусное программное обеспечение, с установленными актуальными базами данных вредоносных программ.
- Персональные межсетевые экраны.
- Файлы сертификатов только доверенных удостоверяющих центров.

Использование принципа предоставления наименьших полномочий в системе достигается за счет соблюдения нескольких правил:

-
- Ограниченные привилегии. Пользователи допускаются к работе в системе только с ограниченными привилегиями.
 - Уровень доступа пользователей к исполняемым модулям любых программ ограничивается Чтением. Право Записи допускается только в те папки и файлы, где это действительно необходимо.
 - Разрешается запускать программы только из заранее составленного списка, всё остальное должно блокироваться.
 - Обновления безопасности должны своевременно устанавливаться как для самой операционной системы, так и для связанных с ней компонентов, а также производственных программ.
 - Политики безопасности. Параметры системы «по умолчанию» не всегда безопасны. Для повышения уровня защиты необходима детальная настройка политик безопасности компьютера.

6 СООБЩЕНИЯ ОПЕРАТОРУ

1. Сообщение об успешном выполнении операции тестирования «**SUCCESS: selftest passed**».

2. Сообщение о выполнении операции тестирования с ошибками «**ERROR: hash test failed**».

Решение: перезапустить приложение и снова выполнить операцию тестирования. Если ошибка появляется снова, выполнить переустановку программы.

