**РЕСПУБЛИКАНСКОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ**

**«НАЦИОНАЛЬНЫЙ ЦЕНТР ЭЛЕКТРОННЫХ УСЛУГ»**

**ИНСТРУКЦИЯ**

**по установке и настройке доступа к мСМДО**

Минск 2023

Оглавление

[1. Введение 3](#_Toc125019126)

[2. Нормативные ссылки 4](#_Toc125019127)

[3. Обозначения и сокращения 5](#_Toc125019128)

[4. Условия выполнения программ 6](#_Toc125019129)

[4.1 Программное обеспечение 6](#_Toc125019130)

[4.2 Аппаратное обеспечение 6](#_Toc125019131)

[5. Порядок установки и настройки «GsecTLS» клиент 7](#_Toc125019132)

[5.1 Порядок установки «GsecTLS» клиент 7](#_Toc125019133)

[5.2 Настройка подключения посредством скрипта 9](#_Toc125019134)

[5.5. Дополнительные настройки в системе 10](#_Toc125019135)

[6. Проверка доступа 10](#_Toc125019136)

[6.1. Проверка доступа на тестовую страницу сайт 10](#_Toc125019137)

[6.2. Проверка доступа на API мСМДО 11](#_Toc125019138)

[Приложение 1 13](#_Toc125019139)

[Порядок ручной настройки «GsecTLS» клиент 13](#_Toc125019140)

# 1. Введение

Данная инструкция описывает порядок настройки доступа для взаимодействия с мСМДО.

«GsecTLS» клиент предназначен для обеспечения функций криптографической защиты информации и аутентификации сторон при их взаимодействии в информационной системе организации с применением алгоритмов электронной цифровой подписи в соответствии с СТБ 34.101.45-2013

Для пользователей СЭД использующих «Приложение СЭД АИС МВ» из состава автоматизированной информационной системы межведомственное взаимодействие посредством личного кабинета модернизированной ОАИС необходима установка и настройка «GsecTLS» клиент и Клиентского приложения для работы с идентификационной картой (КП).

«GsecTLS» клиент представляет собой программное обеспечение, выполняющего функции локального обратного прокси-сервера, а именно принимает запросы на локальном интерфейсе по заданным портам и перенаправляет их на конечный сервис через «GsecTLS» сервер с использованием протокола защиты транспортного уровня TLS «GsecTLS» согласно СТБ 34.101.65-2014.

КП предназначена для взаимодействия пользователя с Единой системой идентификации физических и юридических лиц (ЕС ИФЮЛ), предназначенной для предоставления информационным системам различных государственных органов и иных организаций Республики Беларусь сервиса идентификации и аутентификации, электронной цифровой подписи (ЭЦП) и информационной системы (ИС).

# 2. Нормативные ссылки

Настоящая Инструкция разработана в соответствии с требованиями следующих нормативных правовых и технических нормативных правовых актов, а также локальных распорядительных документов НЦЭУ:

* Указ Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации»;
* Закон Республики Беларусь от 10.11.2008 г. № 455‑З «Об информации, информатизации и защите информации»;

- СТБ.34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности»;

- СТБ.34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»;

- СТБ.34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых»;

- СТБ.34.101.65-2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)»;

- СТБ.34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел»;

# 3. Обозначения и сокращения

В настоящей Инструкции используются следующие обозначения и сокращения:

|  |  |  |
| --- | --- | --- |
| ИБ | – | информационная безопасность; |
| ОЗУ | – | оперативное запоминающее устройство; |
| ОС | – | операционная система; |
| ПЭВМ | ‒ | персональная электронно-вычислительная машина; |
| СКЗИ | – | средства криптографической защиты информации; |
| СОС | – | список отозванных сертификатов |
|  |  |  |

«GsecTLS» клиент предназначен для обеспечения функций криптографической защиты информации. Шифрованию подлежит канал связи между сервером ВСЭД организации и НЦЭУ.

Клиентское приложение «GSecTLS» устанавливается на сервер ВСЭД при следующих условиях:

- сервер ВСЭД расположен в инфраструктуре организации, количество пользователей, работающих в ВСЭД не превышает 15;

- в организации незначительный объем трафика (до 100 писем в месяц).

# 4. Условия выполнения программ

## 4.1 Программное обеспечение

Программное обеспечение «GsecTLS» клиент предназначен для работы на ПЭВМ, под управлением следующих ОС:

а) Операционная система Windows

– Windows 8 x32/64;

– Windows 10 x32/64.

## 4.2 Аппаратное обеспечение

Программа реализации защищенного взаимодействия должна эксплуатироваться на ПЭВМ и устройствах со следующими техническими характеристиками:

– тактовая частота процессора не менее 2 ГГц;

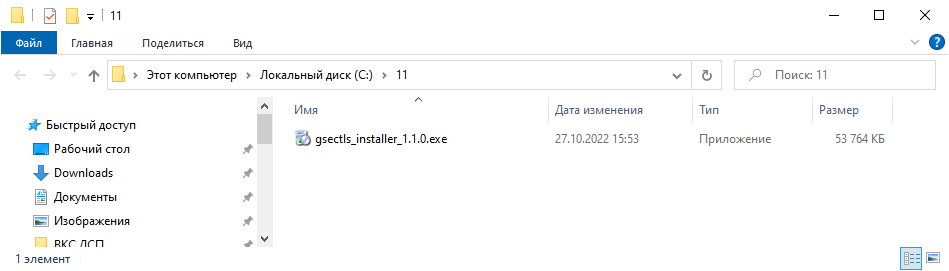
– объем ОЗУ не менее 2 Гб;

– объем памяти на жестком диске не менее 100 Мб.

# 5. Порядок установки и настройки «GsecTLS» клиент

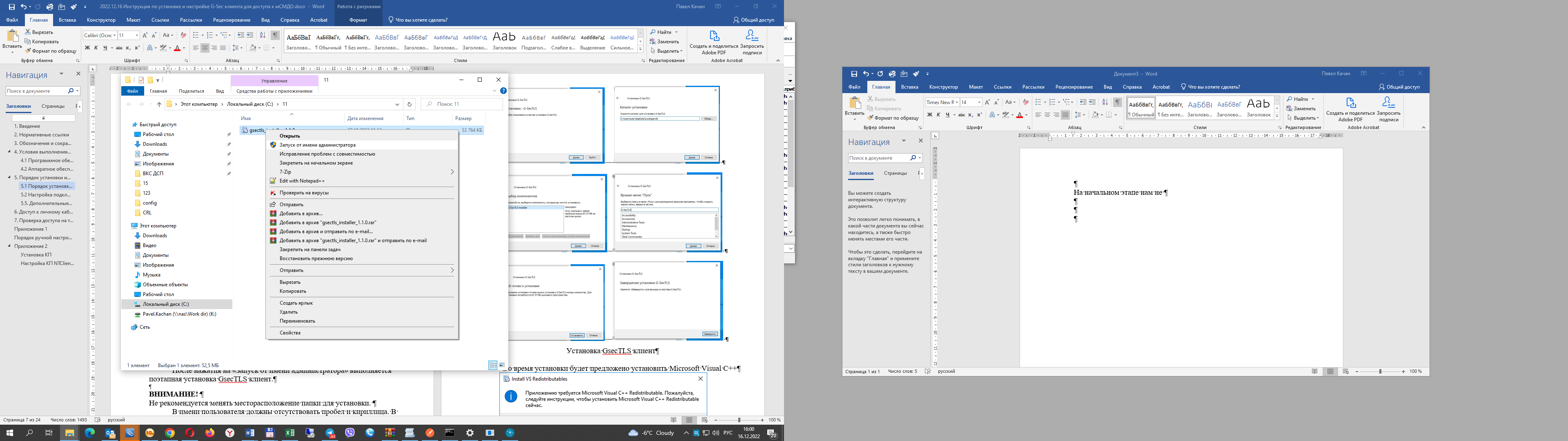
## 5.1 Порядок установки «GsecTLS» клиент

Для установки клиента GsecTLS необходимо загрузить дистрибутив GsecTLS клиента на персональный компьютер (далее – ПК).



Загрузка дистрибутива GsecTLS клиента

Нажав правой кнопкой мыши на загруженное приложение, выбрать «Запуск от имени администратора» и запустить его, кликнув левой кнопкой мыши.



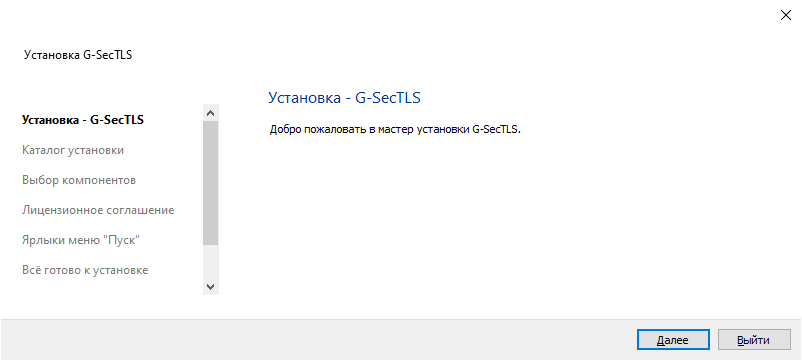
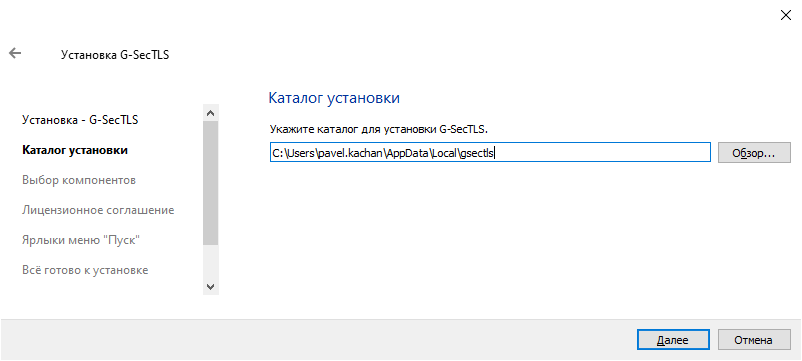
Запуск приложения

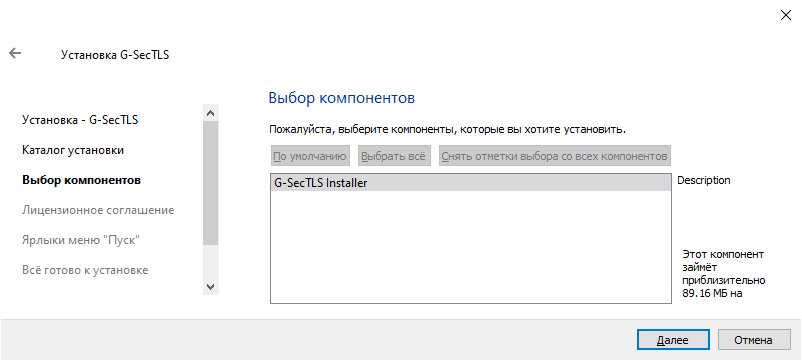
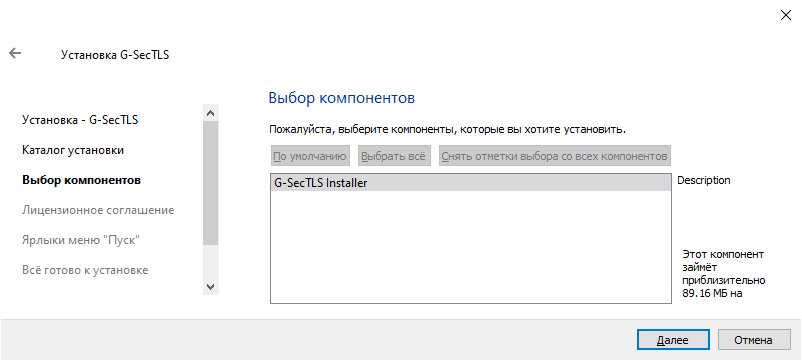
После нажатия на «Запуск от имени администратора» выполняется поэтапная установка GsecTLS клиент.

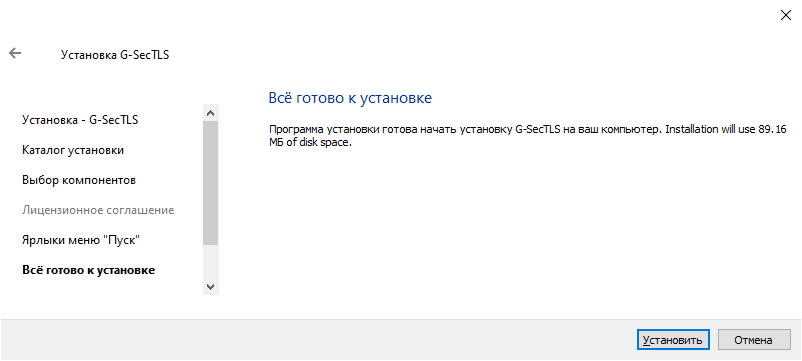
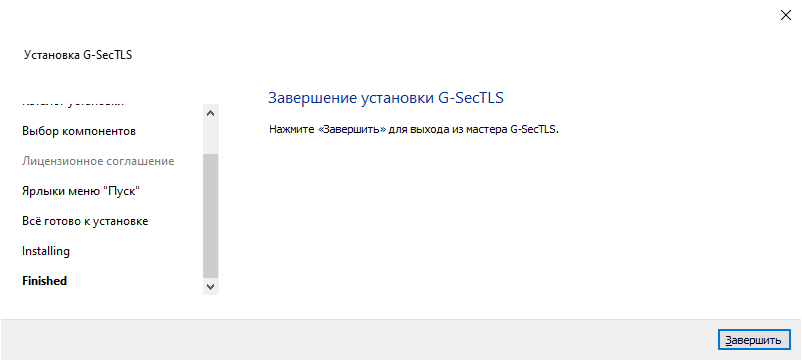
**ВНИМАНИЕ!**

Не рекомендуется менять месторасположение папки для установки.

В пути должны отсутствовать пробел и кириллица. В случае, если в пути присутствуют пробел и кириллица пользователю необходимо установить в доступную папку (например, создать папку c:\gsectls) и произвести настройку ПО в ручном режиме в соответствии с порядком установки и настройки GsecTLS (Приложение 1).

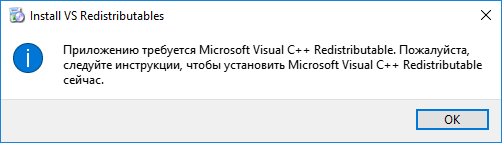
 

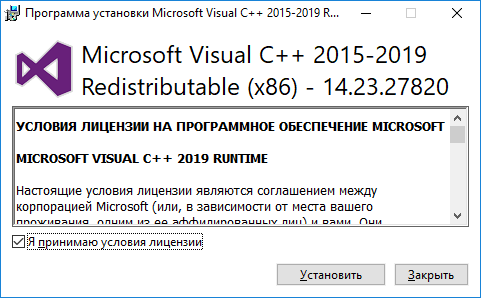
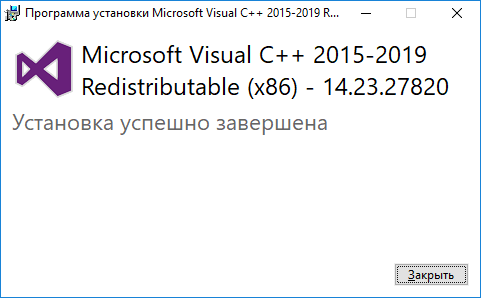
 

Установка GsecTLS клиент

Во время установки может быть предложено установить Microsoft Visual C++



После завершения установки GsecTLS клиент необходимо запустить ярлык GsecTLS на рабочем столе.



Ярлык GsecTLS клиента

Установка завершена. Для начала настройки необходимо запустить установленный «GsecTLS» клиент.



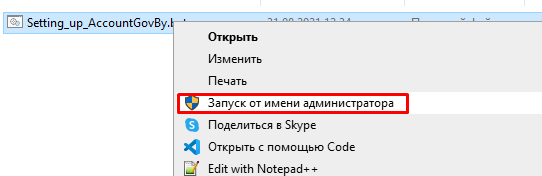
GsecTLS клиент

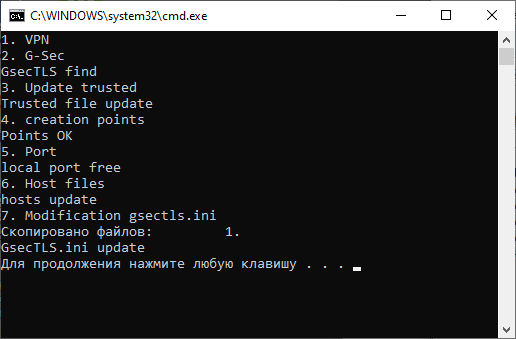
## 5.2 Настройка подключения посредством скрипта

Для автоматической настройки GsecTLS необходимо использовать скрипт в зависимости от типа подключения.

|  |  |
| --- | --- |
| Способ подключения | Имя исполняемого файла |
| Internet | mSMDO\_Inter.bat |
| VPN через БОТ | mSMDO\_BOT.bat |
| VPN через БФТ | mSMDO\_BFT.bat |
| VPN через БТК и другие | mSMDO\_VPN.bat |

Для корректной отработки скрипта следует запустить от имени администратора





запуск и отработка скрипта

В случае возникновения ошибок, либо невозможности настройки «GsecTLS» клиент с использованием скрипта, необходимо произвести настройку ПО в ручном режиме в соответствии с порядком установки и настройки GsecTLS (Приложение 1).

## 5.5. Дополнительные настройки в системе

В антивирусной программе нужно добавить в доверенные домены *account.gov.by, is.gov.by, esiful-idp.gov.by, gv.gov.by, esiful.gov.by*

На ПК необходимо проверить настройки даты/ времени и часового пояса. Часовой пояс должен быть +3 Минск, дата и время актуальные, должна быть установлена галочка "Синхронизация времени в Интернете"

# 6. Проверка доступа

## 6.1. Проверка доступа на тестовую страницу сайт

Запускаем «GsecTLS» далее – на кнопку «Запуск», выполняется запуск GsecTLS

Для перехода к тестовой странице в браузере необходимо набрать

http://127.0.0.1:9080

Переходите на тестовый сайт



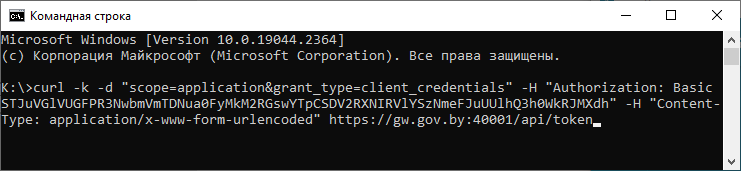
## 6.2. Проверка доступа на API мСМДО

Проверка выполняется в два этапа, сначала получаем токен доступа, потом используя токен доступа проверяем доступ к API мСМДО

**Этап 1.**

Для получения токена делаем запрос в командной строке:

*curl -k -d "scope=application&grant\_type=client\_credentials" -H "Authorization: Basic STJuVGlVUGFPR3NwbmVmTDNua0FyMkM2RGswYTpCSDV2RXNIRVlYSzNmeFJuUUlhQ3h0WkRJMXdh" -H "Content-Type: application/x-www-form-urlencoded" https://gw.gov.by:40001/api/token*



В ответ, на запрос будет получен json объект вида:

*{"access\_token":"b109d1da-0bd6-324d-a96c-75ca662c0dcf","scope":"application","token\_type":"Bearer","expires\_in":3453}*

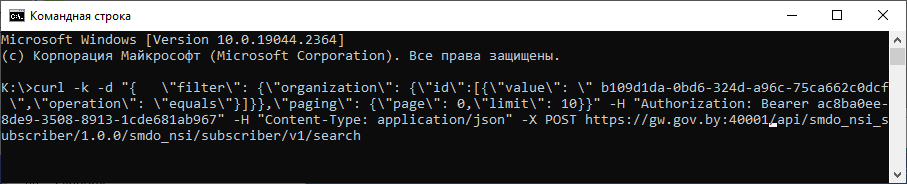
Срок действия токена 1 час.

**Этап 2.**

Выполняем запрос

*curl -k -d "{ \"filter\": {\"organization\": {\"id\":[{\"value\": \"055ef52c-d037-4202-bc15-fd1f35f293a8\",\"operation\": \"equals\"}]}},\"paging\": {\"page\": 0,\"limit\": 10}}" -H "Authorization: Bearer <****access\_token>****" -H "Content-Type: application/json" -X POST https://gw.gov.by:40001/api/smdo\_nsi\_subscriber/1.0.0/smdo\_nsi/subscriber/v1/search*

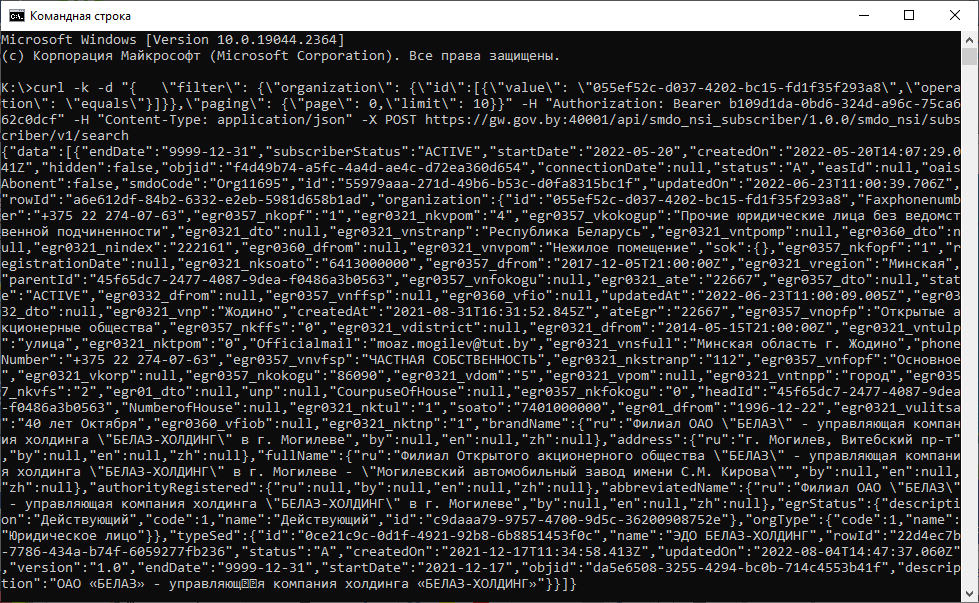
подставив значение *access\_token* из предыдущего ответа



***Пример:***

*curl -k -d "{ \"filter\": {\"organization\": {\"id\":[{\"value\": \"055ef52c-d037-4202-bc15-fd1f35f293a8\",\"operation\": \"equals\"}]}},\"paging\": {\"page\": 0,\"limit\": 10}}" -H "Authorization: Bearer b109d1da-0bd6-324d-a96c-75ca662c0dcf" -H "Content-Type: application/json" -X POST https://gw.gov.by:40001/api/smdo\_nsi\_subscriber/1.0.0/smdo\_nsi/subscriber/v1/search*

При корректном доступе в ответ получим список вида

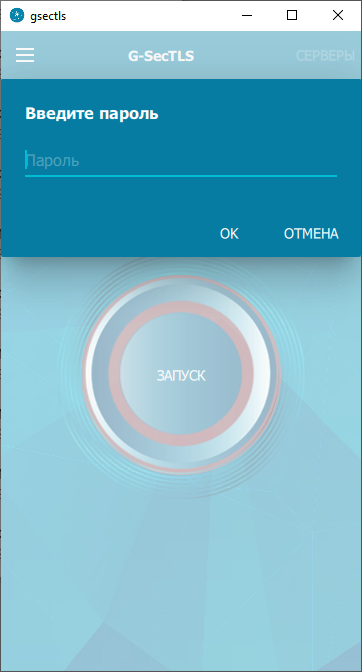


# Приложение 1

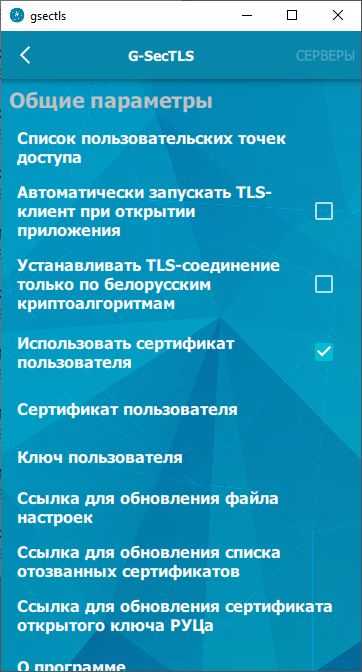
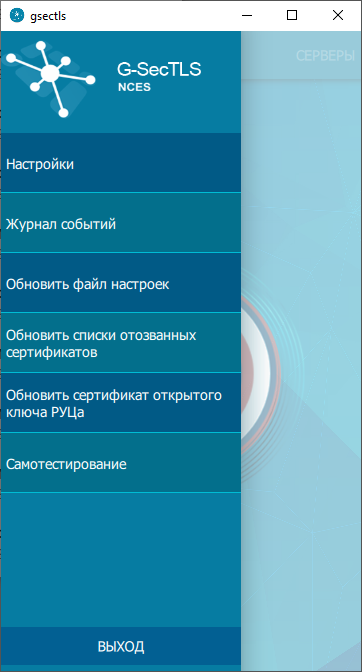
# Порядок ручной настройки «GsecTLS» клиент

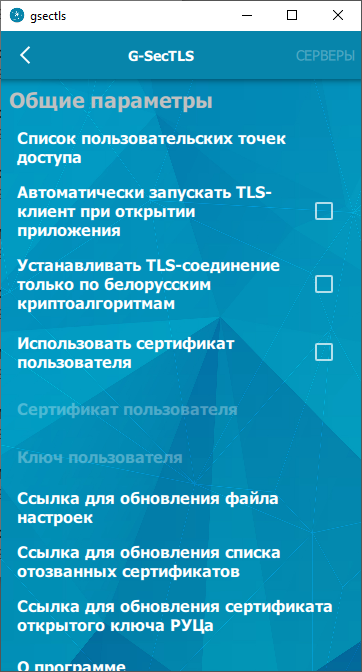
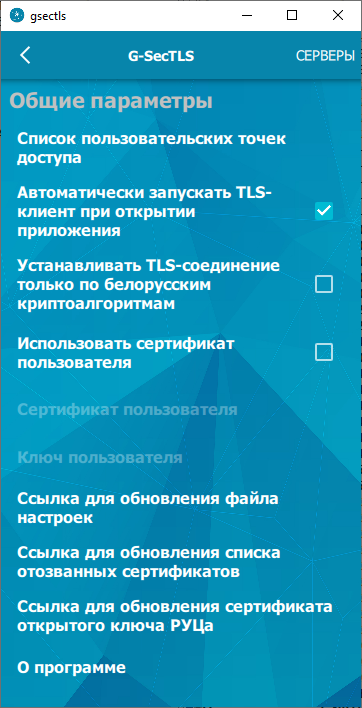
После выполнения установки «GsecTLS» клиент в соответствии с п. 5.1 Инструкции необходимо осуществить настройку точки подключения.

При первом запуске может появиться сообщение о необходимости введения пароля



Для этого необходимо в открывшемся окне зайти в верхнем левом углу в меню , прейти в «Настройки» и снять галочку «использовать сертификат пользователя». Для автоматического запуска точек доступа можно установить галочку «Автоматически запускать TLS-клиент при открытии приложения»



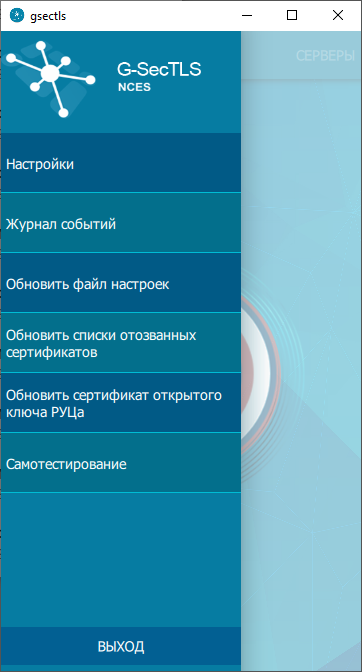
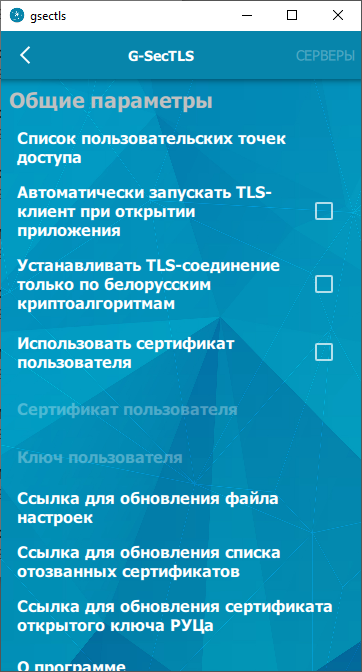
 

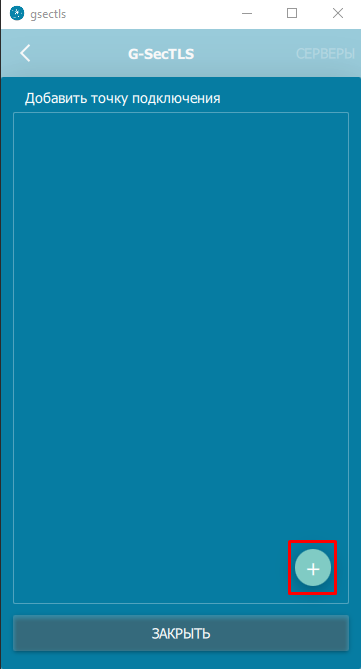
После запуска программы необходимо настроить точки подключения. Для этого необходимо в открывшемся окне зайти в верхнем левом углу в меню .



Пункт меню «GsecTLS» клиент

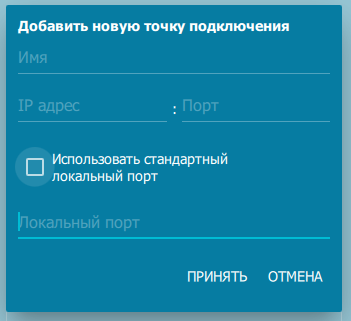
Выбрать «Настройки -> Список пользовательских точек доступа» и нажать в нижнем правом углу на .



Настройка точки подключения

В открывшемся окне необходимо ввести данные точки подключения.



Добавление точки подключения

Для подключения к личному кабинету, требуется настроить три точки подключения со следующими атрибутами:

В соответствии от провайдера используются следующие IP адреса:

Internet – 185.227.96.96

VPN от БОТ – 10.252.0.35

VPN от БФТ – 10.53.8.35

VPN от БТК и другие – 10.101.1.35

**Имя**: AISMVprod.GsecTLS.nces

**IP адрес**: <IP адрес провайдера>

**Порт**: 11001

**Локальный** **порт**: 40001

Повторить создание второй точки

**Имя**: AISMVdev.GsecTLS.nces

**IP** **адрес**: <IP адрес провайдера>

**Порт**: 11002

**Локальный** **порт**: 40002

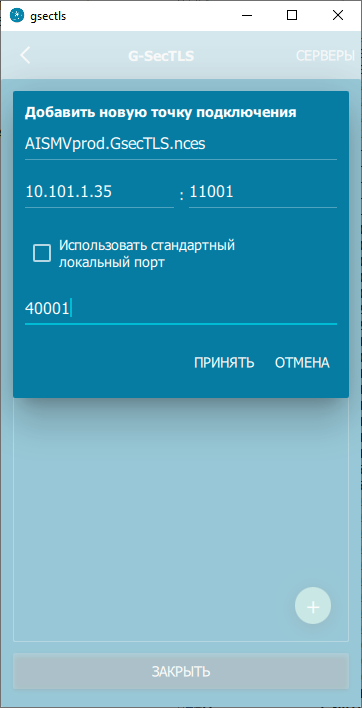
Повторить создание третьей точки

**Имя**: TestPage.GsecTLS.nces

**IP адрес**: <IP адрес провайдера>

**Порт**: 11000

**Локальный** **порт**: 9080



Добавление точки подключения account.gov.by

Для обновления СОС и СОК РУЦ следует зайти в верхнем левом углу в меню .

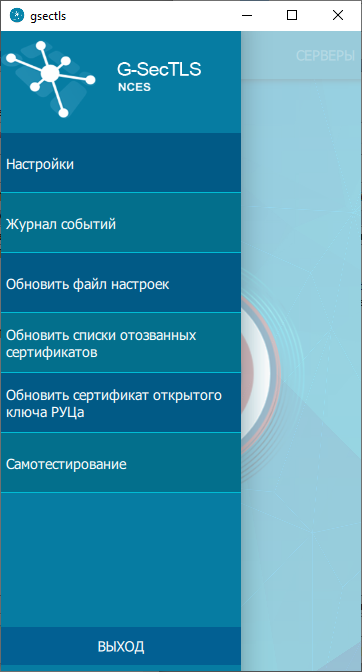
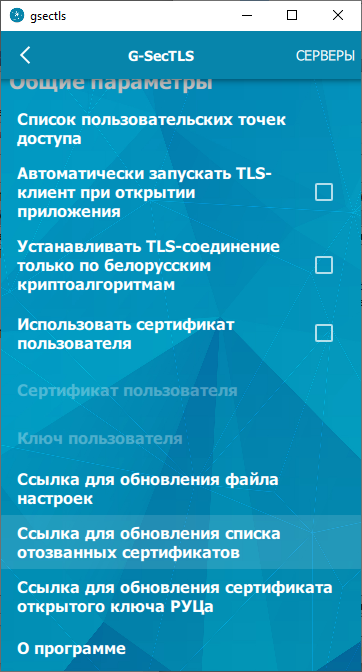
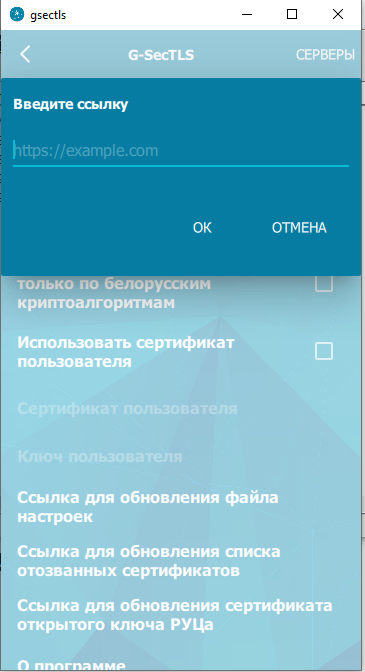


Пункт меню «GsecTLS» клиент

Выбрать «Настройки».

Для обновления СОС выбрать «Ссылка для обновления списка отозванных сертификатов» и ввести ссылку:

http://<IP адрес провайдера>:10480/files/ruc\_pem.crl

Настройка обновления СОС

**Настройка файла hosts**

Чтобы отредактировать файл требуется открыть блокнот с правами администратора, и открыть файл расположенном по пути C:\Windows\System32\drivers\etc.

|  |  |
| --- | --- |
|  |  |

Запуск «Блокнот» от имени администратора

В файл hosts следует добавить следующие записи:

**Интернет**

127.0.0.1 gw.gov.by

127.0.0.1 esiful-idp.gov.by

127.0.0.1 ei.gov.by

127.0.0.1 is.gov.by

127.0.0.1 am.gov.by

127.0.0.1 gw.nces.by

127.0.0.1 esiful-idp.nces.by

127.0.0.1 ei.nces.by

127.0.0.1 is.nces.by

127.0.0.1 am.nces.by

127.0.0.1 archive.nces.by

**БTK и другие:**

127.0.0.1 gw.gov.by

127.0.0.1 esiful-idp.gov.by

127.0.0.1 ei.gov.by

127.0.0.1 is.gov.by

127.0.0.1 am.gov.by

127.0.0.1 gw.nces.by

127.0.0.1 esiful-idp.nces.by

127.0.0.1 ei.nces.by

127.0.0.1 is.nces.by

127.0.0.1 am.nces.by

127.0.0.1 archive.nces.by

10.101.1.109 esiful.gov.by

**БОТ:**

127.0.0.1 gw.gov.by

127.0.0.1 esiful-idp.gov.by

127.0.0.1 ei.gov.by

127.0.0.1 is.gov.by

127.0.0.1 am.gov.by

127.0.0.1 gw.nces.by

127.0.0.1 esiful-idp.nces.by

127.0.0.1 ei.nces.by

127.0.0.1 is.nces.by

127.0.0.1 am.nces.by

127.0.0.1 archive.nces.by

10.252.0.109 esiful.gov.by

**БФТ:**

127.0.0.1 gw.gov.by

127.0.0.1 esiful-idp.gov.by

127.0.0.1 ei.gov.by

127.0.0.1 is.gov.by

127.0.0.1 am.gov.by

127.0.0.1 gw.nces.by

127.0.0.1 esiful-idp.nces.by

127.0.0.1 ei.nces.by

127.0.0.1 is.nces.by

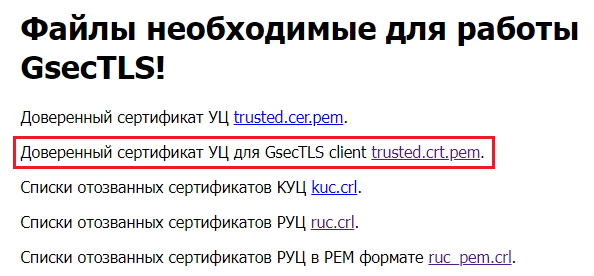
127.0.0.1 am.nces.by

127.0.0.1 archive.nces.by

10.53.5.109 esiful.gov.by

**Обновление файла СОС КУЦ**

Одновременно, в связи с выпуском СОС КУЦ, требуется вручную заменить в программном обеспечении GsecTLS файл (trusted.crt.pem). Файлы можно скачать, перейдя по ссылке:  
 **http://<IP адрес провайдера>:10480/**



Файлы СОС КУЦ

Замена на клиенте GsecTLS выполняется следующим образом:

Для клиента используется файл **trusted.crt.pem**

Заменить файл в каталоге

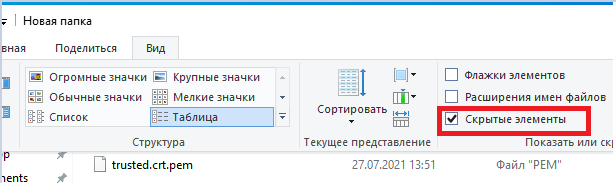
Для пользователей **Windows**:

С:\Users*\<Имя\_пользователя>\*AppData\Local\gsectls\certs\

***Примечание:***

Если папка AppData не отображается:

1. Откройте проводник.
2. Поставьте галочку напротив «Скрытые элементы».



Отображение скрытых элементов

После замены необходимо перезагрузить клиент.