ИНСТРУКЦИЯ

по установке и настройке ПО «G-SecTLS» сервер

для доступа к ЕПЭУ\_v2 (account.gov.by), ядру ОАИС и Национальному сегменту, EDI провайдер

Минск 2023

Оглавление

[1. Введение 4](#_Toc151558335)

[2. Нормативные ссылки 5](#_Toc151558336)

[3. Обозначения и сокращения 6](#_Toc151558337)

[4. Условия выполнения программы 7](#_Toc151558338)

[4.1. Программное обеспечение 7](#_Toc151558339)

[4.2. Аппаратное обеспечение 7](#_Toc151558340)

[5. Порядок установки и настройки «GsecTLS» сервер на ОС семейства Linux 7](#_Toc151558341)

[5.1. Порядок установки «GsecTLS» сервер на ОС семейства Linux 7](#_Toc151558342)

[5.2. Порядок настройки «GsecTLS» сервер на ОС семейства Linux 8](#_Toc151558343)

[5.2.1. Создание каталога логирования 8](#_Toc151558344)

[5.2.2. Настройка автоматического обновления СОС 9](#_Toc151558345)

[5.2.3. Настройка обновление СОС КУЦ 9](#_Toc151558346)

[5.3. Проверка запуска сервера GSecTLS 10](#_Toc151558347)

[6. Порядок установки и настройки «GsecTLS» сервер на  
 ОС семейства Windows 11](#_Toc151558348)

[6.1. Порядок установки «GsecTLS» сервер на ОС семейства Windows 11](#_Toc151558349)

[6.2. Настройка автоматического обновления СОС на  
 ОС семейства Windows 12](#_Toc151558350)

[6.3. Проверка запуска сервера «GSecTLS» 15](#_Toc151558351)

[7. Редактирование файла host 16](#_Toc151558352)

[7.1. При настройке доступа к ЕПЭУ\_v2 (account.gov.by) 16](#_Toc151558353)

[7.2. При настройке к ядру ОАИС 17](#_Toc151558354)

[7.3. При настройке к Нацсегменту 18](#_Toc151558355)

[7.4. При настройке к EDI провайдером 18](#_Toc151558356)

[8. Ручное обновление СОС 20](#_Toc151558357)

[9. Настройка G-Seс TLS сервера 20](#_Toc151558358)

[9.1. Настройка файла конфигурации 20](#_Toc151558359)

[9.1.1. Пример конфигурационного файла для ОС Linux   
для доступа к тестовой странице 21](#_Toc151558360)

[9.1.2. Пример конфигурационного файла для ОС   
Windows для доступа к тестовой странице 22](#_Toc151558361)

[9.1.3. Настройка доступа к ЕПЭУ\_v2 (account.gov.by) 22](#_Toc151558362)

[9.1.4. Настройка доступа к ядру ОАИС 23](#_Toc151558363)

[9.1.5. Настройка доступа к Нацсегменту 23](#_Toc151558364)

[9.1.6. Настройка доступа EDI провайдерам 24](#_Toc151558365)

[10. Проверка работоспособности 25](#_Toc151558366)

[10.1. Проверка канала 25](#_Toc151558367)

[10.2. Проверка доступности по порту 25](#_Toc151558368)

[10.3. Проверка работы «GsecTLS» сервера 25](#_Toc151558369)

[10.4. Проверка доступа к ядру ОАИС (если настроено). 26](#_Toc151558370)

# Введение

Данная инструкция предназначена для настройки и использования программного обеспечения «GsecTLS» сервер.

«GsecTLS» сервер предназначен для криптографической защиты информации и аутентификации сторон при взаимодействии в информационной системе организации с применением алгоритмов электронной цифровой подписи и транспорта ключа согласно требованиям СТБ 34.101.45-2013.

Программное обеспечение представляет собой локальный обратный прокси-сервер. «GsecTLS» сервер принимает запросы на локальном интерфейсе по заданным портам и перенаправляет их на конечный сервис через «GsecTLS» сервер с использованием протокола защиты транспортного уровня TLS. Таким образом, «GsecTLS» сервер может использоваться не только для браузеров, но и для других приложений, работающих по порту.

# 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»;

# 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 |
| РМ | – | рабочее место |

# Условия выполнения программы

## Программное обеспечение

Программное обеспечение «GsecTLS» сервер предназначен для работы на ПЭВМ (ЭВМ), под управлением следующих операционных систем:

а) Операционная система Windows

– Windows 8 x32/64;

– Windows 10 x32/64.

б) Операционная система Linux

– Ubuntu 18.04 версии ядра 4.18

GsecTLS» сервер предназначен для обеспечения функций криптографической защиты информации.

## Аппаратное обеспечение

Программа реализации защищенного взаимодействия должна эксплуатироваться на ЭВМ 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 80 ГБ |

# Порядок установки и настройки «GsecTLS» сервер на ОС семейства Linux

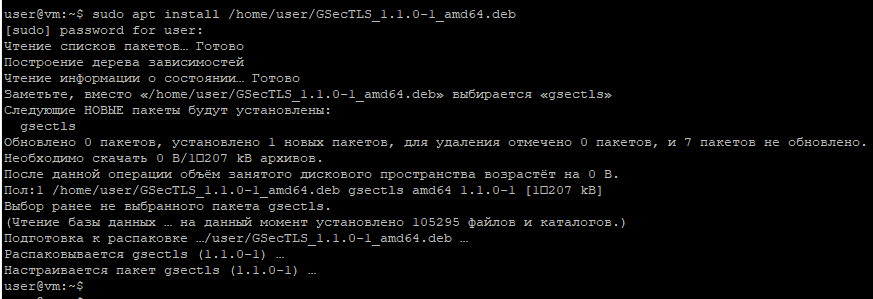
## Порядок установки «GsecTLS» сервер на ОС семейства Linux

Для установки «GsecTLS» сервер необходимо:

1. загрузить дистрибутив GsecTLS сервер на ПВЭМ.
2. запустить файл “**GSecTLS\_1.1.0-1\_amd64.deb**” на сервере, введя в терминале команду:

**sudo apt install /home/user/GSecTLS\_1.1.0-1\_amd64.deb**

Ввести «Y» для продолжения и завершения процесса установки сервера.



Установка «GsecTLS» сервер

|  |  |
| --- | --- |
|  | Программное обеспечение устанавливается  по следующим путям:  /usr/local/etc/GSecTLS/  /usr/local/sbin/ |

## Порядок настройки «GsecTLS» сервер на ОС семейства Linux

### Создание каталога логирования

После успешной установки «GsecTLS» сервера нужно настроить логирование работы «GsecTLS» сервера. Для этого надо создать каталог:

**sudo mkdir /var/log/GsecTLS/**

Установить в созданном каталоге при помощи *chmod* права, достаточные для его редактирования пользователем, под учетной записью которого будет запускаться «GsecTLS» сервер. После этого раcкомментировать строку *error\_log /var/log/GsecTLS/GsecTLS.log info;* в конфигурационном файле и перезагрузить «GsecTLS» сервер командой:

**sudo GSecTLS –s reload**

### Настройка автоматического обновления СОС

Для корректной работы сервера GsecTLS, необходимо настроить синхронизацию времени (отредактировать файл timesyncd.conf).

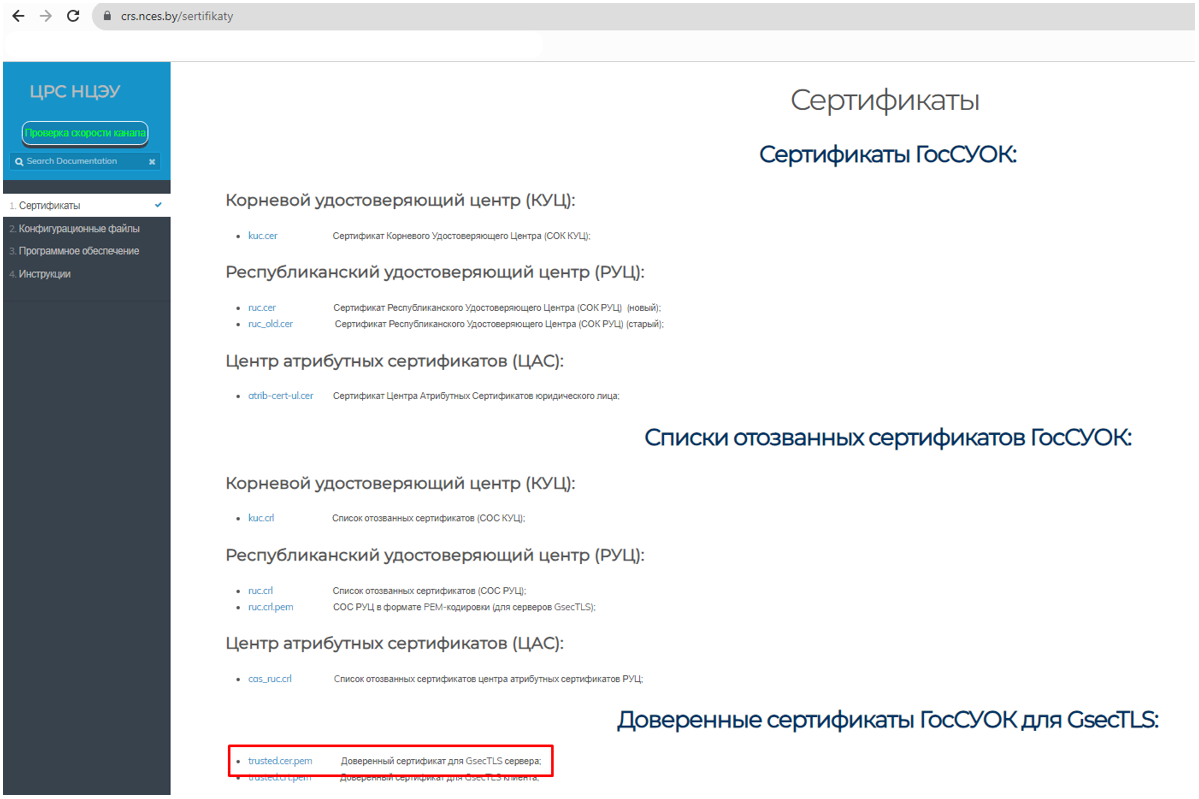
|  |  |
| --- | --- |
|  | Редактирование timesyncd.conf:  Файл располагается по следующему пути:  /etc/systemd/timesyncd.conf  NTP=ipaddress  systemctl restart systemd-timesyncd  timedatectl set-timezone Europe/Minsk |

Затем следует настроить автообновление СОС. Для этого можно использовать планировщик задач *cron*.

|  |
| --- |
| Использование планировщика задач cron для обновления СОС:  Открыть на редактирование конфигурацию cron:  **crontab -e**  Добавить задание (одной строкой):  *0 0 \* \* \* wget -O /usr/local/etc/GSecTLS/certs/ruc.crl.pem https://crs.nces.by/files/sertifikaty/ruc.crl.pem* |

### Настройка обновление СОС КУЦ

В связи с выпуском СОС КУЦ, требуется вручную заменить в программном обеспечении GsecTLS файл (**trusted.cer.pem**). Файлы можно скачать, перейдя по ссылке:  
 **https://crs.nces.by/files/sertifikaty/**



Заменить файл в директории "/usr/local/etc/GSecTLS/certs/”

## Проверка запуска сервера GSecTLS

После первичной настройки можно проверить запускается ли сервер GSecTLS. Сервер запускается командой:

**sudo GSecTLS**

**sudo GSecTLS –s stop – остановка сервера**

|  |  |
| --- | --- |
|  | Если сервер запустился без ошибок, то не будет никаких сообщений |

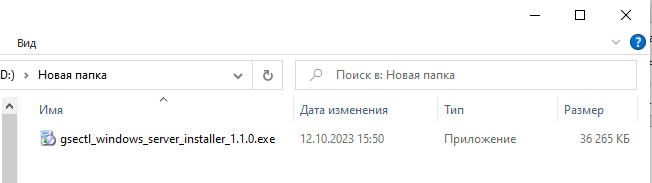
В противном случае выведется сообщение об ошибке с указанием

что помешало началу работы сервера.

# Порядок установки и настройки «GsecTLS» сервер на ОС семейства Windows

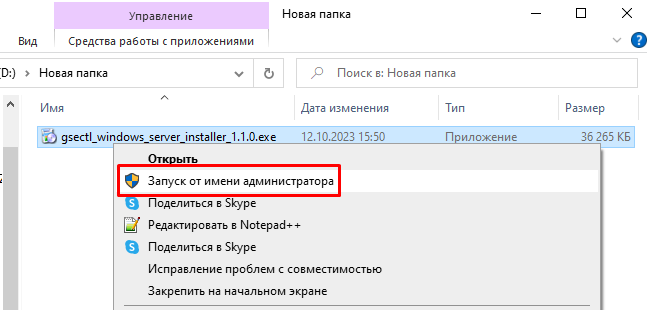
## Порядок установки «GsecTLS» сервер на ОС семейства Windows

Загрузить дистрибутив GsecTLS сервер «gsectl\_windows\_server\_installer\_1.1.0.exe» на ПВЭМ.



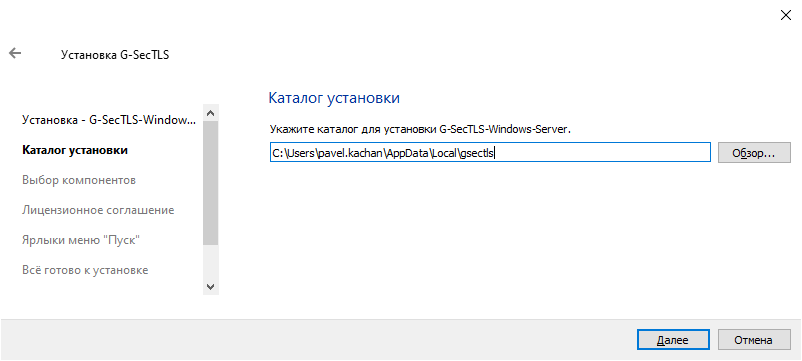
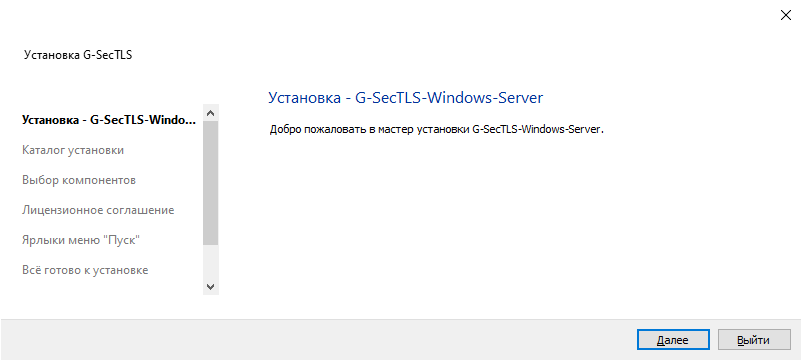
Загрузка дистрибутива GsecTLS сервера

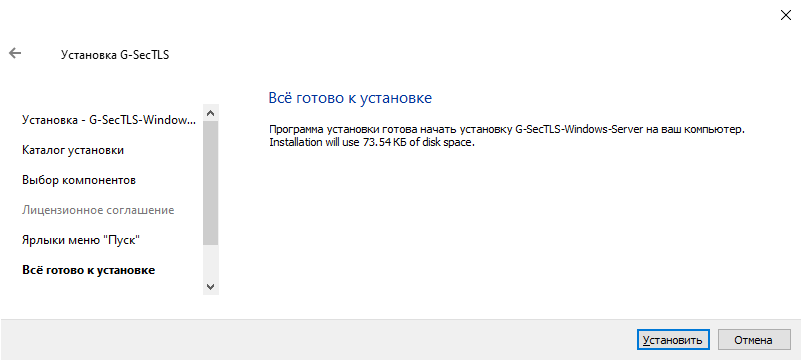
Запустить загруженное приложение от имени администратора. Для этого необходимо нажать правой кнопкой мыши на него, выбрать пункт меню «Запуск от имени администратора» и запустить его, кликнув левой кнопкой мыши. Далее - следовать инструкциям мастера установки.

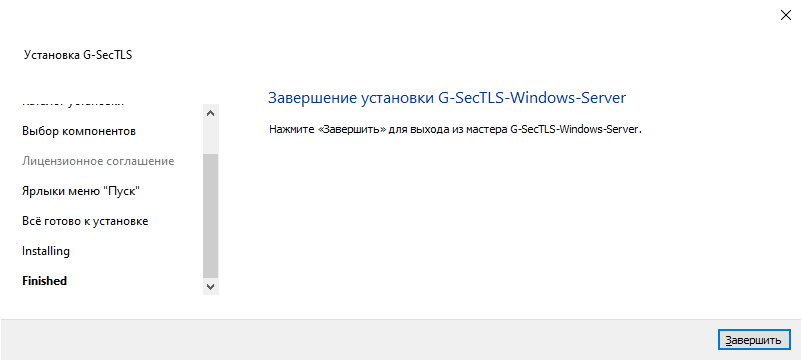


Запуск приложения

Выполнить поэтапную установку «GsecTLS» сервер с использованием мастера установки.







Установка GsecTLS сервер

## Настройка автоматического обновления СОС на ОС семейства Windows

Для настройки автоматического обновления СОС необходимо:

Создать текстовый файл с расширением \*.ps1

(Например: Update\_CRL.ps1)

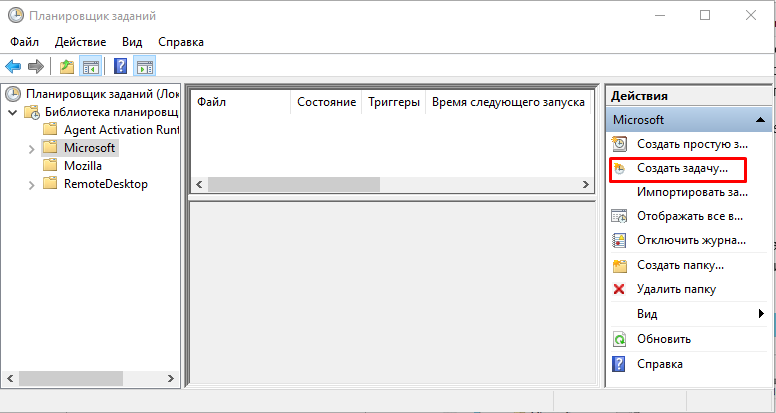
Открыть файл текстовым редактором и ввести две команды:

start-bitstransfer -source https://crs.nces.by/files/sertifikaty/ruc.crl.pem c:\users\*<username>*\appdata\local\gsectls\certs\ruc.crl.pem

start-bitstransfer -source https://crs.nces.by/files/sertifikaty/trusted.cer.pem c:\users\*<username>*\appdata\local\gsectls\certs\trusted.cer.pem

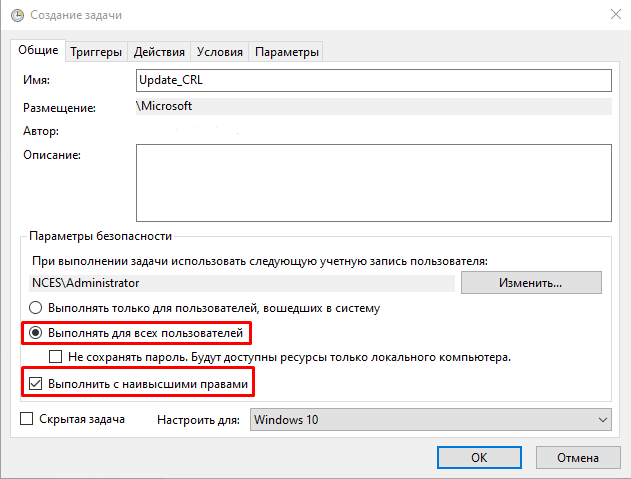
Для запуска скрипта требуется воспользоваться оснасткой

«Планировщик заданий», в разделе «Действия» выбрать пункт «Создать задачу».



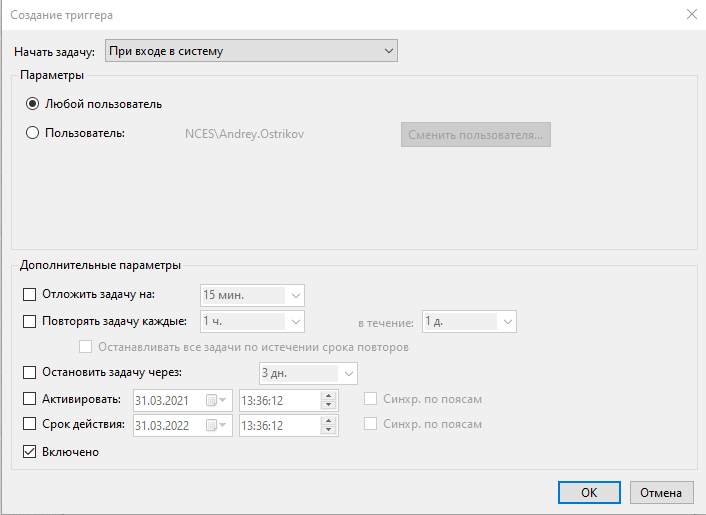
Создание задачи «Планировщик заданий»

На вкладке «Общие» требуется указать имя и описание задания, а также пользователя, от имени которого будет запускаться задание. Для того, чтобы задание выполнялось вне зависимости от того, авторизован ли пользователь в системе, следует выбрать опцию «Выполнять для всех пользователей»



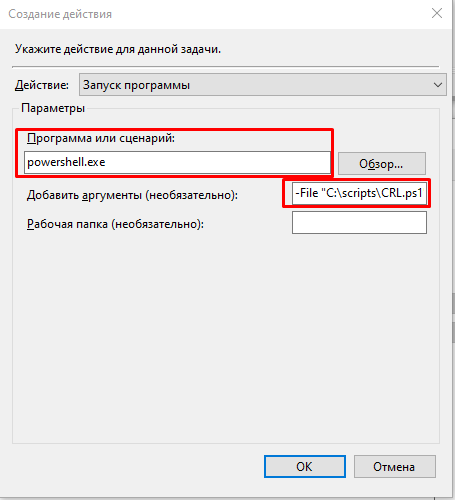
Создание задачи «Планировщик заданий»

Во вкладке «Триггеры» создаем новый триггер, в котором будет храниться расписание запуска задания. Указать в опции «Начать задачу» - «При входе в систему».



Настройка триггера

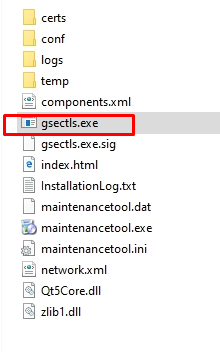
Во вкладке «Действия» требуется создать действие по запуску скрипта. Скрипты PowerShell могут выполняться только интерактивно, поэтому в поле «Программа или сценарий» следует указать powershell.exe и в поле «Добавить аргументы» указать параметр -File и путь к вашему скрипту.



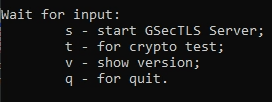
Создание действия

## Проверка запуска сервера «GSecTLS»

После первичной настройки можно осуществить проверку запуска сервера «GSecTLS». Сервер запускается исполняемым файлом gsectls.exe в директории С:\Users*\<Имя\_пользователя>*\AppData\Local\gsectls:



После запуска, «GsecTLS» сервер пройдет тестирование и пользователю выведется меню, изображенное на рисунке.

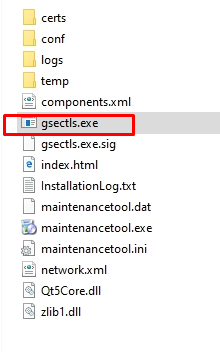


|  |  |
| --- | --- |
|  | Где:  s - запуск GSecTLS сервера  t - тестирование работоспособности  v - версия продукта  q - выход из программы |

При запуске сервера (S) выведется сообщение: *GsecTLS Server started.*

В противном случае, выведется сообщение об ошибке с указанием того, что помешало началу работы «GsecTLS» сервера.

Для завершения работы сервера следует нажать q и закрыть окно программы. Чтобы запусить «GSecTLS» сервер следует заново запустить файл gsectls.exe в директории С:\Users*\<Имя\_пользователя>*\AppData\Local\gsectls.



Запуск «GsecTLS» сервер

# Редактирование файла host

После успешной установки «GsecTLS» сервера нужно настроить файл hosts. Для этого открываем файл hosts:

Для ОС семейства Linux

sudo nano /etc/hosts

Для ОС семейства Windows файл расположен

c:\Windows\System32\drivers\etc\

В файл hosts следует добавить следующие записи в зависимости от выбранной услуги, типа доступа и провайдера.

## При настройке доступа к ЕПЭУ\_v2 (account.gov.by)

**Интернет**

127.0.0.1 is.gov.by

127.0.0.1 esiful-idp.gov.by

127.0.0.1 gw.gov.by

**БTK и другие:**

127.0.0.1 account.gov.by

127.0.0.1 is.gov.by

127.0.0.1 esiful-idp.gov.by

10.101.1.109 esiful.gov.by

127.0.0.1 gw.gov.by

10.101.1.35 crs.nces.by

**БОТ:**

127.0.0.1 account.gov.by

127.0.0.1 is.gov.by

127.0.0.1 esiful-idp.gov.by

10.252.0.109 esiful.gov.by

127.0.0.1 gw.gov.by

10.252.0.35 crs.nces.by

**БФТ:**

127.0.0.1 account.gov.by

127.0.0.1 is.gov.by

127.0.0.1 esiful-idp.gov.by

10.53.5.109 esiful.gov.by

127.0.0.1 gw.gov.by

10.53.5.35 crs.nces.by

## При настройке к ядру ОАИС

**Интернет**

127.0.0.1 gw.gov.by

127.0.0.1 apimgw.core.oais.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

**VPN от БTK и другие:**

127.0.0.1 gw.gov.by

127.0.0.1 apimgw.core.oais.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

10.101.1.35 crs.nces.by

10.101.1.109 esiful.gov.by

**VPN от БОТ:**

127.0.0.1 gw.gov.by

127.0.0.1 apimgw.core.oais.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

10.252.0.35 crs.nces.by

10.252.0.109 esiful.gov.by

**VPN от БФТ:**

127.0.0.1 gw.gov.by

127.0.0.1 apimgw.core.oais.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

10.53.8.35 crs.nces.by

10.53.5.109 esiful.gov.by

## При настройке к Нацсегменту

В файл hosts следует добавить следующие запись:

127.0.0.1 wso2-api.oais.by

127.0.0.1 nseec.oais.by

А также добавить запись в соответствии с организованным VPN каналом

**БTK и другие:**

10.101.1.35 crs.nces.by

**БОТ:**

10.252.0.35 crs.nces.by

**БФТ:**

10.53.8.35 crs.nces.by

## При настройке к EDI провайдером

**Интернет**

127.0.0.1 gw.gov.by

127.0.0.1 apimgw.core.oais.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

**VPN от БTK и другие:**

127.0.0.1 gw.gov.by

127.0.0.1 apimgw.core.oais.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

10.101.1.35 crs.nces.by

10.101.1.109 esiful.gov.by

**VPN от БОТ:**

127.0.0.1 gw.gov.by

127.0.0.1 apimgw.core.oais.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

10.252.0.35 crs.nces.by

10.252.0.109 esiful.gov.by

**VPN от БФТ:**

127.0.0.1 gw.gov.by

127.0.0.1 apimgw.core.oais.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

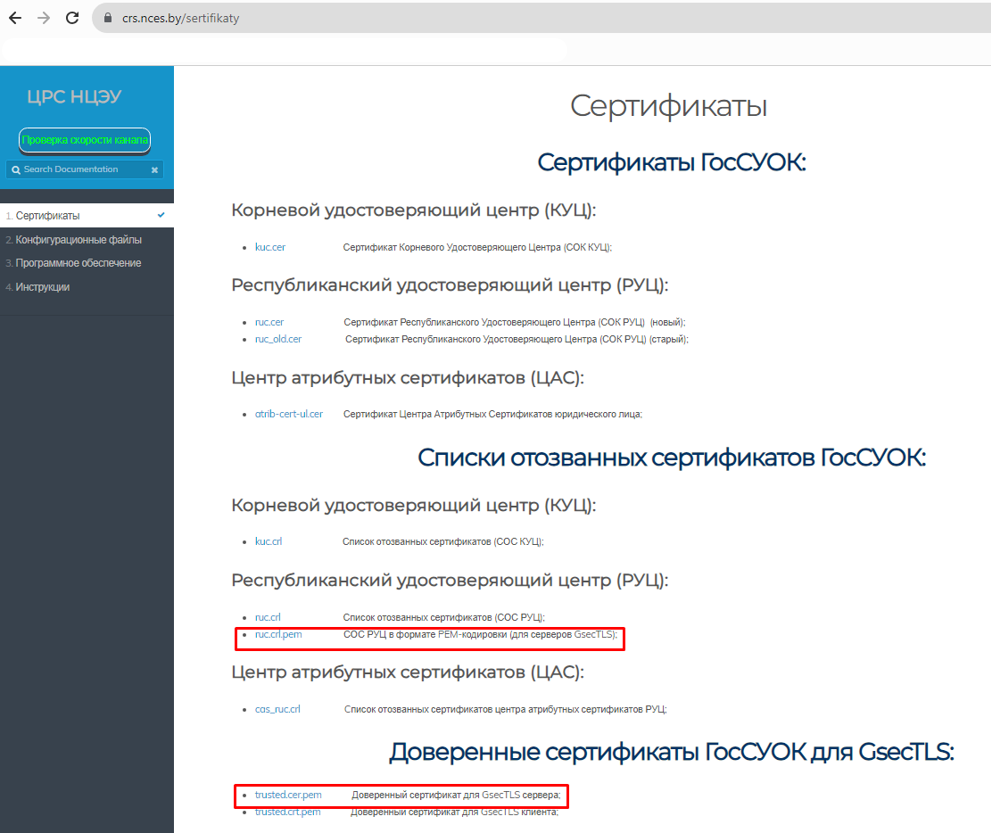
127.0.0.1 am.nces.by

10.53.8.35 crs.nces.by

10.53.5.109 esiful.gov.by

# Ручное обновление СОС

При необходимости файлы СОС в pem формате можно скачать, перейдя по ссылке:  
 **https://crs.nces.by/files/sertifikaty/**



Заменить файлы в соответствующих директориях

# Настройка G-Seс TLS сервера

## Настройка файла конфигурации

Для получения электронных услуг, необходимо указать в файле конфигурации (GSecTLS.conf в Linux или nginx.cfg в Windows) адреса и порты, на которые будут приниматься и переправляться запросы. Для этого необходимо открыть nginx.cfg текстовым редактором и добавить блоки **server** с описанием параметров подключения.

в *<ipaddr>*указываем адрес в зависимости от провайдера:

|  |  |
| --- | --- |
| Провайдер | <ipaddr> |
| БФТ | 10.53.8.35 |
| БОТ | 10.252.0.35 |
| Другие | 10.101.1.35 |
| Internet | 185.227.96.96 |

***Примечание:*** Невозможно одновременно настроить доступ к ЕПЭУ\_v2 (account.gov.by) и национальному сегменту по web интерфейсу (NatzSegArm) в связи с использованием 443 локального порта.

### Пример конфигурационного файла для ОС Linux для доступа к тестовой странице

**user root;**

**daemon on;**

**master\_process on;**

**worker\_processes auto;**

**worker\_priority -20;**

**worker\_rlimit\_nofile 262144;**

**error\_log /var/log/GsecTLS/GsecTLS.log info;**

**events {**

**multi\_accept on;**

**worker\_connections 4096;**

**}**

**stream {**

**proxy\_ssl on;**

**proxy\_ssl\_protocols TLSv1.2;**

**proxy\_ssl\_ciphers DHT-BIGN-BELT-CTR-MAC-HBELT;**

**proxy\_ssl\_server\_name on;**

**proxy\_ssl\_session\_reuse on;**

**proxy\_ssl\_verify on;**

**proxy\_ssl\_verify\_depth 3;**

**ssl\_session\_timeout 15m;**

**ssl\_session\_cache shared:SSL:100m;**

**proxy\_ssl\_trusted\_certificate cert/trusted.cer.pem;**

**proxy\_ssl\_crl cert/ruc.crl.pem;**

**#====================================================**

**# Test Page**

**#====================================================**

**server {**

**listen \*:9080;**

**proxy\_pass <ipaddr>:11000;**

**proxy\_ssl\_name TestPage.GsecTLS.nces;**

**}**

**}**

### Пример конфигурационного файла для ОС Windows для доступа к тестовой странице

**daemon off;**

**master\_process off;**

**error\_log logs/alert.logs alert;**

**error\_log logs/error.logs error;**

**error\_log logs/info.logs info;**

**events {**

**multi\_accept on;**

**}**

**stream {**

**ssl\_protocols TLSv1.2;**

**ssl\_session\_tickets on;**

**ssl\_session\_timeout 15m;**

**ssl\_session\_cache shared:SSL:100m;**

**ssl\_ciphers DHT-BIGN-BELT-CTR-MAC-HBELT;**

**ssl\_conf\_command SignatureAlgorithms bign\_with\_hbelt;**

**ssl\_prefer\_server\_ciphers on;**

**ssl\_crl ../cert/ruc.crl.pem;**

**ssl\_client\_certificate ../cert/trusted.cer.pem;**

**ssl\_verify\_client on;**

**ssl\_verify\_depth 3;**

**#====================================================**

**# Test Page**

**#====================================================**

**server {**

**listen \*:9080;**

**proxy\_pass <ipaddr>:11000;**

**proxy\_ssl\_name TestPage.GsecTLS.nces;**

**}**

**}**

### Настройка доступа к ЕПЭУ\_v2 (account.gov.by)

Для доступа к ЕПЭУ\_v2 в конфиг после последнего блока server {} необходимо добавить блок:

#====================================================

# ACCOUNT

#====================================================

server {

listen \*:443;

proxy\_pass <ipaddr>:11004;

proxy\_ssl\_name account.GsecTLS.nces;

}

### Настройка доступа к ядру ОАИС

Для доступа к ЕПЭУ\_v2 в конфиг после последнего блока server {} необходимо добавить блок:

#====================================================

# coreOAIS

#====================================================

server {

listen \*:10446;

proxy\_pass <ipaddr>:11006;

proxy\_ssl\_name coreOAIS.GsecTLS.nces;

}

### Настройка доступа к Нацсегменту

Для доступа к Нацсегменту в конфиг после последнего блока server {} необходимо добавить блоки:

#====================================================

# NatzSeg

#====================================================

server {

listen \*:40005;

proxy\_pass <ipaddr>:11005;

proxy\_ssl\_name NatzSeg.GsecTLS.nces;

}

#====================================================

# NatzSegArm

#====================================================

server {

listen \*:443;

proxy\_pass <ipaddr>:11011;

proxy\_ssl\_name NatzSegArm.GsecTLS.nces;

}

### Настройка доступа EDI провайдерам

Для доступа EDI провайдерам в конфиг после последнего блока server {} необходимо добавить блоки:

#====================================================

# AISMV prod

#====================================================

server {

listen \*:40001;

proxy\_pass <ipaddr>:11001;

proxy\_ssl\_name AISMVprod.GsecTLS.nces;

}

#====================================================

# AISMV dev

#====================================================

server {

listen \*:40002;

proxy\_pass <ipaddr>:11002;

proxy\_ssl\_name AISMVdev.GsecTLS.nces;

}

#====================================================

# ACCOUNT

#====================================================

server {

listen \*:443;

proxy\_pass <ipaddr>:11004;

proxy\_ssl\_name account.GsecTLS.nces;

}

#====================================================

# coreOAIS

#====================================================

server {

listen \*:10446;

proxy\_pass <ipaddr>:11006;

proxy\_ssl\_name coreOAIS.GsecTLS.nces;

}

# Проверка работоспособности

В соответствии от провайдера используются следующие IP адреса:

БОТ – 10.252.0.35

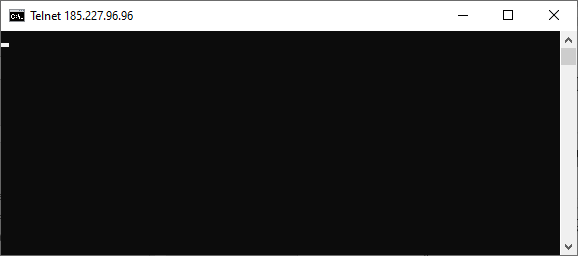
БФТ – 10.53.8.35

Другие – 10.101.1.35

Internet – 185.227.96.96

## Проверка канала

telnet <IP адрес> 443

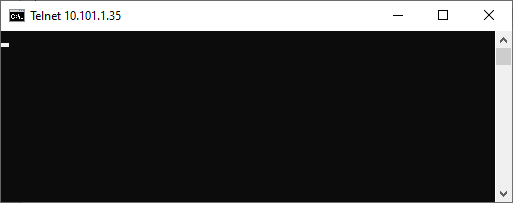


корректное подключение telnet

Если связи нет, необходимо обратиться к провайдеру для уточнения состояния канала связи.

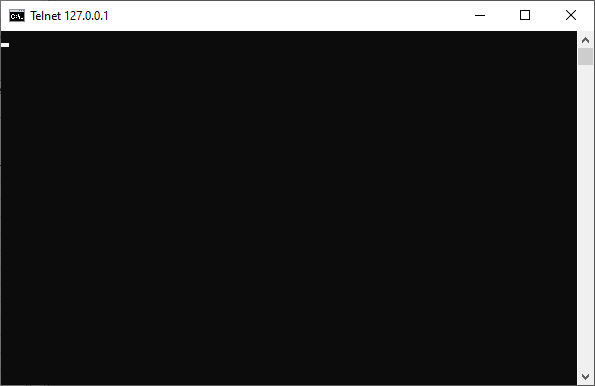
## Проверка доступности по порту

Выполните команду telnet <IP адрес> 11006, должен быть настроен



## Проверка работы «GsecTLS» сервера

Выполните команду telnet 127.0.0.1 10446, должен быть настроен



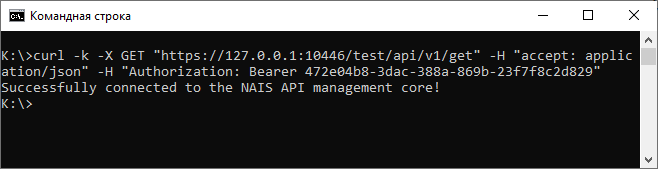
## Проверка доступа к ядру ОАИС (если настроено).

Выполните тестовый запрос в ядро ОАИС.

curl -k -X GET "**https://127.0.0.1:10446**/test/api/v1/get" -H "accept: application/json" -H "Authorization: Bearer 472e04b8-3dac-388a-869b-23f7f8c2d829"

В ответ должно прийти сообщение:

Successfully connected to the NAIS API management core!



Запрос делается с использованием утилиты curl. Если данной утилиты нет на ПК, ее можно скачать в Интернете и установить.