Инструкция

по установке и настройке ПО «G-SecTLS» сервер

для доступа к АИС «Ведомственный архив»

Минск 2023

Оглавление

[1. Введение 3](#_Toc146191601)

[2. Нормативные ссылки 4](#_Toc146191602)

[3. Обозначения и сокращения 5](#_Toc146191603)

[4. Возможные схемы использования GsecTLS сервера для доступа к АИС «Ведомственный архив» 6](#_Toc146191604)

[5. Порядок установки и настройки «GsecTLS» сервер 7](#_Toc146191605)

[5.1. Порядок установки «GsecTLS» сервер 7](#_Toc146191606)

[5.2. Настройка G-Seс TLS сервера 7](#_Toc146191607)

[5.3. Создание каталога логирования 8](#_Toc146191608)

[5.4. Редактирование файла host 8](#_Toc146191609)

[5.4.1. Редактирование файла host 8](#_Toc146191610)

[5.4.1. Создание каталога логирования 10](#_Toc146191611)

[5.4.1. Настройка автоматического обновления СОС 11](#_Toc146191612)

[5.4.2. Настройка обновление СОС КУЦ 11](#_Toc146191613)

[5.5. Настройка файла конфигурации 12](#_Toc146191614)

[5.6. Проверка запуска сервер GSecTLS сервера 14](#_Toc146191615)

[6. Проверка работоспособности 15](#_Toc146191616)

[6.1. Проверка доступности по порту 15](#_Toc146191617)

[6.2. Проверка доступа на API АИС «Ведомственный архив» 15](#_Toc146191618)

# 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 |
|  |  |  |

Для организации доступа к АИС «Ведомственный архив» используется программное обеспечение «GsecTLS» сервер.

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

– Ubuntu 18.04 версии ядра 4.18

«GsecTLS» сервер предназначен для обеспечения функций криптографической защиты информации.

**ВНИМАНИЕ!** **Шифрованию подлежит канал связи между сервером ВСЭД организации и НЦЭУ.**

# Возможные схемы использования GsecTLS сервера для доступа к АИС «Ведомственный архив»

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

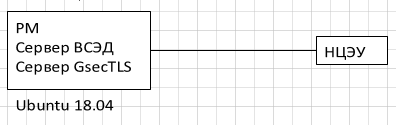
- Тактовая частота процессора не менее 2 ГГц;

- Объем ОЗУ не менее 2 ГБ;

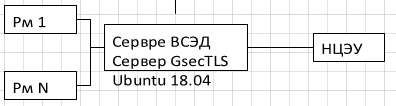
- Объем памяти на жестком диске не менее 80 ГБ.

Возможные схемы использования GsecTLS сервера для доступа к АИС «Ведомственный архив»:

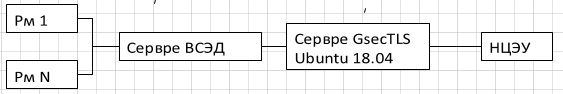
1. Рабочее место пользователя и сервер ВСЭД расположены на одном ПК с ОС Ubuntu 18.04 версии ядра 4.18



1. Сервер ВСЭД находится отдельно от рабочих мест пользователей и расположен на ПК с ОС Ubuntu 18.04 версии ядра 4.18



1. Сервер ВСЭД находится отдельно от рабочих мест пользователей и расположен **не** на ПК с ОС Ubuntu 18.04 версии ядра 4.18



# Порядок установки и настройки «GsecTLS» сервер

## Порядок установки «GsecTLS» сервер

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, рисунок 11.

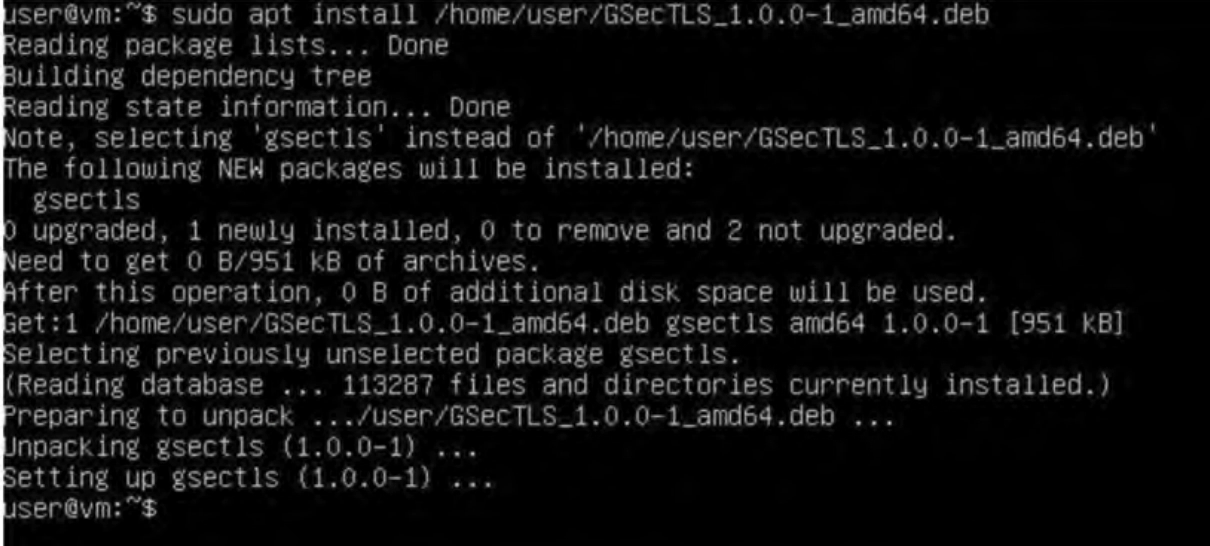


Рисунок 11 – Установка «GsecTLS» сервер

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

## Настройка G-Seс TLS сервера

**ВАЖНО !**

В зависимости от провайдера используются следующие IP адреса:

БОТ – 10.252.0.35

БФТ – 10.53.8.35

Другие – 10.101.1.35

## Создание каталога логирования

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

*mkdir /var/log/GsecTLS/*

Установить в созданном каталоге при помощи *chmod* права, достаточные для его редактирования пользователем, под учетной записью которого будет запускаться сервер.

## Редактирование файла host

После успешной установки сервера нужно настроить файл host/ Для этого открываем файл host:

*sudo nano /etc/hosts*

В файл **hosts** следует добавить следующие записи.

Если используются схемы подключения 1,2:

### Редактирование файла host

После успешной установки сервера нужно настроить файл host/ Для этого открываем файл host:

sudo nano /etc/hosts

В файл hosts следует добавить следующие записи.

Если используются схемы подключения 1,2:

**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

**VPN от 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

10.101.1.35 crs.nces.by

10.101.1.109 esiful.gov.by

127.0.0.1 archive.nces.by

**VPN от 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

10.101.1.35 crs.nces.by

10.252.0.109 esiful.gov.by

127.0.0.1 archive.nces.by

**VPN от 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

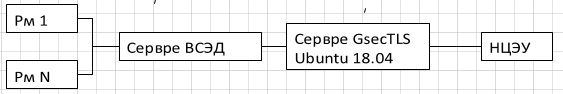
127.0.0.1 am.nces.by

10.101.1.35 crs.nces.by

10.53.5.109 esiful.gov.by

127.0.0.1 archive.nces.by

Если будет использоваться схема подключения 3



В случае, если в организации отсутствует DNS-сервер, то на сервере ВСЭД в hosts необходимо добавить следующие записи:

<IP адрес сервера GsecTLS> gw.gov.by

<IP адрес сервера GsecTLS> esiful-idp.gov.by

<IP адрес сервера GsecTLS> ei.gov.by

<IP адрес сервера GsecTLS> is.gov.by

<IP адрес сервера GsecTLS> am.gov.by

<IP адрес сервера GsecTLS> gw.nces.by

<IP адрес сервера GsecTLS> esiful-idp.nces.by

<IP адрес сервера GsecTLS> ei.nces.by

<IP адрес сервера GsecTLS> is.nces.by

<IP адрес сервера GsecTLS> am.nces.by

<IP адрес сервера GsecTLS> crs.nces.by

<IP адрес сервера GsecTLS> esiful.gov.by

<IP адрес сервера GsecTLS> archive.nces.by

В случае, если в организации используется DNS-сервер, то на DNS-сервере необходимо добавить следующие A-записи:

<IP адрес сервера GsecTLS> gw.gov.by

<IP адрес сервера GsecTLS> esiful-idp.gov.by

<IP адрес сервера GsecTLS> ei.gov.by

<IP адрес сервера GsecTLS> is.gov.by

<IP адрес сервера GsecTLS> am.gov.by

<IP адрес сервера GsecTLS> gw.nces.by

<IP адрес сервера GsecTLS> esiful-idp.nces.by

<IP адрес сервера GsecTLS> ei.nces.by

<IP адрес сервера GsecTLS> is.nces.by

<IP адрес сервера GsecTLS> am.nces.by

<IP адрес сервера GsecTLS> crs.nces.by

<IP адрес сервера GsecTLS> esiful.gov.by

<IP адрес сервера GsecTLS> archive.nces.by

### Создание каталога логирования

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

mkdir /var/log/GsecTLS/

Установить в созданном каталоге при помощи *chmod* права, достаточные для его редактирования пользователем, под учетной записью которого будет запускаться сервер.

### Настройка автоматического обновления СОС

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

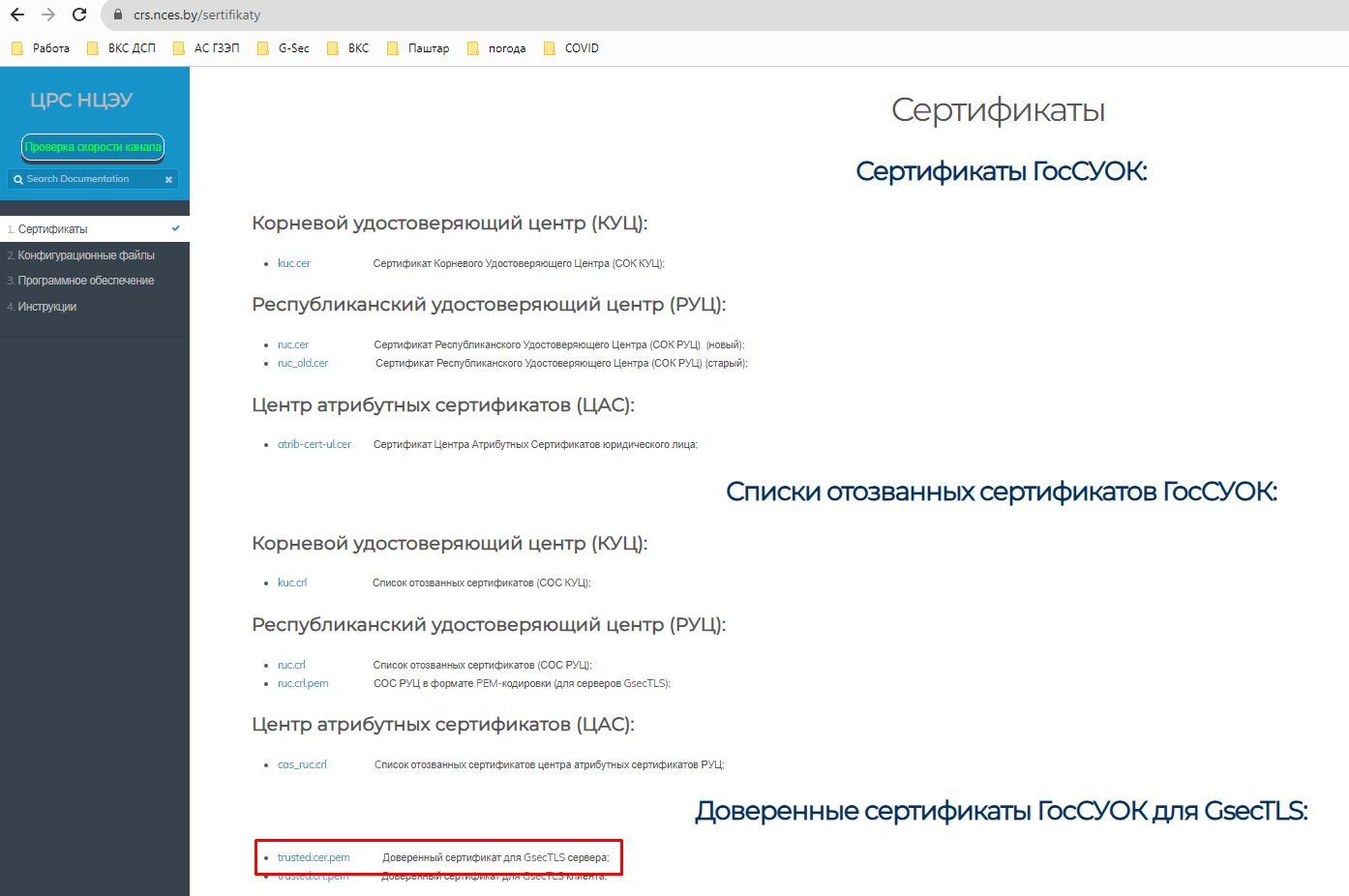
|  |  |
| --- | --- |
|  | Редактирование timesyncd.conf:  Файл располагается по следующему пути:  /etc/systemd/timesyncd.conf  NTP=ipaddress  systemctl restart systemd-timesyncd  timedatectl set-timezone Europe/Minsk |

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/”

## Настройка файла конфигурации

Преднастроенный файл конфигурации **GSecTLS.conf** направляется вместе с инструкцией в зависимости от провайдера.

|  |  |
| --- | --- |
| **Провайдер** | **Конфигурационный файл** |
| БФТ | GSecTLS\_bft.conf |
| БОТ | GSecTLS\_bot.conf |
| Другие | GSecTLS\_vpn.conf |

Скачанный файл следует переименовать в **GSecTLS.conf** и заменитьв директории **usr/local/etc/GSecTLS.**

Пример для ОС Linux “/usr/local/etc/GSecTLS/GSecTLS.conf”

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;

proxy\_ssl\_trusted\_certificate certs/trusted.cer.pem;

proxy\_ssl\_crl certs/ruc.crl.pem;

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

# Ved Archiv

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

server {

listen \*:8000;

proxy\_pass *<ipaddr>*:11010;

proxy\_ssl\_name VedArchiv.GsecTLS.nces;

}

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

# Test page

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

server {

listen \*:9080;

proxy\_pass *<ipaddr>*:11000;

proxy\_ssl\_name TestPage.GsecTLS.nces;

}

}

В зависимости от провайдера используются следующие *<ipaddr>*:

БОТ – 10.252.0.35

БФТ – 10.53.8.35

Другие – 10.101.1.35

После замены необходимо сохранить внесенные изменения и перезапустить GsecTLS:

sudo GSecTLS -s stop (остановка службы)

sudo GSecTLS (запуск службы)

## Проверка запуска сервер GSecTLS сервера

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

sudo GSecTLS (запуск службы)

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

В противном случае появится сообщение об ошибке с указанием,

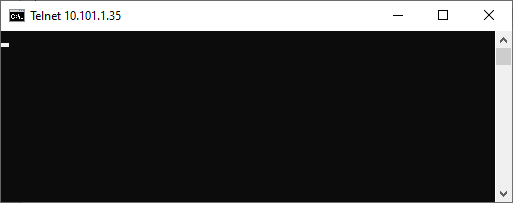
что помешало началу работы сервера.

# Проверка работоспособности

В зависимости от выбранной схемы использования GsecTLS сервера для доступа к АИС «Ведомственный архив» выполняется следующая проверка настройки и работоспособности

## Проверка доступности по порту

Выполните команду telnet <IP адрес провайдера>:11010



корректное подключение telnet

## Проверка доступа на API АИС «Ведомственный архив»

Для проверки доступа к АИС «Ведомственный архив» в браузере необходимо ввести внешний wsdl с указанием своего client152ws (предоставлялся с пакетом документов – инструкция 1\_Регистрация АИС ВА, при подключении услуги):

http://archive.nces.by:8000/client152ws/external/integration?wsdl

Должна открыться страница:

