**РЕСПУБЛИКАНСКОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ**

**«НАЦИОНАЛЬНЫЙ ЦЕНТР ЭЛЕКТРОННЫХ УСЛУГ»**

|  |  |  |
| --- | --- | --- |
| УДК 004.56 | |  |
|  | |  |
|  | |  |
|  |  | |
|  |  | |
|  |  | |
|  |  | |

**ИНСТРУКЦИЯ**

**по установке и настройке доступа к личному кабинету ОАИС**

**со строгой аутентификацией**

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

Минск 2023

Оглавление

[1. Введение 3](#_Toc145412447)

[2. Нормативные ссылки 4](#_Toc145412448)

[3. Обозначения и сокращения 5](#_Toc145412449)

[4. Условия выполнения программ 6](#_Toc145412450)

[4.1 Программное обеспечение 6](#_Toc145412451)

[4.2 Аппаратное обеспечение 6](#_Toc145412452)

[4.3 Порядок получения «GsecTLS» клиент и КП 6](#_Toc145412453)

[5. Порядок установки и настройки «GsecTLS» клиент 7](#_Toc145412454)

[5.1 Порядок установки «GsecTLS» клиент на ОС семейства Windows 7](#_Toc145412455)

[5.2 Настройка подключения посредством скрипта 9](#_Toc145412456)

[5.3 Установка КП 10](#_Toc145412457)

[5.4. Настройка КП NTClientSoftware при доступе через VPN 13](#_Toc145412458)

[5.5. Дополнительные настройки в системе 14](#_Toc145412459)

[6. Доступ к личному кабинету 14](#_Toc145412460)

[7. Проверка доступа на тестовый сайт 17](#_Toc145412461)

[Приложение 1 Ручная настройка доступа](#_Toc145412462) [20](#_Toc145412463)

[Приложение 2](#_Toc145412464)[Регистрация в Облачном хранилище, скачивание программного обеспечения 27](#_Toc145412465)

# **1. Введение**

Данная инструкция описывает порядок доступа к личному кабинету общегосударственной автоматизированной информационной системы (ОАИС) посредством строгой аутентификации.

В случае необходимости доступа в личный кабинет по строгой аутентификации в личный кабинет пользователя необходима установка и настройка «GsecTLS» клиент и Клиентского приложения для работы с идентификационной картой (КП).(Для работы с TPSClientустановка КП не нужна)

«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

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) (Предназначена для работы с личным кабинетом в «Е-Паслуге». Для работы с TPSClientустановка КП не нужна)

«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.

# **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 от16.04.2013 № 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 |
|  |  |  |

# **4. Условия выполнения программ**

## **4.1 Программное обеспечение**

Программное обеспечение «GsecTLS» клиент НЦЭУ рекомендует устанавливать на ПЭВМ , под управлением следующих ОС:

а) Операционная система Windows

– Windows 8 x32/64;

– Windows 10 x32/64.

(В ТаможПроектСофт **GsecTLS** и **NTClient** (КП) были успешно установлены и работают на **Windows 7 max ServicePack 1** )

## **4.2 Аппаратное обеспечение**

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

– тактовая частота процессора не менее 1.4 ГГц;

– объем ОЗУ не менее 2 Гб;

– объем памяти на жестком диске не менее 80 Гб.

КП функционирует на ПЭВМ со следующими характеристиками:

– объем свободного пространства – не менее 100 МБ;

– объем оперативной памяти – не менее 1 ГБ;

– тактовая частота процессора – не менее 2 ГГц.

КП совместим со следующими браузерами: Firefox, Safari, Opera, Chrome.

## **4.3 Порядок получения «GsecTLS» клиент и КП**

Для получения сертифицированных копий программного обеспечения «GsecTLS» клиент и КП необходимо скачать их, пройдя регистрацию в облачном хранилище (заполнить соответствующие формы, размещенные по ссылке - <https://nces.by/service/po/>).(ПрограммаКП предназначена для работы с личным кабинетом в «Е-Паслуге». Для работы с TPSClientустановка КП не нужна)

Порядок регистрации в Облачном хранилище и скачивания программного обеспечения отражены в Приложении 2.

Техническая поддержка по вопросам установки и настройки скаченного программного обеспечения оказывается в Автоматизированной системе технической поддержки пользователей – <https://support.nces.by/>.

**Внимание! Техническая поддержка не оказывается в случае получения вышеуказанного программного обеспечения любыми другими способами, отличными от определенных в данном документе (регистрация в Облачном хранилище).**

# **5. Порядок установки и настройки «GsecTLS» клиент**

## **5.1 Порядок установки «GsecTLS» клиент на ОС семейства Windows**

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

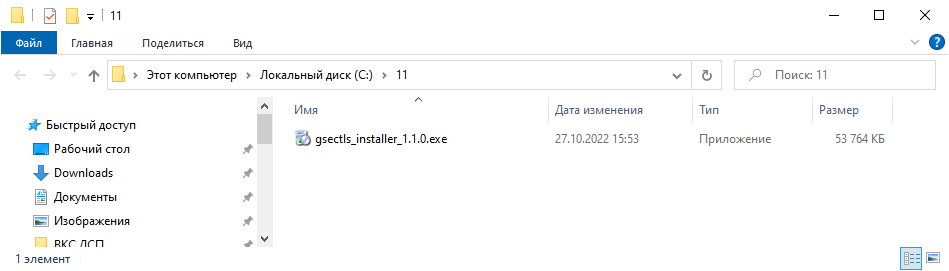


Рисунок 1 – Загрузка дистрибутива GsecTLS клиента

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

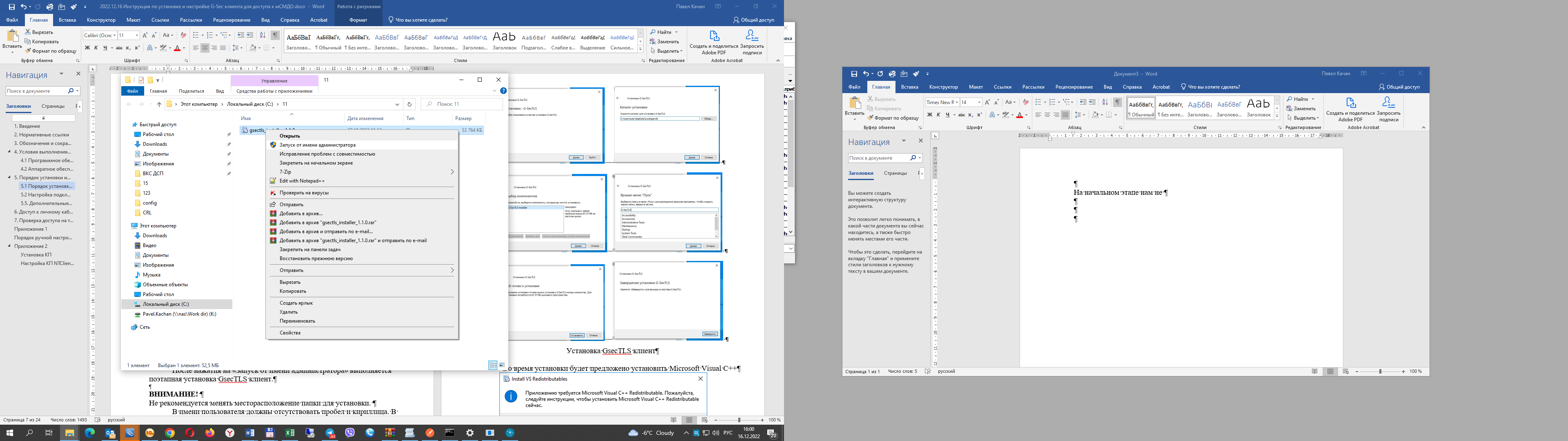


Рисунок 2 – Запуск приложения

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).

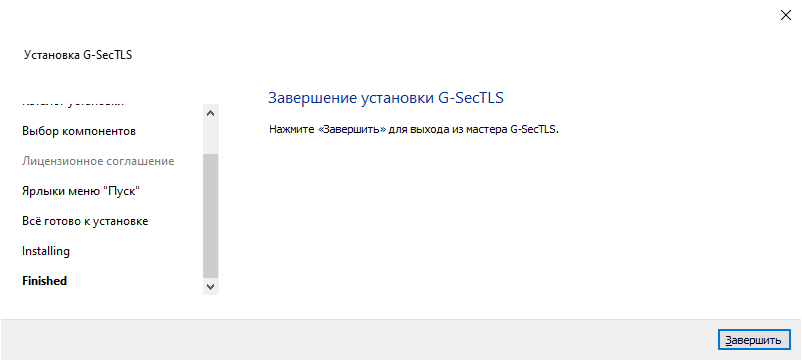
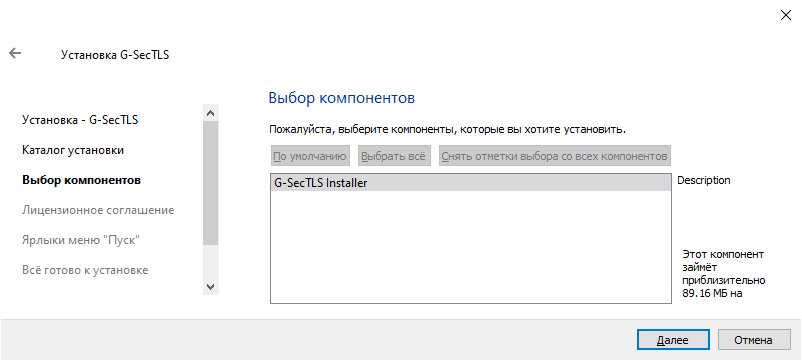
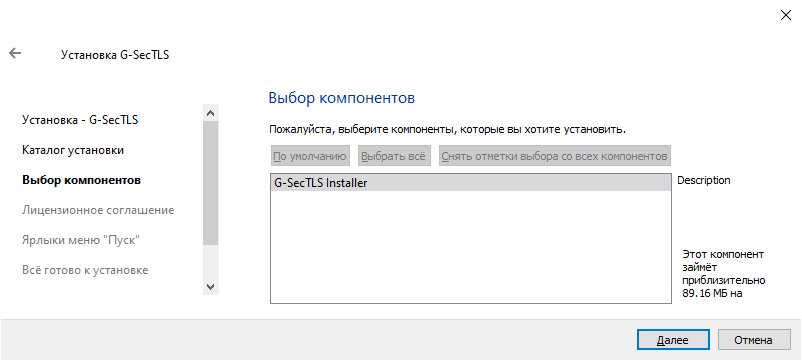
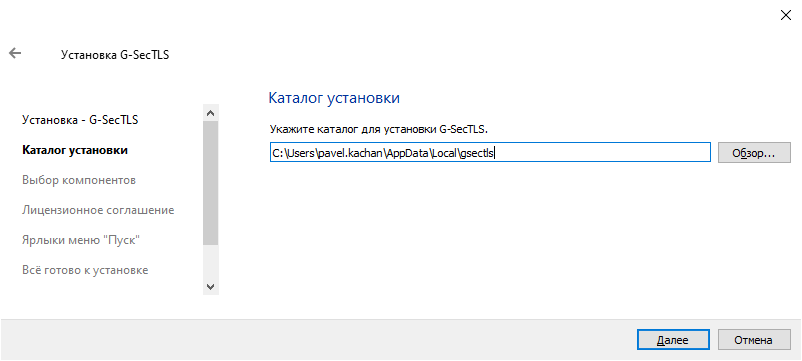
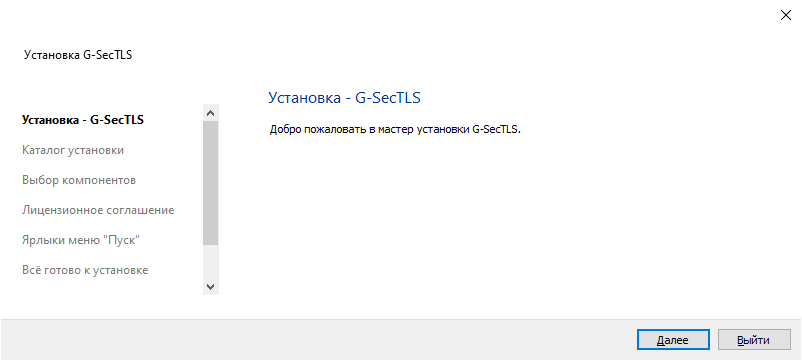
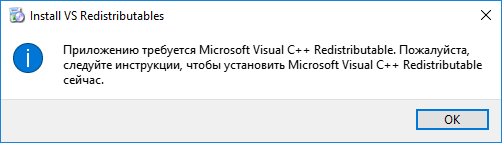
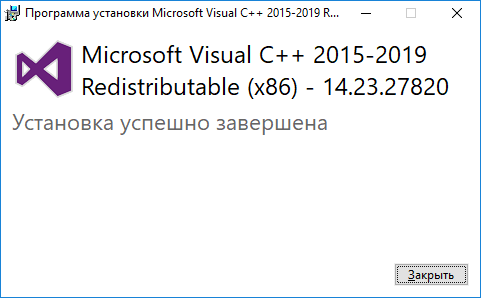
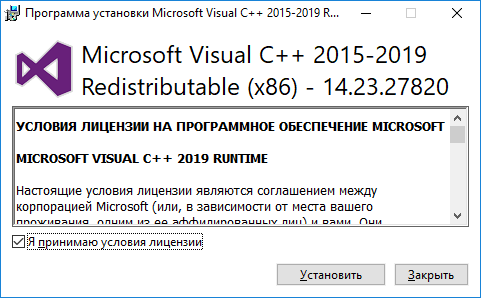


Рисунок 3 – Установка GsecTLS клиент

Во время установки будет предложено установитьMicrosoftVisualC++





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



Рисунок 4 – Ярлык GsecTLS клиент

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



Рисунок 5 –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 | Setting\_up\_AccountGovBy\_Inter\_new.bat |
| VPN через БОТ | Setting\_up\_AccountGovBy\_BOT\_new.bat |
| VPN через БФТ | Setting\_up\_AccountGovBy\_BFT\_new.bat |
| VPNчерез БТК и другие | Setting\_up\_AccountGovBy\_VPN\_new.bat |

Для корректной отработки скрипта, его следует запустить от имени администратора.

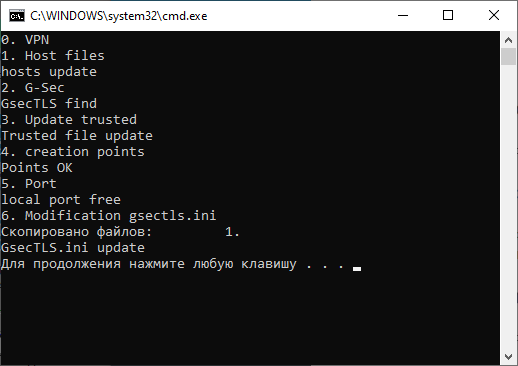
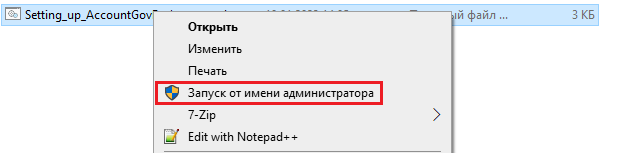


Рисунок 6 – запуск и отработка скрипта

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).

## **5.3 Установка КП**

Для установки КП необходимо запустить файл «NTClientSoftware\_*версия системы\_дата сборки*.exe». На экране появится окно мастера установки (рисунок7), нажать «Далее»

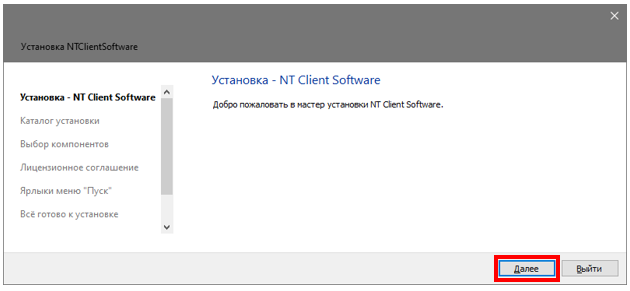


Рисунок 7 – Окно мастера установки

Выбрать каталог для установки программы (рисунок 8), после чего следовать инструкциям мастера установки (Рисунки 9-11).

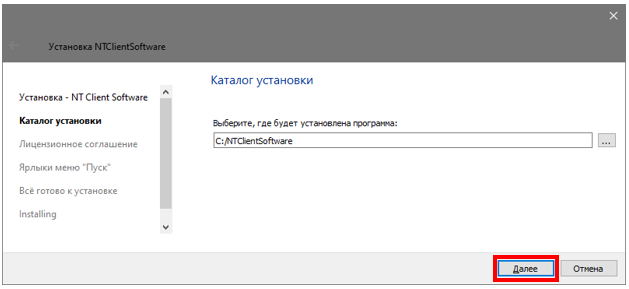


Рисунок 8 – Выбор каталога установки

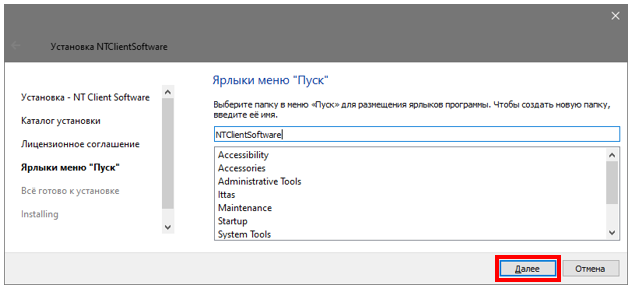


Рисунок 9

Нажать «Установить»

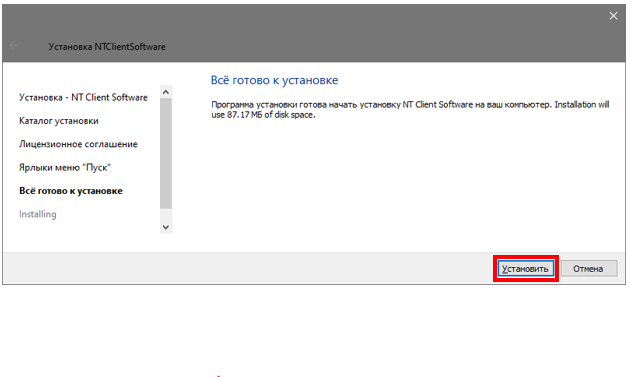


Рисунок 10

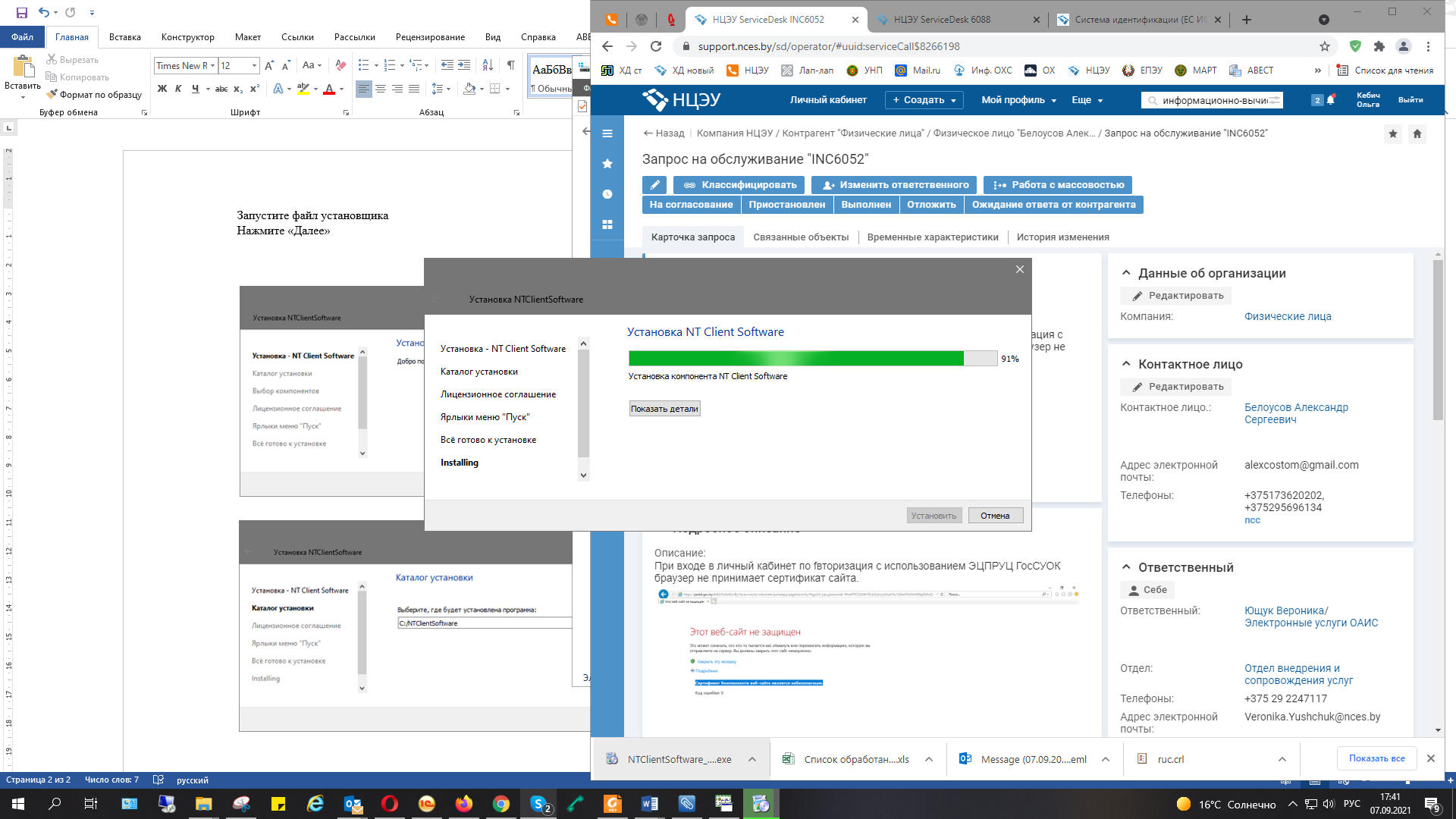


Рисунок 11

 В случае отсутствия сборки наборов библиотек и плагинов   
«MicrosoftVisualC++ Redistributable» на экране появится предложение установить эту сборку (Рисунок 12).

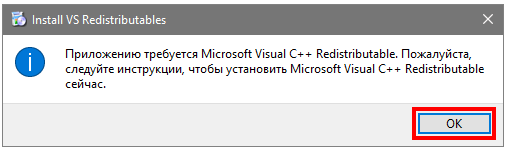


Рисунок 12

Далее необходимо следовать инструкциям мастера установки (Рисунки 13-14).

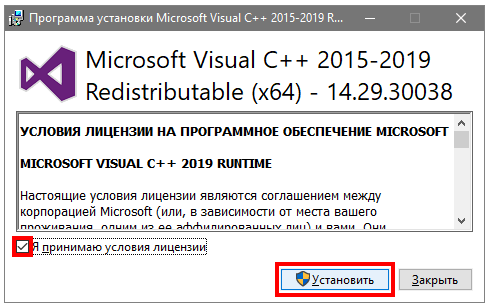


Рисунок 13

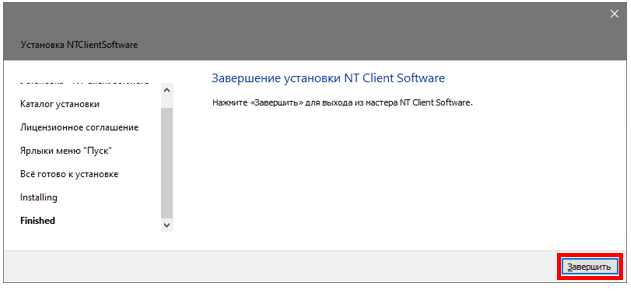


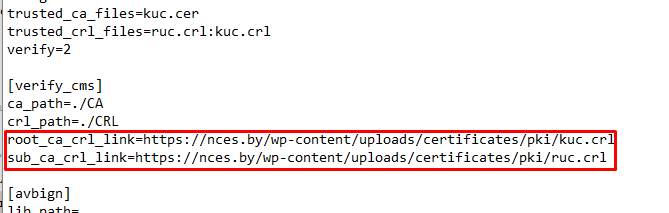
Рисунок 14

Установка завершена, на рабочем столе создан ярлык . Программа установлена в папку «NTClientSoftware» на диске C (если при установке данный путь не был изменен – Рисунок 8).



## **5.4. Настройка КП NTClientSoftware при доступе через VPN**

Для рабочих мест, на которых нет интернета и которые заходят на account.gov.by через VPN сети, необходимо в файле настройки КП **NTClientSoftware (C:\NTClientSoftware\config\NTClientSoftware.ini**) в секции **[**verify\_cms] заменить пути для скачивания CRL



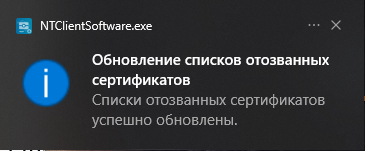
на

*root\_ca\_crl\_link=https://crs.nces.by/files/sertifikaty/kuc.crl*

*sub\_ca\_crl\_link=https://crs.nces.by/files/sertifikaty/ruc.crl*

Для данной настройки в hosts должна быть добавлена запись на crs.nces.by в зависимости от того, vpn-канал какого провайдера используется. Данные записи добавляются скриптом автоматической настройки GsecTLS. В случае выполнения ручной настройки GsecTLS,порядок добавления записи в hosts описан в Приложении 1 инструкции.

После настройки обновления СОС, следует запустить **NTClientSoftware** с рабочего стола. После того как приложение запуститься, в трее должно появится сообщение «Обновление списков отозванных сертификатов. Списки отозванных сертификатов обновлены»



## **5.5. Дополнительные настройки в системе**

В Брандмауэр Windows необходимо добавить в исключения NTClientSoftware.

В антивирусной программе нужно добавить в доверенные домены*account.gov.by,is.gov.by,esiful-idp.gov.by,platform.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. Доступ к личному кабинету**

До попытки входа в личный кабинет ОАИС необходимо запустить «GsecTLS» клиент и «NTClientSoftware».

Для запуска «GsecTLS» клиент необходимо дважды нажать на ярлык GsecTLS, далее – на кнопку «Запуск», рисунок 15, выполняется запуск GsecTLS и осуществляется автоматический переход в раздел «Серверы», рисунок 16.



Рисунок 15 – Переход в раздел «Серверы»

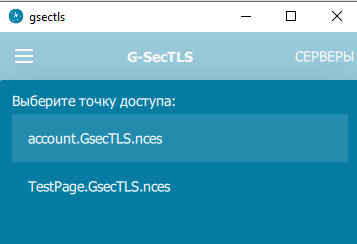


Рисунок 16 – Переход в раздел «Серверы»

Результат запуска.

**Выбирать (нажимать)сервера не нужно**, просто нажимаете «ЗАКРЫТЬ»

Далее двойным щелчком мыши запускается «NTClientSoftware». В сплывающих окнах необходимо нажать «ОК».

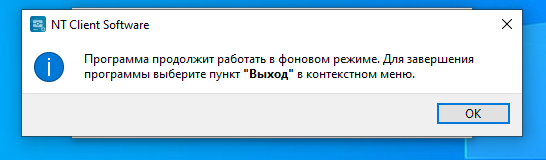
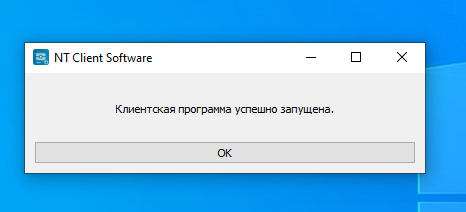


Рисунок 17 – Запуск «NTClientSoftware»

**Внимание!** Программа будет работать в фоновом режиме. Для выхода необходимо в панели задач нажать правой кнопкой мыши на иконку «NTClientSoftware». В открывшемся меню «NTClientSoftware» нажать «Выход».

Далее следует открыть браузер и в адресной строке ввести адрес:

<https://account.gov.by> ,рисунок 18.

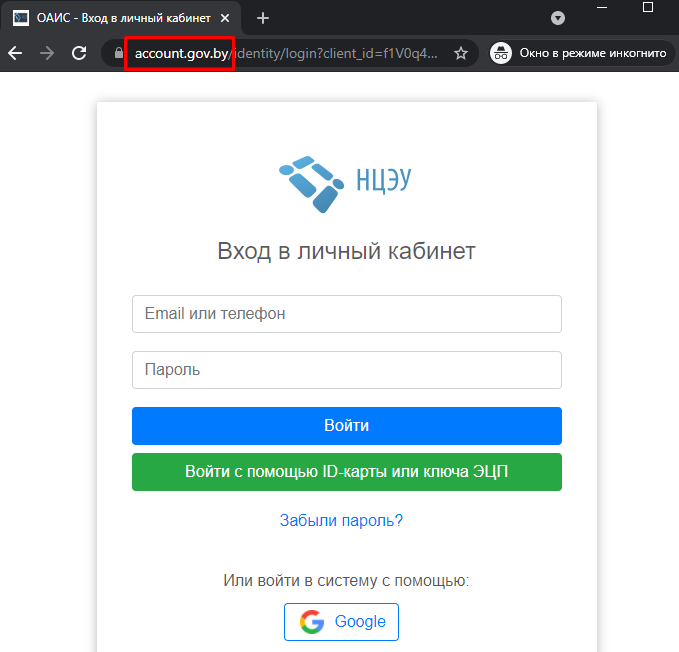


Рисунок 18 – Вход в личный кабинет ОАИС

Порядок авторизации в личном кабинете ОАИС с использованием ключа ЭЦП или ID-карты описаны в соответствующих инструкциях.

# **7. Проверка доступа на тестовый сайт**

Запускаем «GsecTLS», рисунок 19, выполняется автоматический запуск GsecTLS

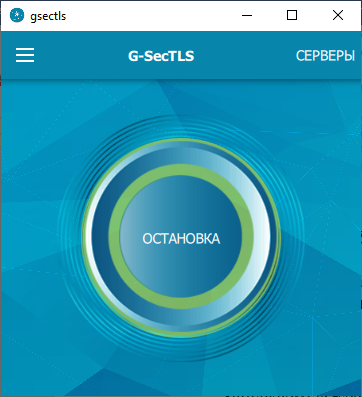


Рисунок 19 –запуск G-Sec

Для перехода к тестовой странице в браузере необходимо набрать

http://127.0.0.1:9080/

Переходите на тестовый сайт



# **Приложение 1**

# **Ручная настройка доступа**

**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 account.gov.by

127.0.0.1 is.gov.by

127.0.0.1 esiful-idp.gov.by

127.0.0.1 gw.gov.by

127.0.0.1 apimgw.core.oais.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

10.53.5.109esiful.gov.by

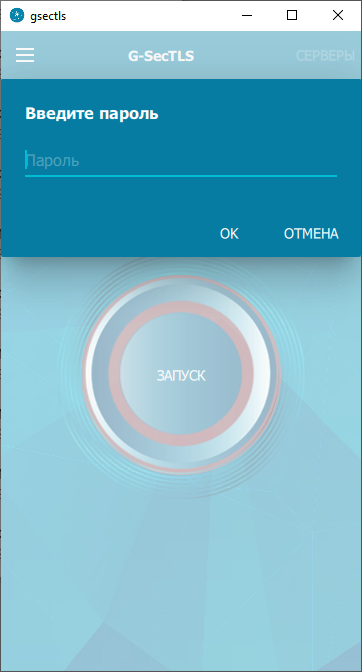
127.0.0.1 gw.gov.by

10.53.8.35 crs.nces.by

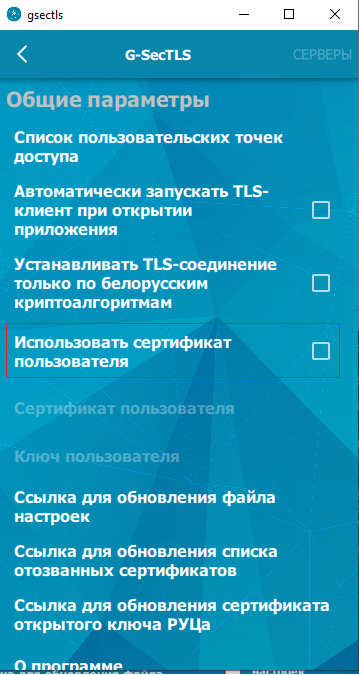
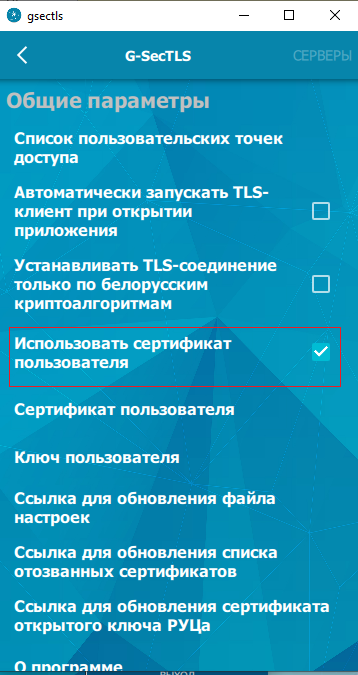
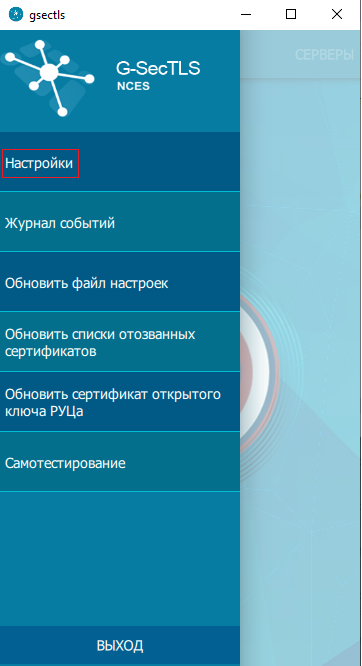
# **Порядок настройки «GsecTLS» клиент**

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 окнезайти 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»

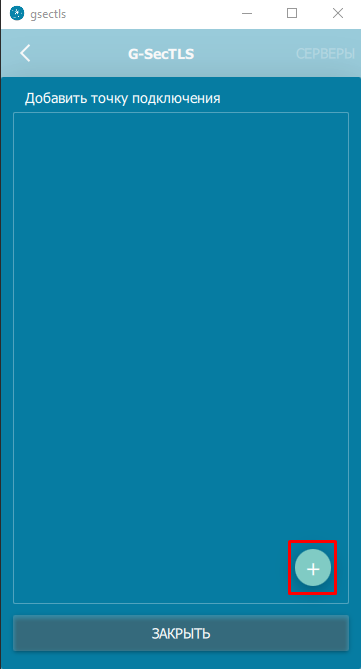
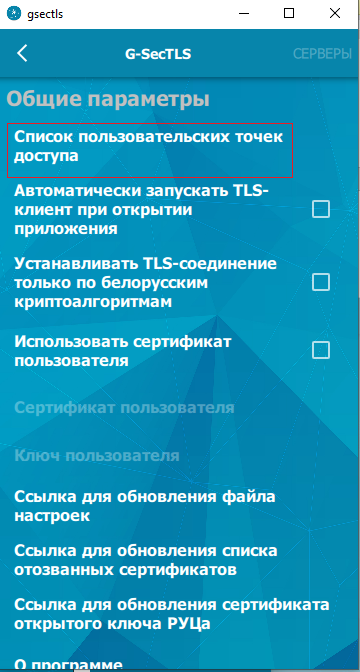
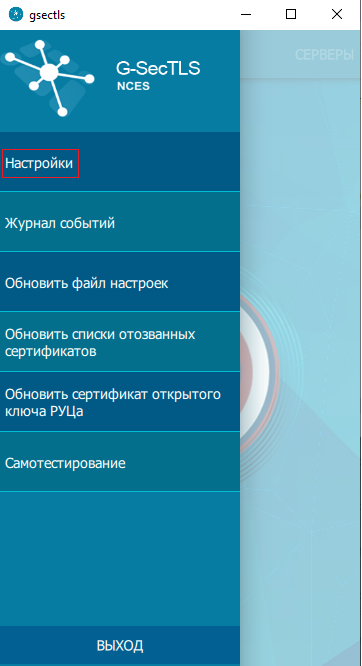


После запуска программы необходимо настроить точки подключения. Для этого необходимо в открывшемся окне зайти в верхнем левом углу в меню .



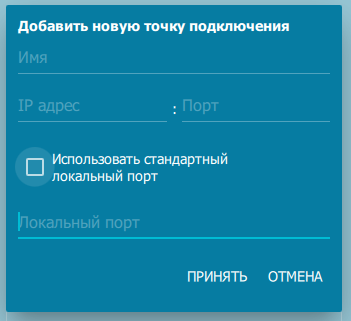
Пункт меню «GsecTLS» клиент

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 две точки подключения со следующими атрибутами:

В соответствии от провайдера используются следующие IP адреса:

Internet – 185.227.96.96

VPNот БОТ – 10.252.0.35

VPNот БФТ – 10.53.8.35

VPNот БТК и другие – 10.101.1.35

**Имя:**account.GsecTLS.nces

**IP адрес:** <IPадрес провайдера>

**Порт:** 11004

**Локальный порт:**443

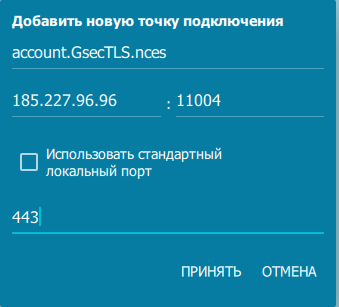
Повторить создание второй точки

**Имя:**TestPage.GsecTLS.nces

**IP адрес:** <IPадрес провайдера>

**Порт:** 11000

**Локальный порт:**9080



Добавление точки подключения account.gov.by

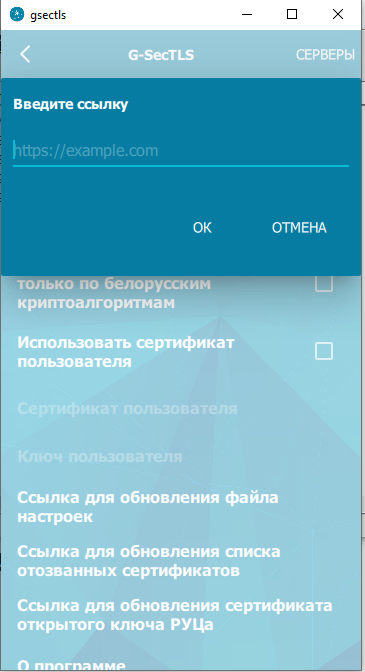
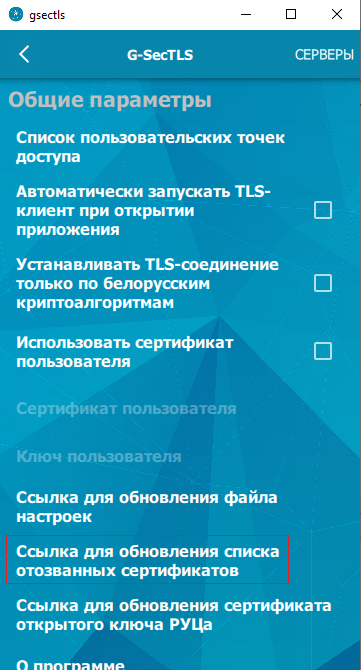
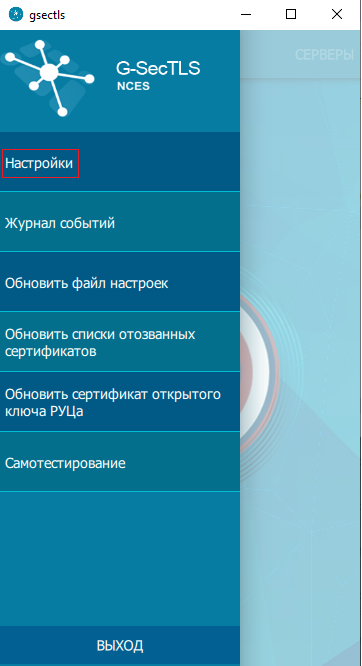
Для обновления СОС следует зайти в верхнем левом углу в меню .



Пункт меню «GsecTLS» клиент

Выбрать «Настройки ->Ссылка для обновления списка отозванных сертификатов» и ввести ссылку:

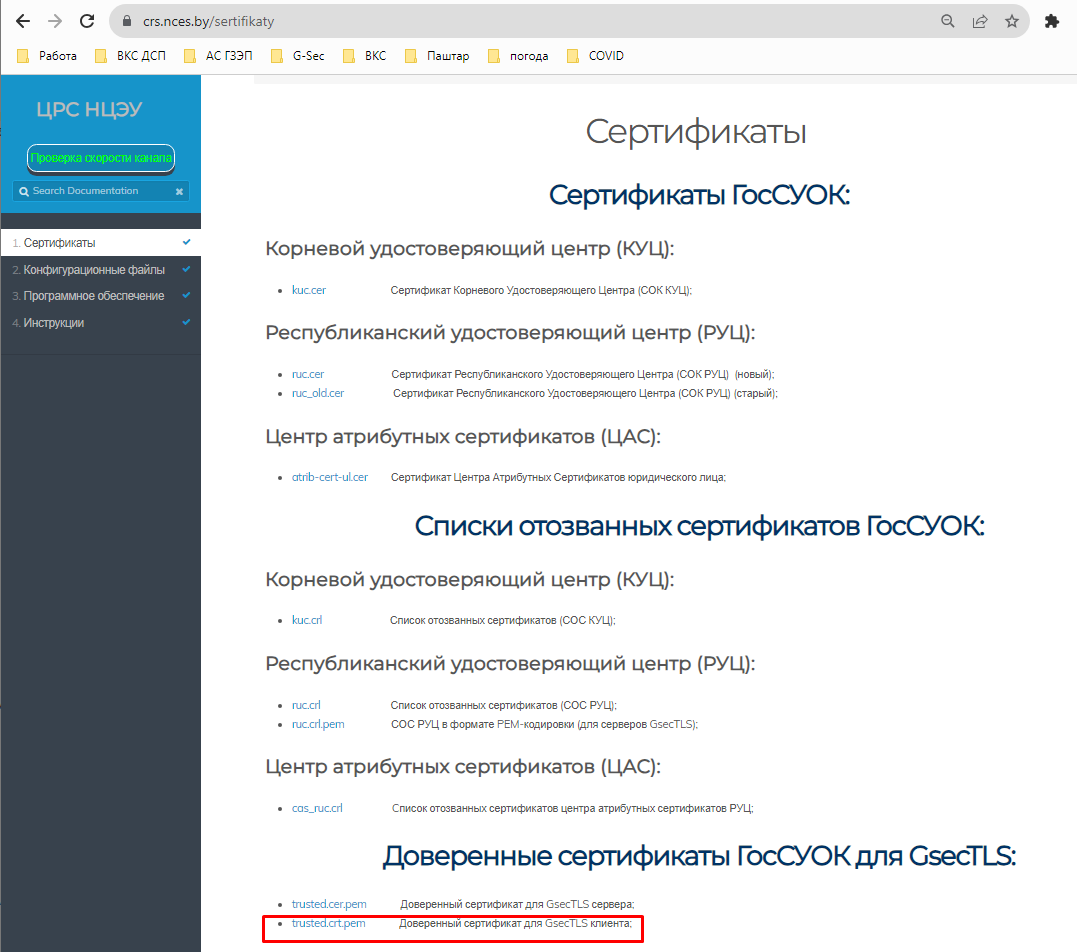
https://crs.nces.by/files/sertifikaty/ruc.crl.pem



Настройка обновления СОС

**Обновление файла СОС КУЦ**

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



Файлы СОС КУЦ

Замена на клиенте GsecTLS выполняется следующим образом:

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

Заменить файл в каталоге

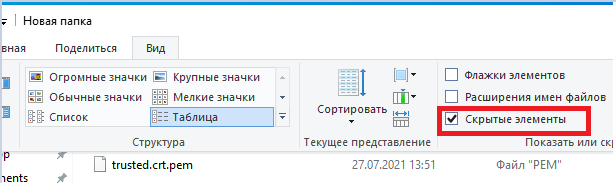
Для пользователей **Windows**:

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 GsecTLS клиент.

# **Приложение 2**

# **Регистрация в Облачном хранилище, скачивание программного обеспечения**

Для получения сертифицированных копий программного обеспечения «GsecTLS» клиент и КП необходимо скачать их, пройдя регистрацию в облачном хранилище заполнить соответствующие формы, размещенные по ссылке - <https://nces.by/service/po/>.

Для получения реквизитов доступа к облачному хранилищу необходимо заполнить все обязательные поля, и нажать «Отправить код» (Рисунок 1)

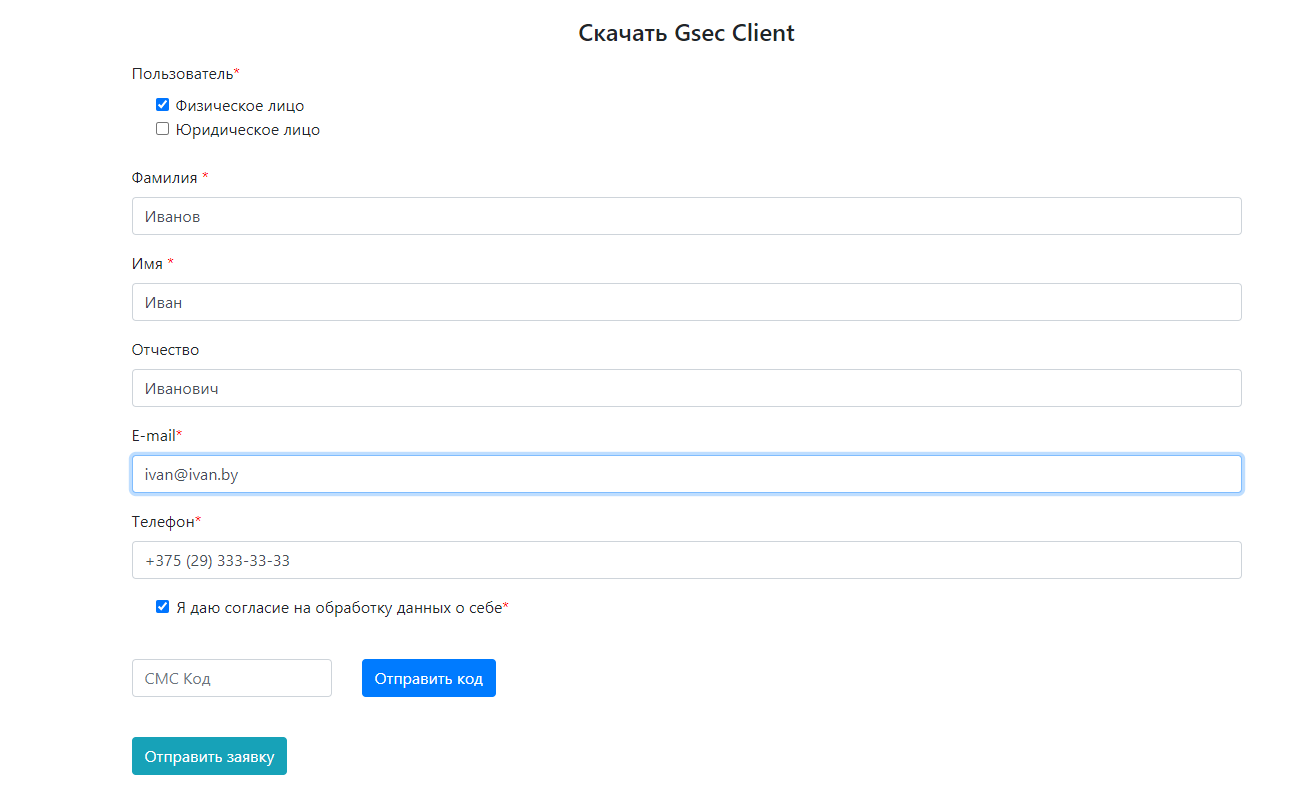


Рисунок 1

Далее в поле необходимо ввести код, поступивший на номер мобильного телефона, указанный в форме, после нажатия на кнопку «Отправить код», и нажать «Отправить заявку».

После выполнения указанных действий на e-mail, указанный в форме, поступит сообщение, содержащее ссылку, логин и пароль для входа в облачное хранилище.

Для скачивания «GsecTLS» клиент необходимо в Облачном хранилище выделить вложенные файлы (GsecTLS и скрипт для настройки GsecTLS) и нажать «Скачать» (Рисунок 2).

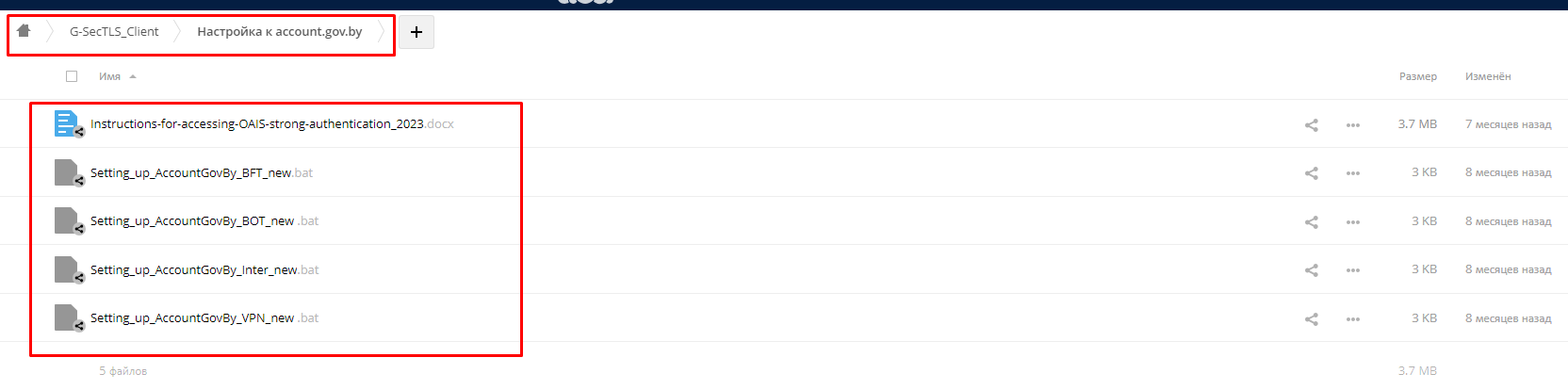
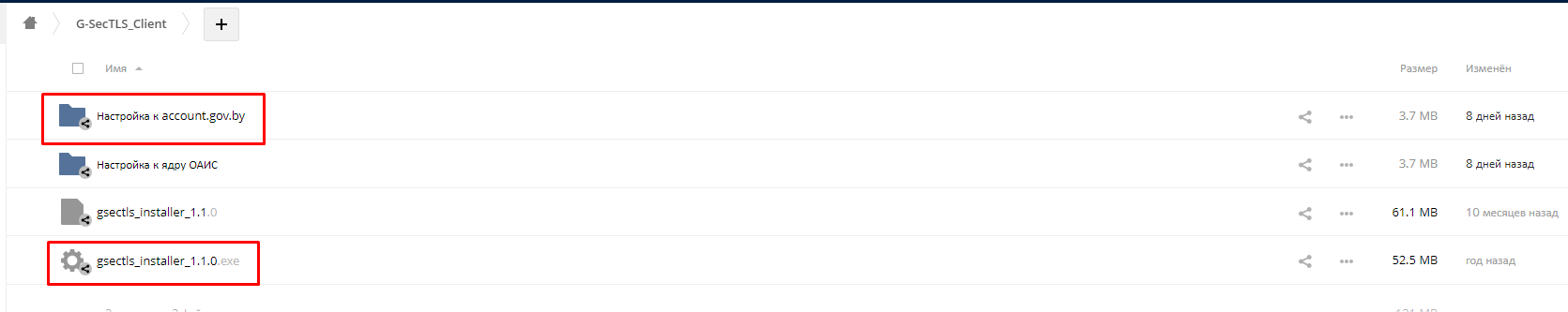


Рисунок 2

Для установки скаченного программного обеспечения необходимо совершить действия, описанные в п.п. 5.1 и 5.2 настоящей инструкции.

Порядок регистрации в облачном хранилище для получения КП аналогичен, описанному для получения «GsecTLS» клиент.

После заполнения формы для получения КП в созданное Облачное хранилище (при получении «GsecTLS» клиент) будет добавлена возможность скачать КП (Рисунок 3).

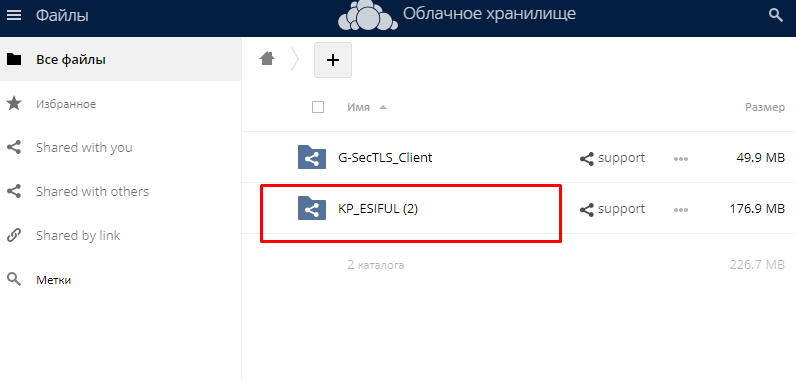


Рисунок 3

Для установки КП необходимо скачать в Облачном хранилище файл и и продолжить установку в соотвествии с п.п. 5.3 настоящей иснтрукции.