**РЕСПУБЛИКАНСКОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ**

**«НАЦИОНАЛЬНЫЙ ЦЕНТР ЭЛЕКТРОННЫХ УСЛУГ»**

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

**ИНСТРУКЦИЯ**

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

**со строгой аутентификацией**

Минск 2024

Оглавление

[1. Введение 3](#_Toc158729891)

[2. Нормативные ссылки 4](#_Toc158729892)

[3. Обозначения и сокращения 5](#_Toc158729893)

[4. Условия выполнения программ 6](#_Toc158729894)

[4.1 Программное обеспечение 6](#_Toc158729895)

[4.2 Аппаратное обеспечение 6](#_Toc158729896)

[4.3 Порядок получения КП и «GsecTLS» клиент 6](#_Toc158729897)

[5. Установка КП 7](#_Toc158729898)

[5.1 Дополнительные настройки в системе 11](#_Toc158729899)

[6. Порядок установки и настройки «GsecTLS» клиент на ОС семейства Windows 11](#_Toc158729900)

[6.1 Настройка доступа посредством скрипта 15](#_Toc158729901)

[6.2 Ручная настройка доступа 16](#_Toc158729902)

[6.2.1 Настройка файла hosts 18](#_Toc158729903)

[6.2.2 Обновление файла СОС КУЦ 20](#_Toc158729904)

[7. Проверка доступа к тестовому сайту 21](#_Toc158729905)

[8. Доступ к личному кабинету 22](#_Toc158729906)

[Приложение 1 Регистрация в Облачном хранилище, скачивание программного обеспечения 25](#_Toc158729907)

# **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 Клиентского приложения для работы с идентификационной картой (КП).

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).

С целью обеспечения требований законодательства в области защиты информации юридическим и физическим лицам для обеспечения криптографической защиты передаваемых данных рекомендуется установка «GsecTLS» клиент. «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.

«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 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 |
|  |  |  |

# **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 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 КП и «GsecTLS» клиент**

Для получения сертифицированных копий программного обеспечения КП и «GsecTLS» клиент необходимо скачать их, пройдя регистрацию в облачном хранилище (заполнить соответствующие формы, размещенные по ссылке <https://nces.by/service/po/>). Порядок регистрации в Облачном хранилище и скачивания программного обеспечения отражены в Приложении 1.

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. Установка КП**

Для установки КП необходимо запустить файл «NTClientSoftware\_*версия системы\_дата сборки*.exe». На экране появится окно мастера установки (Рисунок 1), нажать «Далее».

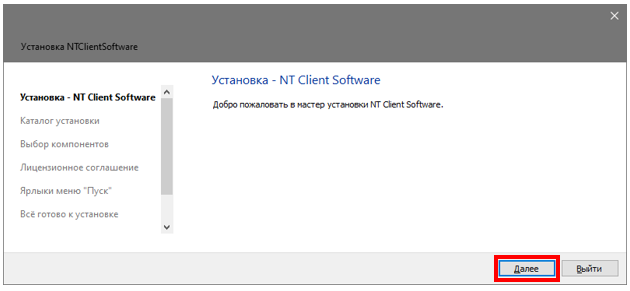


Рисунок 1

Выбрать каталог для установки программы (Рисунок 2), после чего следовать инструкциям мастера установки (Рисунки 3-5).

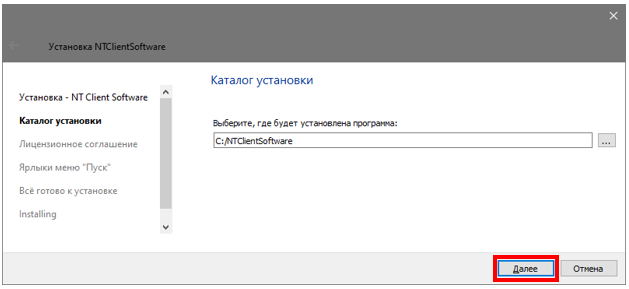


Рисунок 2

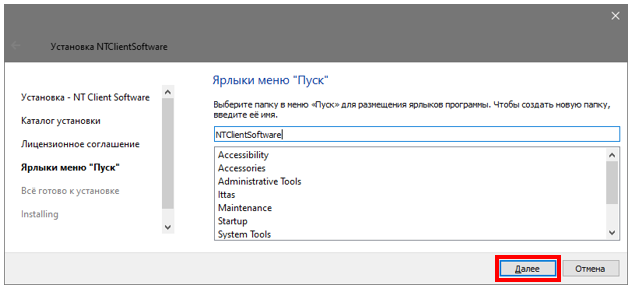


Рисунок 3

Нажать «Установить».

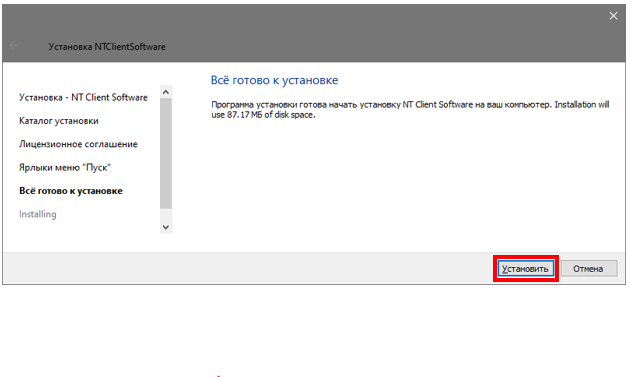


Рисунок 4

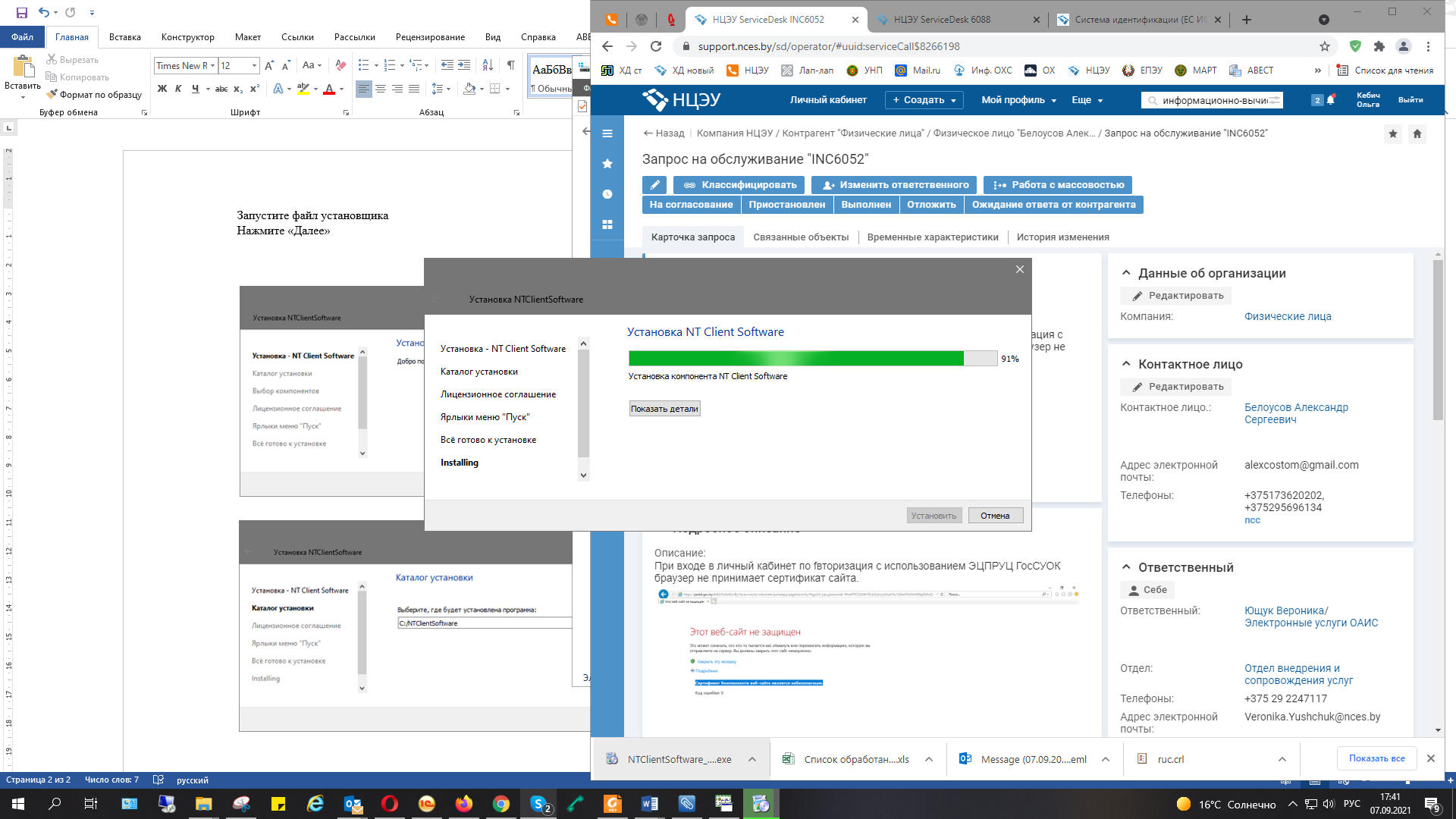


Рисунок 5

 В случае отсутствия сборки наборов библиотек и плагинов   
«Microsoft Visual C++ Redistributable» на экране появится предложение установить эту сборку (Рисунок 6).

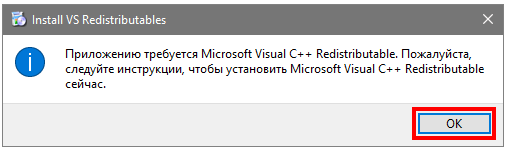


Рисунок 6

Далее необходимо следовать инструкциям мастера установки (Рисунки 7-8).

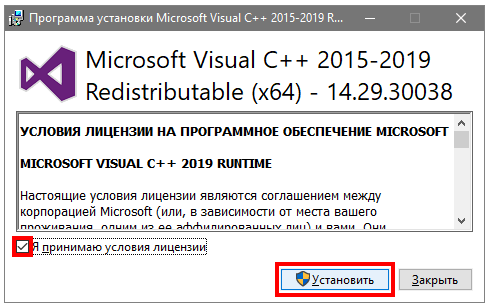


Рисунок 7

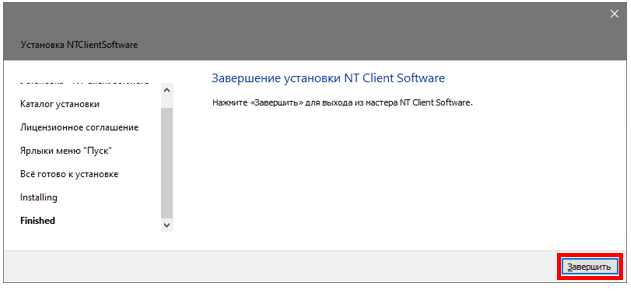


Рисунок 8

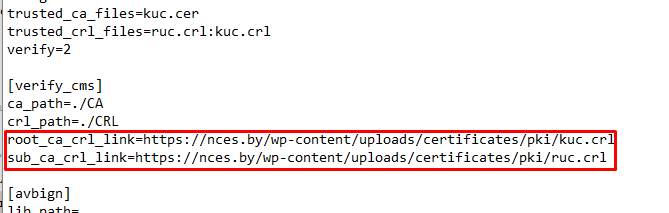
Установка завершена, на рабочем столе создан ярлык NTClientSoftware.



Рисунок 9

Программа установлена в папку «NTClientSoftware» на диске C:\ (если при установке данный путь не был изменен – Рисунок 2).

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 файл hosts необходимо добавить запись на crs.nces.by в зависимости от того, VPN какого провайдера используется.

|  |  |
| --- | --- |
| Способ подключения\* | Добавляемая запись |
| VPN через БОТ | 10.252.0.35 crs.nces.by |
| VPN через БФТ | 10.53.8.35 crs.nces.by |
| VPN через БТК и другие | 10.101.1.35 crs.nces.by |

\* БОТ – Белорусские облачные технологии

БФТ – Банковско-финансовая телесеть

БТК – Белтелеком

Чтобы отредактировать файл hosts вручную, необходимо открыть блокнот с правами администратора и открыть файл, расположенный по пути C:\Windows\System32\drivers\etc. Внести соответствующую запись.

**ВНИМАНИЕ!** В случае установки и настройки «GsecTLS» при помощи скрипта, данные записи добавляются автоматически (см. [п. 6.1](#_6.1__Настройка)).

После настройки обновления СОС необходимо запустить NTClientSoftware с рабочего стола. После того, как приложение запустится, в трее должно появиться сообщение «Обновление списков отозванных сертификатов. Списки отозванных сертификатов обновлены».

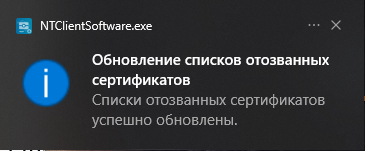


Рисунок 10

## **5.1 Дополнительные настройки в системе**

В Брандмауэр Windows необходимо добавить в исключения NTClientSoftware.

В антивирусной программе необходимо 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. Порядок установки и настройки «GsecTLS» клиент на ОС семейства Windows**

С целью обеспечения требований законодательства в области защиты информации юридическим и физическим лицам для обеспечения криптографической защиты передаваемых данных рекомендуется установка «GsecTLS» клиент[[1]](#footnote-1).

Для этого необходимо загрузить дистрибутив «GsecTLS» клиент на персональный компьютер (далее – ПК) (Рисунок 11).

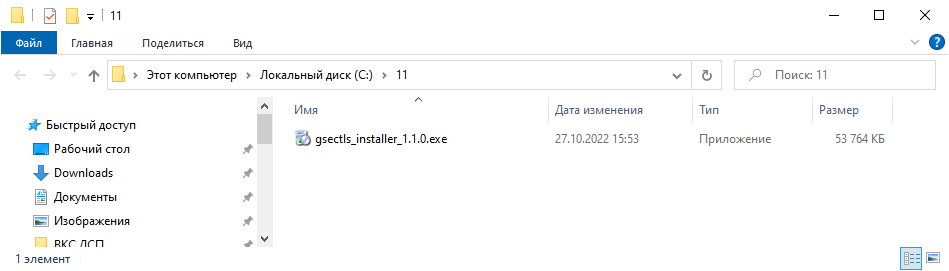


Рисунок 11

Нажав правой кнопкой мыши на загруженное приложение (Рисунок 12), выбрать «Запуск от имени администратора» и запустить его, кликнув левой кнопкой мыши.

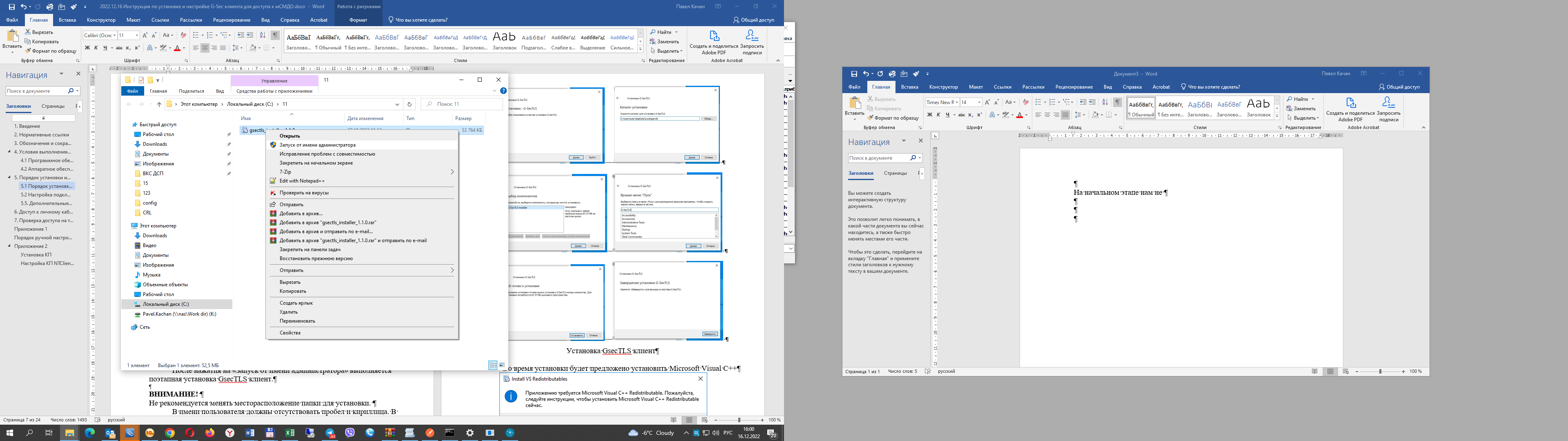


Рисунок 12

После нажатия на «Запуск от имени администратора» выполняется поэтапная установка «GsecTLS» клиент (Рисунок 13).

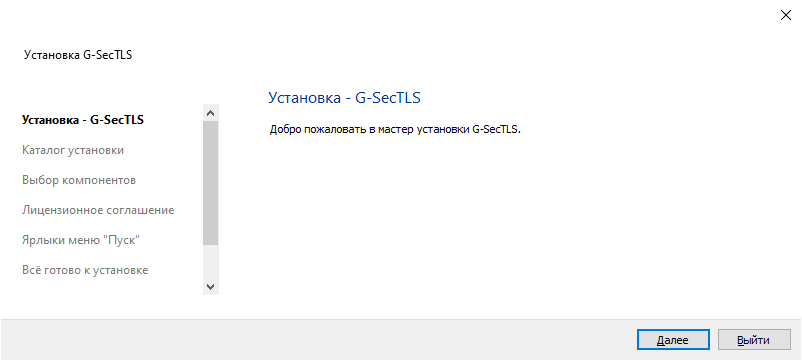
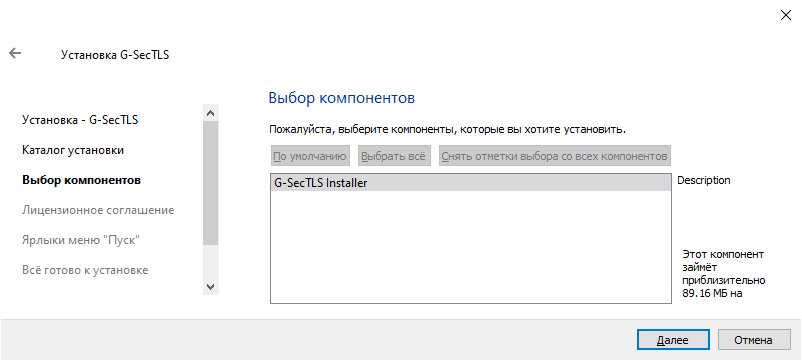
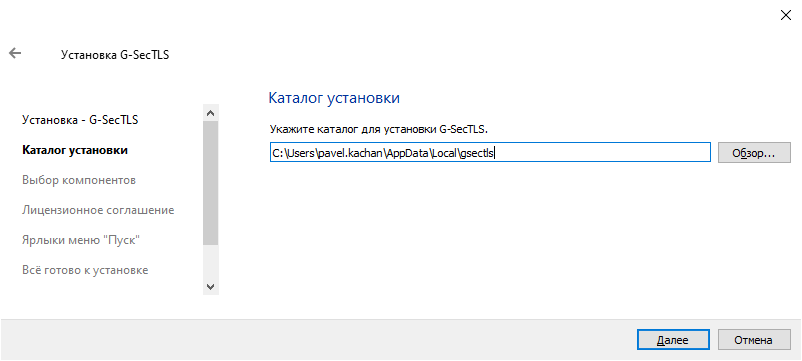
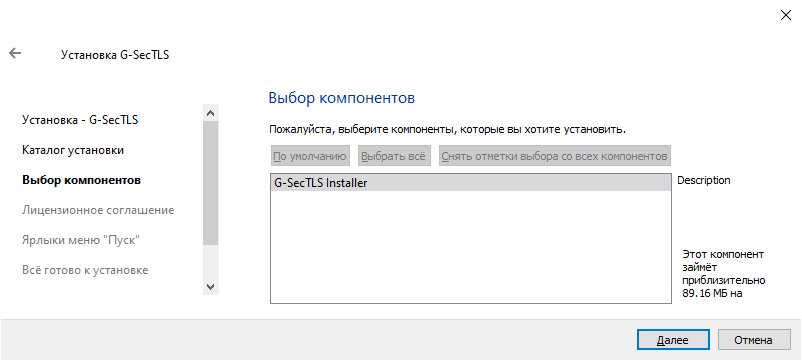
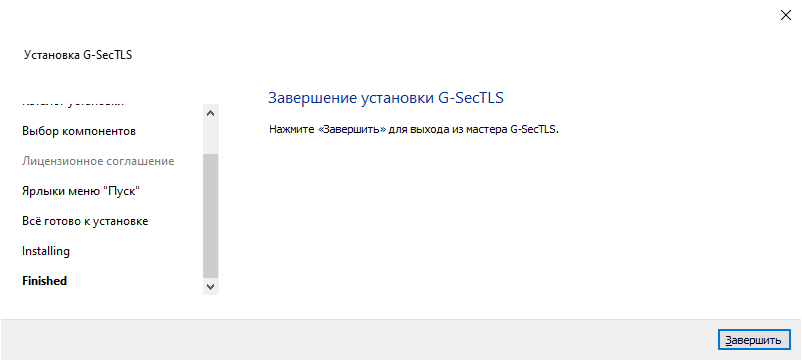
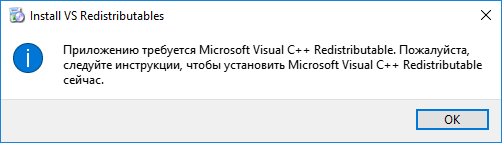
   

Рисунок 13

Во время установки будет предложено установить Microsoft Visual C++



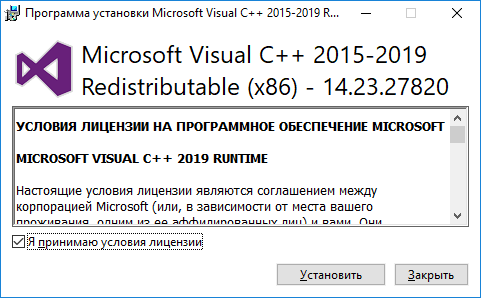
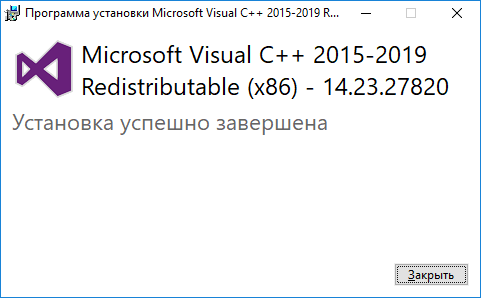
 

Рисунок 14

**ВНИМАНИЕ!**

Не рекомендуется менять месторасположение папки для установки.

В пути должны отсутствовать пробел и кириллица. Если в пути присутствуют пробел и кириллица, пользователю необходимо установить ПО в доступную папку (например, создать папку c:\gsectls) и произвести настройку ПО в ручном режиме в соответствии с порядком установки и настройки «GsecTLS» ([п.6.2](#_6.2_Ручная_настройка)).

После завершения установки «GsecTLS» клиент необходимо запустить ярлык «GsecTLS» на рабочем столе (Рисунок 15).



Рисунок 15

При первом запуске может появиться сообщение о необходимости введения пароля.

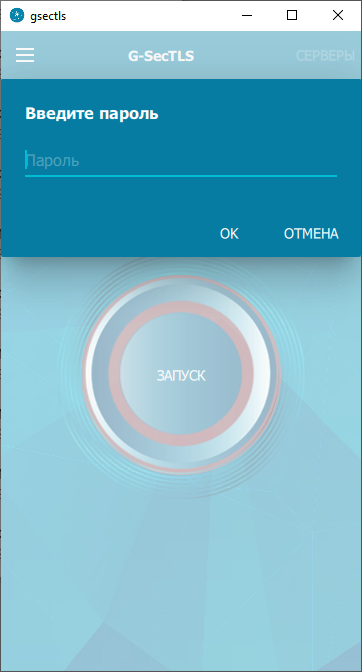


Рисунок 16

Для продолжения необходимо нажать «ОТМЕНА». Далее необходимо в открывшемся окне зайти в верхнем левом углу в меню , перейти в «Настройки» и снять галочку «Использовать сертификат пользователя».

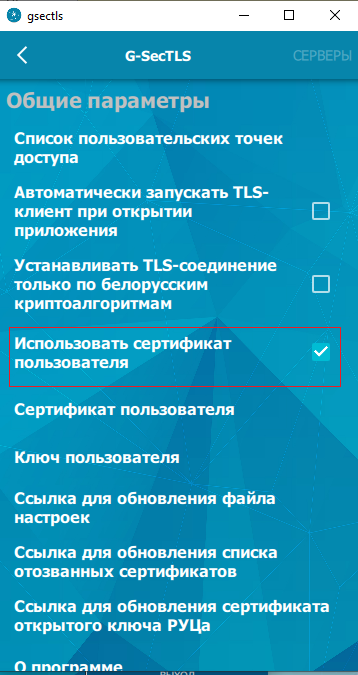
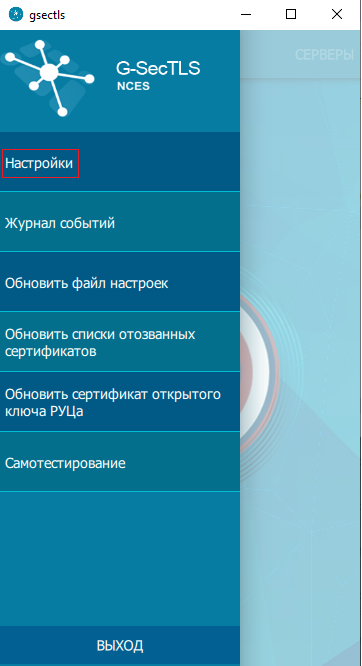


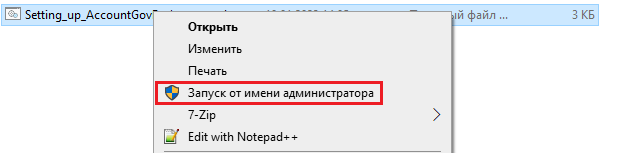
Рисунок 17

### **6.1 Настройка доступа посредством скрипта**

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

|  |  |
| --- | --- |
| Способ подключения | Имя исполняемого файла |
| Интернет | Setting\_up\_AccountGovBy\_Inter\_new.bat |
| VPN через БОТ | Setting\_up\_AccountGovBy\_BOT\_new.bat |
| VPN через БФТ | Setting\_up\_AccountGovBy\_BFT\_new.bat |
| VPN через БТК и другие | Setting\_up\_AccountGovBy\_VPN\_new.bat |

Скрипт необходимо запустить от имени администратора.



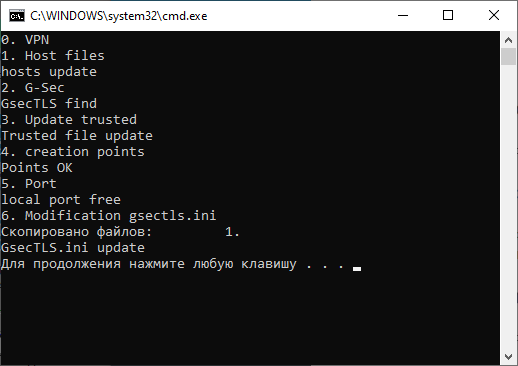


Рисунок 18

При возникновении ошибок или при отсутствии возможности настроить «GsecTLS» клиент с использованием скрипта, необходимо произвести настройку ПО в ручном режиме. Порядок ручной настройки описан в п. [6.2](#_6.2_Ручная_настройка) настоящей инструкции.

В случае корректного завершения настройки, необходимо перейти к [проверке доступа к тестовому сайту](#_7._Проверка_доступа).

### **6.2 Ручная настройка доступа**

**ВНИМАНИЕ!** Данный пункт выполняется в случае возникновения ошибок либо при отсутствии возможности настроить «GsecTLS» клиент с использованием скрипта (изменен путь установки «GsecTLS»).

Если «GsecTLS» настроен при помощи скрипта, данный пункт необходимо пропустить и перейти к [проверке доступа к тестовому сайту](#_7._Проверка_доступа)

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



Рисунок 19

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

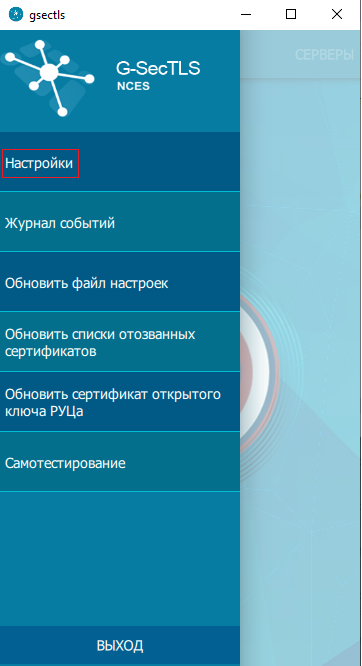
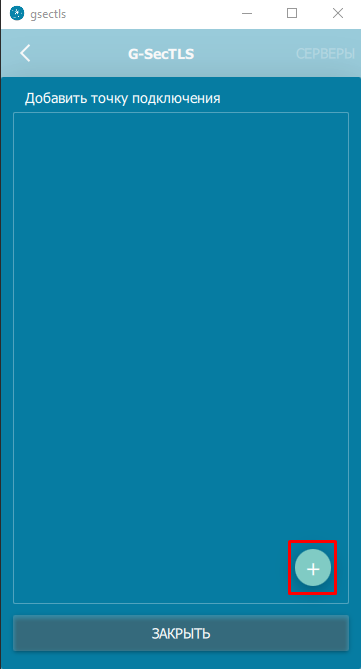
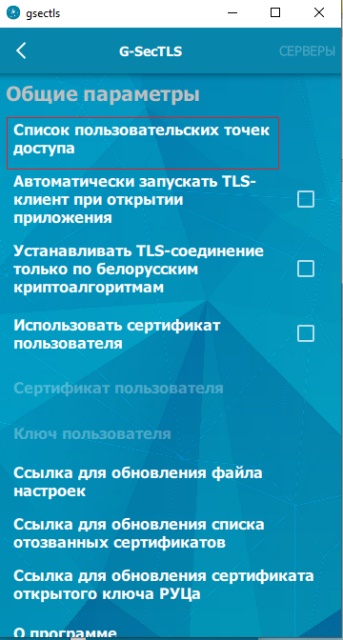
  

Рисунок 20

В открывшемся окне необходимо ввести данные точки подключения.

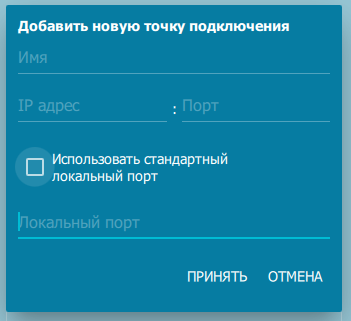


Рисунок 21

Для подключения к личному кабинету необходимо настроить две точки подключения со следующими атрибутами:

**ВНИМАНИЕ!** В зависимости от провайдера используются следующие IP адреса:

Интеренет – 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

**Точки подключения:**

**Имя:** account.GsecTLS.nces

**IP адрес:** <IP адрес провайдера>

**Порт:** 11004

**Локальный порт:** 443

Повторить создание второй точки

**Имя:** TestPage.GsecTLS.nces

**IP адрес:** <IP адрес провайдера>

**Порт:** 11000

**Локальный порт:** 9080

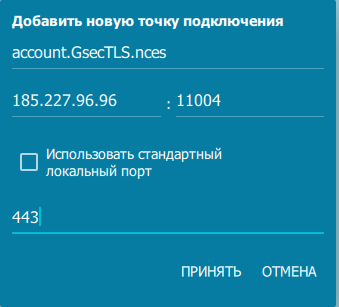


Рисунок 22

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



Рисунок 23

Выбрать «Настройки -> Ссылка для обновления списка отозванных сертификатов» и ввести ссылку (Рисунок 24):

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

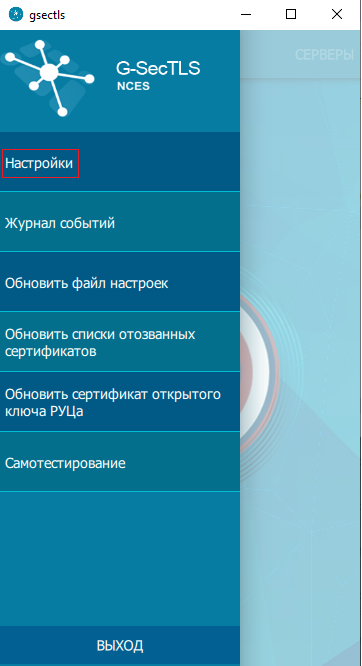
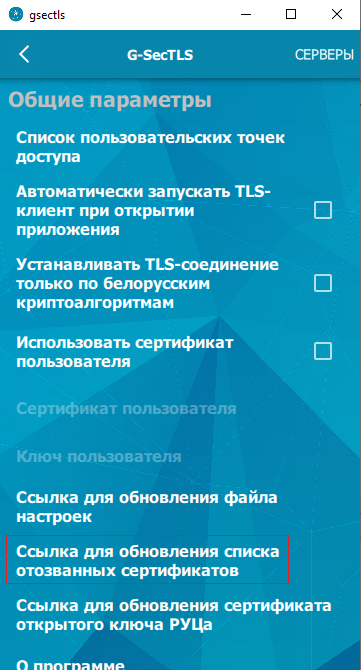
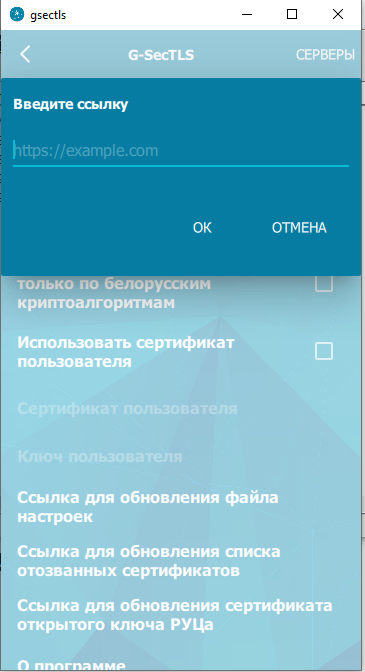
  

Рисунок 24

### **6.2.1 Настройка файла hosts**

Чтобы отредактировать файл необходимо открыть блокнот с правами администратора и открыть файл, расположенный по пути C:\Windows\System32\drivers\etc (Рисунок 25).

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

Рисунок 25

Для доступа к сайту [**https://account.gov.by/**](https://account.gov.by/)необходимо (в зависимости от способа подключения (провайдера) в файле **hosts** (C:\Windows\System32\drivers\etc) прописать:

**Интернет[[2]](#footnote-2)**

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

**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

10.53.8.35 crs.nces.by

## **6.2.2 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/**](https://crs.nces.by/sertifikaty/) **.**

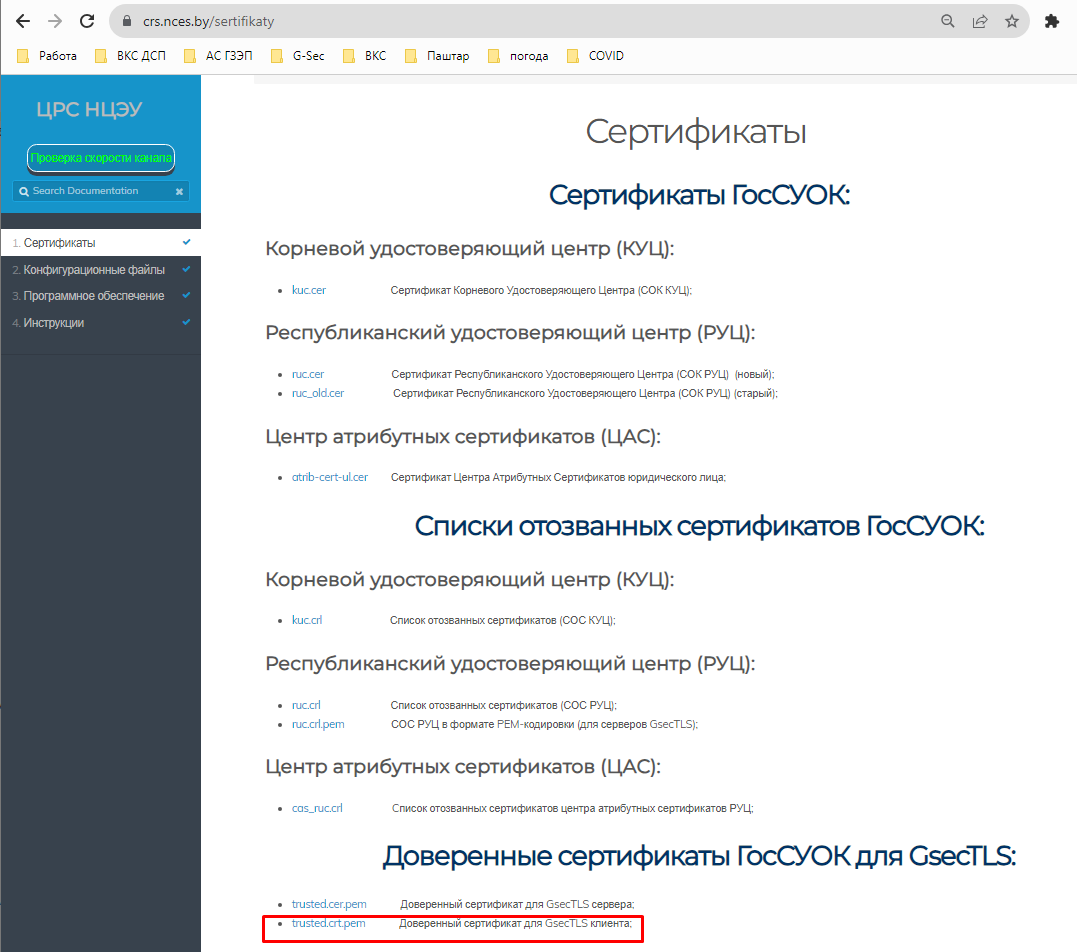


Рисунок 26

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» (Рисунок 27).

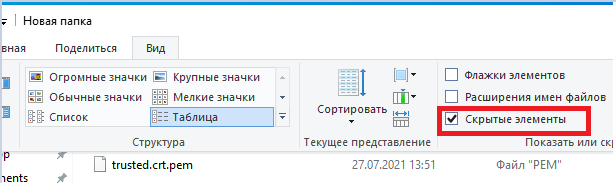


Рисунок 27

После замены необходимо перезагрузить клиент.

# **7. Проверка доступа к тестовому сайту**

Запускаем «GsecTLS», выполняется автоматический запуск «GsecTLS» (Рисунок 28).

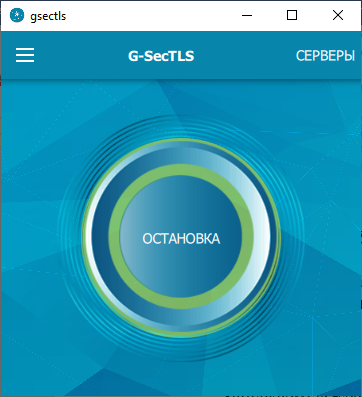


Рисунок 28

Для перехода к тестовой странице в браузере необходимо набрать <http://127.0.0.1:9080/>. Должен открыться тестовый сайт.



Рисунок 29

# **8. Доступ к личному кабинету**

До попытки входа в личный кабинет ОАИС необходимо запустить «NTClientSoftware» и «GsecTLS»[[3]](#footnote-3) клиент.

Для запуска «GsecTLS» клиент необходимо дважды нажать на ярлык «GsecTLS». Далее – на кнопку «Запуск». Выполнится запуск «GsecTLS» и произойдет автоматический переход в раздел «Серверы» (Рисунок 31).



Рисунок 30

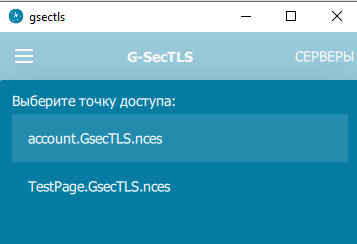
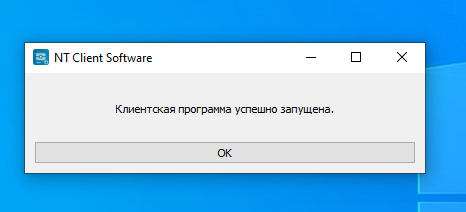


Рисунок 31

**В окне «Серверы» выбирать (нажимать)** **сервер не нужно**. Необходимо нажать «ЗАКРЫТЬ» внизу окна.

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



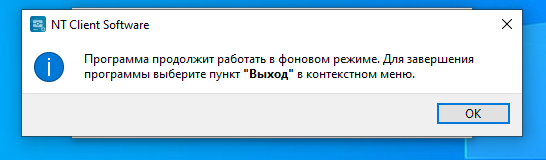


Рисунок 32

**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 33

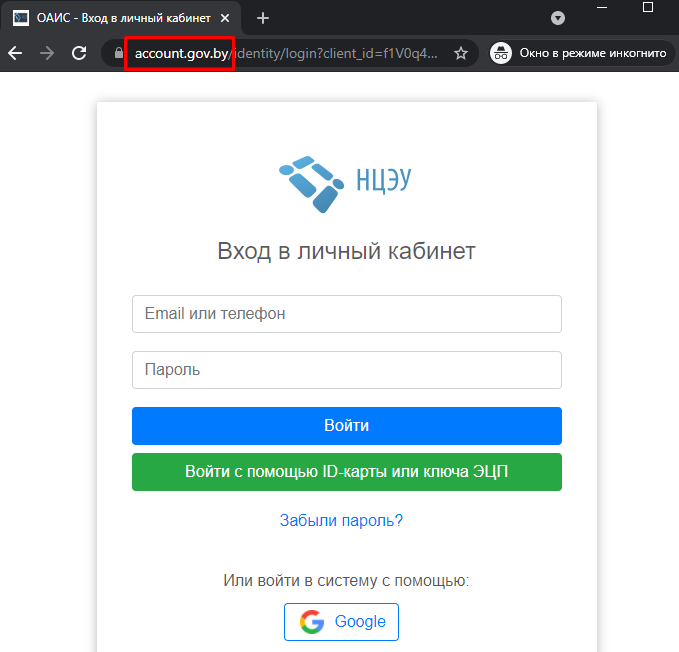


Рисунок 33

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

# **Приложение 1**

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

Для получения сертифицированных копий программного обеспечения КП и «GsecTLS» клиент 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, нажать «Выслать код подтверждения» (Рисунок 1).

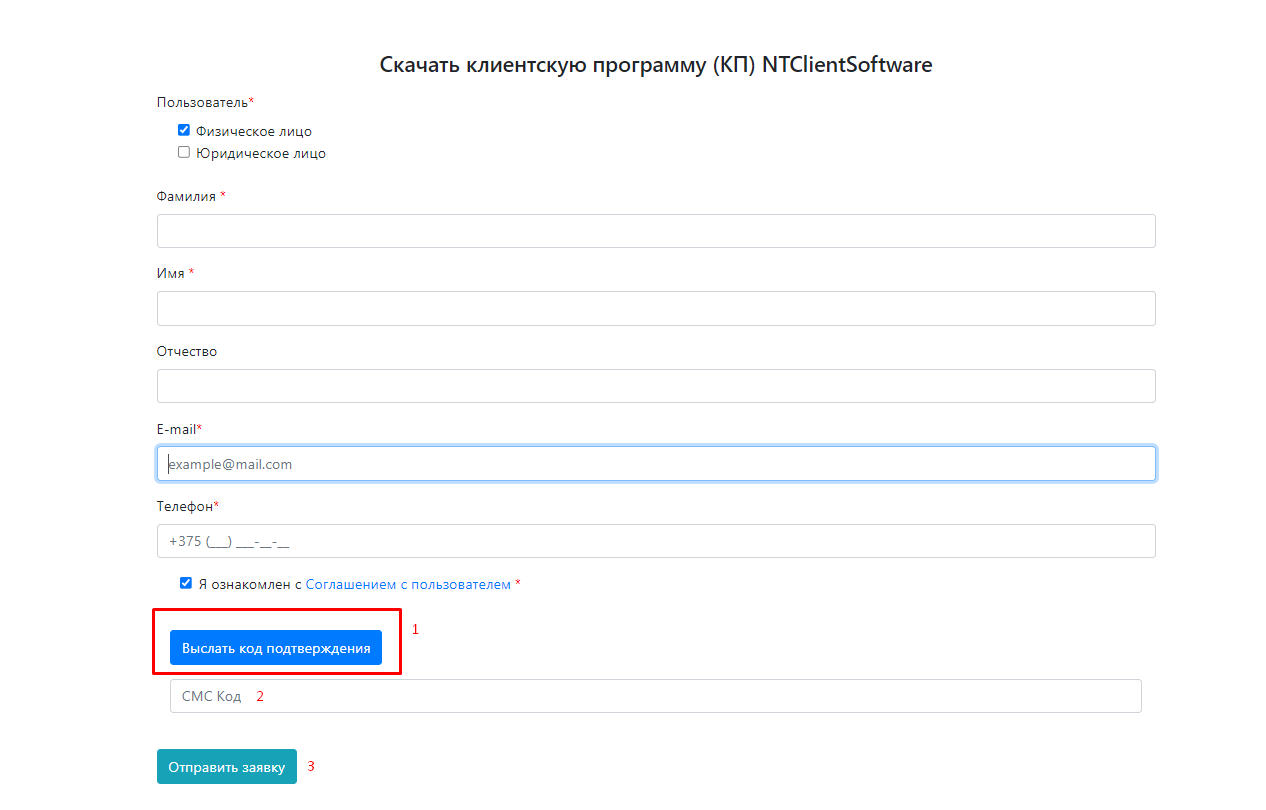


Рисунок 1

На указанный в форме номер мобильного телефона поступит код. Данный код необходимо ввести в поле «СМС 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 установки КП необходимо в Облачном хранилище выделить необходимый файл[[4]](#footnote-4) и нажать «Скачать» (Рисунок 2). Установку осуществить в соотвествии с [п. 5](#_5._Установка_КП) настоящей инструкции.

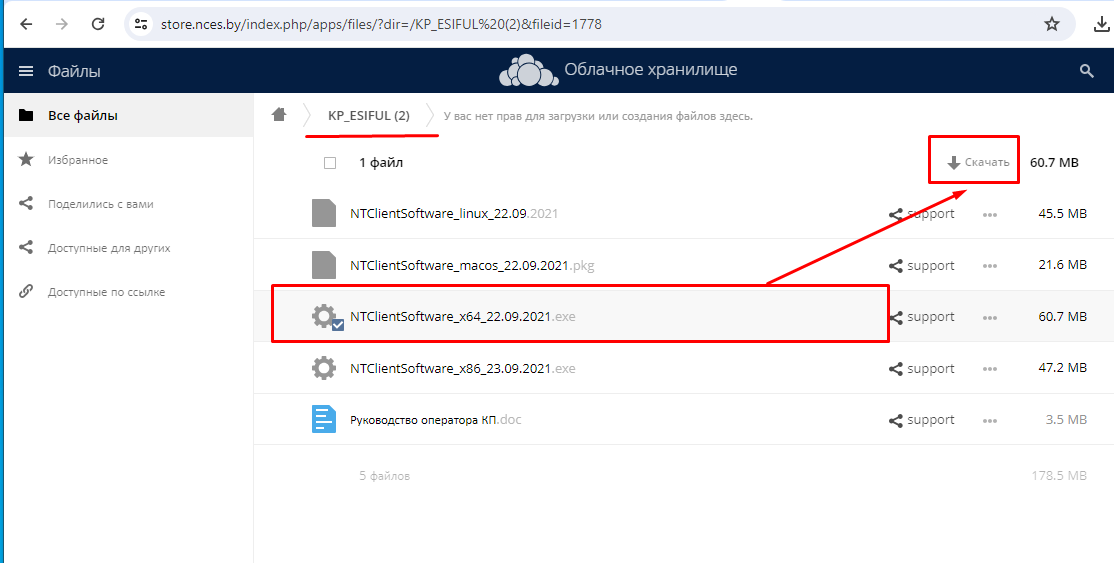


Рисунок 2

Порядок скачивания «GsecTLS» клиент аналогичен описанному порядку для получения КП.

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



Рисунок 3

Для скачивания «GsecTLS» клиент необходимо в Облачном хранилище скачать «GsecTLS» клиент (gsectls\_installer\_.exe), перейти в папку «Настройка к account.gov.by», скачать необходимый (в зависимости от типа подключения[[5]](#footnote-5)) скрипт (bat-файл) (Рисунок 4).

Для установки скаченного программного обеспечения необходимо совершить действия, описанные в [п. 6](#_6._Порядок_установки) настоящей инструкции.

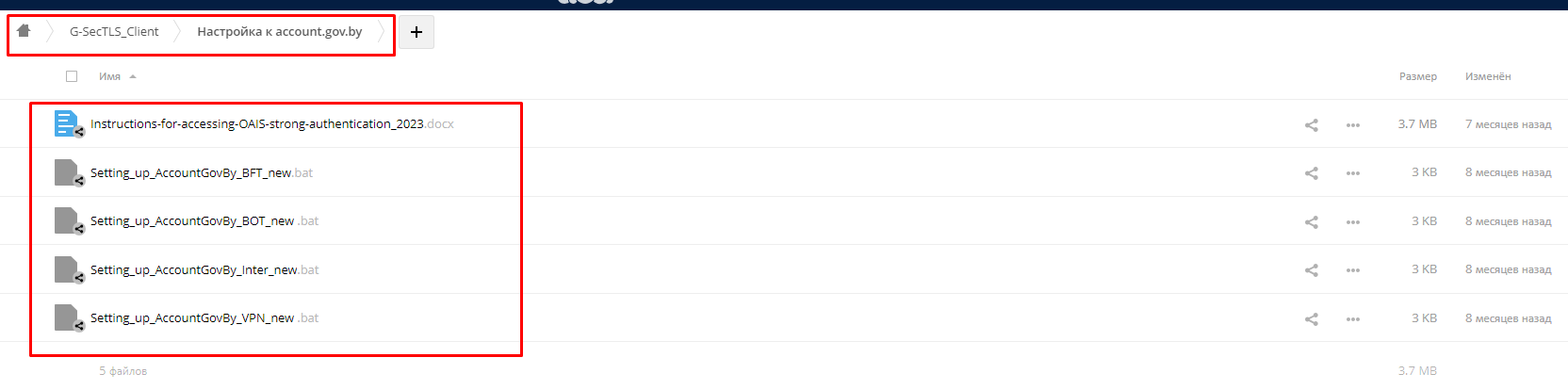
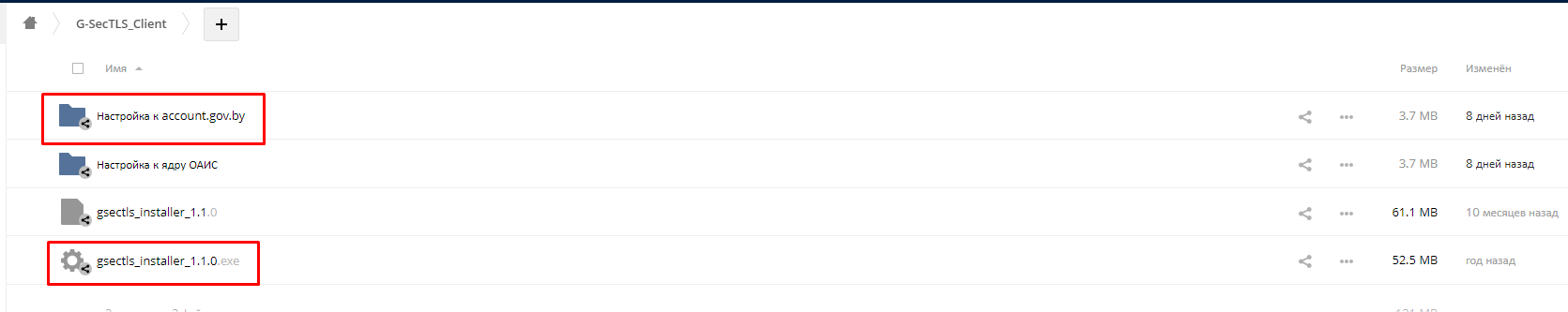


Рисунок 4

1. Обращаем внимание, что ответственность за соблюдение норм законодательства в области защиты информации лежит в том числе на стороне конечного потребителя услуг. [↑](#footnote-ref-1)
2. При этом доступ к услугам ОАИС будет осуществляться исключительно через GSecTLS и станет недоступен из сети Интернет без его применения. [↑](#footnote-ref-2)
3. В случае установки. [↑](#footnote-ref-3)
4. Для 32-разрядной системы необходим файл NTClientSoftware\_x86 [↑](#footnote-ref-4)
5. При подключении по сети Интернет – Setting\_up\_AccountGovBy\_Inter\_new.bat [↑](#footnote-ref-5)