Версия 1.1 от 03.03.2022

Столичное Кредитное Бюро

Инструкция по организации защищенного канала связи с использованием технологии на базе СКЗИ «КриптоПро NGate» (настройка VPN-туннеля)

Москва, 2022 г.

Оглавление

1. Общие положения

1.1. В целях выполнения требований действующего законодательства Российской Федерации в сфере информационной безопасности, доступ внешних пользователей (далее – Клиентов) к внутренним защищаемым информационным ресурсам и сервисам (далее – защищаемые ресурсы) общества с ограниченной ответственностью «Столичное кредитное бюро» (далее – ООО «СКБ») предоставляется по защищенному каналу связи реализованному на базе средства криптографической защиты информации «Криптографический сетевой программный комплекс «КриптоПро NGate» (далее – КСПК NGate).

1.2. КСПК NGate используется для обеспечения и предоставления Клиентам безопасного доступа (в туннельном режиме, а также по технологии ГОСТ TLS) к защищаемым ресурсам ООО «СКБ» и защиты этих ресурсов от несанкционированного доступа со стороны сетей общего пользования.

1.3. Программное обеспечение «КриптоПро NGate Клиент», используется для построения VPN-соединения между Клиентов и защищаемыми ресурсами ООО «СКБ».

1.4. В настоящей Инструкции определяются условия и требования по организации защищенного канала связи. Данная Инструкция предназначена для Клиентов и помогает выполнить самостоятельную установку и настройку программного обеспечения «КриптоПро NGate Клиент».

1.5. В инструкции рассмотрен вариант настройки программного обеспечения «КриптоПро NGate Клиент» для операционной системы Microsoft Windows 10 (далее – ОС).

2. Технические условия

2.1. Для обеспечения работоспособности программного обеспечения «КриптоПро NGate Клиент» необходимо наличие на автоматизированном рабочем месте сертифицированной версии и сборки криптопровайдера «Крипто-Про CSP». Установка и настройка криптопровайдера «Крипто-Про CSP» осуществляется в соответствии с технической и эксплуатационной документацией к нему (в том числе, размещенной на официальном сайте разработчика https://cryptopro.ru/products/csp/).

2.2. Аутентификация Клиента осуществляется по сертификату ключа проверки электронной подписи (далее – сертификат), который удовлетворяет следующим требованиям:

- обеспечивает возможность работы с криптографией в соответствии с алгоритмами ГОСТ Р 34.11-2012/34.10-2012;
- содержит расширение (OID) «Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)»;
- в составе сертификата обязательно присутствует поле «Organization (O)», в котором указывается наименование организации (по данному полю будет проходить дополнительная проверка сертификата Клиента, который используется для аутентификации).

2.3. Приобретение сертификата, лицензии на право использования криптопровайдера «Крипто-Про CSP» осуществляется Клиентом самостоятельно.

2.4. Установка и первоначальная настройка программного обеспечения «КриптоПро NGate Клиент» осуществляется в соответствии с эксплуатационной и технической документацией, размещенной на официальном сайте разработчика, в том числе:

- Средство криптографической защиты информации «Криптографический сетевой программный комплекс «КриптоПро NGate». Руководство пользователя MS Windows ЖТЯИ.00104-01 91 01 (приложение 1);
- Средство криптографической защиты информации «Криптографический сетевой программный комплекс «КриптоПро NGate». Руководство пользователя. ОС Linux ЖТЯИ.00104-01 91 02 (приложение 2).

2.5. Актуальный дистрибутив программного обеспечения «КриптоПро NGate Клиент» (сборка должна быть не ниже 1.0.0-649) системы можно загрузить со следующих ресурсов:

- http://ng-repo.cryptopro.ru/ng-client-installer/offline/windows_x64_beta/
- http://ng-repo.cryptopro.ru/ng-client-installer/offline/linux_x64_beta/

3. Экспорт и отправка сертификата Клиента

3.1. В целях обеспечения взаимной аутентификации Клиент в адрес ООО «СКБ» направляет свой личный сертификат, по которому будет осуществляться аутентификация Клиента на шлюзе при создании подключения (VPN-туннеля).

3.2. Перед отправкой сертификата его необходимо экспортировать и сохранить файлом в формате PKCS #7 (.p7b) с добавлением всех сертификатов пути сертификации.

3.2.1. При наличии файла сертификата (в формате отличном от PKCS #7 (.p7b)) откройте его двойным кликом мыши, затем выберите вкладку «**Состав**» и нажмите кнопку «**Копировать в файл**» (рис. 1), далее переходите сразу к пункту **3.3** Инструкции:

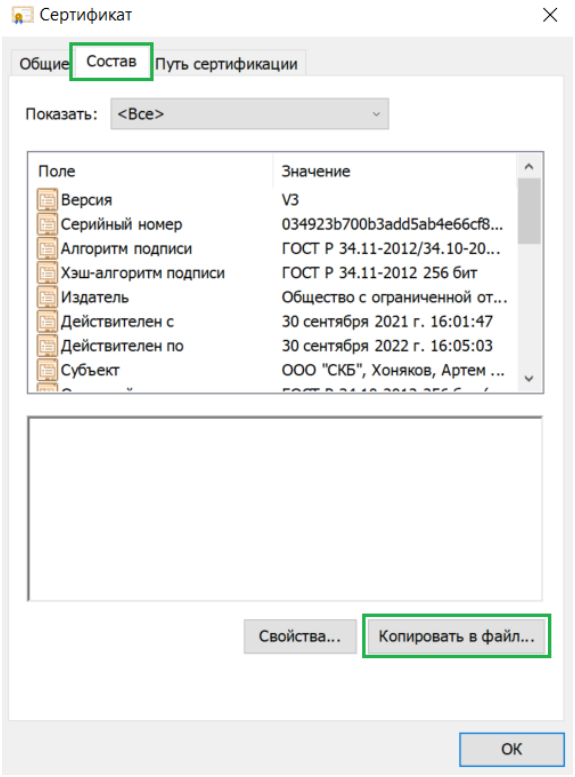

Рис. 1 – сертификат вкладка «Состав»

3.2.2. При отсутствии файла сертификата экспорт сертификата возможен через оснастку менеджера сертификатов ОС «certmgr.msc»:

– нажмите сочетание клавиш «**Win**» + «**R**» либо + «**R**» (в зависимости от типа клавиатуры) в результате будет вызван инструмент быстрого доступа к различным элементам ОС – «**Выполнить**», а затем для вызова оснастки введите «**certmgr.msc**» и нажмите «**ОК**» (рис. 2):

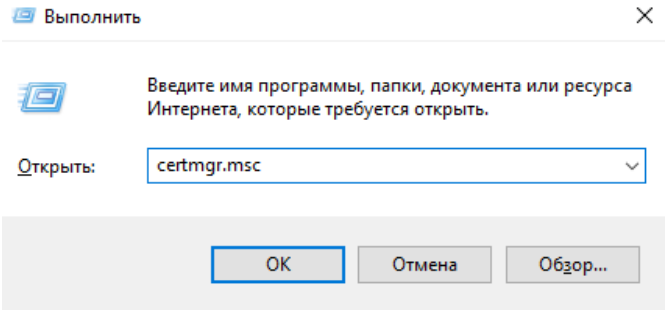

Рис. 2 – запуск оснастки «certmgr.msc» с помощью команды «Выполнить»

– для экспорта личного (пользовательского) сертификата раскройте оснастку «**Сертификаты – текущий пользователь**» / «**Личные**» / «**Сертификаты**» и выберите нужный сертификат (рис. 3):

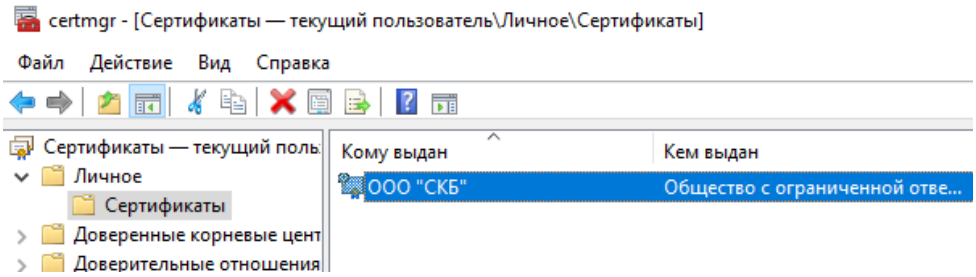

Рис. 3 – личный сертификат в оснастке «certmgr.msc»

– откроется сертификат (рис. 1), для его экспорта выберите вкладку «**Состав**», затем нажмите кнопку «**Копировать в файл**» (пункт **3.2.1** Инструкции).

3.3. Экспорт и сохранение файла сертификата для передачи в ООО «СКБ»:

– в результате выполнения пунктов **3.2.1** либо **3.2.2** Инструкции будет вызван «**Мастер экспорта сертификатов**» (рис. 4), для начала экспорта нажмите «**Далее**»:

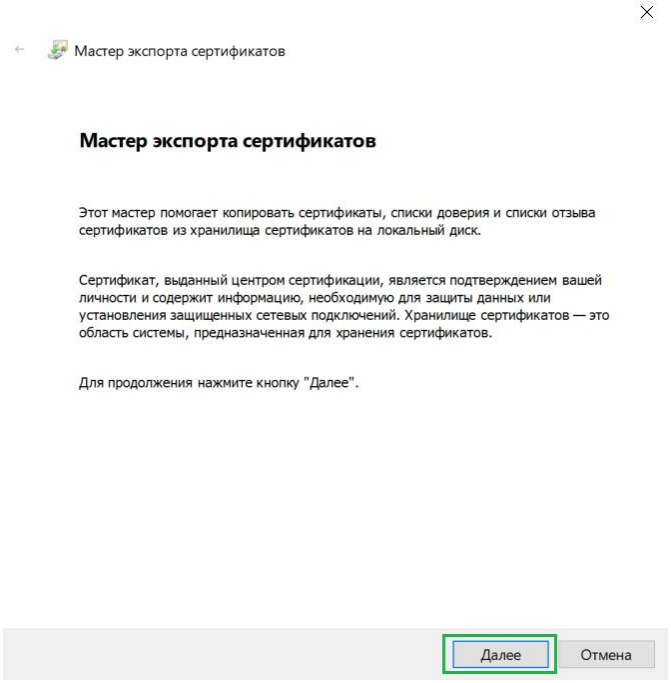

Рис. 4 – «Мастер экспорта сертификатов»

– необходимо экспортировать только сертификат, закрытый ключ (при наличии возможности экспорта) экспортировать и передавать **не нужно**, это может привести к компрометации ключа, поэтому при запросе экспорта закрытого ключа укажите «**Нет, не экспортировать закрытый ключ**» (рис. 5):

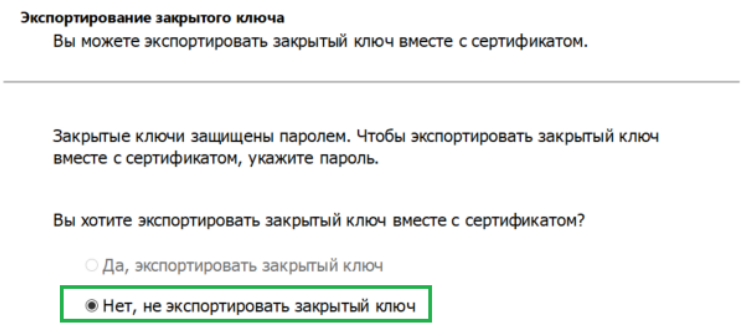

Рис. 5 – запрос экспорта закрытого ключа

– выберите формат для экспорта сертификата «**Стандарт Cryptographic Message Syntax – сертификаты PKCS #7 (.p7b)**» и добавьте опцию «**Включить по возможности все сертификаты в путь сертификации**», затем нажмите «**Далее**» (рис. 6):

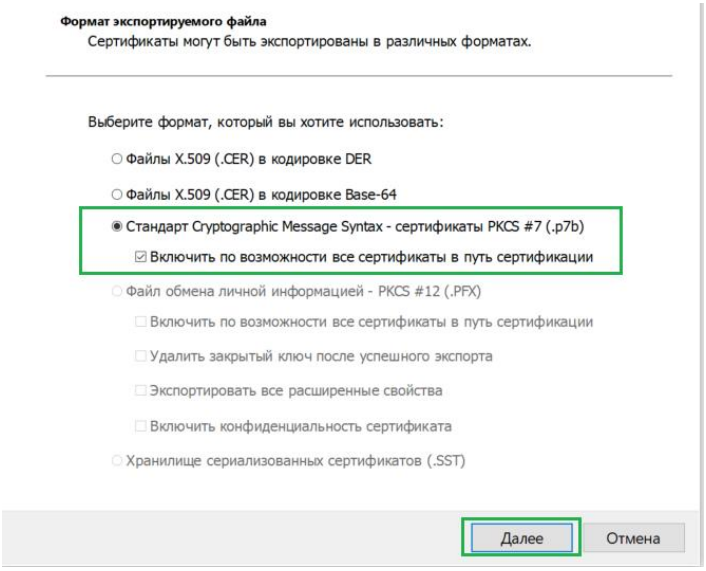

Рис. 6 – выбор формата для экспорта сертификата

– задайте имя экспортируемого файла сертификата, рекомендуем при наличии возможности, указать в качестве имени файла ИНН и краткое наименование организации, например: «7701720592 - ООО_СКБ», а также укажите путь для сохранения файла нажав кнопку «**Обзор**», по умолчанию задан путь: «**C:\Windows\System32**» (рис. 7):

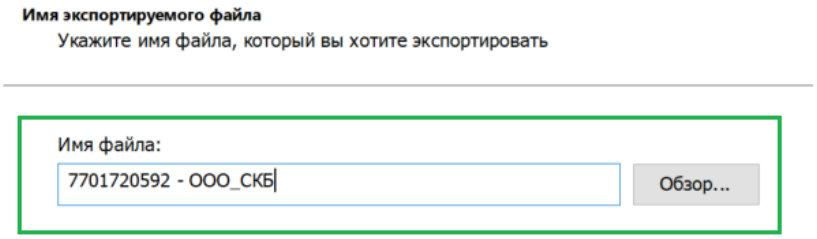

Рис. 7 – выбор имени файла сертификата и директории для сохранения

– по окончании работы «**Мастер экспорта сертификатов**» нажмите кнопку «**Готово**», при успешном выполнении экспорта сертификата появится соответствующее уведомление, для завершения экспорта сертификата нажмите кнопку «**ОК**» (рис. 8):

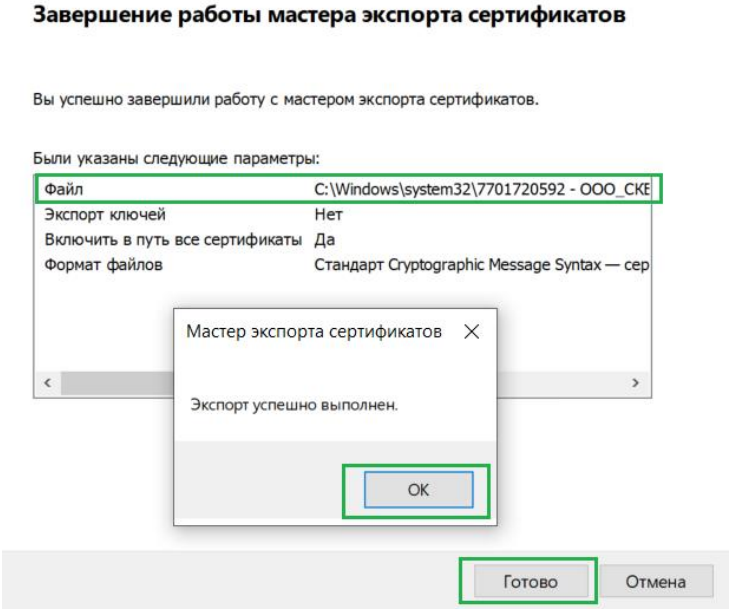

Рис. 8 – завершение мероприятий по экспорту сертификата

3.4. Экспортированный (сохраненный) файл сертификата в формате PKCS #7 (.p7b) необходимо направить в адрес ООО «СКБ».

4. Установка корневого сертификата

4.1. В адрес Клиента направляется корневой сертификат удостоверяющего центра для установления доверия к сертификату шлюза безопасности «КриптоПро NGate» ООО «СКБ» (файл сертификата: «*ПЗ_CryptoPro VPN CA GOST 2012.cer*» – приложение 3). Данный сертификат необходимо установить в хранилище сертификатов «Доверенные корневые центры сертификации» на автоматизированном рабочем месте Клиента.

4.2. Установка корневого сертификата в системное хранилище сертификатов ОС:

– двойным кликом мыши откройте файл корневого сертификата (приложение 3) и во вкладке «**Общее**» нажмите кнопку «**Установить сертификат…**» (рис. 9):

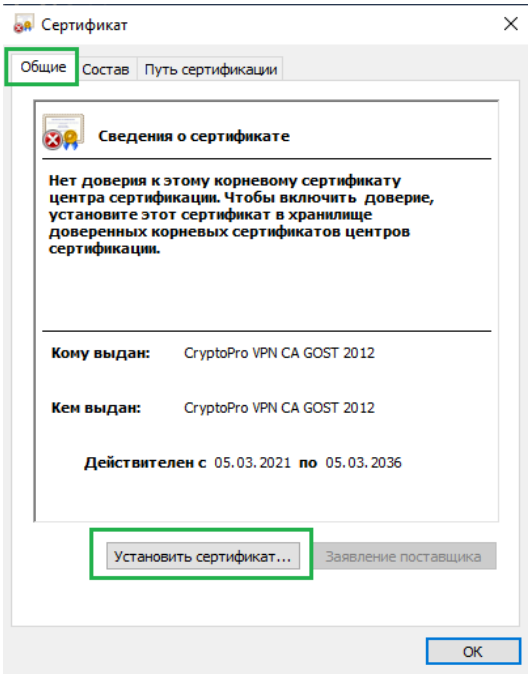

Рис. 9 – открытый файл сертификата (вкладка «Общее»)

– выберите расположение – «**Текущий пользователь**» (рис. 10), нажмите «**Далее**»:

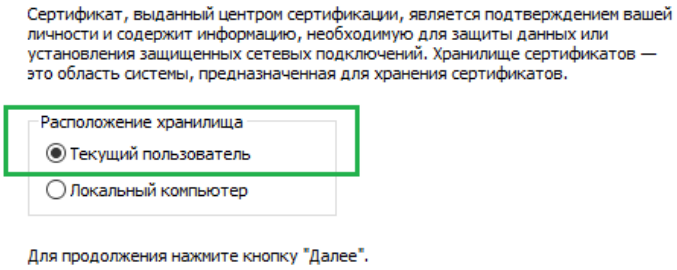

Рис. 10 – выбор расположения хранилища сертификатов

– укажите вариант «**Поместить все сертификаты в следующее хранилище**» (т.е. вручную) и нажмите кнопку «**Обзор**» (рис. 11):

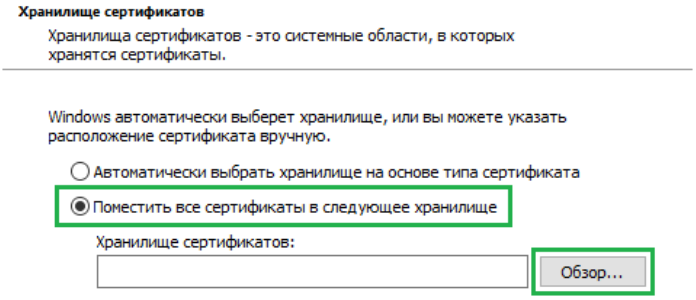

Рис. 11 – выбор хранилища для расположения корневого сертификата вручную

– в появившемся окне выберите хранилище – «**Доверенные корневые центры сертификации**» (рис. 12):

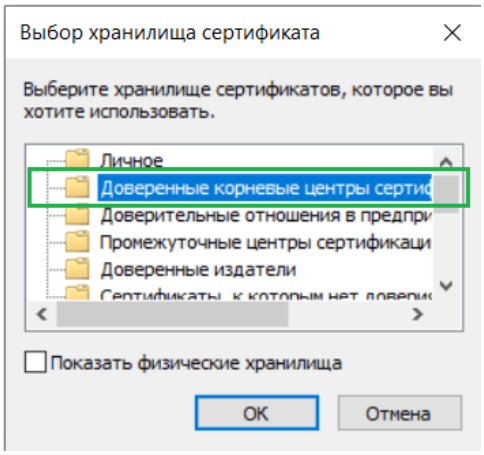

Рис. 12 – выбор хранилища из списка

– в итоге будет выбрано нужное хранилище, нажмите «**Далее**» (рис. 13):

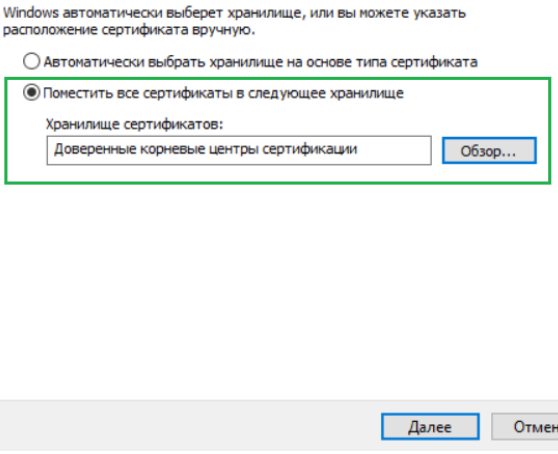

Рис. 13 – выбор хранилища – «Доверенные корневые центры сертификации»

– на завершающем этапе установки сертификата нажмите «**Готово**»;

– далее появится стандартное предупреждение системы безопасности ОС, появляющееся при добавлении корневого (самоподписанного) сертификата, и для корректного добавления сертификата в системное хранилище ОС, а также последующего его использования необходимо согласиться с установкой сертификата и нажать «**Да**» (рис. 14):

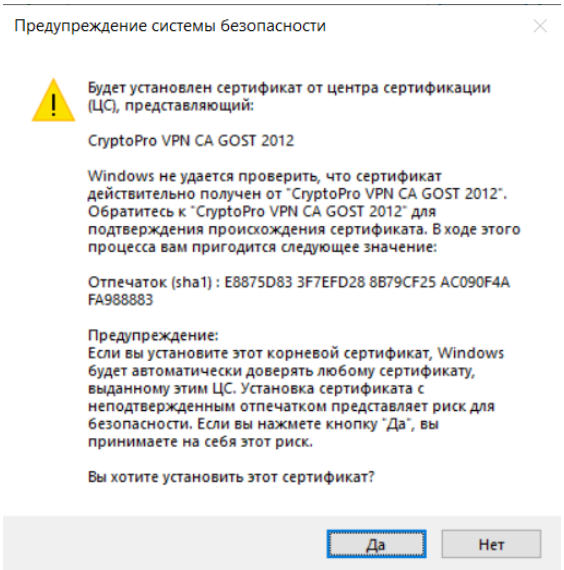

Рис. 14 – окно предупреждения системы безопасности

5. Подключение VPN-туннеля

5.1. Для подключения VPN-туннеля необходимо выполнить следующее:

- запустить клиентское программное обеспечение «КриптоПро NGate Клиент», по умолчанию при запуске должна открыться вкладка «**Состояние**» (рис. 15)
- указать URL адрес и соответствующий порт: https://ngw.cbch.ru:50000
- нажать кнопку «**Подключить**»

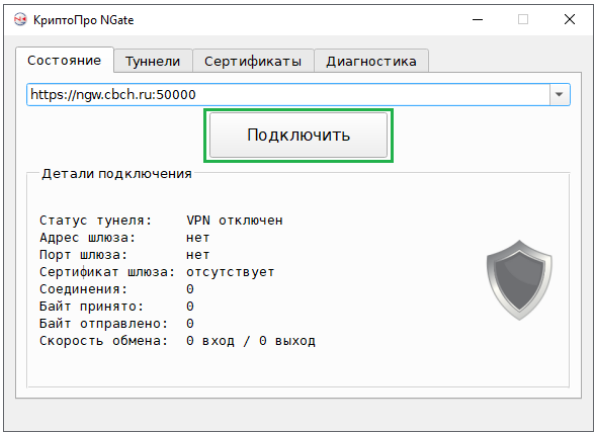

Рис. 15 – интерфейс клиентского программного обеспечения «КриптоПро NGate Клиент» (вкладка «Состояние»)

5.2. появившемся окне «**Аутентификация пользователя**» необходимо выбрать сертификат для аутентификации (сертификат, который был направлен в ООО «СКБ» в соответствии с пунктом **3.4** Инструкции) и ввести пароль / PIN закрытого ключа (рис. 16).

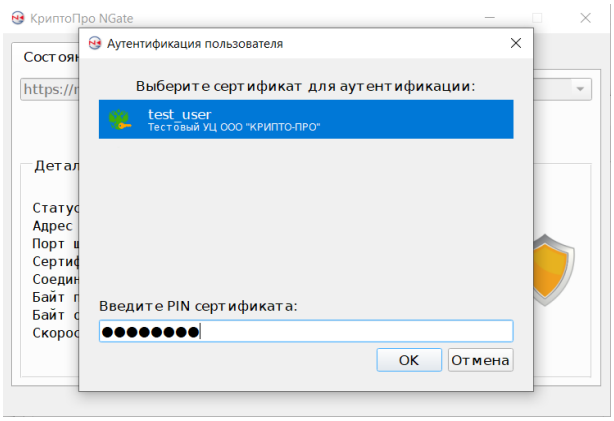

Рис. 16 – окно аутентификации пользователя (выбор сертификата)

5.3. В случае успешного выполнения настройки подключения статус туннеля изменится и поменяется индикация подключения (рис. 17). С этого момента авторизованному Клиенту будет предоставлен доступ к соответствующим его правам защищаемым ресурсам ООО «СКБ».

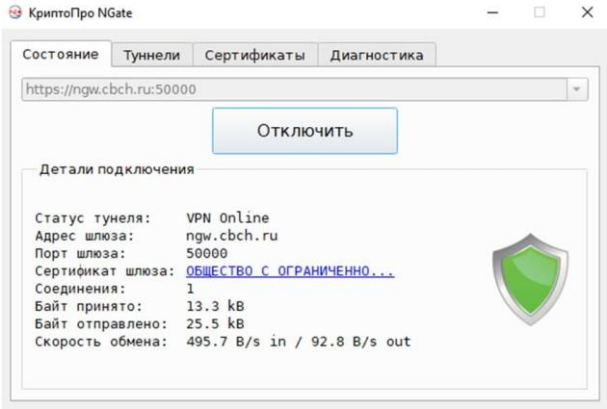

Рис. 17 – индикация статуса подключения — VPN соединение установлено

6. Дополнительная настройка (Автоподключение)

6.1. В целях обеспечения непрерывности подключения и автоматического восстановления соединения в случае его разрыва рекомендуем настроить автоподключение. Для этого перейдите на вкладку «**Состояние**» и при отключенном соединении **зажмите** сочетание клавиш «**Ctr**» + «**Alt**», кнопка «Подключить» изменится на «Настроить автоподключение» (рис. 18).

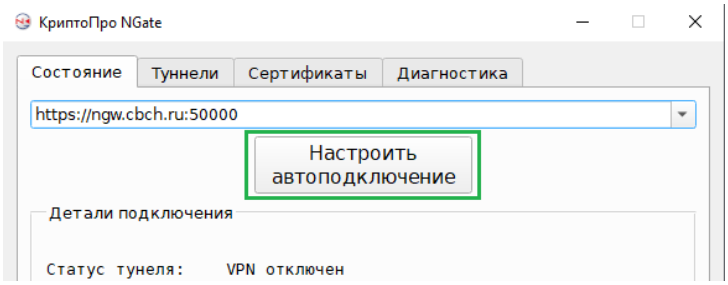

Рис. 18 – Настройка автоподключения

6.2. Нажмите на кнопку «**Настроить автоподключение**» – будет выполнена соответствующая настройка, текущее подключение и его параметры (URL адрес, порт и сертификат аутентификации) будут сохранены (запомнены). Слева от URL адреса появится соответствующий значок (рис. 19).

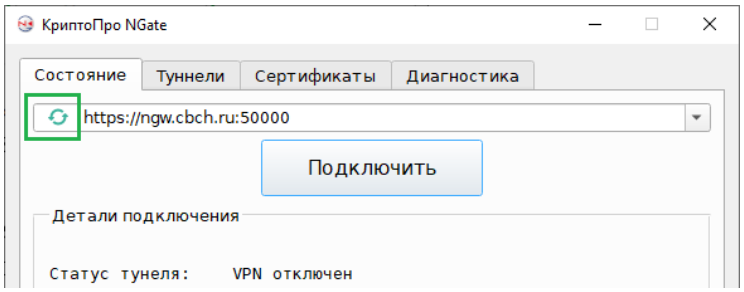

Рис. 19 – Значок настроенного (включенного) автоподключения

6.3. Далее перейдите на вкладку «**Диагностика**» и нажмите сочетание клавиш «**Ctr**» + «**Alt**» + «**P**», появится дополнительное окно настройки параметров (рис. 20). Допустимо изменение **только** нижеуказанных параметров с указанием **только** нижеуказанных значений, остальные значения параметров менять строго **запрещено** (это может повлиять на работоспособность программного обеспечения «КриптоПро NGate Клиент»):

- Интервал восстановления (в мс): **50**
- Интервал переподключения (в сек): **1**
- Держать соединение: **включить данный параметр**

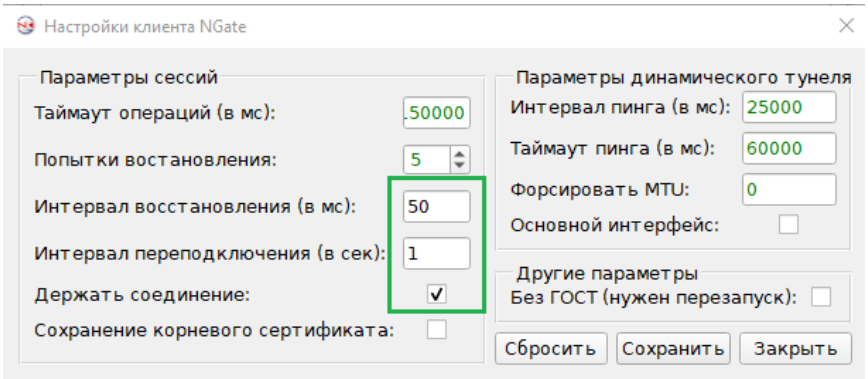

Рис. 20 – Параметры сессии для автоподключения

6.4. Для завершения настройки автоподключения нажмите кнопку «**Сохранить**».