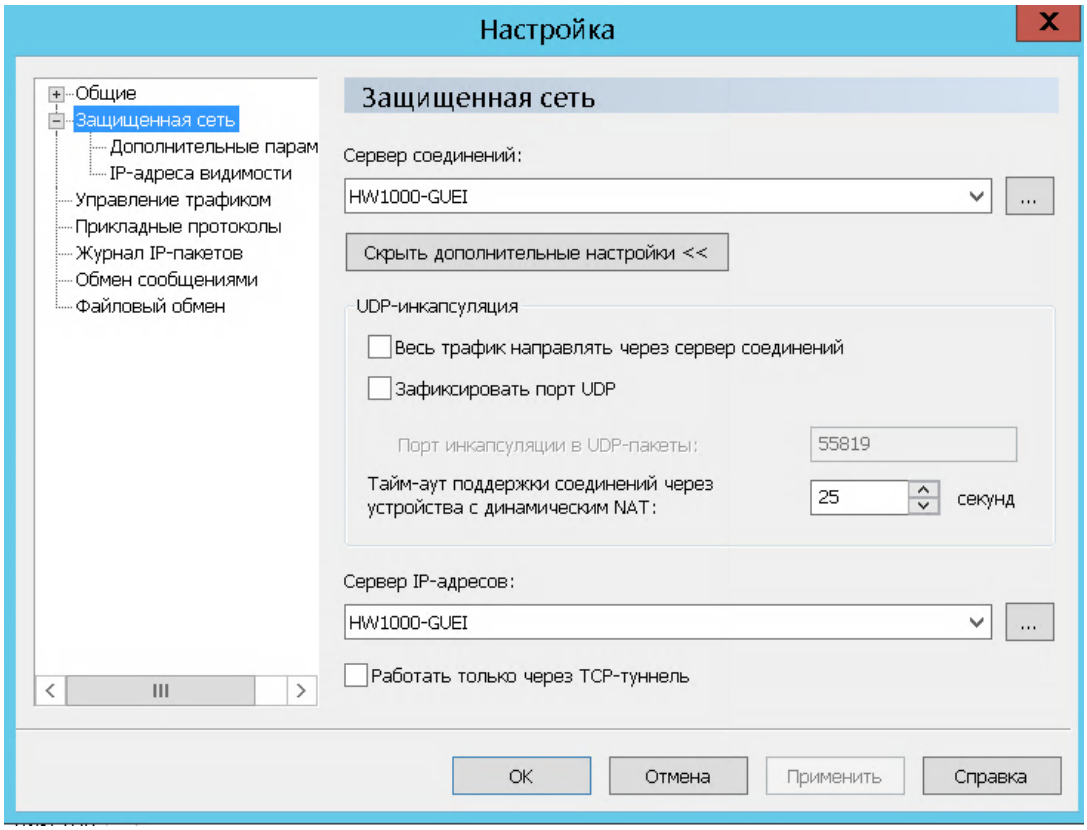
Пошаговая инструкция по настройке рабочего места пользователя ЕИС

1. Проверка доступности ЕИС при использовании различных вариантов подключения к защищенной сети

1.1. Вариант подключения с помощью ViPNet-клиента (версия 4.x)

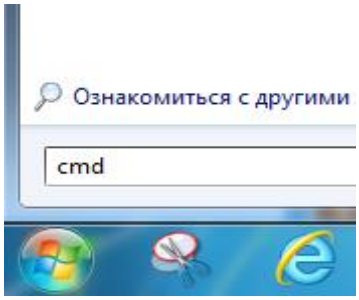
Для повышения стабильности работы защищенного канала связи необходимо настроить клиент как на рисунке ниже (ViPNet Client [Монитор] → закладка «Сервис» → пункт меню «Настройка приложения» → «Защищенная сеть» → «Показать дополнительные настройки»):

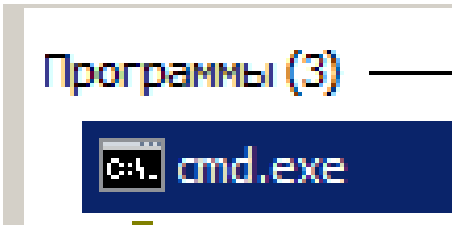


Также необходимо убедиться в том, что в качестве сервера соединений и сервера IP-адресов используется один и тот же ViPNet-координатор HW1000-GUEI, версия клиента при это должна быть не ниже 4.3.2.

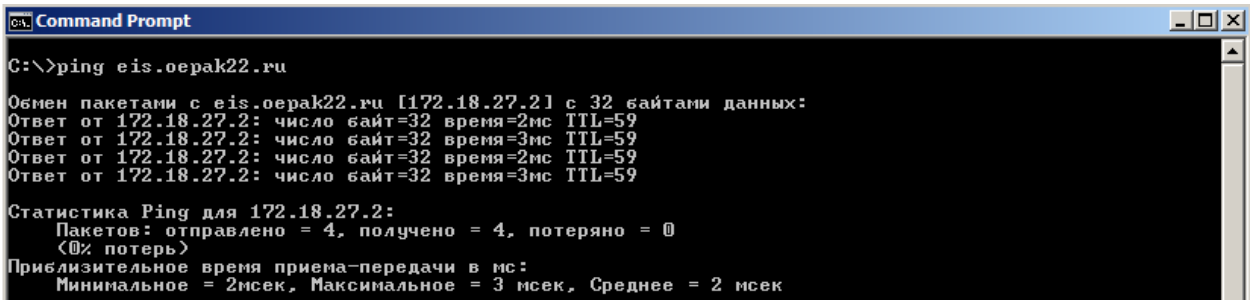
Для проверки доступности ЕИС запускаем интерпретатор командной строки:

нажимаем кнопку «Пуск», в появившейся строке поиска набираем **cmd**, и нажимаем ENTER (с 17.06.2020 работа ЕИС в Windows XP не поддерживается):

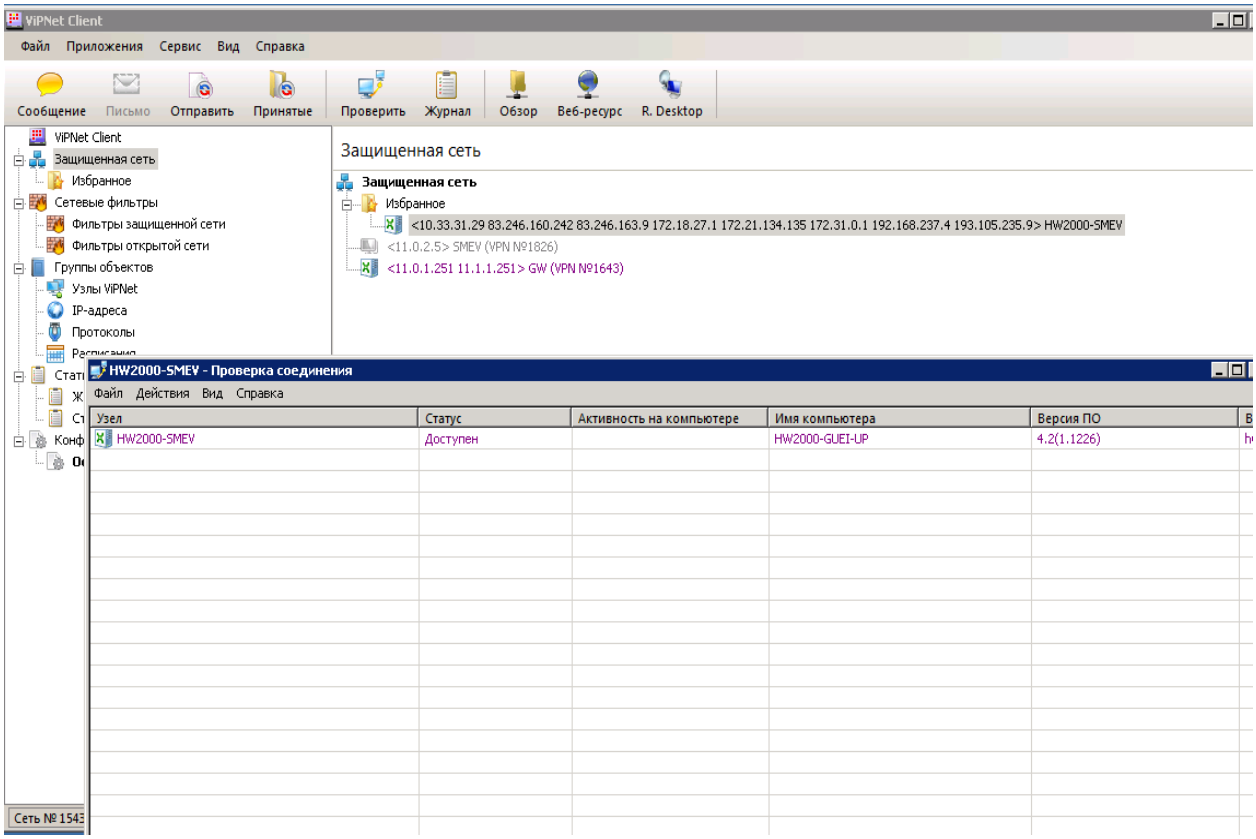




В открывшемся окне выполняем команду **ping**:
ping eis.alregn.ru



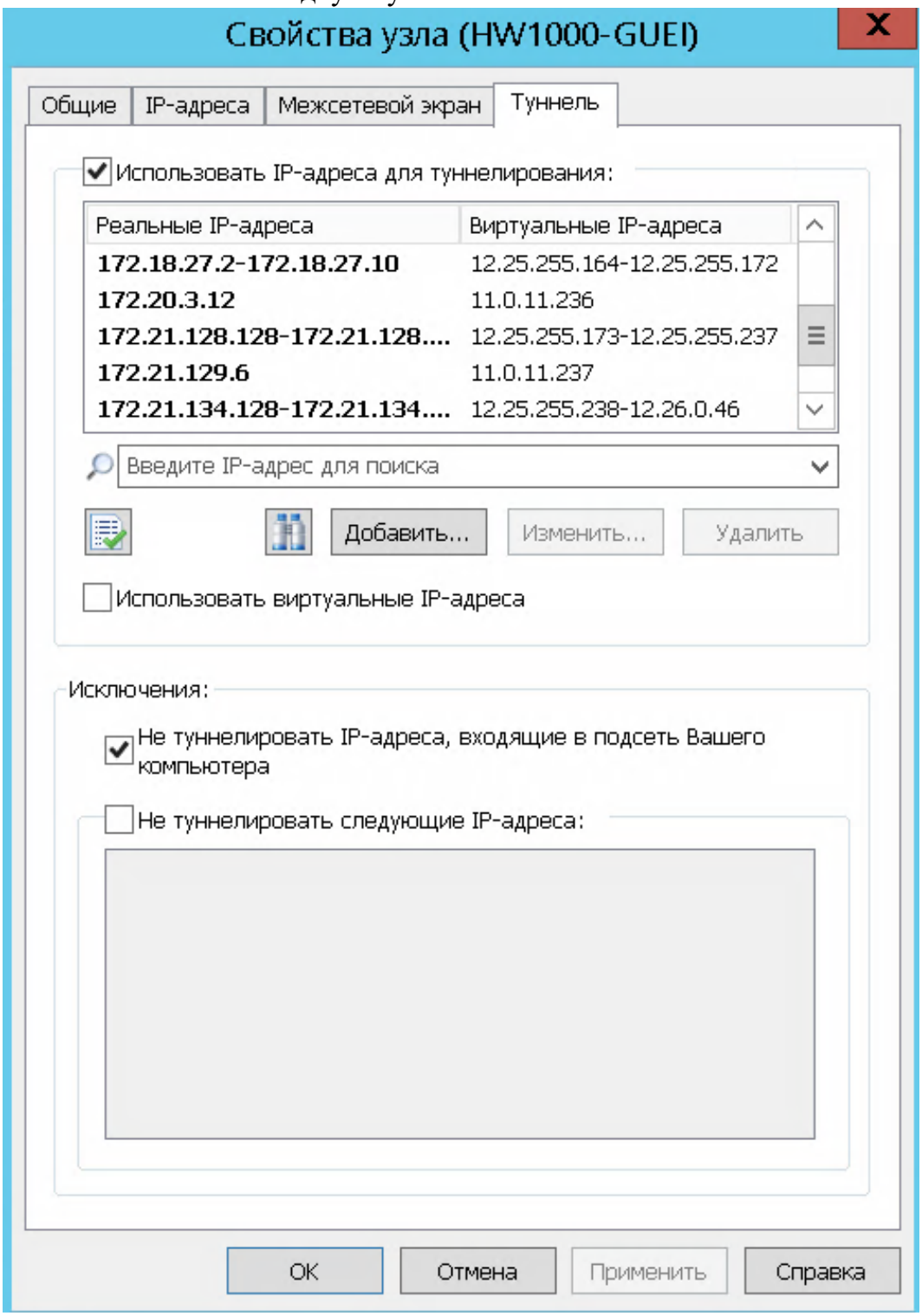
Если ответы от **172.18.27.4** не приходят, необходимо проверить доступность координатора HW1000-GUEI. Для этого нужно открыть ViPNet Client [Монитор], в окне «Защищенная сеть» найти координатор HW1000-GUEI, одним щелчком мыши кликнуть по координатору HW1000-GUEI, и клавишей F5 проверить его доступность:



Если координатор доступен, нужно еще раз выполнить команду **ping**.

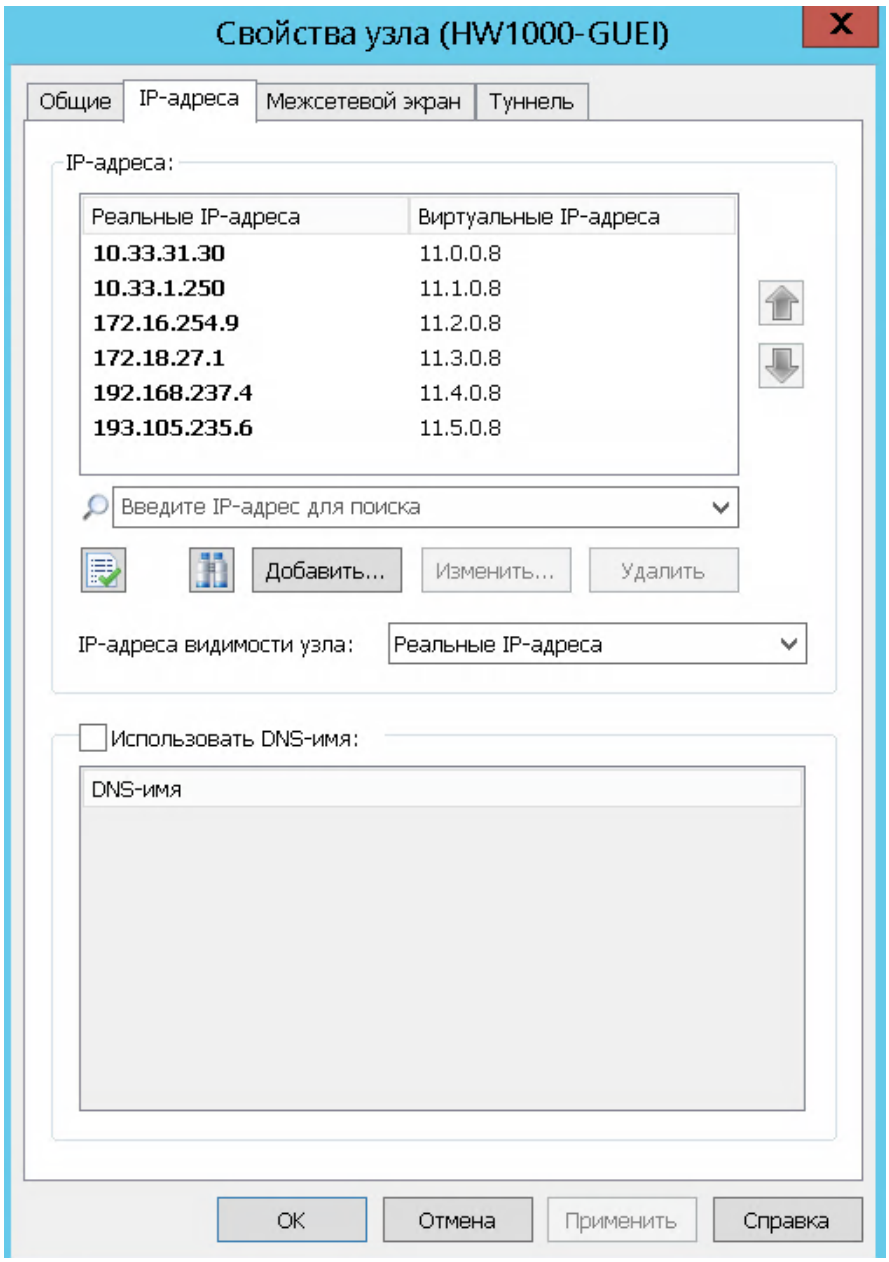
В том случае, если координатор доступен, но ответы от **172.18.27.4** после выполнения команды **ping** не приходят, необходимо проверить наличие прописанных туннелей для координатора HW1000-GUEI. Для этого нужно открыть ViPNet Client [Монитор], в окне «Защищенная сеть» найти координатор HW1000-GUEI, затем двойным щелчком мыши по координатору активировать окно

«Свойства узла (Координатор HW1000-GUEI)», и выбрать одиночным щелчком мыши в появившемся окне закладку «Туннель»:



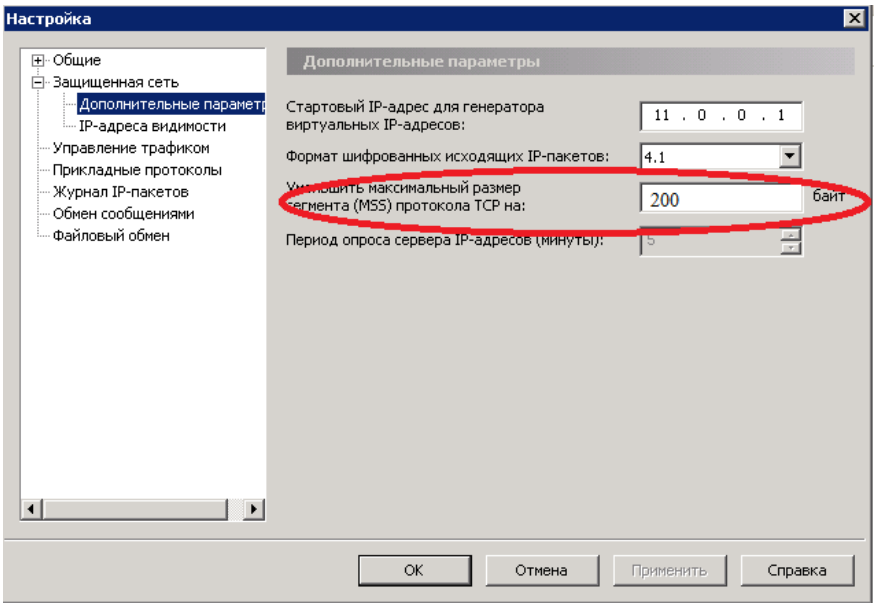
Отсутствующие IP-адреса туннелированных узлов должных быть добавлены в соответствии с вышеприведенным изображением.

Далее перейти во вкладку «IP-адреса» и проверить чтоб был добавлен IP-адрес **193.105.235.6**. Если он отсутствует, то нажать кнопку «Добавить» и ввести данный адрес вручную. Чуть ниже, в секции «IP-адреса видимости узла» выбрать из выпадающего списка параметр «Реальные IP-адреса».



В том случае, если координатор доступен, и выполнены все настройки, перечисленные выше, но ответы от **172.18.27.4** после выполнения команды **ping** по-прежнему не поступают (либо координатор HW2000-SMEV изначально недоступен), нужно для решения проблемы обратиться к специалистам КГБУ ОЭПАК, позвонив по телефону **(3852) 205-563** или написав письмо на адрес электронной почты **vvb@oepak.alregn.ru** или **aam@oepak.alregn.ru**

Если после выполнения команды **ping** ответы от **172.18.27.4** приходят, однако страница входа ЕИС не открывается, рекомендуется установить параметр «Уменьшить максимальный размер сегмента (MSS) протокола TCP на:» равным 200 Байт (ViPNet Client [Монитор] → закладка «Сервис» → пункт меню «Настройка приложения» → «Защищенная сеть» → «Показать дополнительные настройки»):



1.2. Вариант подключения без ViPNet-клиента, с помощью ViPNet-координатора

Для подключения через ViPNet-координатор нового рабочего места (компьютера), без установленного на нем ViPNet-клиента, необходимо:

- Добавить на сетевой интерфейс второй IP-адрес вида 172.25.X.Y, с маской 255.255.255.0, где X – октет, выделенный для ОМСУ специалистами, производившими настройку ViPNet-координатор, а Y – произвольное «неиспользуемое» число из диапазона [2-254] (необходимо учитывать, что добавляемые IP-адреса должны быть уникальными).
- Настроить альтернативный маршрут:
  a) Запустить командную строку от имени администратора.
  b) Выполнить следующие команды:
  route add –p 172.18.27.0 mask 255.255.255.240 172.25.X.1
  route add –p 10.33.0.0 mask 255.255.0.0 172.25.X.1

  ВНИМАНИЕ! Вышеприведенный формат команды route применим в среде Windows 10; для Windows 7, 8 нужные команды выглядят так:
  route –p add 172.18.27.0 mask 255.255.255.240 172.25.X.1
  route –p add 10.33.0.0 mask 255.255.0.0 172.25.X.1

  Чтобы не ошибиться, Вы всегда можете получить справочную информацию о корректном формате команды route, выполнив данную команду из командной строки с универсальным ключом для получения справки /? :
  route /?
  Для создания статического маршрута на Astra Linux воспользуйтесь статьей из Справочного центра Astra Linux
- Проверить доступность ЕИС, выполнив команду **ping**:
  ping eis.alregn.ru

В том случае, если ответы от **172.18.27.4** после выполнения команды **ping** не поступают, нужно для решения проблемы обратиться к специалистам КГБУ ОЭПАК, позвонив по телефону **(3852) 205-563** или написав письмо на адрес электронной почты **vvb@oepak.alregn.ru** или **aam@oepak.alregn.ru**

При обращении необходимо предоставить результаты выполнения команд:

Для Windows:

- **ipconfig /all**
- **route print**
- **ping 172.18.27.4**
- **ping 10.33.1.7**
- **tracert -d 172.18.27.4**
- **tracert -d 10.33.1.7**

Для Linux:

- **ip a**
- **ifconfig**
- **ip route**
- **ping 172.18.27.4**
- **ping 10.33.1.7**
- **traceroute 172.18.27.4**
- **traceroute 10.33.1.7**

1.3. Вариант подключения с помощью ViPNet TLS Gateway

Для подключения через ViPNet TLS Gateway необходимо воспользоваться инструкцией по настройке подключения к информационным системам Минцифры Алтайского края посредством TLS-шифрования

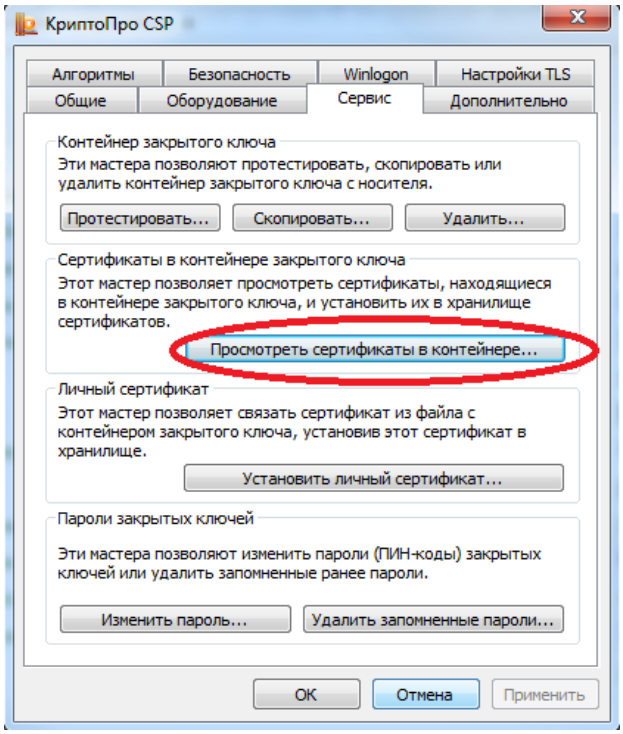
2. Дополнительное программное обеспечение

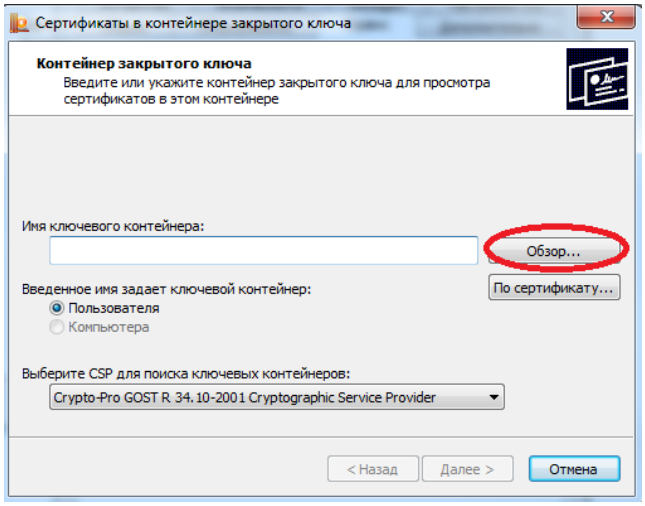
Для корректной работы с ЕИС необходимо, чтобы на компьютере было установлено и правильно сконфигурировано следующее ПО:

- Криптопровайдер (КриптоПро CSP)
- Браузер (Рекомендованы Яндекс браузер либо Chromium-Gost)
- Драйвер ключевого носителя (eToken / Рутокен).
- Операционная система Windows 7 и выше (с 17.06.2020 работа ЕИС в Windows XP не поддерживается)

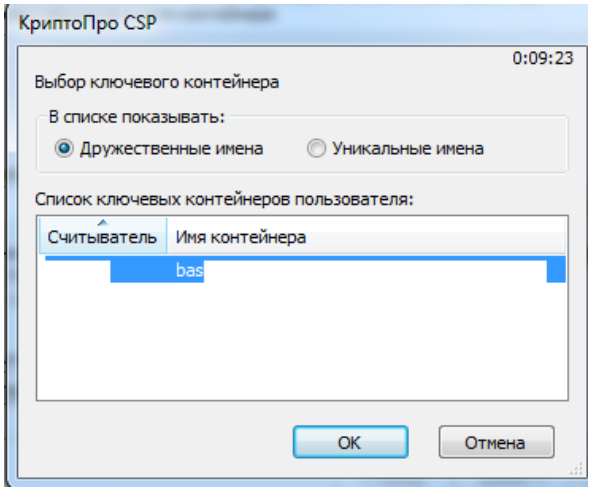
  Также, необходимо установить сертификат ЭП в хранилище сертификатов пользователя «Личные», с привязкой на закрытый ключ (средствами используемого криптопровайдера). Указанная установка производится следующим образом:

Для СКЗИ КриптоПро CSP (см. приведенную ниже последовательность скриншотов):

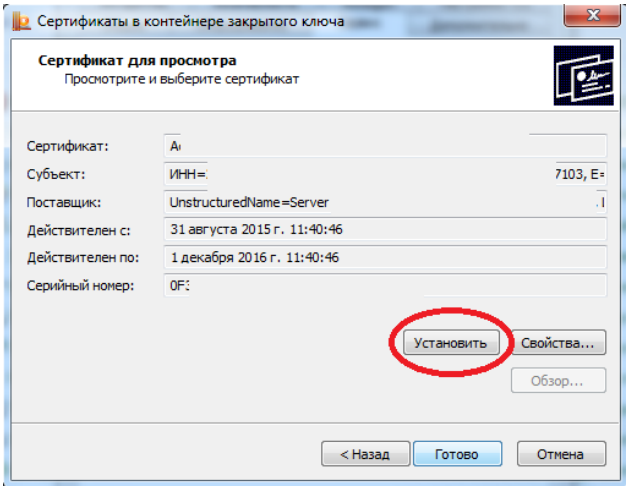




Далее необходимо выбрать на носителе интересующий ключевой контейнер, и нажать «ОК»:



Далее необходимо нажать «Установить»:



Установка произведена.

Для корректной работы функции подписания в ГИС ЕИС необходимо иметь актуальную версию браузера, КриптоПро ЭЦП Browser plug-in и КрипПро CSP.
Также просьба ознакомиться с инструкцией по использованию инструментов для просмотра xml-файлов, полученных из Росреестра.