Небанковская кредитная организация
акционерное общество
«НАЦИОНАЛЬНЫЙ РАСЧЕТНЫЙ ДЕПОЗИТАРИЙ»

Инструкция по настройке рабочего места при подключении к WEB сервисам НРД с использованием TLS соединения

Москва, 2022

Под термином **«подключение к WEB сервисам НРД»** имеется в виду подключение клиентов НРД для целей электронного взаимодействия (промышленный контур) или для целей тестирования (тестовый контур) с использованием Файлового шлюза или локального рабочего места Системы электронного документооборота НРД (далее - ЛРМ СЭД НРД) ПО «Луч» в режиме «WEB канала» или WEB-кабинетов, развернутых на стороне НРД, имеющему адрес (URL) в сети Интернет через TLS соединение.

1. Для подключения к WEB-сервисам НРД через TLS соединение необходимо получить, установить и настроить средства криптографической защиты (далее - СКЗИ). Подробно процесс получения СКЗИ описан на сайте ПАО Московская Биржа в разделе «Первичное подключение к СЭД». Порядок настройки СКЗИ описан на сайте Московской Биржи в разделах ГОСТ-криптография и RSA-криптография.

Для работы с WEB-сервисом в тестовом и промышленном контурах НРД требуются следующие версии СКЗИ и их компоненты:

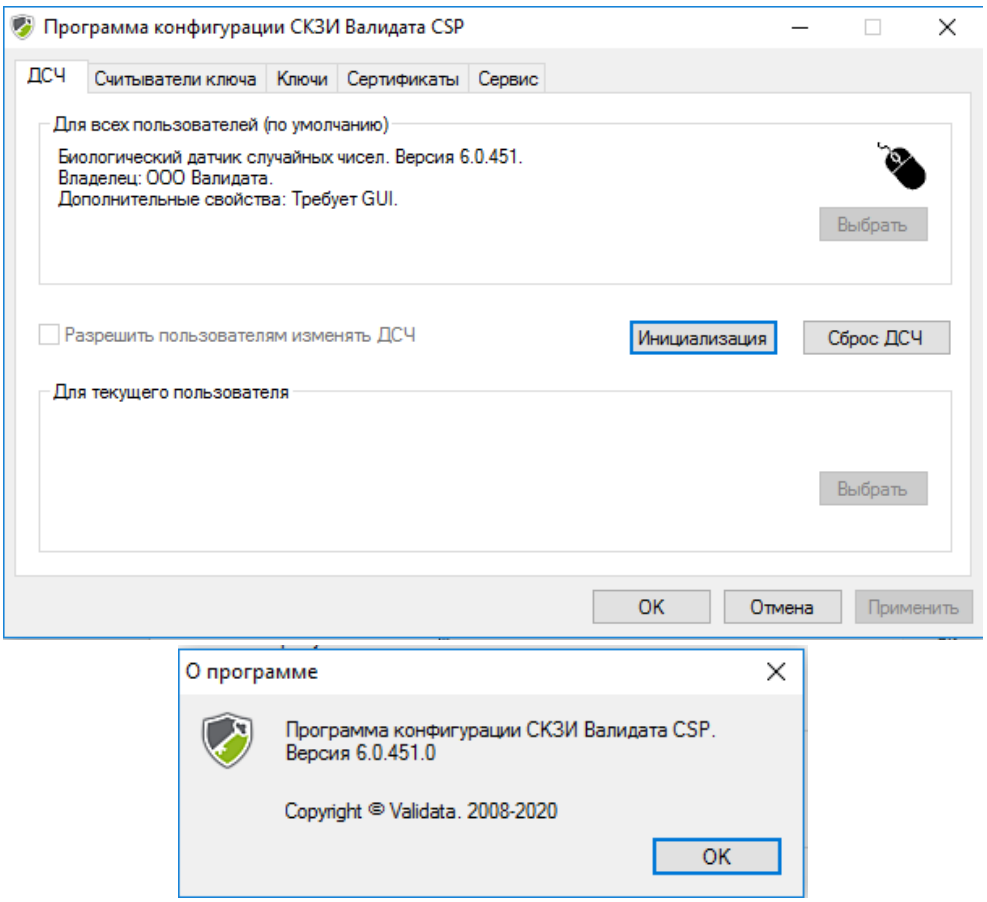
1.1 При использовании сертифицированных СКЗИ, неквалифицированных сертификатов ключей проверки электронной подписи (далее – СКПЭП ГОСТ или сертификаты ГОСТ):

- криптопровайдер "Валидата CSP" и программный комплекс «АПК Валидата Клиент Справочник сертификатов» для 32bit или 64bit в зависимости от операционной системы (далее – ОС), установленной на компьютере (**для 64bit ОС устанавливаются ПК Справочник сертификатов 32bit и 64bit**) версии **не ниже расположенной на странице** http://www.moex.com/s1292

СКЗИ "Валидата CSP" версия 6 и АПК "Валидата Клиент" функционируют на ЭВМ с x86 и x64 архитектурами, а также на виртуальных машинах, находящихся под управлением гипервизоров Microsoft Hyper-V и VMware ESXi версий 6.0/6.5/6.7 из состава VMware vSphere, в следующих ОС Windows:

- Windows 7 (x86 и x64) с пакетом обновлений 1 (SP1) и выше;
- Windows Server 2008 R2 (x64) с пакетом обновлений 1 (SP1) и выше;
- Windows 8.1 (x86 и x64);
- Windows Server 2012 R2 (x64);
- Windows 10 (x86 и x64);
- Windows Server 2016 (x64);
- Windows Server 2019 (x64).

Версии криптобиблиотеки Валидата-CSP и «АПК Валидата Клиент Справочник сертификатов» можно посмотреть в меню «Панель управления – программы и компоненты» или «Пуск - Все программы - папка Валидата CSP - Программа конфигурации СКЗИ - окно Программа конфигурации Валидата CSP - верхний левый угол экрана (значок «Щит») – О программе.».



Вместе с криптобиблиотекой Валидата-CSP при начальной установке СКЗИ должна быть установлена программа монитора TLS. Устанавливается автоматически при установке по умолчанию.

В тестовом контуре необходимо использовать высылаемый по вашей заявке тестовый криптографический ключ и СКПЭП криптосервера НРД. Тестовый криптоключ получается клиентом только в НРД. Ключ криптосервера НРД (тестовая криптосессия) входит в комплект сертификатов, высылаемых с ключом.

Собственный криптографический ключ генерируется клиентом самостоятельно в личном кабинете участника на сайте ПАО Московская Биржа.

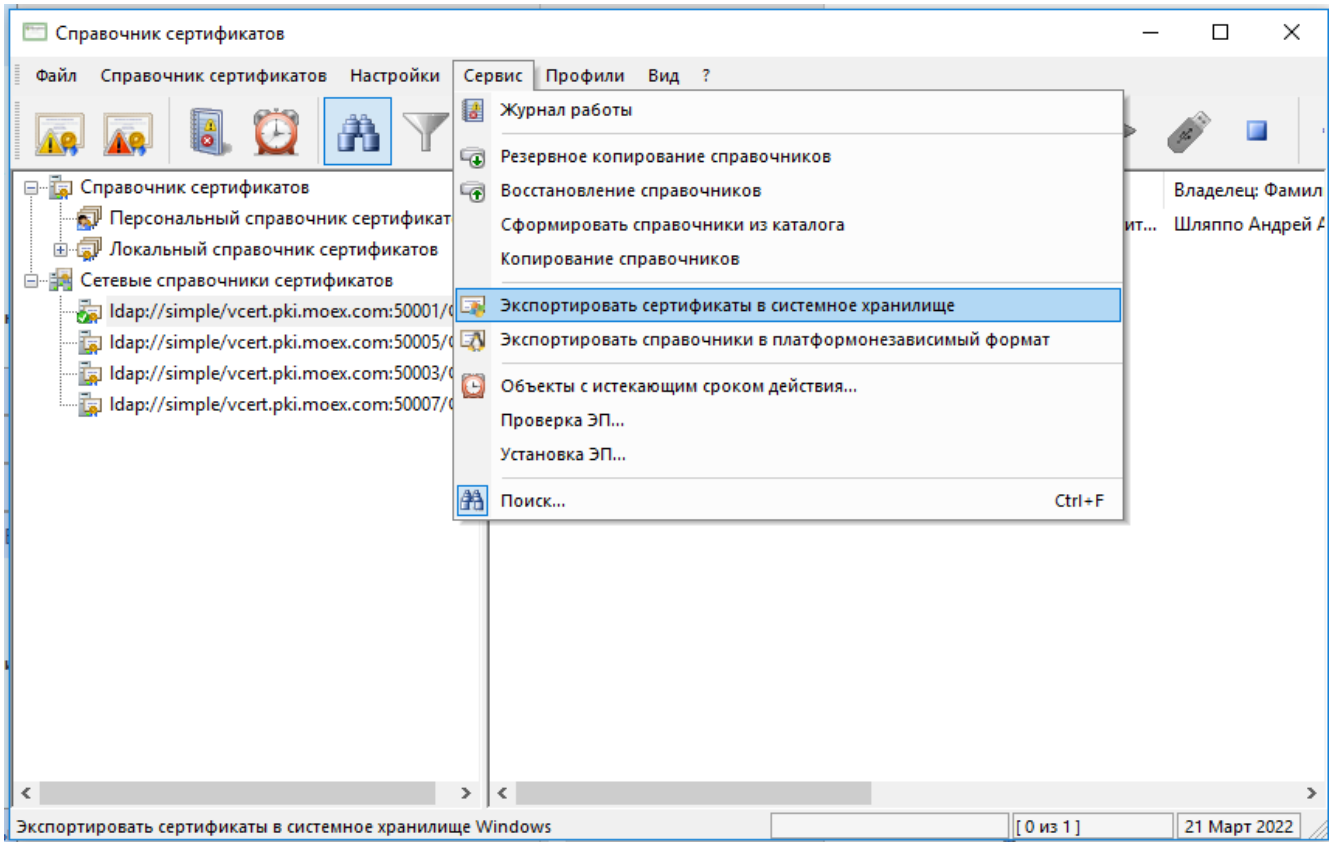
1.2 При использовании несертифицированных СКЗИ, неквалифицированных сертификатов (RSA) программный комплекс (ПК) «Справочник сертификатов» (RCS)

Программное обеспечение ПК "Справочник сертификатов" работает на ЭВМ, совместимых с IBM типа PC AT (процессор типа Pentium и выше) под управлением 32-х и 64-х разрядных версий операционных систем на платформе x86 или x64

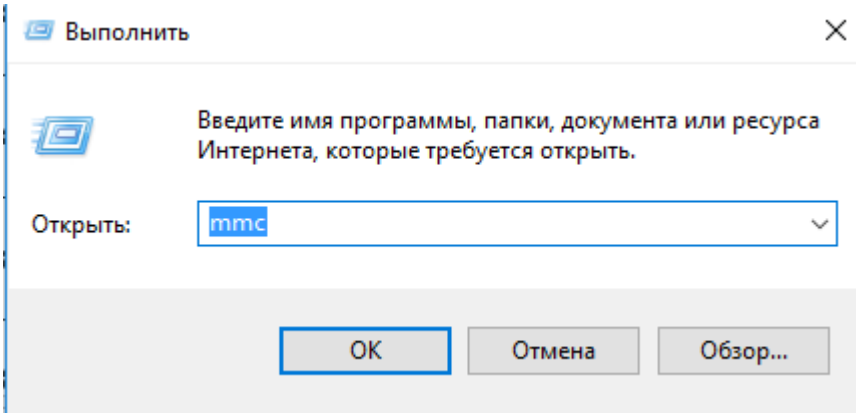
- Windows Vista SP1 или выше (начиная с версии Home Premium);
- Windows Server 2008 SP1 или выше;
- Windows 7 (начиная с версии Home Premium);
- Windows Server 2008 R2;
- Windows 8 / 8.1 (за исключением Windows RT);
- Windows Server 2012 / 2012 R2;
- Windows 10.

2. После установки СКЗИ необходимо обеспечить перенос криптографических ключей в системное хранилище WINDOWS для организации защищённого TLS соединения с WEB

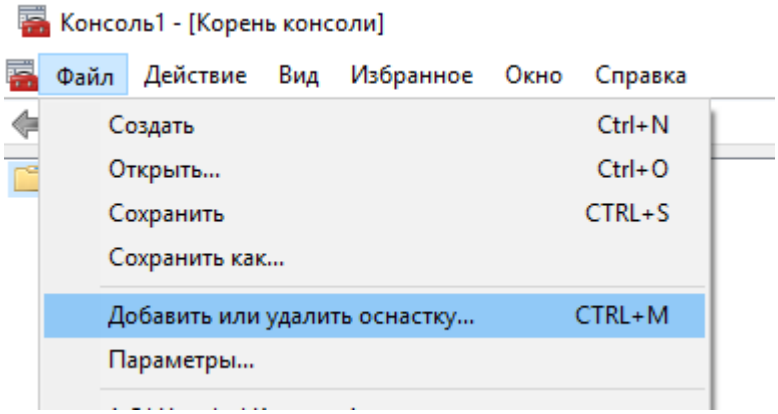
сервером НРД. Для корректного добавления криптоключа в системное хранилище необходимо, используя меню программы «АПК Валидата Клиент - Справочник сертификатов» или «ПКЗИ СЭД МБ», в зависимости от типа используемого ключа, выбрать меню «сервис-экспортировать сертификаты в системное хранилище» и согласиться со всеми задаваемыми программой вопросами.



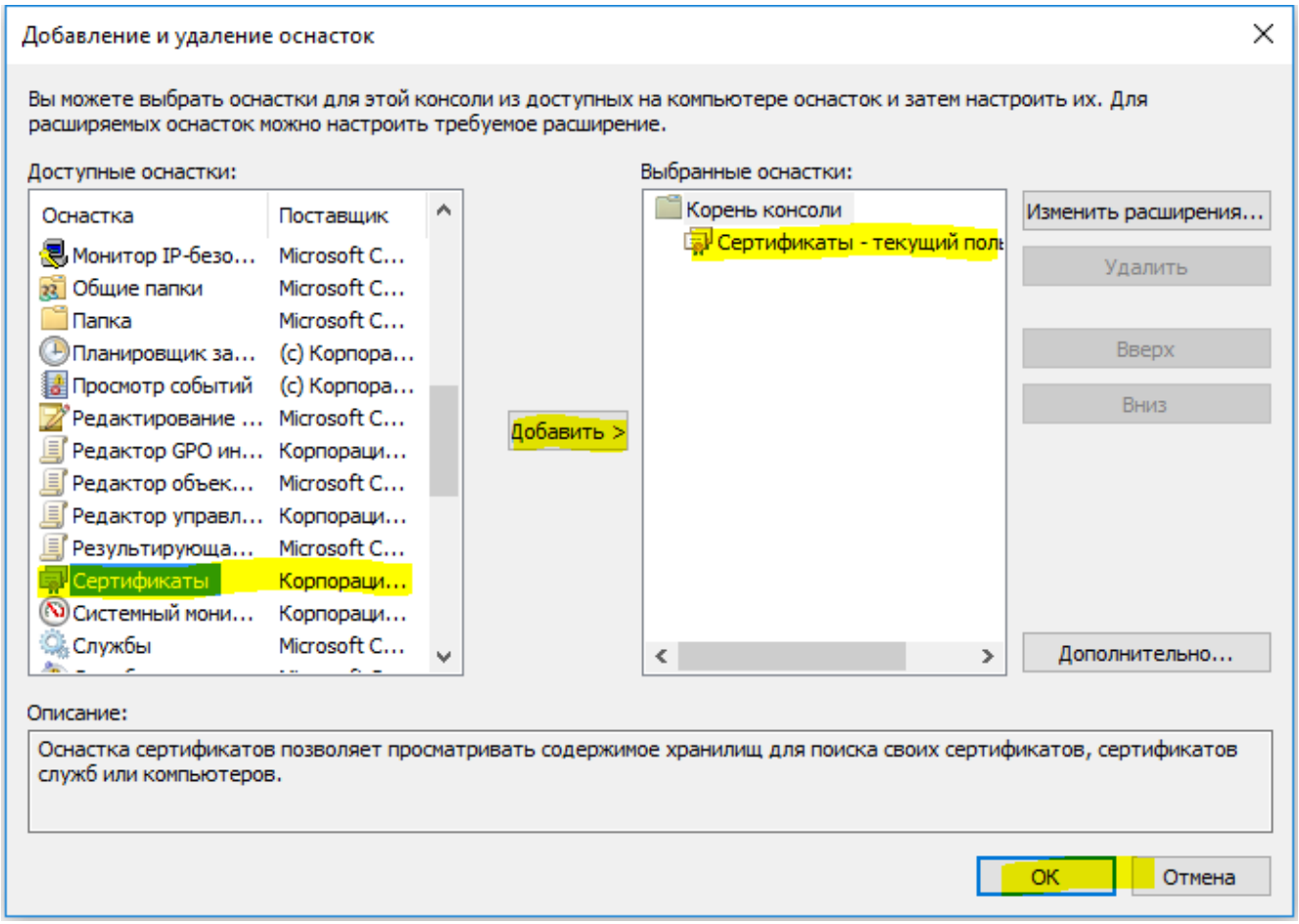
Необходимо убедится, что Ваши сертификаты перенесены в системное хранилище сертификатов WINDOWS. Правой кнопкой нажать «Пуск» - «Выполнить», набрать mmc



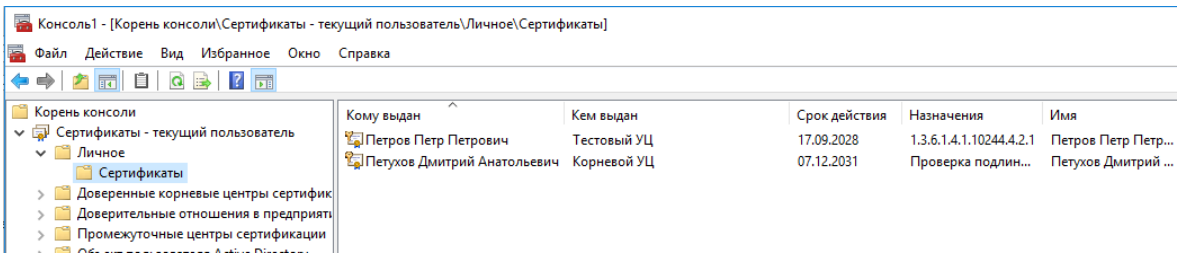
Выбрать из меню «Добавить или удалить оснастку…»



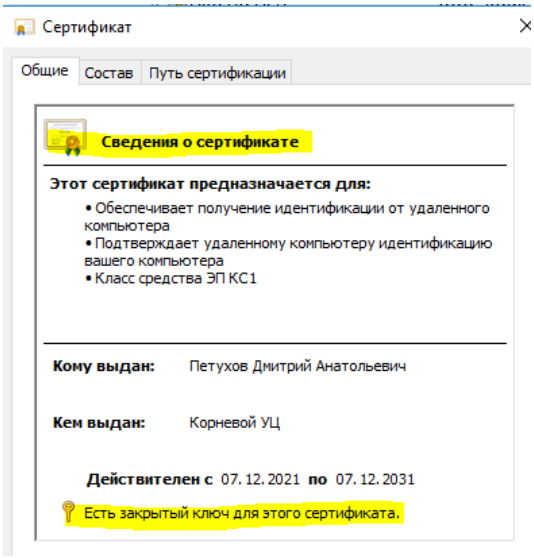
Выбрать сертификаты, нажать «Добавить» и «ОК».



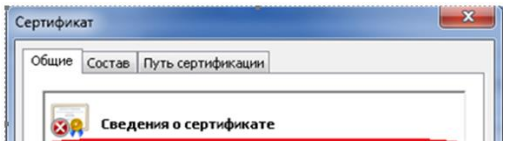
Находим личный сертификат.



Кликаем по нему дважды, убеждаемся, что сертификат не имеет предупреждающих отметок в поле «Сведения о сертификате» и есть закрытый ключ.

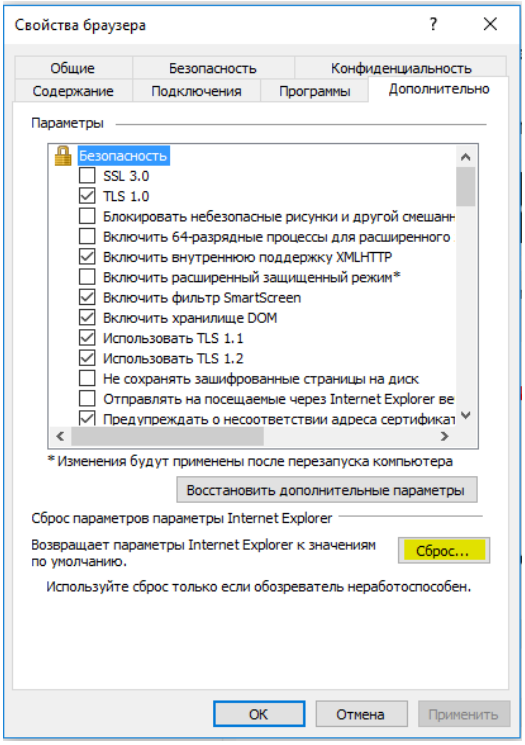


Если на значке сертификата есть крест в круге, то это означает что сертификат ключа добавлен некорректно. Тогда нужно удалить сертификат из системного хранилища и экспортировать его туда заново.



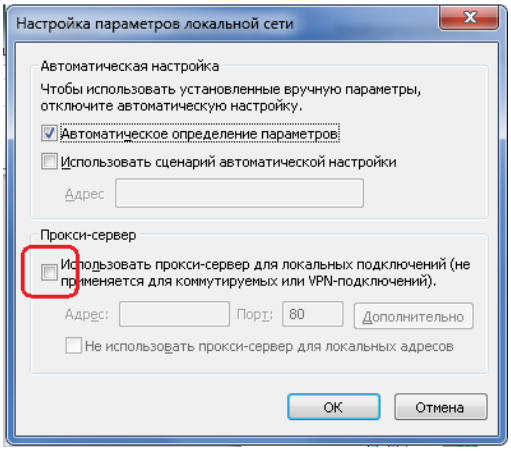
3. Для проверки доступа к странице WEB сервиса WEB-кабинетов и ПО «Луч» в режиме «WEB канала» необходимо выполнить настройки интернет-обозревателя (далее – IE):

- Сбросьте настройки IE в вариант «по умолчанию», убедитесь, что настройки SSL и TLS установлены как в окне:

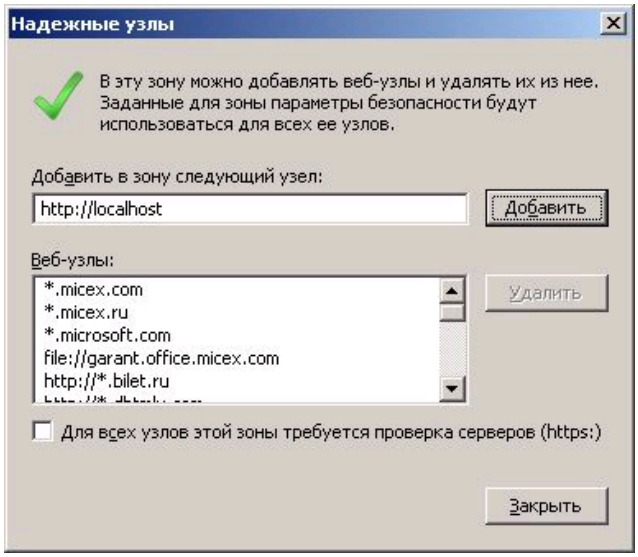


- Очистите куки и кэш память IE;

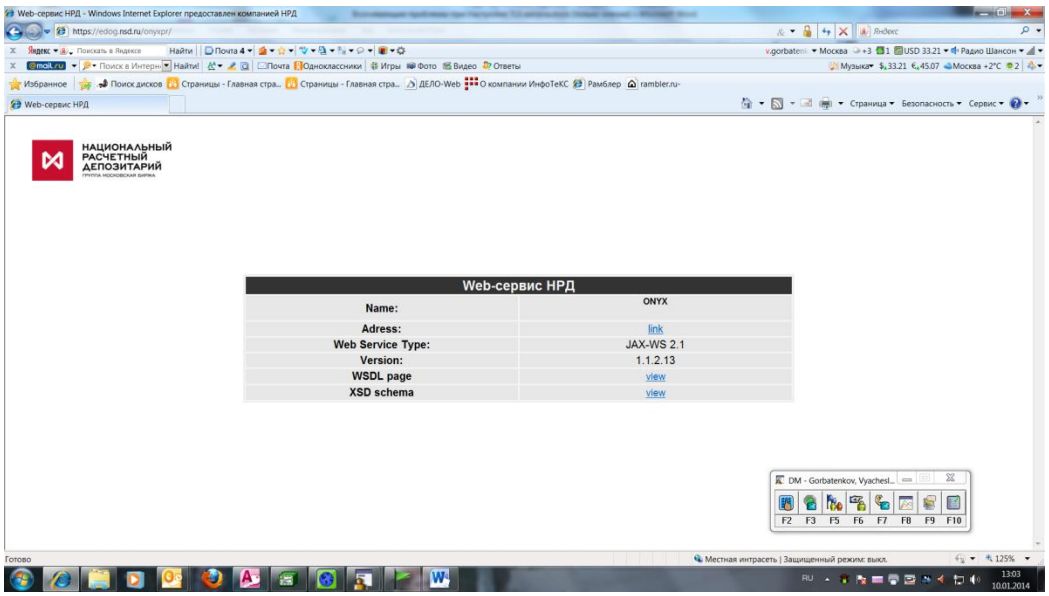
- Проверьте отсутствие галочки «прокси-сервер» (в меню: «Свойства обозревателя-Подключения-Настройки сети»);



- В форме «Надежные узлы» необходимо снять галку «Для всех узлов этой зоны требуется проверка серверов (https:)», если она включена;



В адресную строку браузер IE11 нужно вставить URL https://edog.nsd.ru/onyxpr - для ключей ГОСТ или https://edor.nsd.ru/onyxpr - для RSA ключей. Для тестового контура https://gost.nsd.ru и https://rsa.nsd.ru соответственно. Если все настройки выполнены правильно, то вы увидите страницу:

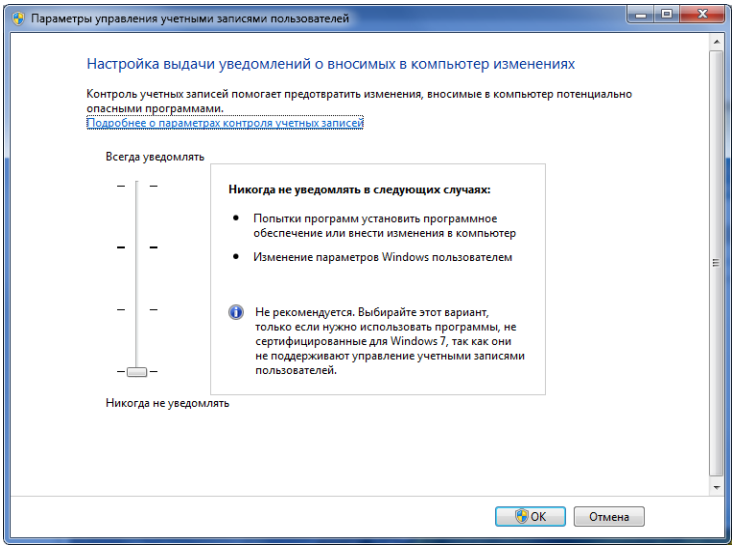


Если вместо отбражения таблицы вы получите сообщение о невозможности отображения страницы, нужно проверить доступность узла командами:

telnet edog.nsd.ru 443 и nslookup edog.nsd.ru, при отсутствии доступа попытаться настроить прокси и файервол для доступа к указанным узлам. Если не удается настроить доступ, нужно вывести машину из корпоративной сети или создать новую установив на неё предварительно СКЗИ и проверить доступ.

Известные проблемы:

Одной из проблем является высокий приоритет в параметрах управления учетными записями пользователей «движок» должен находиться в положении «Никогда не уведомлять», если это не так, то переведите его в это положение.



Часто возникают проблемы при установке на одной машине различных СКЗИ, причем даже удаление ранее установленных СКЗИ не позволяет восстановить работоспособность. Исправить можно только переустановкой ОС.

Если после всех манипуляций у вас все равно не работает WEB доступ необходимо включить протоколирование операций через реестр

- SYSTEM\CurrentControlSet\Control\Session Manager\Debug Print Filter

VD_LOGMASK_CSP,
VD_LOGMASK_SSP,
VD_LOGMASK_CNG,
VD_LOGMASK_HOOKS
все значения выставить в 496 десятичное;

- перезагрузка ПК (!!!);
- почистите все системные протоколы (Приложения и Система);
- попытайтесь подключиться ТОЛЬКО через IE к https://gost.nsd.ru - для тестового контура или https://edog.nsd.ru - для рабочего контура пару раз и пришлите системные протоколы (Приложения и Система).

После выполнения выше описанных процедур пришлите логи журналов Windows Приложения и Система, а также скриншоты, подтверждающие выполнение процедур настройки, на адрес soed@nsd.ru.

По всем возникшим вопросам необходимо обращаться к первой линии технической поддержки (адрес электронной почты soed@nsd.ru , телефон 8(495)956-09-34).