РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ ПО РАБОТЕ В ЛИЧНОМ КАБИНЕТЕ ИТП АО «ОЭК» С УСОВЕРШЕНСТВОВАННОЙ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Оглавление

1 ТРЕБОВАНИЯ К РАБОЧЕМУ МЕСТУ

Компьютер, с которого осуществляется доступ к личному кабинету информационное-технического портала АО «ОЭК» с возможностью подписания документов усовершенствованной квалифицированной электронной подписью, должен иметь следующее программное обеспечение:

- Операционная система - Windows 7, 8, 8.1,10 (подробнее в п.1.1.1);
- Средства криптографической защиты информации (СКЗИ) (подробнее в пункте 2)

Внимание: Средства криптографической защиты информации (СКЗИ) являются лицензируемым программным обеспечением. Убедитесь, что на рабочем месте установлены действующие лицензии поставщика программного обеспечения (подробнее в пункте 5).

- КриптоПро ЭЦП Browser plug-in (подробнее в пункте 3);
- Браузер Internet Explorer (версии не ниже 9) или Google Chrome, Mozilla Firefox, Apple Safari, Yandex Browser, Opera (подробнее в п.1.3);
- Установленный квалифицированный сертификат физического лица, должностного лица организации или доверенного лица (подробнее в пункте 4.1)
- Установленный корневой сертификат и кросс-сертификаты удостоверяющего центра, выпустившего квалифицированный сертификат физического лица, должностного лица организации или доверенного лица
- Установленный корневой сертификат сервера штампов времени удостоверяющего центра, выпустившего квалифицированный сертификат физического лица, должностного лица организации или доверенного лица
- Драйверы носителя электронной подписи (подробнее в пункте 4.2).
- Компьютер должен иметь доступ в Интернет (подробнее в п.1.2).

Для подготовки рабочего места к работе с личным кабинетом АО «ОЭК» пользователь операционной системы Windows должен иметь права администратора локального компьютера.

1.1 Требования к носителю ключевой информации

Носитель ключевой информации, используемый для электронно-цифровой подписи в ЛК ИТП АО «ОЭК» должен содержать квалифицированную электронную подпись, выданную аккредитованным удостоверяющим центром. Со списком аккредитованных

удостоверяющих центров можно ознакомиться на сайте Министерства связи и массовых коммуникаций РФ по ссылке http://minsvyaz.ru/ru/activity/govservices/2/

Квалифицированная электронная подпись должна поддерживать включение в электронную подпись информации о времени создания подписи (TSP) и о статусе сертификата электронной подписи в момент подписания.

Внимание: Носители, не содержащие квалифицированную электронную подпись (КЭП), не могут быть использованы для подписания документов на информационно-технологическом портале АО «ОЭК»

1.2 Операционная система

Прежде чем начать работу с Личным кабинетом с использованием электронно-цифровой подписи пользователя информационно-технологического портала АО «ОЭК» (ЛК ИТП), необходимо удостовериться, что в используемой Операционной Системе (MS Windows 7, 8, 8.1 или 10, а также Mac OS) установлены все критические и рекомендуемые обновления. Обращаем внимание на то, что для успешной работы с квалифицированной электронной подписью в ОС Windows 10 необходима установка специальной версии СКЗИ (подробнее в разделе «Установка СКЗИ»).

Внимание: Средства криптографической защиты информации (СКЗИ) являются лицензируемым программным обеспечением. Убедитесь, что на рабочем месте установлены действующие лицензии поставщика программного обеспечения (подробнее в пункте 5).

1.3 Доступ в интернет

Компьютер, на котором планируется работать с Порталом АО «ОЭК», должен иметь доступ к сети Интернет.

В случае если доступ в Интернет осуществляется через корпоративную сеть использующую прокси-сервер или межсетевой экран (файервол, брандмауэр), необходимо открыть порты 80 и 443 (TCP/IP) для доступа к адресам:

- https://itp.uneco.ru – Личный кабинет пользователя информационно-технологического портала АО «ОЭК».

1.4 Браузеры

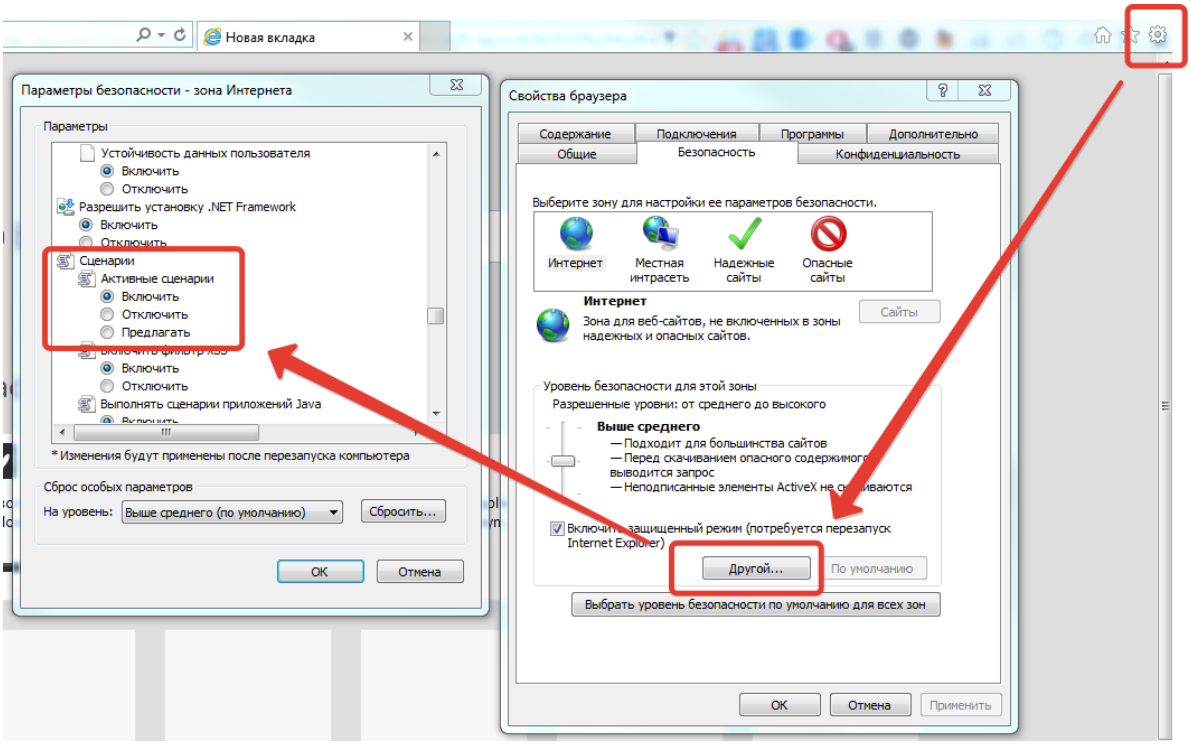
Для работы с ЛК ИТП АО «ОЭК» необходимо использовать современный браузер.

В частности, поддерживается работа со следующими браузерами:

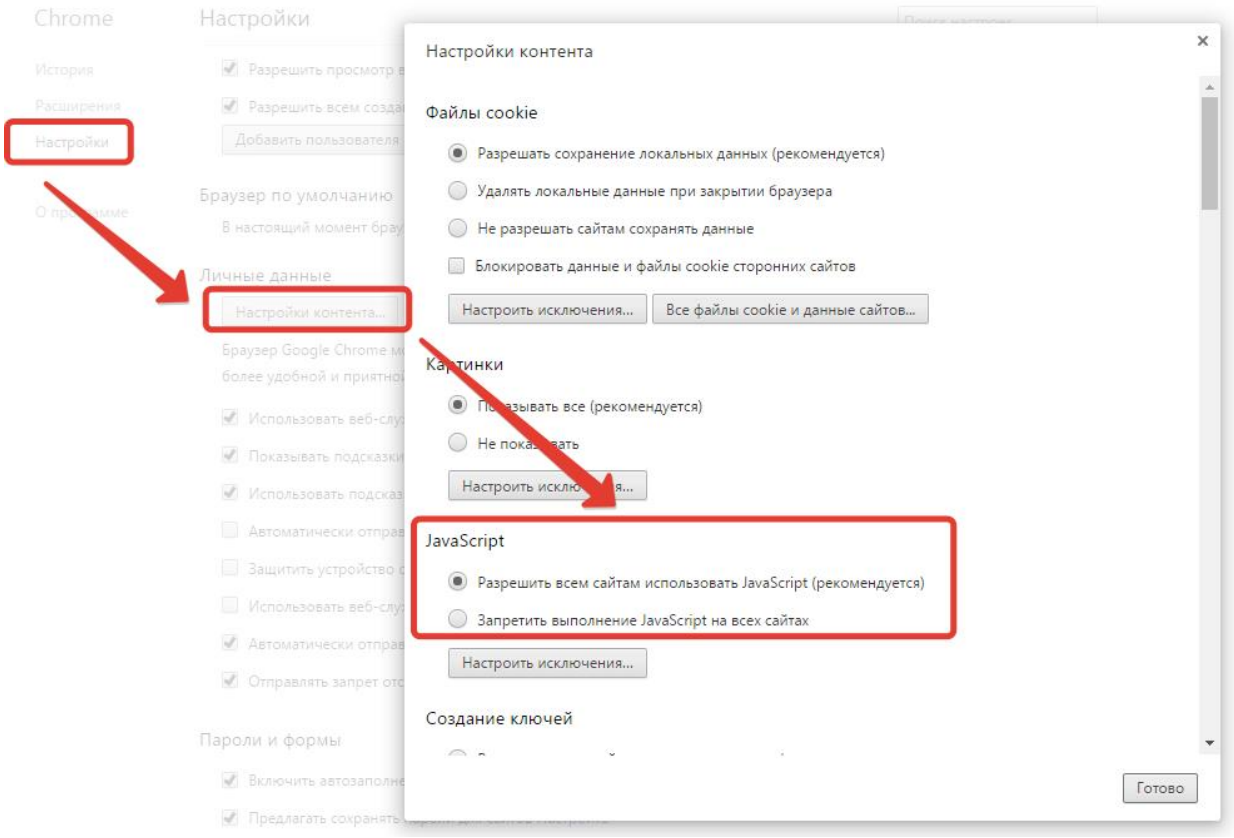
- IE 9, 10, 11: http://windows.microsoft.com/ie
- Mozilla Firefox: https://mozilla.org актуальной версии
- Opera: http://www.opera.com актуальной версии
- Google Chrome: https://www.google.com/chrome/browser актуальной версии
- Yandex Browser: http://browser.yandex.ru актуальной версии
- Apple Safari (входит в поставку ОС) актуальной версии

В используемом браузере необходимо осуществить разрешение выполнения сценариев JavaScript (обычно, данная опция включена по-умолчанию):

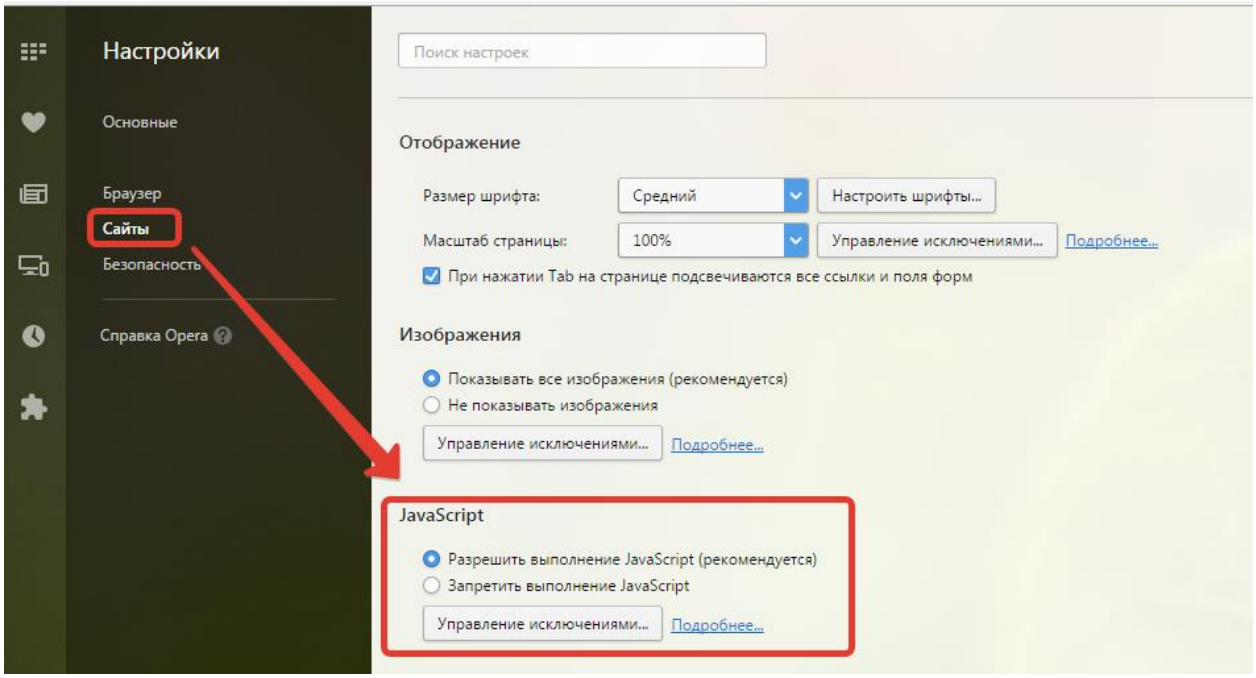
- Для IE – **Свойства браузера → безопасность → параметры безопасности (клавиша «Другой») → сценарии → «Активные сценарии» в положение «Включить»**



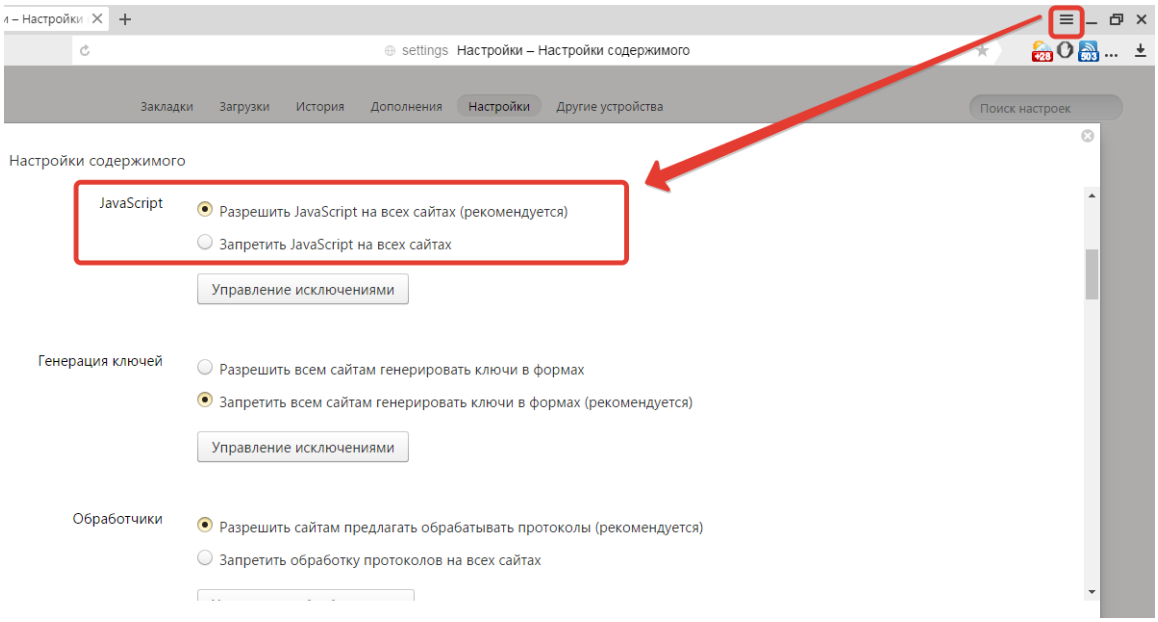
- Для Google Chrome – **настройки → настройки контента → JavaScript → разрешить всем сайтам использовать JavaScript**



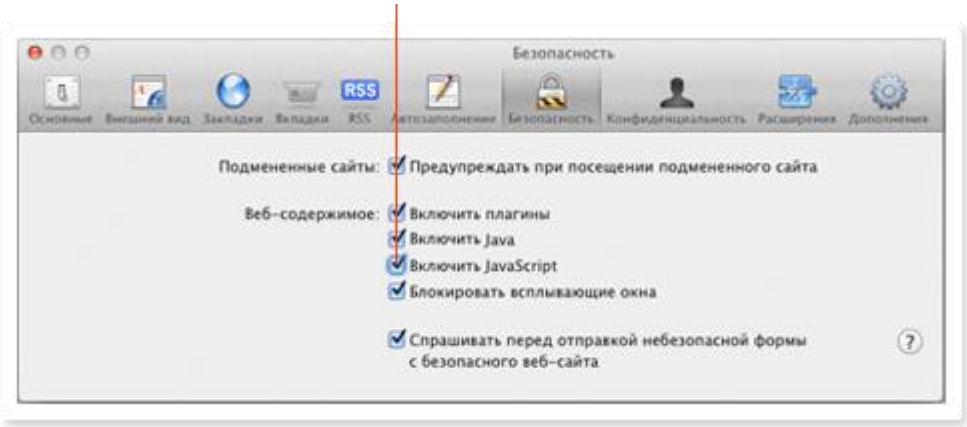
- Opera – **настройки → сайты → JavaScript → разрешить выполнение JavaScript**



- Yandex Browser – **настройки → Нажмите ссылку «Показать дополнительные настройки» внизу страницы → JavaScript → разрешить JavaScript на всех сайтах**



- Safari – **настройки → Безопасность → Включить JavaScript**



2 УСТАНОВКА СКЗИ

Установка дистрибутива СКЗИ должна производиться пользователем, имеющим права администратора.

Внимание: Удостоверяющие центры могут выпускать носители ключевой информации, предназначенные для работы со строго определенными СКЗИ – КриптоПро CSP, VipNET CSP и др. Подробную информацию, с каким СКЗИ работает Ваш носитель ключевой информации, можно узнать в удостоверяющем центре, выпустившем носитель. Рекомендуется приобретать носители ключевой информации, совместимые с СКЗИ КриптоПро CSP. В случае, если Ваш носитель не работает с СКЗИ КриптоПро CSP, необходимо иметь на рабочем месте СКЗИ, указанный при выпуске носителя и установленный согласно руководству

поставщика программного обеспечения. Убедитесь, согласно руководству поставщика, программного обепечения, что установлены действующие лицензии на СКЗИ. При этом устанавливать дополнительно КриптоПро CSP не требуется и не рекомендуется ввиду необходимости установки специализированных настроек совместимости разных СКЗИ на одном рабочем месте.

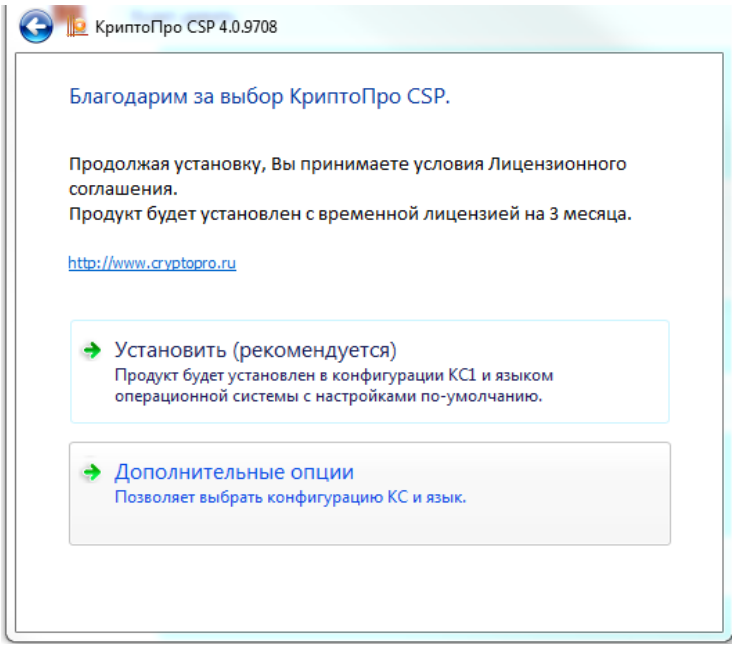
2.1 Установка СКЗИ КриптоПро CSP

Для установки программного обеспечения вставьте компакт-диск в дисковод или запустите установку дистрибутива из скачанного из сети интернет файла CSPSetup.exe (https://www.cryptopro.ru/products/csp). Из предлагаемых дистрибутивов выберите дистрибутив, подходящий для Вашей операционной системы (соответствие версий КриптоПРО CSP и операционной системы MS Windows представлено в таблице ниже), имеющий нужный Вам уровень защищенности и удобный для Вас язык установки.

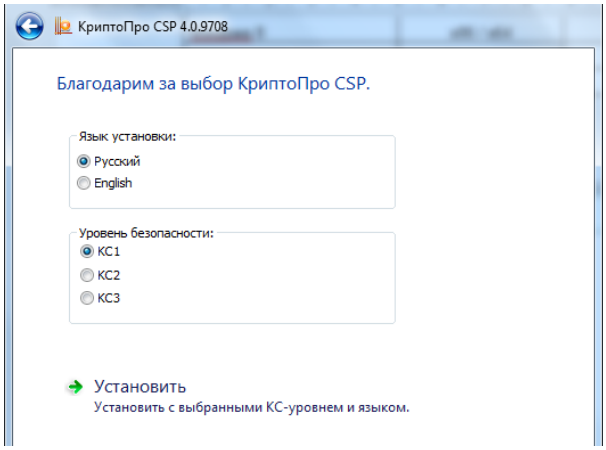
Таблица 1 Соответствие версий КриптоПро CSP и Windows

	CSP 3.6	**CSP 3.9**	**CSP 4.0**
Windows 10		x86 / x64 (CSP 3.9 R2)	x86 / x64
Windows 2012 R2		x64	x64
Windows 8.1		x86 / x64	x86 / x64
Windows 2012	x64	x64	x64
Windows 8	x86 / x64	x86 / x64	x86 / x64
Windows 2008 R2	x64 / itanium	x64	x64
Windows 7	x86 / x64	x86 / x64	x86 / x64

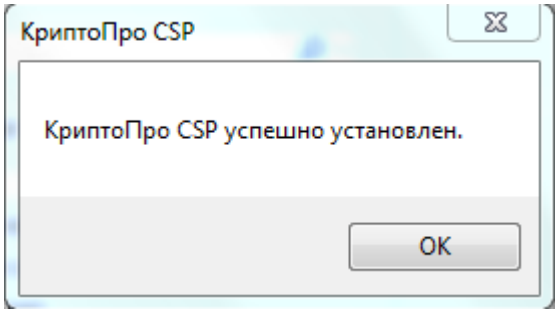
Запустите выполнение установки.



Перед запуском мастера установки есть возможность осуществить настройки установки, выбрав язык установки и уровень безопасности путем нажатия кнопки «Дополнительные опции»).



После нажатия клавиши «Установить» произведется установка КриптоПРО на компьютере пользователя, при завершении которой пользователь увидит информационное окно.

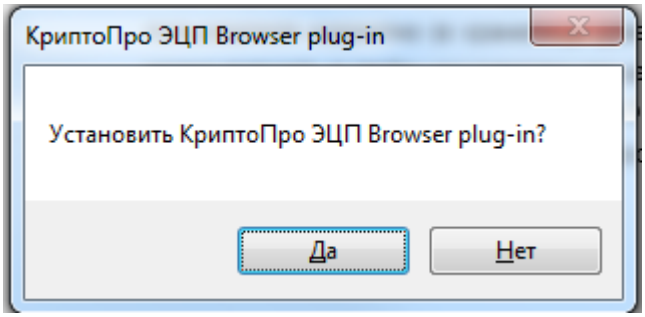


Внимание: Средство криптографической защиты информации (СКЗИ) КриптоПро CSP является лицензируемым программным обеспечением. Убедитесь, что на рабочем месте установлены действующие лицензии поставщика программного обеспечения (подробнее в пункте 5).

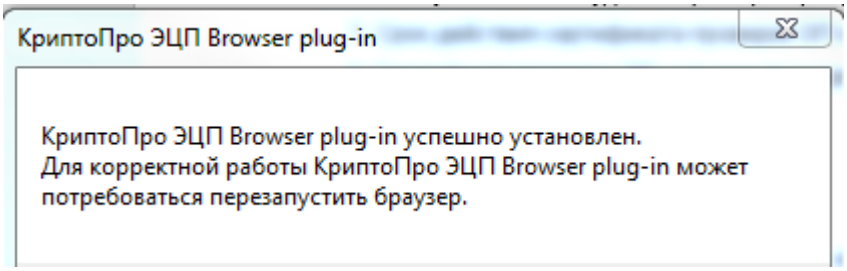
3 УСТАНОВКА КРИПТОПРО ЭЦП BROWSER PLUG-IN

КриптоПро Browser plug-in плагин имеет бессрочную бесплатную лицензию Для установки КриптоПро Browser plug-in необходимо открыть в браузере страницу http://www.cryptopro.ru/products/cades/plugin/get_2_0 и загрузить на свой компьютер предлагаемую программу установки.. и выполнить установку:

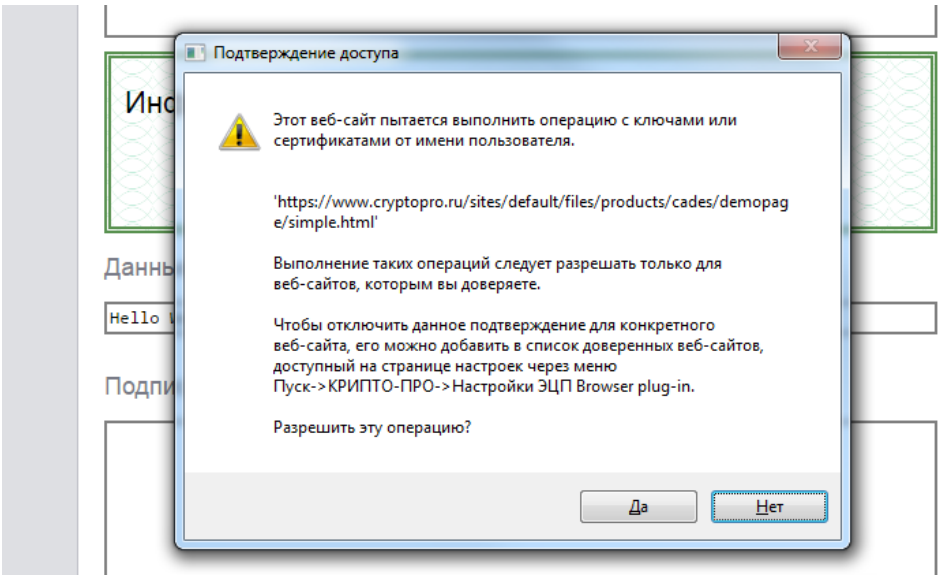
1. Запустить скачанный файл с установщиком плагина



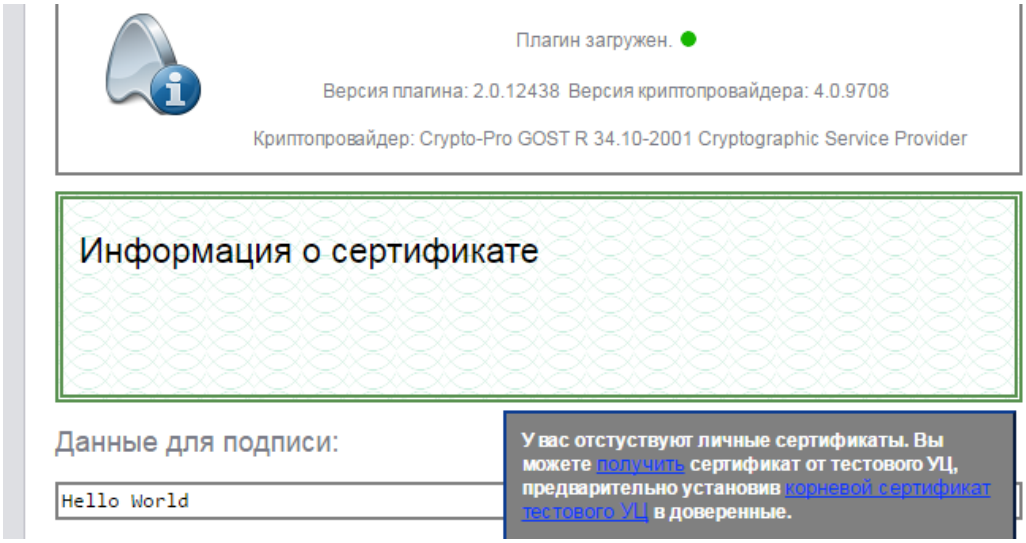
2. По окончанию установки отобразится информационное окно об успешной установке



3. Для подтверждения работоспособности плагина перезапустите браузер и перейдите на страницу проверки работоспособности https://www.cryptopro.ru/sites/default/files/products/cades/demopage/simple.html. В появившемся информационном окне разрешите выполнение операции



4. В случае если плагин установлен верно, в открывшемся окне появится информация о версии плагина и установленного криптопровайдера, а также информация о доступных личных сертификатах

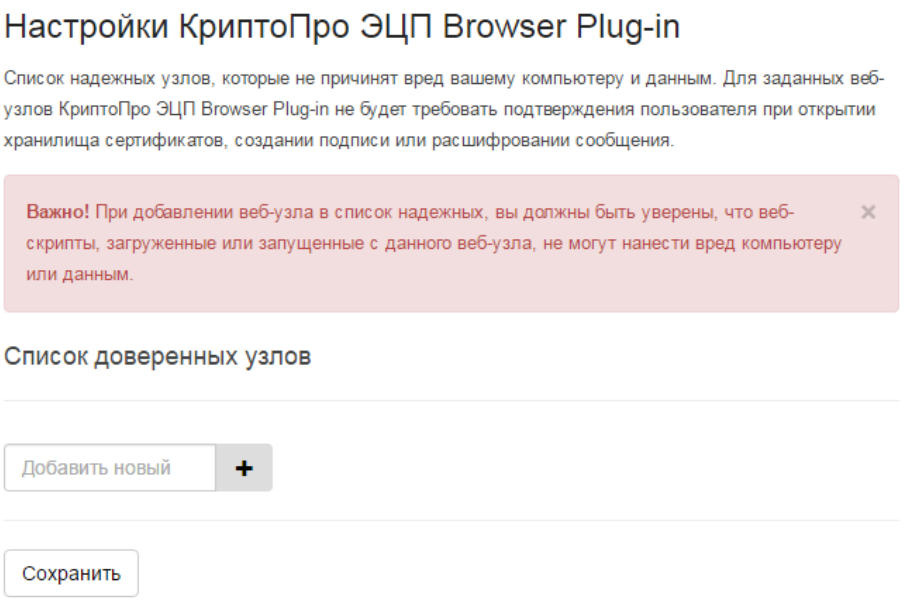


Установка КриптоПро ЭЦП Browser Plug-in Настройка КриптоПро ЭЦП Browser Plug-in должна быть произведена после установки СКЗИ, используемого для Вашего носителя ключевой информации.

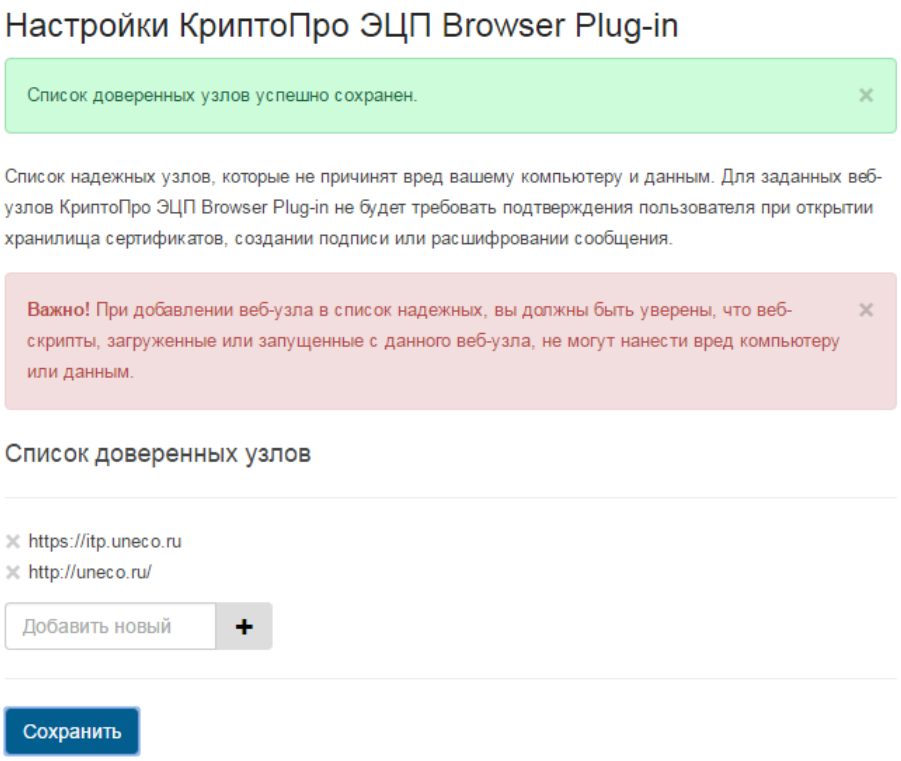
Для настройки КриптоПро ЭЦП Browser Plug-in найдите в установленных на компьютере программах в разделе КРИПТО-ПРО пункт «Настройки ЭЦП Browser Plug-in»:

- Для операционных систем, имеющих кнопку «Пуск» (Windows 7) - **Пуск / Все программы / КРИПТО-ПРО / Настройки ЭЦП Browser Plug-in**
- Для операционных систем, имеющих «плиточный» интерфейс (Windows 8,8.1,10) – **Все приложения / блок КРИПТО-ПРО / Настройки ЭЦП Browser Plug-in**

После этого откроется окно настройки КриптоПро ЭЦП Browser Plug-in:



Выполните для узла https://itp.uneco.ru добавление в список надежных узлов. Для этого в поле «Добавить узел» впишите добавляемый узел и нажмите кнопку «Добавить». После того как узлы будут добавлены, нажмите клавишу «Сохранить».



4 СЕРТИФИКАТЫ ДЛЯ ЭЦП

4.1 Квалифицированный сертификат ключа проверки электронной подписи физического лица, должностного лица организации или доверенного лица (квалифицированный сертификат, сертификат)

Для работы с личным кабинетом используется квалифицированный сертификат ключа проверки электронной подписи физического лица, доверенного лица, руководителя организации или специального должностного лица, ответственного за работу с личным кабинетом. Сертификат записывается на персональные идентификаторы – носители ключевой информации (далее – носители). Для работы с Порталом рекомендуется использовать сертифицированные ФСТЭК России носители ключевой информации типа eToken или Rutoken. Как правило, тип используемого носителя можно определить визуально по надписи на носителе:

Также тип указывается в документах при получении сертификата. Кроме этого его можно уточнить в удостоверяющем центре, выдавшем сертификат.

Внимание: Удостоверяющие центры могут выпускать носители ключевой информации, предназначенные для работы со строго определенными СКЗИ – КриптоПро CSP, VipNET CSP и др. Подробную информацию, с каким СКЗИ работает Ваш носитель ключевой информации, можно узнать в удостоверяющем центре, выпустившем носитель. Рекомендуется приобретать носители ключевой информации, совместимые с СКЗИ КриптоПро CSP. В случае, если Ваш носитель не работает с СКЗИ КриптоПро CSP, необходимо иметь на рабочем месте СКЗИ, указанный при выпуске носителя и установленный согласно руководству поставщика программного обеспечения. Убедитесь, согласно руководству поставщика программного обепечения, что установлены действующие лицензии на СКЗИ. При этом устанавливать дополнительно КриптоПро CSP не требуется и не рекомендуется ввиду необходимости установки специализированных настроек

совместимости разных СКЗИ на одном рабочем месте.

4.2 Установка драйвера носителя ключевой информации

Для работы с носителем ключевой информации eToken или Rutoken необходимо, чтобы на Вашем компьютере был установлен соответствующий драйвер.

Как правило, драйвер носителя предоставляется удостоверяющим центром непосредственно при выдаче сертификата. Если у Вас нет драйвера, Вы можете загрузить его самостоятельно.

Если Вы получили подпись на носителе какого-либо другого типа или не можете определить тип своего носителя, пожалуйста, обратитесь за консультацией в техническую поддержку своего удостоверяющего центра.

4.2.1 Установка драйвера носителя типа Rutoken

Драйвер носителя обычно предоставляется удостоверяющим центром в комплекте с самим носителем Rutoken, однако его можно загрузить с официального сайта разработчика (http://www.rutoken.ru/support/download/drivers-for-windows/).

Если Вы получили драйвер в удостоверяющем центре – произведите его установку в соответствии с прилагаемой к нему инструкцией.

Если драйвер загружается с сайта, то выберите на открывшейся странице 32- или 64-битную версию в зависимости от вашей операционной системы, и загрузите файл.

Выполните следующие действия:

Войдите в систему с правами администратора.

1. Закройте все приложения.
2. Двойным щелчком запустите загруженный exe - файл.

После запуска файла следуйте указаниям установщика.

4.2.2 Установка драйвера носителя типа eToken

Драйвер носителя обычно предоставляется Удостоверяющим центром в комплекте с самим носителем eToken, однако его можно загрузить с официального сайта разработчика (http://www.aladdin-rd.ru/support/downloads/etoken/).

Если Вы получили драйвер в удостоверяющем центре – произведите его установку в соответствии с прилагаемой к нему инструкцией.

Если драйвер загружен с сайта, распакуйте полученный архивный файл (ZIP-архив).

Архив содержит файлы драйвера (eToken PKI Client) и документацию для его администрирования, включая различные варианты инсталляции, и использования. Для установки ПО eToken PKI Client 5.1 SP1 (драйвер носителя ключевой информации eToken) со стандартными настройками и компонентами выполните следующие действия:

- Войдите в систему с правами администратора.
- Закройте все приложения.

Двойным щелчком запустите мастер установки из файла .msp (выберите 32- или 64-битную версию в зависимости от вашей операционной системы).

После запуска файла следуйте указаниям установщика.

4.2.3 Инициализация драйвера носителя типа eToken

Подключите носитель ключевой информации типа eToken к любому usb-порту вашего персонального компьютера и запустите eToken PKI Client (меню **Пуск ⇒ Все программы ⇒ eToken ⇒ Start eToken PKI Client**).

Для проверки запуска eToken PKI Client выберите правой нижней части экрана значок «Отображать скрытые знаки»

Об успешном запуске клиента будет свидетельствовать появившийся в системном лотке значок PKI Client.

4.3 Установка квалифицированного сертификата ключа проверки электронной подписи физического лица, должностного лица организации или доверенного лица.

Для работы с ЛК ИТП АО «ОЭК» необходимо провести установку квалифицированного сертификата ключа проверки электронной подписи физического лица, должностного лица организации или доверенного лица (далее - Личного сертификата), выданного аккредитованным удостоверяющим центром, на ваш компьютер. Под установкой Личного сертификата понимается установка сертификата в хранилище «Личные» с формированием ссылки на закрытый ключ, соответствующий данному сертификату.

Подключите носитель ключевой информации (eToken или Rutoken) к любому usb-порту вашего персонального компьютера

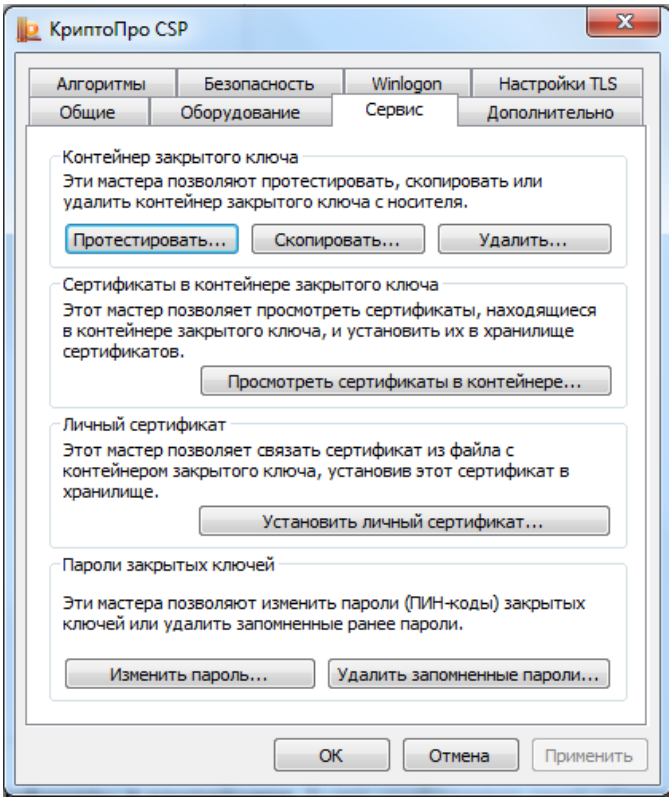
Внимание: Инструкция, приведенная ниже в данном разделе, описывает установку Личного сертификата для СКЗИ КриптоПро CSP. В случае, если на Вашем рабочем месте установлен иной СКЗИ, произведите установку Личного сертификата

согласно руководства поставщика программного обеспечения

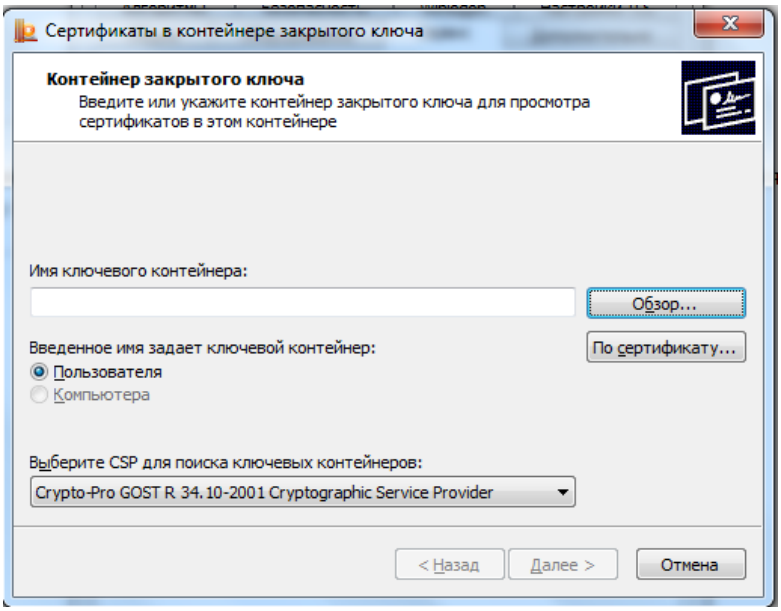
Выполните:

- для классического интерфейса: **Пуск ⇒Программы ⇒ КриптоПро ⇒ КриптоПро CSP**;
- для «плиточного» интерфейса: **КриптоПро CSP**.

Откроется интерфейс управления СКЗИ КриптоПро CSP. Перейдите на вкладку Сервис:



Нажмите кнопку «Просмотреть сертификаты в контейнере». Будет отображено окно «Сертификаты в контейнере закрытого ключа».



При этом Имя ключевого контейнера выбирается из списка или вводится вручную. Для открытия списка нажмите кнопку «Обзор». Откроется форма «КриптоПро CSP» со списком ключевых контейнеров пользователя. Далее выполните следующие действия:

1. Выберите нужный контейнер и нажмите клавишу «ОК».
2. Имя контейнера будет записано в поле Имя ключевого контейнера формы «Сертификаты в контейнере закрытого ключа». Для продолжения установки сертификата нажмите кнопку «Далее». Отобразится окно «Сертификаты в контейнере закрытого ключа».
3. Нажмите кнопку «Установить».
4. Сертификат будет установлен в хранилище «Личные» текущего пользователя.
5. Нажмите кнопку «Свойства». Откроется форма «Сертификат».
6. Нажмите кнопку «Установить».
7. Следуйте указаниям мастера импорта сертификатов.
8. Завершение установки сертификата будет подтверждено соответствующим сообщением.

4.4 Установка корневого и кросс-сертификатов удостоверяющего центра

Для правильной работы ЛК ИТП необходимо скачать и установить корневой и кросс-сертификаты удостоверяющего центра (далее УЦ), выпустившего носитель ключевой информации. Для этого необходимо зайти на веб-сайт УЦ и скачать необходимые сертификаты. Ссылку на скачивание можно получить в технической поддержке УЦ, либо найти самостоятельно на веб-сайте УЦ.

Для запуска процесса установки Вам необходимо дважды щелкнуть левой кнопкой

мыши по скачанному файлу корневого или кросс сертификата. Далее необходимо предпринять следующие действия:

1. В открывшемся окне свойств сертификата нажмите кнопку «**Установить сертификат**».
2. Далее следовать указаниям мастера импорта сертификатов.
3. Корневой сертификат следует установить в хранилище «**Доверенные корневые центры сертификации**», кросс-сертификаты следует установить в хранилище «**Промежуточные центры сертификации**»

4.5 Установка корневого сертификата сервера штампов времени.

Время создания квалифицированной электронной подписи удостоверяется электронной подписью специального сервера точного времени. Для этого в процессе создания подписи происходит обращение к серверу, создается метка точного времени, которая и сохраняется в электронной подписи. Для постановки метки необходимо скачать и установить на рабочее место корневой сертификат сервера штампов времени. Для большинства УЦ достаточно установить только корневой сертификат самого УЦ (см. пункт 4.4). Ссылку на скачивание можно получить в технической поддержке УЦ, либо найти самостоятельно на веб-сайте УЦ.

Для запуска процесса установки Вам необходимо дважды щелкнуть левой кнопкой мыши по скачанному файлу корневого сертификата. Далее необходимо предпринять следующие действия:

4. В открывшемся окне свойств сертификата нажмите кнопку «**Установить сертификат**».
5. Далее следовать указаниям мастера импорта сертификатов.

Корневой сертификат сервера штампов времени следует установить в хранилище «**Доверенные корневые центры сертификации**»

4.6 Установка списка отзыва сертификатов (CRL)

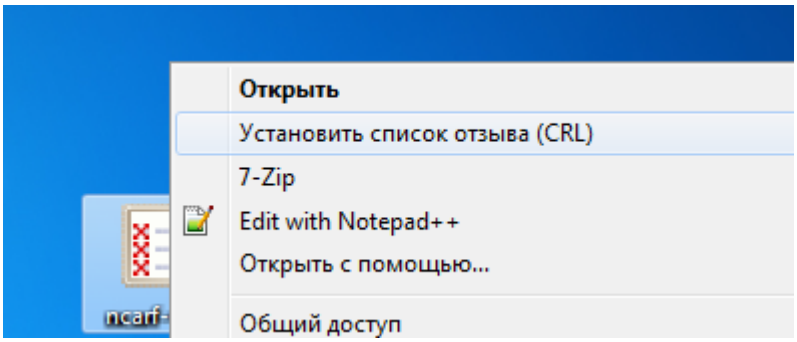
Подпись документа в ЛК ИТП АО «ОЭК» включает в себя информацию о текущем статусе Личного сертификата, подтверждающей, что Личный сертификат пользователя является действующим на момент постановки подписи (не аннулирован и не отозван). В зависимости от услуг, предоставляемых Удостоверяющим Центром, данная информация может быть предоставлена в режиме онлайн (OCSP протокол), либо путем проверки в актуальном списке отзыва сертификатов (CRL). Более точную информацию необходимо получить в Удостоверяющем Центре, выпустившем квалифицированный электронный сертификат физического лица, должностного лица организации или доверенного лица.

Если статус Личного сертификата подтверждается путем проверки в актуальном списке отзыва сертификатов, в стандартных ситуациях данная проверка производится

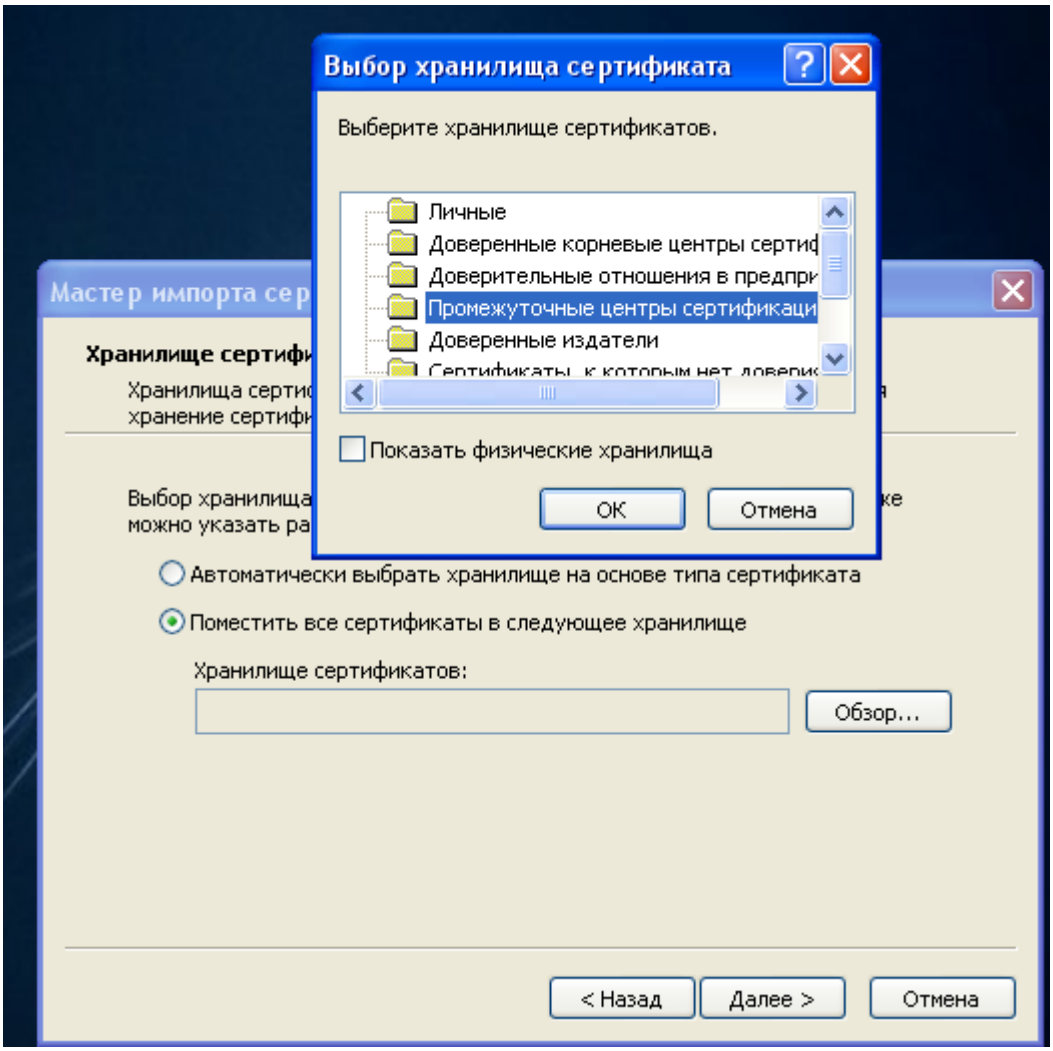
онлайн. Но, в случае недоступности списка онлайн, может возникать необходимость установки списка по ссылке с сайта Удостоверяющего Центра на компьютер пользователя.

Для установки списка отзыва сертификатов необходимо выполнить следующие действия:

1. Скачать на рабочий стол список отзыва сертификатов по ссылке с сайта Удостоверяющего центра.
2. На рабочем столе щелкнуть правой кнопкой мыши по иконке скачанного файла и в появившемся меню Windows выбрать «**Установить список отзыва**»



3. Загружается мастер импорта сертификатов, жмем кнопку «**Далее**»
4. Ставим галку «**Поместить все сертификаты в следующее хранилище**», жмем кнопку «обзор» и в появившемся окне выбираем папку «**Промежуточные центры сертификации**»



5. Жмем кнопку «ОК»
6. В мастере нажимаем «Далее» и «Готово»

Внимание: Список отзыва сертификатов имеет короткий срок действия. Поэтому, при возникновении ошибок подписи, связанных с доступностью списка, необходимо скачивать и устанавливать актуальный список с сайта Удостоверяющего Центра.

4.7 Установка корневого сертификата Головного Удостоверяющего Центра Министерства связи и коммуникаций Российской Федерации и корневого сертификата Национального Удостоверяющего центра

Для правильной работы ЛК ИТП необходимо скачать и установить корневой

сертификат Головного Удостоверяющего Центра Министерства связи и коммуникаций Российской Федерации, корневой сертификат УЦ 1 ИС ГУС и корневые сертификаты Национального Удостоверяющего Центра. Для этого необходимо зайти на веб-сайт Национального Удостоверяющего Центра и скачать необходимые сертификаты по ссылке https://www.nucrf.ru/info/..

Для запуска процесса установки Вам необходимо дважды щелкнуть левой кнопкой мыши по каждому из скачанных файлов корневых сертификатов. Далее необходимо предпринять следующие действия:

6. В открывшемся окне свойств сертификата нажмите кнопку «**Установить сертификат**».
7. Далее следовать указаниям мастера импорта сертификатов.

Корневой сертификат следует установить в хранилище «**Доверенные корневые центры сертификации**»

5 ТРЕБОВАНИЯ К ЛИЦЕНЗИЯМ

При создании и проверке электронно-цифровой подписи в ЛК ИТП АО «ОЭК» используется программное обеспечение, созданное поставщиками, имеющих лицензии от государственных органов на разработку и поставку криптографических средств. Программное обеспечение является лицензионным и требует закупки и установки на рабочее место действующих лицензий от поставщиков ПО

5.1 Лицензия на СКЗИ

На рабочее место должно быть установлено СКЗИ, рекомендуемое удостоверяющим центром, выпустившем носитель ключевой информации.

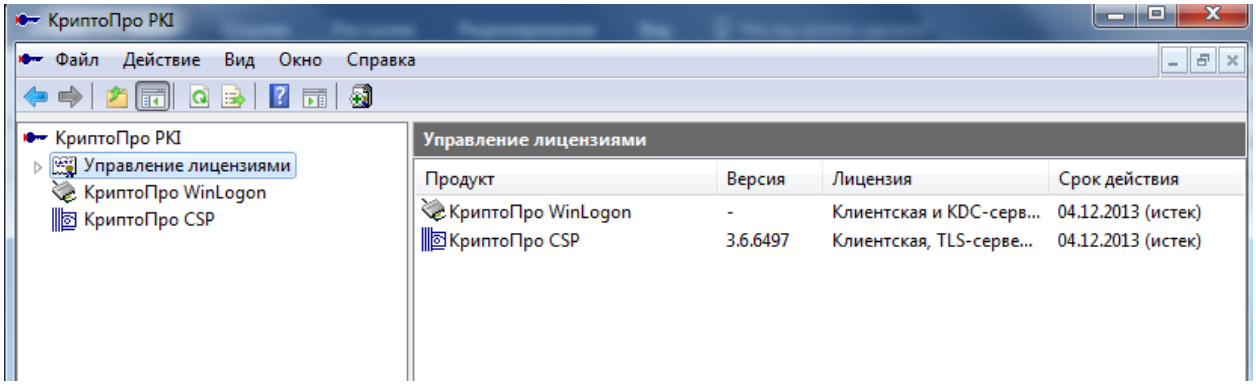
Внимание: Далее в этом разделе описывается установка лицензий на СКЗИ КриптоПро CSP. В случае, если на рабочем месте установлен иной СКЗИ, порядок приобретения и установки лицензий описан в руководствах, предоставляемых поставщиком программного обеспечения

Для проверки и установки действующей лицензии на КриптоПро CSP, необходимо открыть на рабочем месте программу КриптоПро PKI.

- Для операционных систем, имеющих кнопку «Пуск» (Windows 7) - **Пуск / Все программы / КРИПТО-ПРО / КриптоПро PKI**
- Для операционных систем, имеющих «плиточный» интерфейс (Windows 8,8.1,10) – **Все приложения / блок КРИПТО-ПРО / КриптоПро PKI**

В интерфейсе программы, в левом окне, необходимо выделить пункт «Управление

Лицензиями». В правом окне появится список установленных продуктов КриптоПро с информацией о сроке действия установленных лицензий:



Выделите КриптоПро CSP в правом списке, и через меню «Действие – Все задачи – Ввести серийный номер» введите действующую лицензию на КриптоПро CSP. Действующую лицензию можно приобрести на сайте КриптоПро: https://www.cryptopro.ru/products/csp

5.2 Лицензия на КриптоПро TSP Client

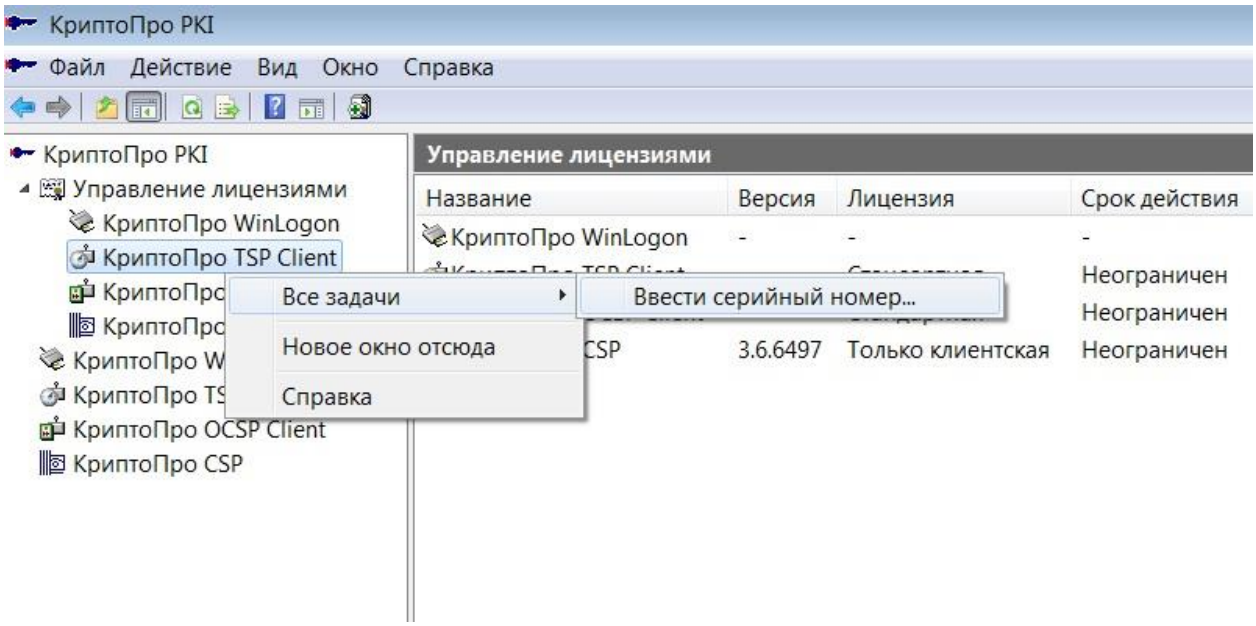
Время создания электронной подписи удостоверяется электронной подписью специального сервера точного времени. Для этого в процессе создания электронной подписи происходит обращение к серверу, создается метка точного времени, которая и сохраняется в электронной подписи. Для выполнения данных операций при установке КриптоПро Browser plug-in происходит установка специального ПО – КриптоПро TSP Client. Данное ПО является лицензионным и требует приобретения и установки действующих лицензий.

Для проверки и установки действующей лицензии на КриптоПро TSP Client, необходимо открыть на рабочем месте программу КриптоПро PKI.

- Для операционных систем, имеющих кнопку «Пуск» (Windows 7) - **Пуск / Все программы / КРИПТО-ПРО / КриптоПро PKI**
- Для операционных систем, имеющих «плиточный» интерфейс (Windows 8,8.1,10) – **Все приложения / блок КРИПТО-ПРО / КриптоПро PKI**

В интерфейсе программы, в левом окне, необходимо выделить пункт «Управление Лицензиями». В правом окне появится список установленных продуктов КриптоПро с информацией о сроке действия установленных лицензий. Выделите КриптоПро TSP Client в правом списке, и через меню «Действие – Все задачи – Ввести серийный номер» введите действующую лицензию на КриптоПро TSP Client. Действующую лицензию можно приобрести на сайте КриптоПро: https://www.cryptopro.ru/order/ - раздел «Другие продукты

КриптоПро»



5.3 Лицензия на КриптоПро OCSP Client

Подпись документа в ЛК ИТП АО «ОЭК» включает в себя информацию о текущем статусе Личного сертификата, подтверждающей, что Личный сертификат пользователя является действующим на момент постановки подписи (не аннулирован и не отозван). В зависимости от услуг, предоставляемых Удостоверяющим Центром, данная информация может быть предоставлена в режиме онлайн (OCSP протокол), либо путем установки на компьютер пользователя актуального списка отозванных сертификатов (CRL). Более точную информацию необходимо получить в Удостоверяющем Центре, выпустившем квалифицированный электронный сертификат физического лица, должностного лица организации или доверенного лица. В случае, если Удостоверяющий Центр предоставляет проверку статуса по OCSP протоколу необходимо приобрести лицензию на специализированное ПО - КриптоПро OSCP Client.

Для проверки и установки действующей лицензии на КриптоПро OSCP Client, необходимо открыть на рабочем месте программу КриптоПро PKI.

- Для операционных систем, имеющих кнопку «Пуск» (Windows 7) - **Пуск / Все программы / КРИПТО-ПРО / КриптоПро PKI**
- Для операционных систем, имеющих «плиточный» интерфейс (Windows 8,8.1,10) – **Все приложения / блок КРИПТО-ПРО / КриптоПро PKI**

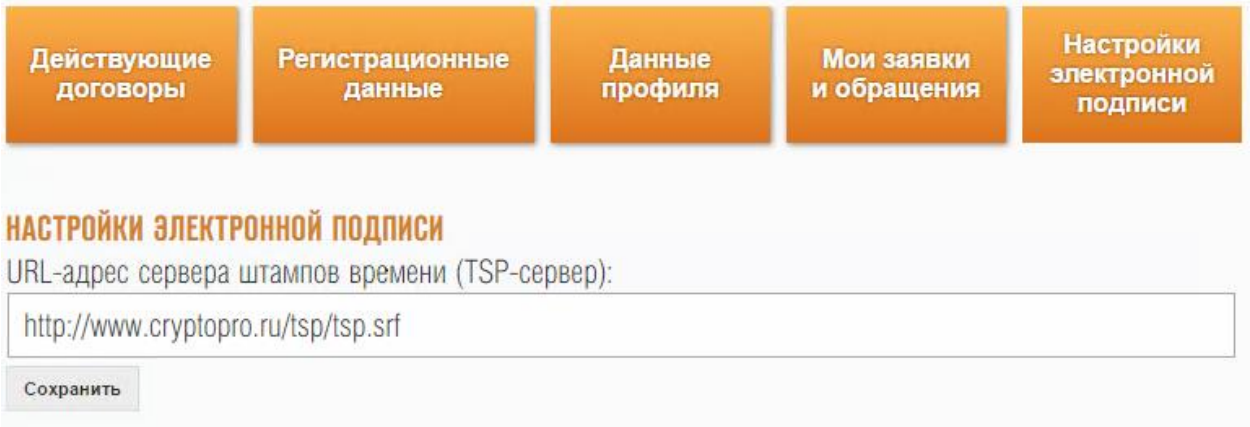
В интерфейсе программы, в левом окне, необходимо выделить пункт «Управление Лицензиями». В правом окне появится список установленных продуктов КриптоПро с

информацией о сроке действия установленных лицензий. Выделите КриптоПро OSCP Client в правом списке, и через меню «Действие – Все задачи – Ввести серийный номер» введите действующую лицензию на КриптоПро OSCP Client. Действующую лицензию можно приобрести на сайте КриптоПро: https://www.cryptopro.ru/order/ - раздел «Другие продукты КриптоПро»

6 НАСТРОЙКИ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ (УКЭП) ДЛЯ ПОДПИСАНИЯ ДОКУМЕНТОВ В ЛК ИТП АО «ОЭК».

6.1 Настройка ссылки на сервер штампов времени.

Время создания электронной подписи удостоверяется электронной подписью специального сервера точного времени. Удостоверяющий центр, при выдаче, усовершенствованной квалифицированной электронной подписи, предоставляет ссылку на доступные для данного носителя ключевой информации сервера точного времени. Для правильной работы с сервером точного времени, ссылка, предоставленная Удостоверяющим Центром, должна быть сохранена в Личном кабинете пользователя в разделе «Настройки электронной подписи».



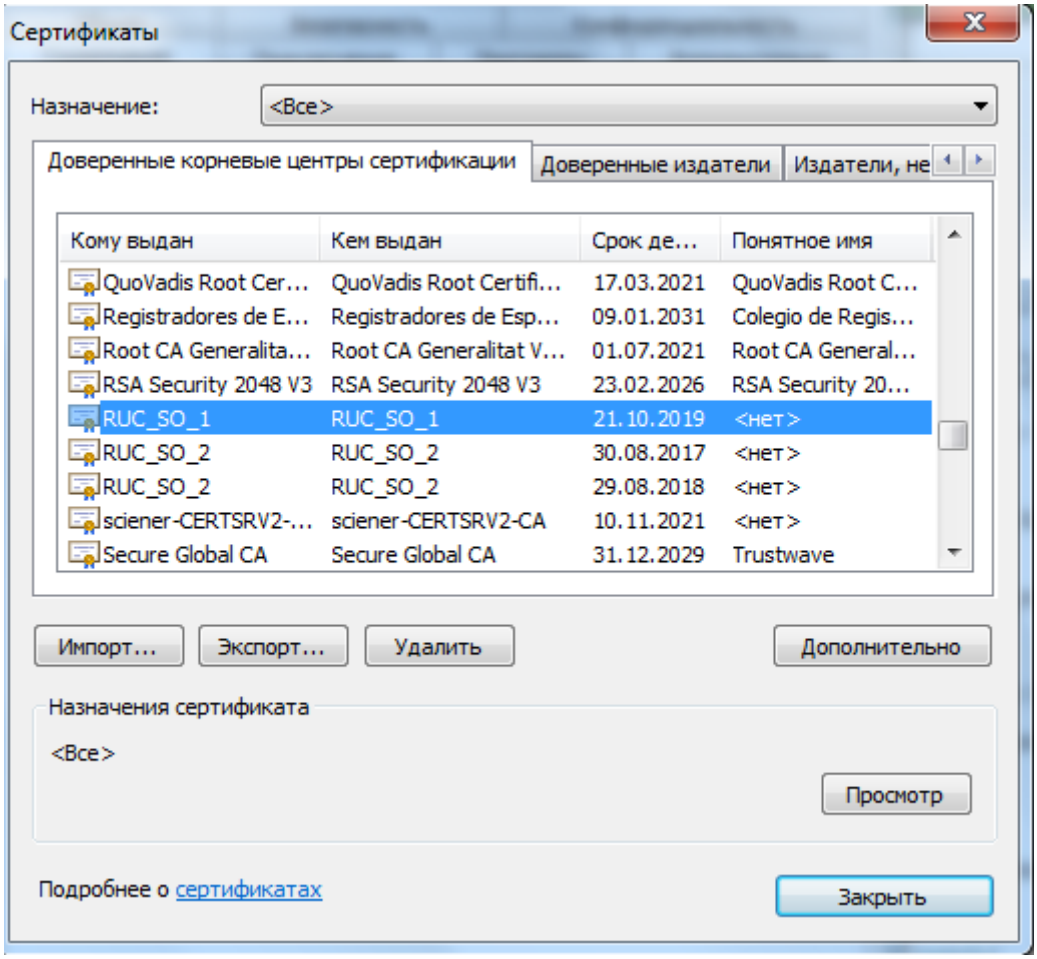
6.2 Настройка ссылки на OCSP сервер Удостоверяющего Центра

Подпись документа в ЛК ИТП АО «ОЭК» включает в себя информацию о текущем статусе Личного сертификата, подтверждающей, что Личный сертификат пользователя является действующим на момент постановки подписи (не аннулирован и не отозван). В зависимости от услуг, предоставляемых Удостоверяющим Центром, данная информация может быть предоставлена в режиме онлайн (OCSP протокол), либо путем проверки в

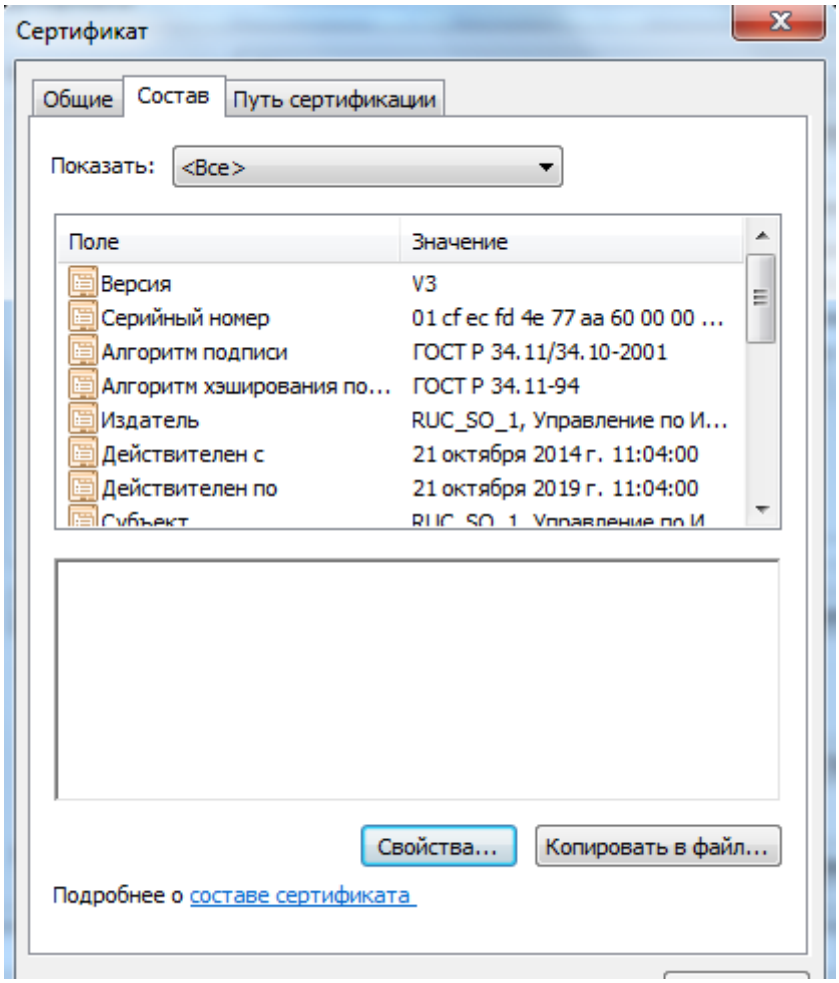
актуальном списке отзыва сертификатов (CRL). Более точную информацию необходимо получить в Удостоверяющем Центре, выпустившем квалифицированный электронный сертификат физического лица, должностного лица организации или доверенного лица.

Уточните в Удостоверяющем Центре, содержит ли ваш сертификат ссылку на OCSP сервер. В случае, если сертификат такой информации не содержит, но проверка статуса сертификата осуществляется по OCSP протоколу, ссылку необходимо указать в свойствах корневого сертификата Удостоверяющего Центра. Для этого необходимо произвести следующие действия на Вашем компьютере:

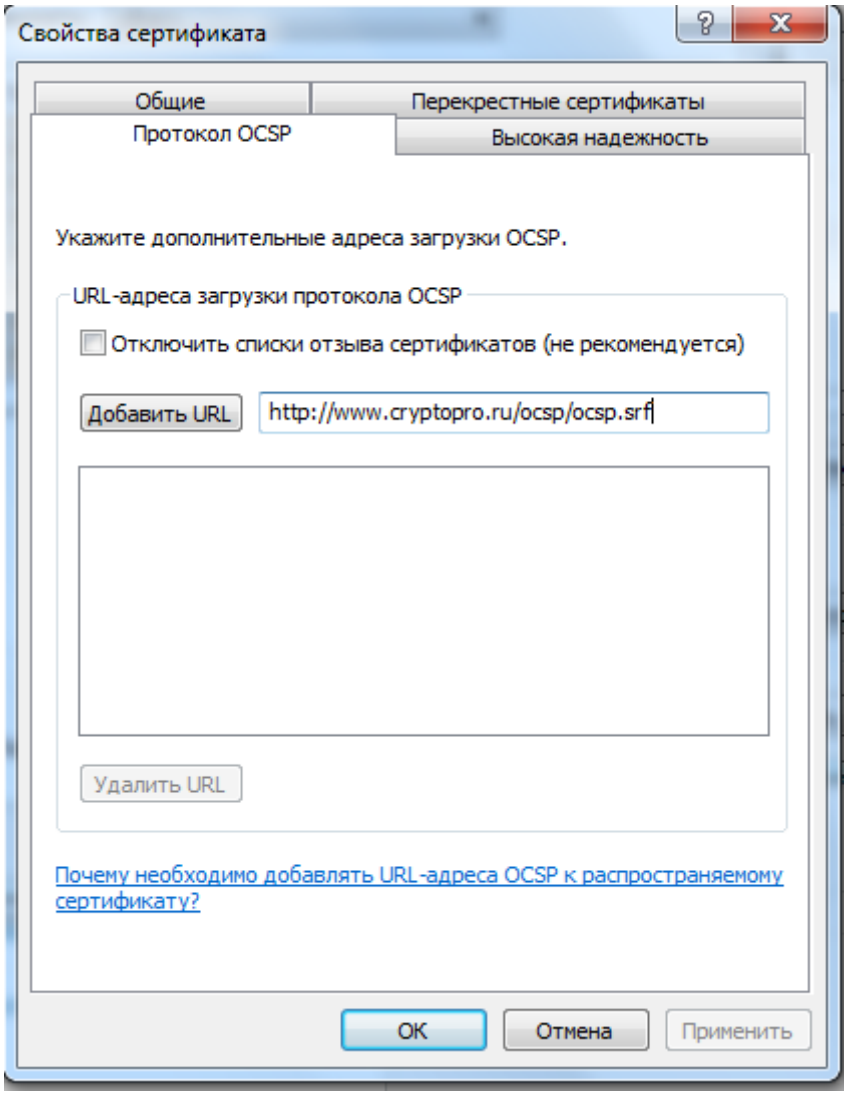
1. Откройте Ваш браузер и перейдите в настройки (для IE- Свойства браузера)
2. В настройках браузера перейдите в раздел «Настройка сертификатов» (для IE – Свойства браузера – Содержание – Сертификаты)
3. В консоли просмотра сертификатов перейдите на вкладку «Доверенные центры сертификации» и найдите установленный корневой сертификат вашего Удостоверяющего Центра



4. Нажмите кнопку «Просмотр». В открывшемся окне выберите вкладку «Состав». На вкладке «Состав» нажмите кнопку «Свойства…»



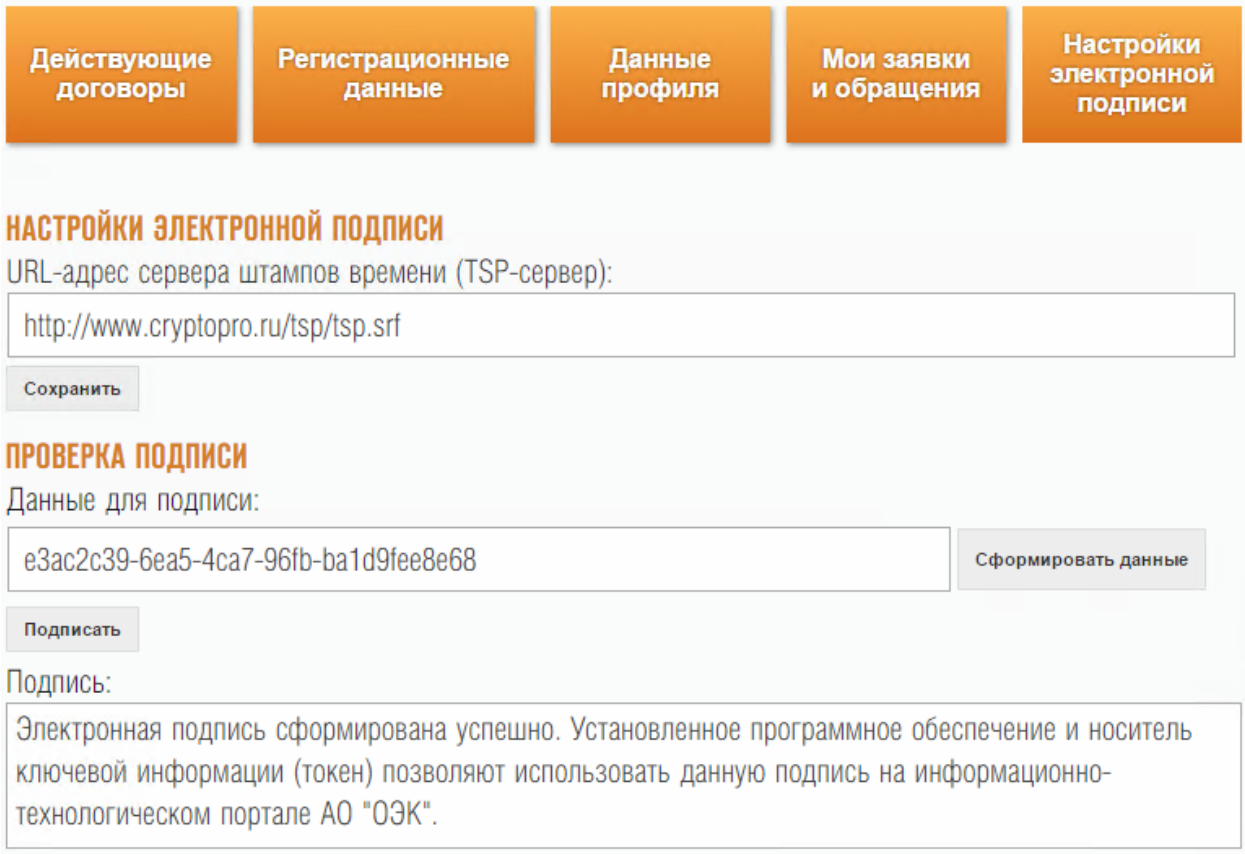
5. В открывшемся окне перейдите на вкладку «Протокол OCSP» и введите ссылку в текстовое поле.



6. Нажмите кнопку «Добавить URL» и сохраните изменения («Применить»).

6.3 Проверка установленного программного обеспечения и носителя ключевой информации на возможность подписания заявок и использования в электронном документообороте на информационно-технологическом портале АО «ОЭК».

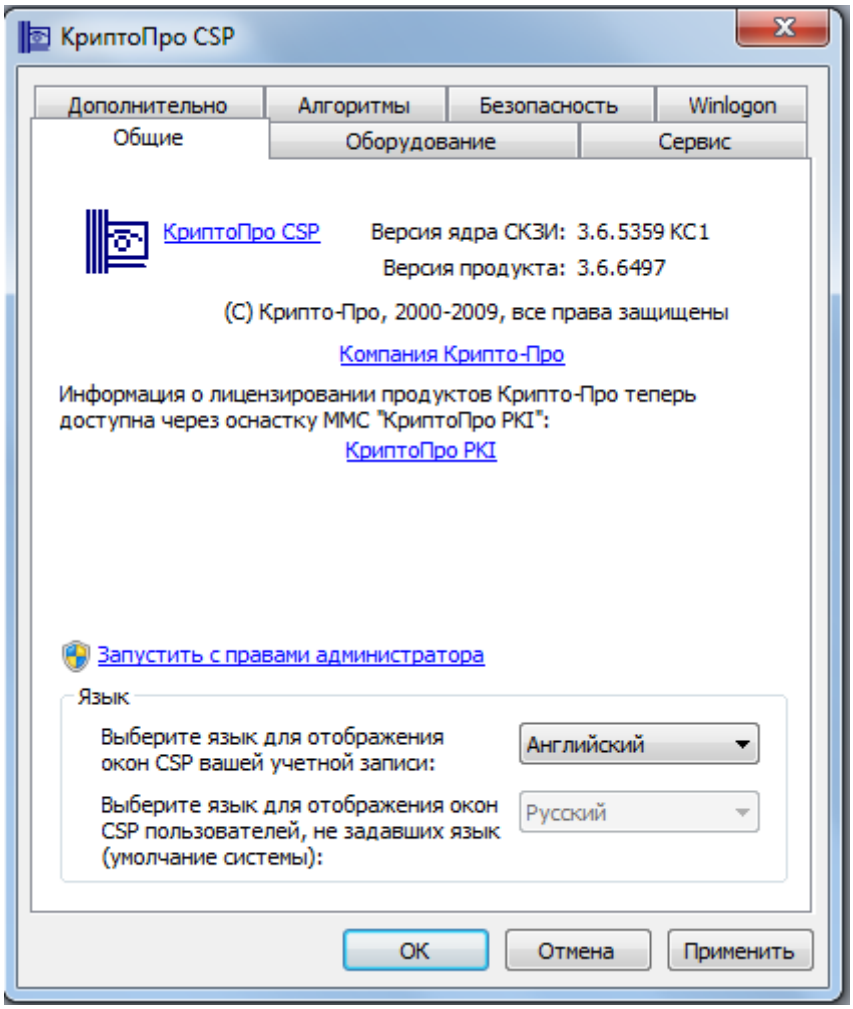
В Личном кабинете клиента на вкладке «Настройки электронной подписи» можно проверить, правильно ли настроено рабочее место, установлено необходимое программное обеспечение и выполнены все настройки. Для проверки используется подписание случайного набора цифр и букв. Если все установлено верно, пользователь получит информацию об успешном тестовом подписании.



В случае, если проверка подписи информирует об ошибках, или невозможно выбрать сертификат для подписания, необходимо перепроверить все настройки согласно нижеследующего листа проверок.

1. Работа PKI клиента. В зависимости от установленного драйвера носителя ключевой информации (п 4.2) на компьютер пользователя устанавливается PKI клиент - КриптоПро PKI Client, eToken PKI client и т.д. В момент постановки подписи PKI клиент должен быть включен, о чем информирует иконка приложения в трее Windows.

2. Носитель ключевой информации. Носитель ключевой информации должен быть доступен для установленного СКЗИ. Чтобы проверить доступность носителя ключевой информации необходимо запустить окно СКЗИ. Например, если установлен КриптоПРО CSP, необходимо запустить программу КриптоПро CSP.



В окне программы СКЗИ необходимо перейти к носителю ключевой информации согласно руководства на СКЗИ. Например, в случае СКЗИ КриптоПро CSP, необходимо перейти на вкладку **«Сервис» - «Просмотреть сертификаты в контейнере…» - «Обзор».** В открывшемся окне должен быть виден ваш носитель ключевой информации. В случае если окно пустое или носитель ключевой информации не виден в данном окне, возможно установлен неверный СКЗИ, или на компьютере были ошибки установки. Уточните в Удостоверяющем Центре, для какого СКЗИ предназначен ваш носитель ключевой информации. Кроме этого, многие Удостоверяющие Центры предоставляют услугу установки СКЗИ на компьютер пользователя и имеет смысл воспользоваться данной услугой.

3. Установка личных и корневых сертификатов. Для проверки правильности установки личных и корневых сертификатов необходимо произвести следующие действия:
    a. Откройте Ваш браузер и перейдите в настройки (для IE- **Свойства браузера**)

b. В настройках браузера перейдите в раздел «Настройка сертификатов» (для IE – **Свойства браузера – Содержание – Сертификаты**)

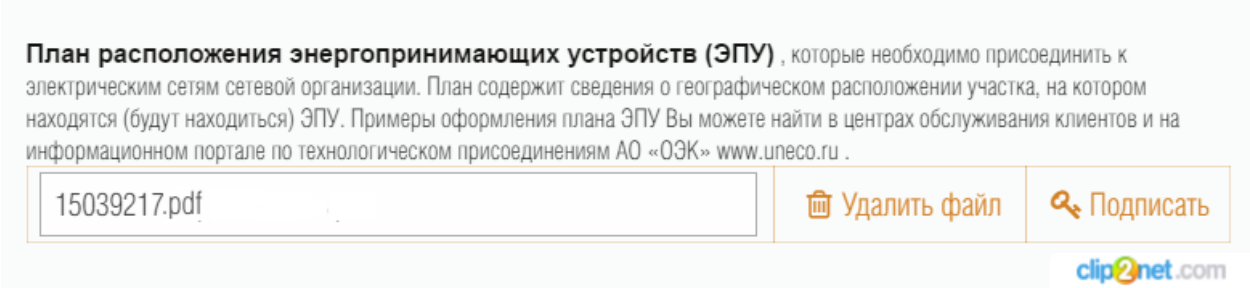
c. В консоли просмотра сертификатов перейдите на вкладку «Личные» и найдите установленный личный сертификат физического лица, доверенного лица, руководителя организации или специального должностного лица, ответственного за работу с личным кабинетом. В случае отсутствия личного сертификата в списке, сертификат был не установлен или установлен неверно. Выполните установку личного сертификата согласно п 4.3. Если личный сертификат есть в списке, откройте его свойства, дважды щелкнув на нем мышкой и перейдите на вкладку «**Пути сертификации**». На данной вкладке должно отобразиться как минимум 2 сертификата: ваш личный сертификат и уровнем выше – корневой сертификат Удостоверяющего центра. Если щелкнуть мышью на каждом отображенном сертификате, в строке «Состояние сертификата» должна быть надпись «Этот сертификат действителен». В случае, если на вкладке «Пути сертификации» отображается всего один сертификат, то на компьютер не был установлен или был установлен неверно корневой сертификат Удостоверяющего центра. Произведите установку корневого сертификата Удостоверяющего Центра, как описано в п. 4.4. данного руководства.

4. Сервер штампов времени и списки отзыва сертификатов. Убедитесь, что вы сохранили ссылку на сервер штампов времени, предоставленную Удостоверяющим Центром, нажав кнопку «Сохранить» повторно, как описано в п. 6.1. Убедитесь также, что доступны списки отзыва сертификатов, как описано в п 4.6 и 6.2 данного руководства. Предварительно уточните в Удостоверяющем центре какой способ проверки отзыва сертификатов поддерживает ваш сертификат – через загрузку CRL или через ссылку на OCSP сервер.
5. Лицензии. Убедитесь, что все установленное программное обеспечение имеет действующие лицензии, как описано в разделе 5 данного руководства.
6. Для корректной работы функционала предоставления информации о подписях при документообороте на информационно-технологическом портале АО «ОЭК» на компьютере пользователя должны быть установлены корневой сертификат Головного Удостоверяющего Центра Министерства связи и коммуникаций Российской Федерации, корневой сертификат УЦ 1 ИС ГУЦ и корневые сертификаты Национального Удостоверяющего центра, как описано в разделе 4.7 настоящего руководства.

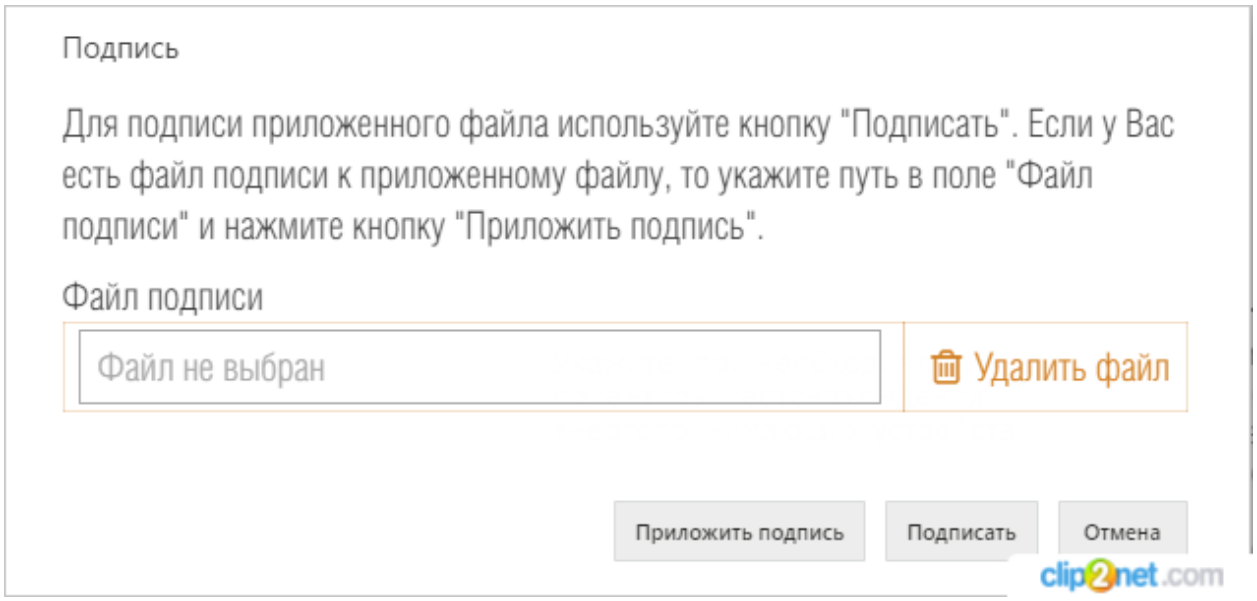
7 ИСПОЛЬЗОВАНИЕ ЭП В ЛИЧНОМ КАБИНЕТЕ

Для осуществления подписания данных формы заявки на технологическое подключение пользователю необходимо:

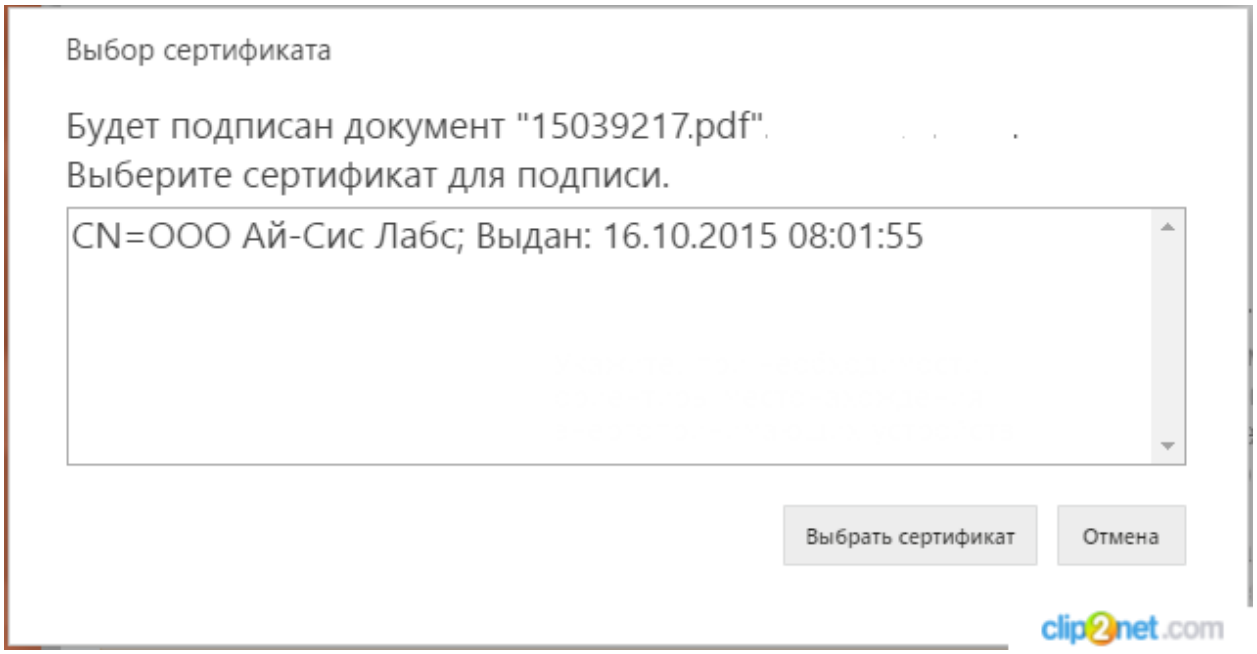
1. Осуществить заполнение формы заявки
2. Внести требуемые вложения
3. Подписать все добавленные вложения электронно-цифровой подписью, используя кнопку «Подписать»



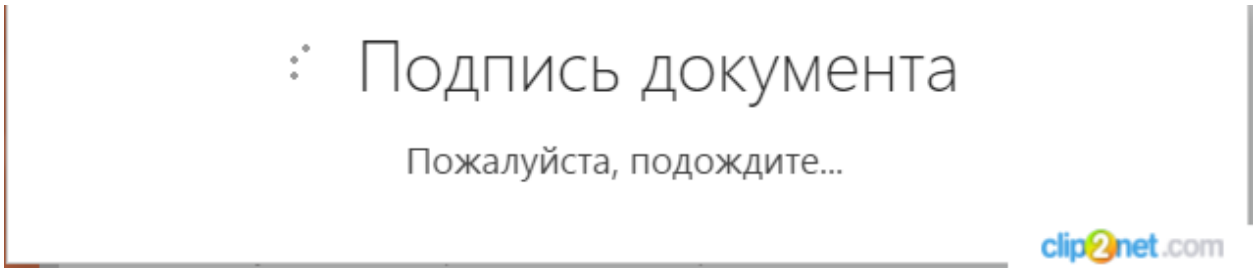
3.1. После клика на кнопку в окне «Подпись» выберите способ подписания – подписать на портале, или приложить сторонний файл подписи.



3.2. В случае, если выбран способ подписания на портале кнопкой «Подписать», появится окно выбора сертификата для подписи.



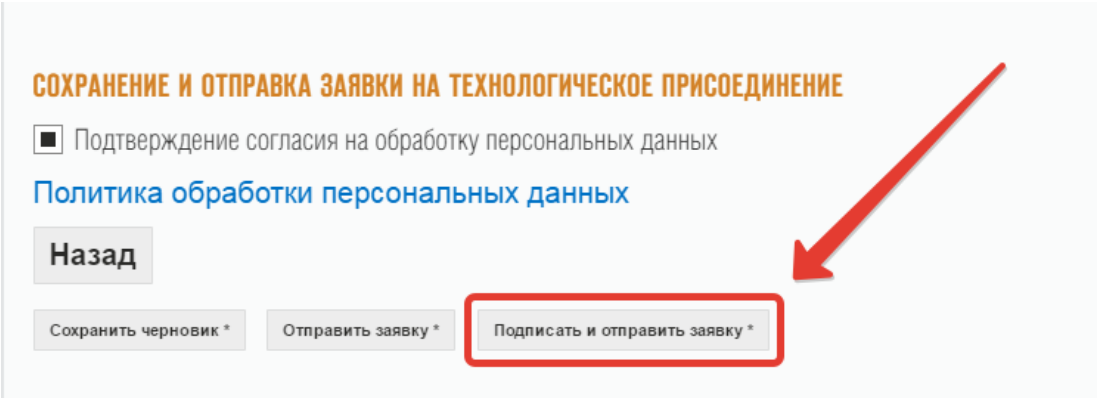
3.3. После выбора сертификата появится уведомляющее окно о постановке подписи



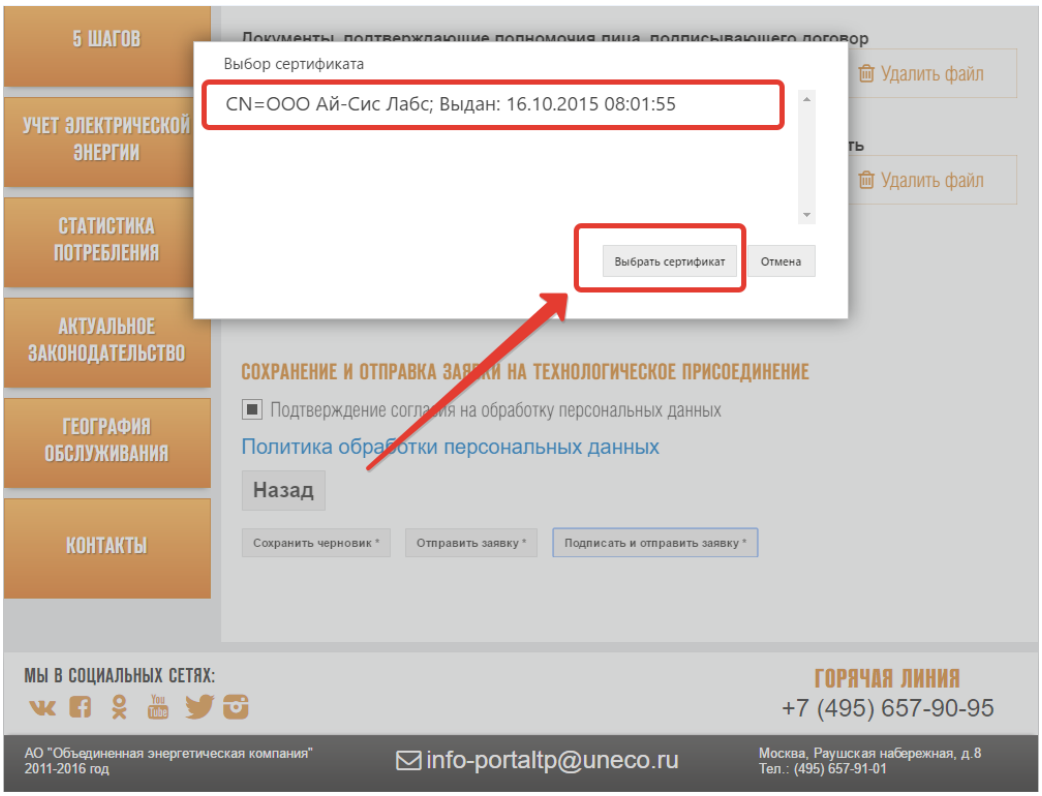
3.4. После завершения подписи пользователь будет проинформирован о подписанном документе и сертификате, используемом для подписи.

3.5. Вышеописанный процесс подписания приложений к заявке необходимо повторить для всех приложенных документов

4. Нажать клавишу «Подписать и отправить заявку»



4.1. В открывшемся окне осуществить выбор сертификата путем выделения нужной строки и нажать «Выбрать сертификат»



4.2. После выбора сертификата происходит процесс подписания заявки и отправки в учетную систему.