Настройка программного обеспечения для работы в подсистеме «Личный кабинет КАУ «АлтайРЦЦС»

Внимание! Данные настройки необходимо применять в случае подписания электронной документации специализированными программами (КриптоАРМ, Cryptcp и др.), не используя для этого функционал вэб-сервиса ЛК КАУ «АлтайРЦЦС». Достаточным условием для работы с функционалом вэб-сервиса являются системные требования из пункта 1, в части операционной системы и браузера.

1. Системные требования

К компьютеру, на котором планируется работать с системой Личный кабинет, предъявляются следующие требования:

Операционная система	• Microsoft Windows XP SP3 • Microsoft Windows Vista / 7 / 8 / 8.1 / 10 • Linux
Браузер	• Google Chrome • Mozilla Firefox • Opera версии 15 и выше • Яндекс.Браузер • Internet Explorer версии 10 и выше
Прочее	• Криптопровайдер «КриптоПро CSP» версии 3.6R4 и выше или «VIPNet CSP» версии 4.0 и выше • ПО «КриптоПро ЭЦП Browser Plug-in» версии 2.0 и выше

2. Порядок установки программного обеспечения

Для установки программного обеспечения пользователь должен обладать правами локального администратора на компьютере.

2.1. Криптопровайдер

Криптопровайдер предназначен для интеграции криптографических функций, посредством которых осуществляется работа с электронной подписью, в клиентское приложение. Поддерживаются – КриптоПро CSP и VIPNet CSP.

Как правило, процесс установки не вызывает сложностей и не требует специфических настроек. При установке и настройке криптопровайдера необходимо следовать инструкциям, предоставленным Удостоверяющим центром. По завершению установки криптопровайдера в случае необходимости перезагрузки компьютера, о которой уведомит мастер установки, необходимо произвести перезагрузку до установки второго пакета.

2.2. ПО «КриптоПро ЭЦП Browser plug-in»

ПО «КриптоПро ЭЦП Browser plug-in» предназначено для создания и проверки электронной подписи в веб-браузерах. Программа необходима независимо от того, какой криптопровайдер используется: КриптоПро CSP или ViPNet CSP. Поставляется бесплатно.

Чтобы установить КриптоПро ЭЦП Browser plug-in:

1. Скачайте программу установки с официального сайта приложения: http://www.cryptopro.ru/products/cades/plugin/get_2_0
2. Запустите файл установки.
3. Дождитесь окончания установки и перезапустите браузер.

3. Настройка программного обеспечения

3.1 Настройка КриптоПро ЭЦП Browser plug-in

Для того, чтобы при работе с сертификатами каждый раз не запрашивались разрешения на доступ, рекомендуется добавить адрес системы Личный кабинет в список надежных узлов приложения. Для этого:

1. Откройте Настройки ЭЦП Browser plug-in (Если используется ОС Windows 7 и ниже, это можно сделать, последовательно выбрав пункты меню **Пуск** => **Крипто-Про** => **Настройки ЭЦП Browser plug-in**).

2. В поле «**Добавить новый»** введите значение **https://personal.rccs22.ru** и последовательно нажмите на кнопки **[+]** и «**Сохранить»**:

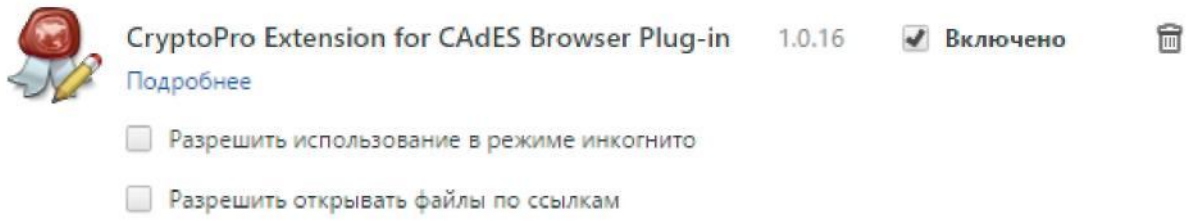
3.2 Настройка Google Chrome

После установки КриптоПро ЭЦП Browser plug-in (согласно пункту 2.2 данной инструкции) перезапустите браузер идождитесь оповещения об установленном расширении «CryptoPro Extension for CAdES Browser Plug-in». Включите это расширение.

Если оповещение об установке не появилось, пройдите по следующей ссылке и установите расширение вручную:

https://chrome.google.com/webstore/detail/cryptopro-extension-for-c/iifchhfnnmpdbibifmljnfjhpififfog

Вы можете убедиться, что расширение включено, воспользовавшись пунктом меню **Расширения**:



3.3 Настройка Mozilla Firefox

3.3.1 Mozilla Firefox версии 52.0 и старше

После установки КриптоПро ЭЦП Browser plug-in (согласно пункту 2.2 данной инструкции) перезапустите браузер и пройдите по следующей ссылке:

https://www.cryptopro.ru/sites/default/files/products/cades/extensions/firefox_cryptopro_extension_latest.xpi

На запрос об установке расширения – ответить утвердительно.

3.3.2. Mozilla Firefox до версии 52.0

Необходимо выполнить следующие настройки:

1. Откройте окно «Управление дополнениями», воспользовавшись кнопкой «**Дополнения»** в меню браузера.
2. В левой части открывшегося окна выберите раздел «**Плагины»**.
3. В списке установленных плагинов найдите элемент с именем «**CryptoPro CAdeS NPAPI Browser Plug-in»** и в выпадающем списке его настроек установите значение «**Всегда включать»**:

3.4 Настройка Internet Explorer 10 и старше

Данный браузер не требует обязательной дополнительной настройки, однако при первой попытке выполнения подписи – заблокирует данную возможность, выводя серию предупреждений в нижней части окна браузера с вопросами на разрешение. Для продолжения работы следует разрешить браузеру выполнять запрошенные действия.

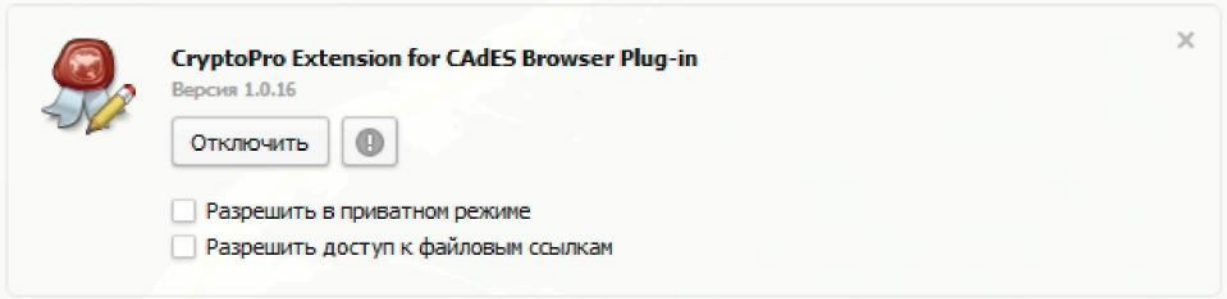
3.5 Настройка Opera / Яндекс.Браузер

После установки КриптоПро ЭЦП Browser plug-in (согласно пункту 2.2 данной инструкции) перезапустите браузер и дождитесь оповещения об установленном расширении «CryptoPro Extension for CAdES Browser Plug-in». Включите это расширение.

Если оповещение об установке не появилось, пройдите по следующей ссылке и установите расширение вручную:

https://addons.opera.com/en/extensions/details/cryptopro-extension-for-cades-browser-plug-in

Вы можете убедиться, что расширение включено, воспользовавшись пунктом меню **Расширения => Менеджер расширений**:



4. Установка сертификатов

Для создания электронной подписи корневой сертификат Удостоверяющего центра и личный сертификат пользователя должны быть установлены в хранилище сертификатов операционной системы. Данные сертификаты и носитель закрытого ключа выдаются аккредитованным Удостоверяющим центром и, как правило, снабжаются инструкциями по их установке или программным обеспечением, выполняющим автоматическую установку. При возникновении трудностей с установкой сертификатов, в первую очередь обратитесь в Удостоверяющий центр, выдавший Вам сертификаты, и лишь затем - к следующим инструкциям.

4.1 Установка личного сертификата

4.1.1. Установка личного сертификата из файла, с использованием ПО «КриптоПРО CSP»

Данный вариант следует использовать, если личный сертификат выдан Вам в виде отдельного файла с расширением .cer или .crt

1. Запустите КриптоПро: **Пуск** => **Все программы** => **КРИПТО-ПРО** => **КриптоПро CSP** или воспользуйтесь одноименным пунктом «**КриптоПро CSP**» в Панели управления Windows.

2. В появившемся окне приложения выберите вкладку «**Сервис**» и нажмите кнопку «**Установить личный сертификат**».

3. Укажите расположение файла сертификата (файл с расширением .cer, или .crt, выданный Удостоверяющим центром), нажмите кнопку «**Далее**».

4. Окно просмотра свойств сертификата позволяет убедиться, что выбран правильный сертификат. Если все верно, переходите к следующему шагу.

5. В следующем окне необходимо задать ключевой контейнер, содержащий в себе закрытые ключи пользователя. Допускаются только съемные USB-носители, смарт-карты и реестр ОС**.** Установите флажок «**Найти контейнер автоматически»**. Если контейнер не находится автоматически, выберите его вручную с помощью кнопки «**Обзор»**. После выбора переходите к следующему шагу.

7. В диалоге выбора хранилища сертификатов выберите параметр «**Личное»** и установите флажок «**Установить сертификат в контейнер»**.

8. В окне «Завершение работы мастера установки личного сертификата» проверьте параметры установки и нажмите на кнопку «**Готово»**.

4.1.2. Установка личного сертификата из контейнера закрытого ключа, с использованием ПО «КриптоПРО CSP»

Данный вариант следует использовать, если личный сертификат, выданный Удостоверяющим центром, установлен в контейнер закрытого ключа.

1. Убедитесь, что съемный носитель с закрытым ключом подключен к компьютеру (или ключ установлен в реестре).

2. Запустите программу КриптоПро CSP.

3. Перейдите на вкладку «**Сервис»**, нажмите на кнопку «**Просмотреть сертификаты в контейнере»**.

4. В окне с выбором контейнера для просмотра убедитесь, что в поле «**Введенное имя задает ключевой контейнер»** выбран пункт «**Пользователя»** и нажмите на кнопку «**Обзор»**.

5. Выберите контейнер на съемном носителе либо в реестре, в зависимости от того, где он установлен, и нажмите на кнопку «**ОК»**.

6. В окне «Контейнер закрытого ключа» нажмите на кнопку «**Далее»**.

7. В окне «Сертификат для просмотра» нажмите на кнопку «**Установить»**.

8. Нажмите на кнопку «**Готово»**.

4.2 Установка корневого сертификата Удостоверяющего центра

В случае, если корневой сертификат Удостоверяющего центра отсутствует на компьютере, необходимо выполнить его установку:

1. Найдите выданный Вам Удостоверяющим центром файл, содержащий корневой сертификат данного центра, и по клику правой кнопкой мыши на нем в

выпадающем меню выберите пункт «**Установить сертификат»**. В открывшемся окне мастера установки сертификатов нажмите «**Далее»**.

2. На данном этапе выберите пункт «**Поместить все сертификаты в следующее хранилище**» и нажмите на кнопку «**Обзор»**.

3. В открывшемся окне «Выбор хранилища сертификата» укажите в качестве хранилища «**Доверенные корневые центры сертификации**».

4. По окончании выбора нажмите на кнопку «**Далее»**. Следующее окно содержит суммарную информацию, нажатие кнопки «**Готово»** приведет к установке сертификата в выбранное хранилище. При этом может появиться диалоговое окно, в котором необходимо подтвердить доверие к данному сертификату.

5. Решение вопросов с неработоспособностью функций создания подписи

Примечание. Дополнительно проверить работоспособность подсистемы подписи Вы можете на демонстрационной странице официального сайта плагина КриптоПро: https://www.cryptopro.ru/sites/default/files/products/cades/demopage/simple.html

5.1. Сообщение «*Ошибка инициализации плагина КриптоПро ЭЦП: Плагин недоступен*» или «*Ошибка инициализации плагина КриптоПро ЭЦП: Истекло время ожидания загрузки плагина*»

Возможны следующие варианты:

1. Приложение «КриптоПро ЭЦП Browser plug-in» не установлено. Проведите установку согласно пункту **2.2** данной инструкции.

2. В браузерах Google Chrome, Яндекс.Браузер, Opera или Firefox 52+ не установлено или отключено расширение, специфическое для данных браузеров. Проведите установку расширения вручную согласно пунктам **3.2** / **3.5 / 3.3.1** данной инструкции и убедитесь, что расширение для браузера «CryptoPro Extension for CAdES Browser Plug-in» установлено и включено.

5.2 Сообщение «*Ошибка инициализации плагина КриптоПро ЭЦП: Плагин загружен, но не создаются объекты*»

Данное сообщение может появиться только при использовании браузера Mozilla Firefox до версии 52.0, и свидетельствует об отключенном расширении браузера «CryptoPro CAdES NPAPI Browser Plug-in». Включите расширение, согласно пункту **3.3.2** данной инструкции.

5.3 Сообщение «*Действительных сертификатов со ссылкой на закрытый ключ найдено: 0*» или в списке выбора сертификатов отсутствует требуемый Вами сертификат.

Возможны следующие варианты:

1. Личный сертификат пользователя не установлен в хранилище сертификатов операционной системы. Чтобы установить личный сертификат, воспользуйтесь инструкциями, предоставленными Вам Удостоверяющим центром или пунктом **4.1** данной инструкции.

2. Личный сертификат пользователя установлен, однако не имеет проставленной ссылки на закрытый ключ. Воспользуйтесь инструкциями, предоставленными Вам Удостоверяющим центром или пунктом **4.1** данной инструкции.

3. Личный сертификат пользователя установлен со ссылкой на закрытый ключ, однако истек срок действия сертификата. Обратитесь в Удостоверяющий центр и получите новый сертификат подписи.

5.4 Сообщение *«Ошибка при создании подписи: Invalid algorithm specified: 0x80090008»*

Данное сообщение свидетельствует о том, что Вы пытаетесь выполнить подпись неквалифицированным сертификатом подписи, или установленные криптопровайдеры не поддерживают требуемый алгоритм подписи.

5.5 Сообщение *«Ошибка создания подписи: A certificate chain could not be built to a trusted root authority. (0x800B010A)»*

Данное сообщение возникает при отсутствии установленного в хранилище сертификатов операционной системы корневого сертификата Удостоверяющего центра, выдавшего личный сертификат, при помощи которого Вы пытаетесь подписать документ. Воспользуйтесь инструкциями, предоставленными Вам Удостоверяющим центром или пунктом **4.2** данной инструкции.

5.6 Сообщение *«Ошибка хэширования документа: Параметр задан неверно. (0x80070057)»*

Данная ошибка может возникнуть при недоступности криптопровайдера, поддерживающего требуемые алгоритмы подписи. Проверьте, установлен ли на

компьютере криптопровайдер (КриптоПро CSP или VIPNet CSP). Если не установлен – установите его, воспользовавшись инструкциями, предоставленными Вам Удостоверяющим центром или пунктом **2.1** данной инструкции. Если криптопровайдер установлен – убедитесь, что не истек срок действия его лицензии.

5.7 Сообщение *«Ошибка при создании подписи: Error calling method on NPObject!»*

Данное сообщение может возникнуть только при использовании браузера Mozilla Firefox до версии 52. К сожалению, данный браузер не имеет возможностей детализировать сведения о возникающих в процессе подписи ошибках, и на любую из возможных ошибок всегда возвращает одинаковое сообщение. Чтобы более точно диагностировать возникающую ошибку, воспользуйтесь другим браузером.