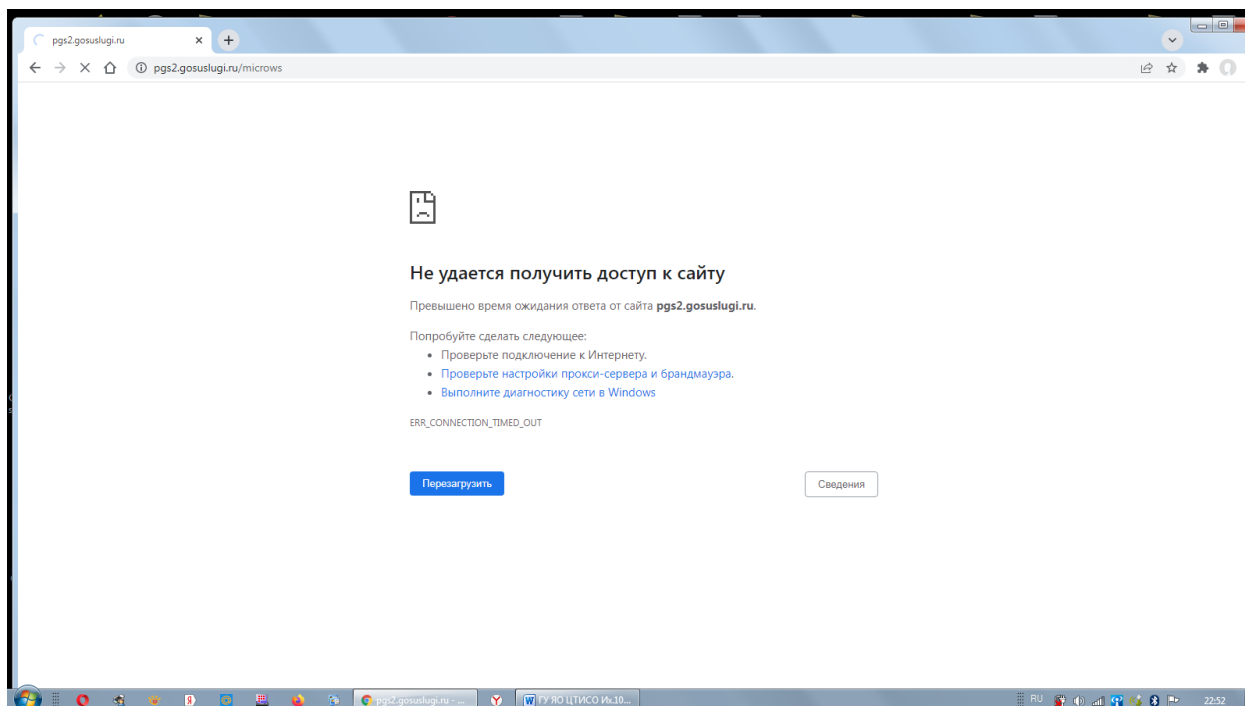


Содержание

Содержание	1
1. Не открывается страница https://pgs2.gosuslugi.ru/microws	2
2. Ошибка входа после авторизации	7
3. Не отображаются тестовые заявление	8
4. Отсутствует возможность обработки заявления	9
5. Проблемы при подписании заявления	10

1. Не открывается страница <https://pgs2.gosuslugi.ru/microws>



Необходимо проверить и сделать обязательные сетевые настройки рабочего места пользователя, а именно:

- Отредактировать файл **hosts**, добавить в него следующие строки:

172.16.90.16 pgs2.gosuslugi.ru sso-pgs2.gosuslugi.ru

192.168.33.166 pgs-datastore.pgss3.gosuslugi.ru

Файл hosts (Тип (расширение) должен быть Файл) является скрытым системным файлом, в операционной системе Windows размещается в папке C:\Windows\System32\drivers\etc

Для редактирования файла скопируйте его на рабочий стол, там по нему щелкните правой кнопкой мыши и откройте в программе Блокнот, а потом этот отредактированный файл переместите обратно в папку C:\Windows\System32\drivers\etc с заменой, нажав продолжить от имени Администратора.

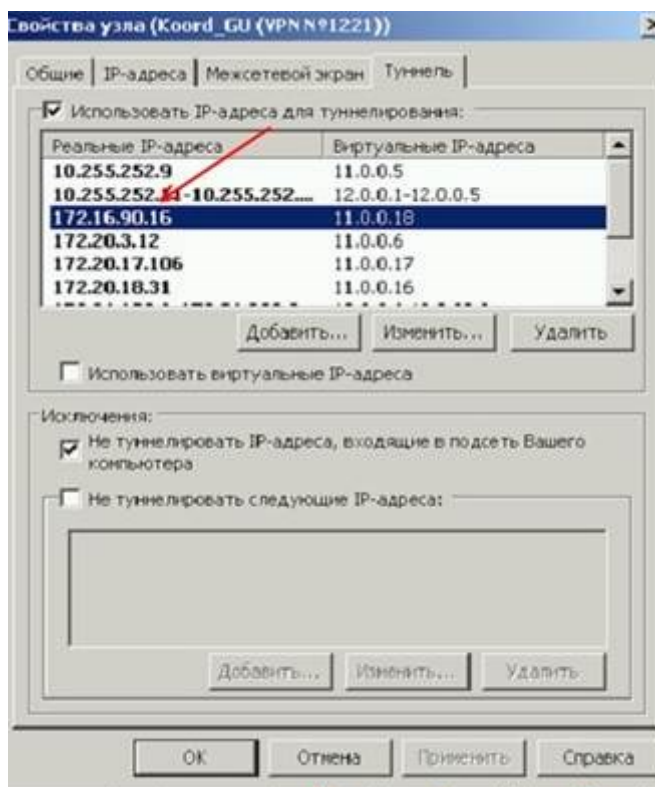
- Проверить настройки vpn-клиента, а именно сделать следующие шаги:

Запустить Vipnet Client (Monitor).

Открыть список доступных координаторов, по координатору Koord_GU щелкнуть дважды левой клавишей мыши.



В открывшемся окне перейти на вкладку «Туннель» и проверить наличие адресов в списке: 172.16.90.16 и 192.168.33.166



Если адреса отсутствуют – добавить их через кнопку «Добавить».

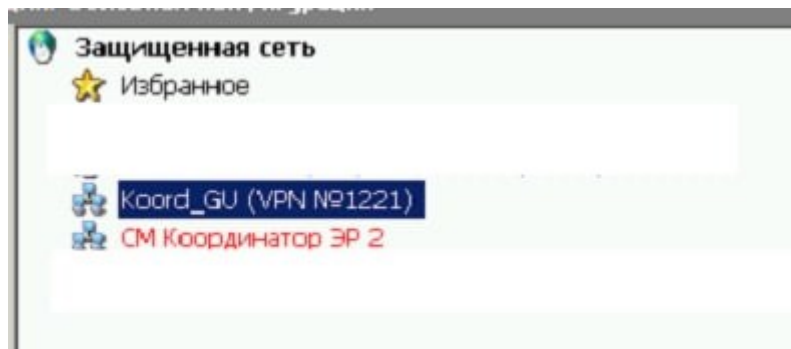
После добавления нажать ОК.

Если VipNet клиент версии 3 (устаревшая), то необходимо один раз перед входом в ПГС сделать следующее:

Открыть список доступных координаторов, выделить координатор Koord_GU и нажать F5 и должно в новом окне выдать сообщение «Доступен».

После этого вход должен заработать.

Но надо проверить еще настройки, указанные в следующем пункте.



- Если у Вас включен прокси, то добавить в исключение следующие адреса:
172.16.90.16; pgs2.gosuslugi.ru; sso-pgs2.gosuslugi.ru; 192.168.33.166; pgs-
datastore.pgss3.gosuslugi.ru

В браузере Internet Explorer: Сервис – Свойства браузера – Подключения – Настройки сети –
Дополнительно - Исключения

Свойства браузера

Общие Безопасность Конфиденциальность

Содержание Подключения Программы Дополнительно

 Для установки подключения компьютера к Интернету щелкните эту кнопку. Установить

Настройка коммутируемого соединения и виртуальных частных сетей

Добавить...

Добавить VPN...

Удалить...

Настройка

Щелкните кнопку "Настройка" для параметры прокси-сервера для этого подключения.

Настройка параметров локальной сети

Параметры локальной сети не применяются для подключений удаленного доступа. Для параметры коммутируемого соединения щелкните кнопку "Настройка", расположенную выше. Настройка сети

 Некоторыми параметрами управляет системный администратор.

OK Отмена Применить

Настройка параметров локальной сети

Автоматическая настройка

Чтобы использовать установленные вручную параметры, отключите автоматическую настройку.

☒ Автоматическое определение параметров

☐ Использовать сценарий автоматической настройки

Адрес:

Прокси-сервер

☒ Использовать прокси-сервер для локальных подключений (не применяется для коммутируемых или VPN-подключений).

Адрес: Порт: Дополнительно

☐ Не использовать прокси-сервер для локальных адресов

OK Отмена

Параметры прокси-сервера

Серверы

Тип	Адрес прокси-сервера	Порт
1. HTTP:		
2. Secure:		
3. FTP:		
4. Socks:		

☐ Один прокси-сервер для всех протоколов

Исключения

Не использовать прокси-сервер для адресов, начинающихся с:

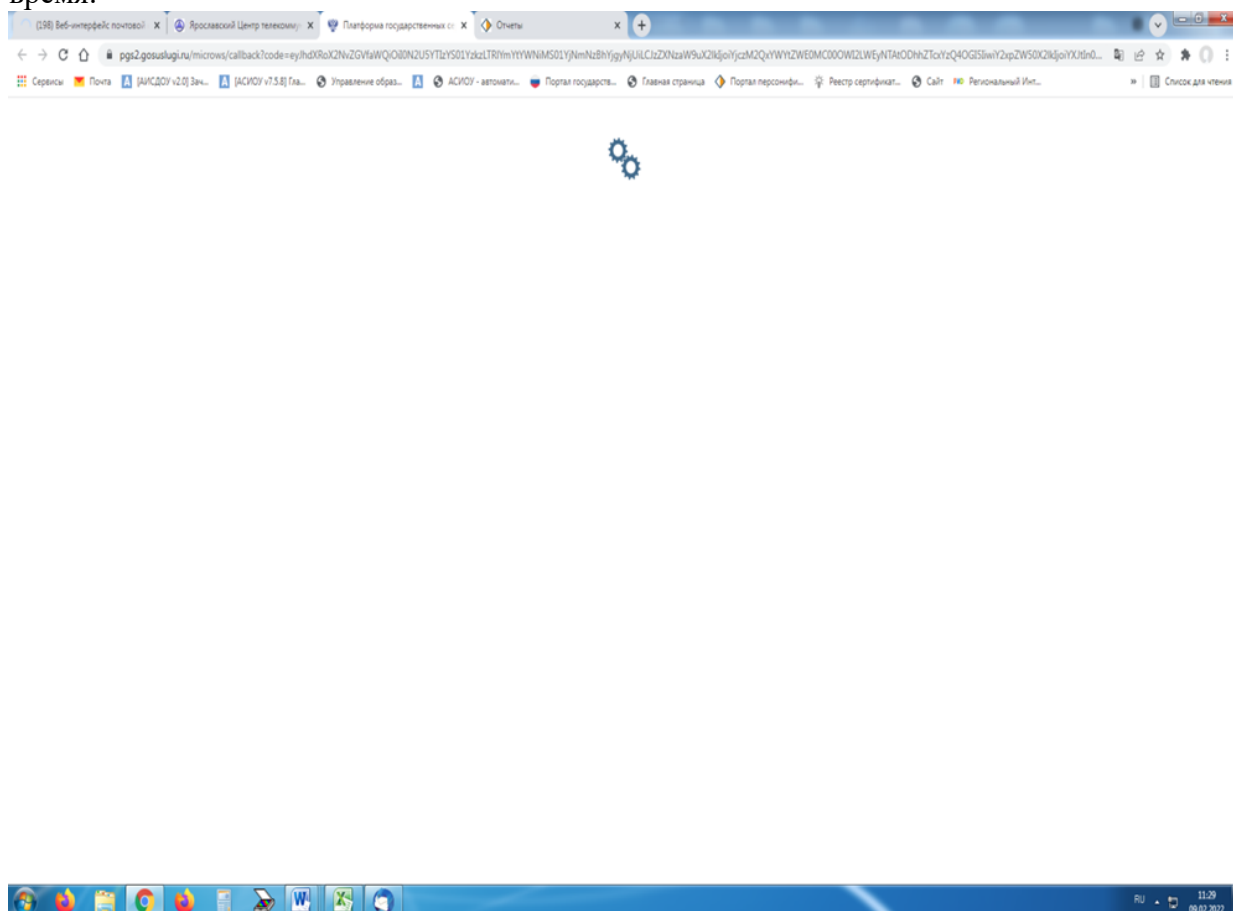
Адреса разделяются точкой с запятой (;).

OK Отмена

После добавления нажать ОК.

2. Ошибка входа после авторизации

Если после авторизации через ЕСИА происходит постоянная загрузка страницы (крутятся «бесконечные шестеренки»), то это означает, что на ПК некорректное время.



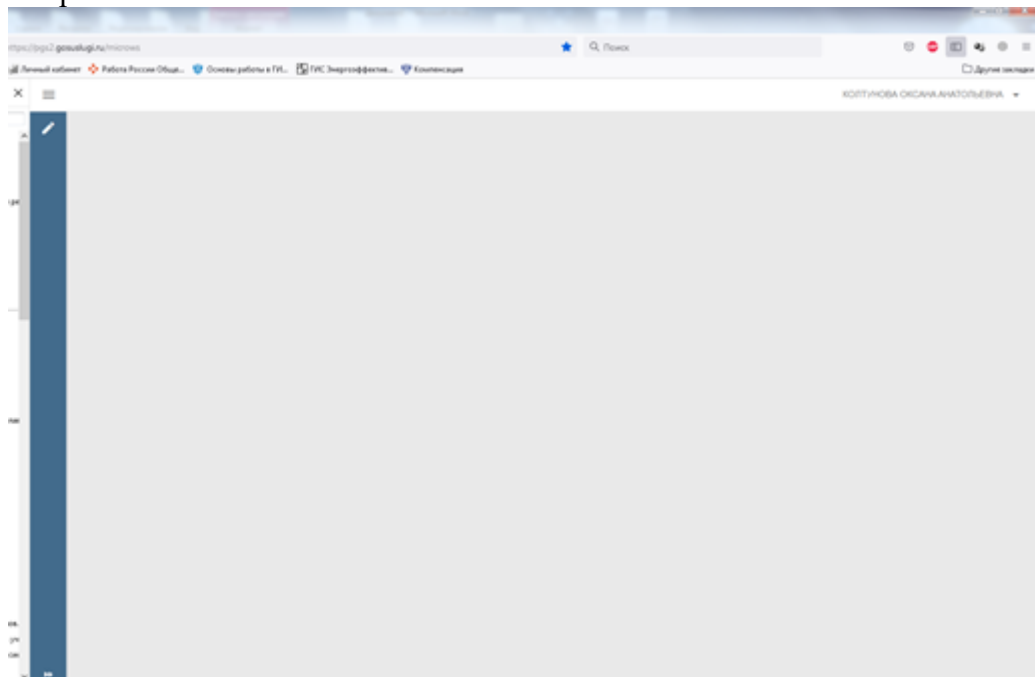
Необходимо настроить корректное времени на ПК, дата и время должно быть правильным вплоть до минуты, часовой пояс должен быть «+3» **обязательно**.

3. Не отображаются тестовые заявления

- Если заявления поданы раньше, чем выполнен первый вход в систему пользователями организации, то такие заявления могут не маршрутизироваться в системе.

Поэтому нужно будет подать заново заявления с ЕПГУ <https://www.gosuslugi.ru/600160/1/form>

- Так же все заявления должны отображаться на вкладке «Заявления», а не «Черновики заявлений».



Если у пользователя в личном кабинете отсутствует вкладка «Заявления», то это означает, что у него не настроены роли в ЕСИА согласно инструкции

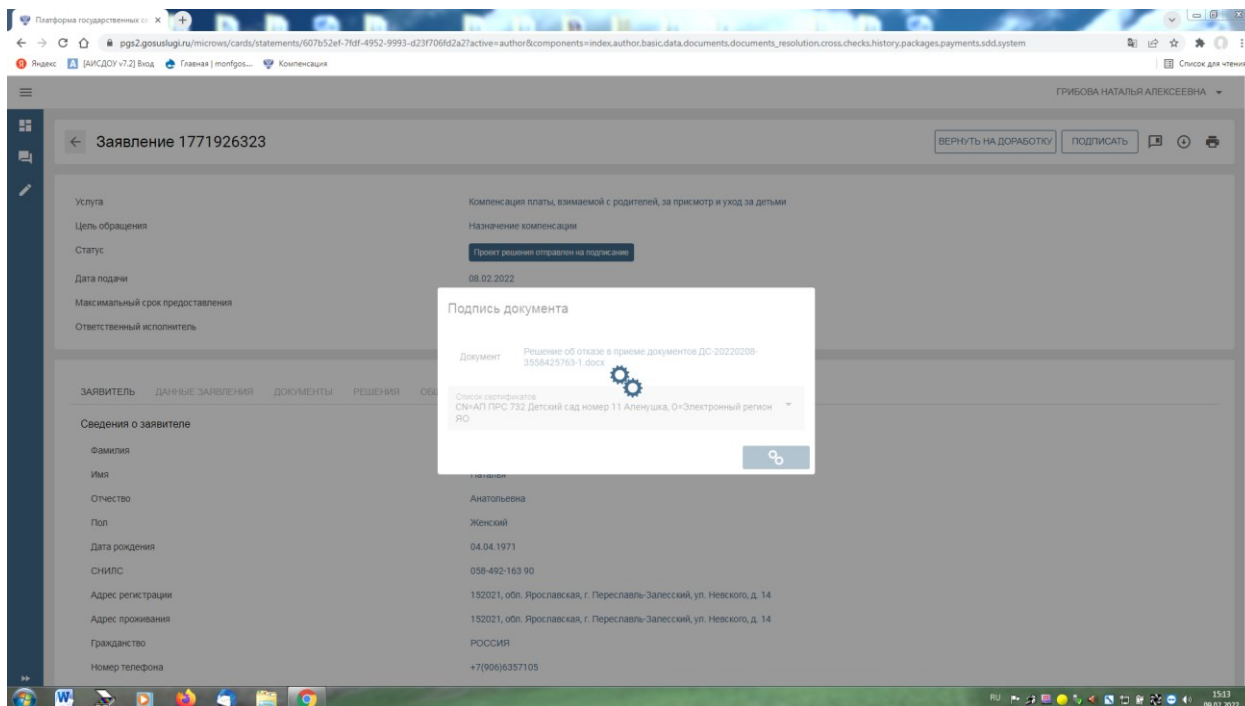
https://mv.er76.ru/content/files/pgs_add_empl_to_groups.pdf

4. Отсутствует возможность обработки заявления

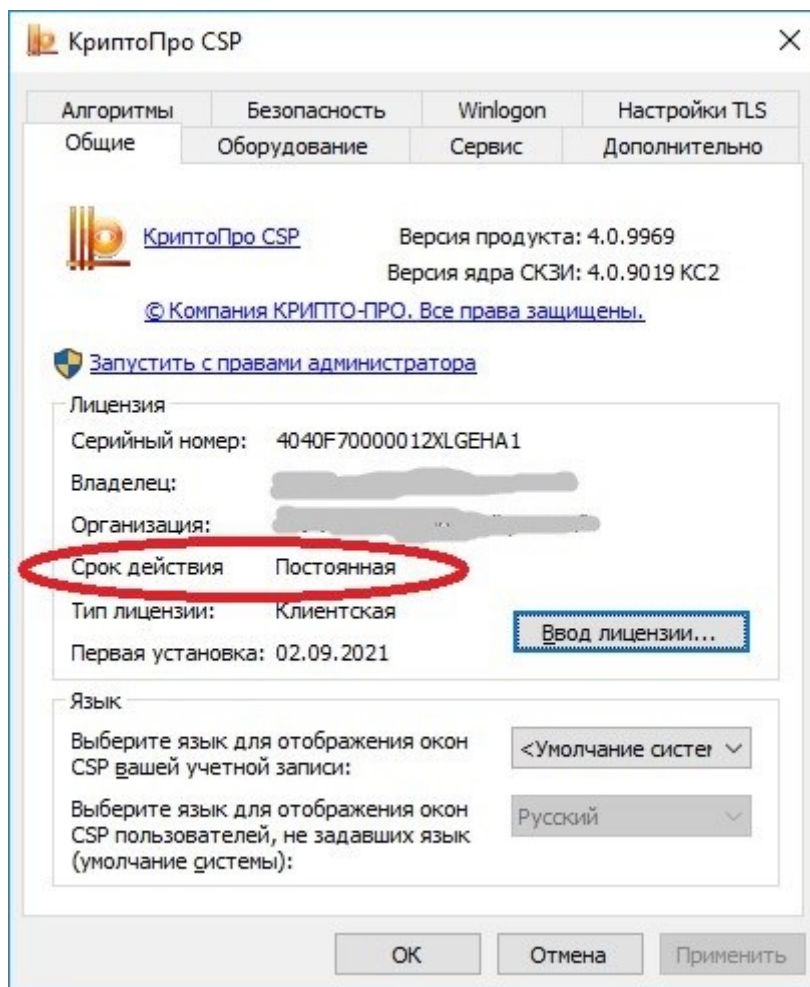
Если внутри заявления в правом верхнем углу отсутствуют кнопки обработки заявления – это означает, что у пользователя настроены не все роли для ПГС, необходимо добавить оставшиеся согласно инструкции

https://mv.er76.ru/content/files/pgs_add_empl_to_groups.pdf

5. Проблемы при подписании заявления



- Проверить сетевые настройки из первого [пункта](#)
- Для работы рекомендуется использовать web-браузеры:
 - Google Chrome версии 85 и выше;
 - Yandex Browser версии 20 и выше.
- Должны быть настроены криптопровайдер КриптоПро CSP, Cades плагин для web-браузера, сертификат ЭП:
 - Проверить актуальность срока действия лицензии Крипто Про CSP: Пуск - Крипто Про CSP



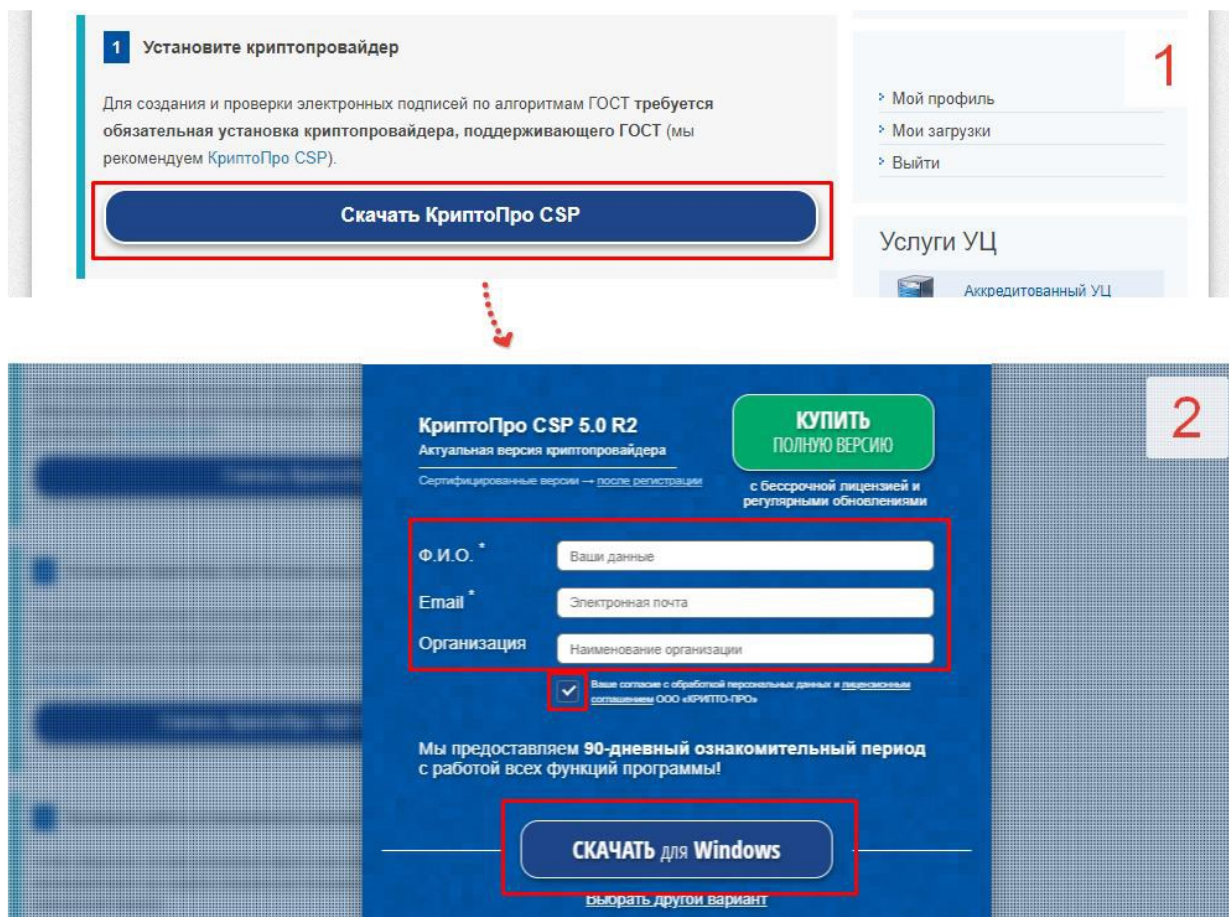
Если срок действия истек, то необходимо ввести действующую лицензию.

- Если на ПК отсутствует криптопровайдер КриптоПро CSP, то необходимо установить:

Установка криптопровайдера КриптоПро CSP версии 4.0. и выше происходит в соответствии с [инструкцией](#) (ссылка:

https://www.cryptopro.ru/sites/default/files/docs/instruction_manual_csp_r3.pdf)

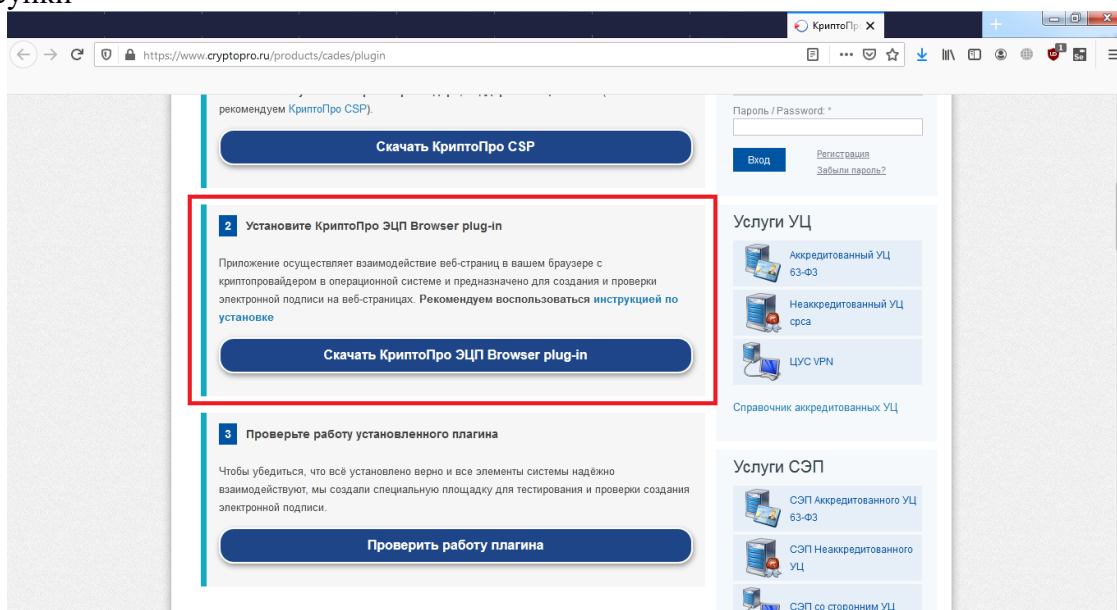
Переходим по ссылке <https://www.cryptopro.ru/products/cades/plugin>. На открывшейся странице нажимаем кнопку «Скачать КриптоПро CSP», заполняем открывшуюся форму и нажимаем кнопку «Загрузить для Windows», см. рисунок 1.



Установка Криптопровайдера

Запускаем установочный файл. В ходе инсталляции оставляем все параметры, предложенные мастером установки. Проходим установку, нажимая «Далее» на каждом шаге. По окончании установки может потребоваться перезагрузка системы/браузера.

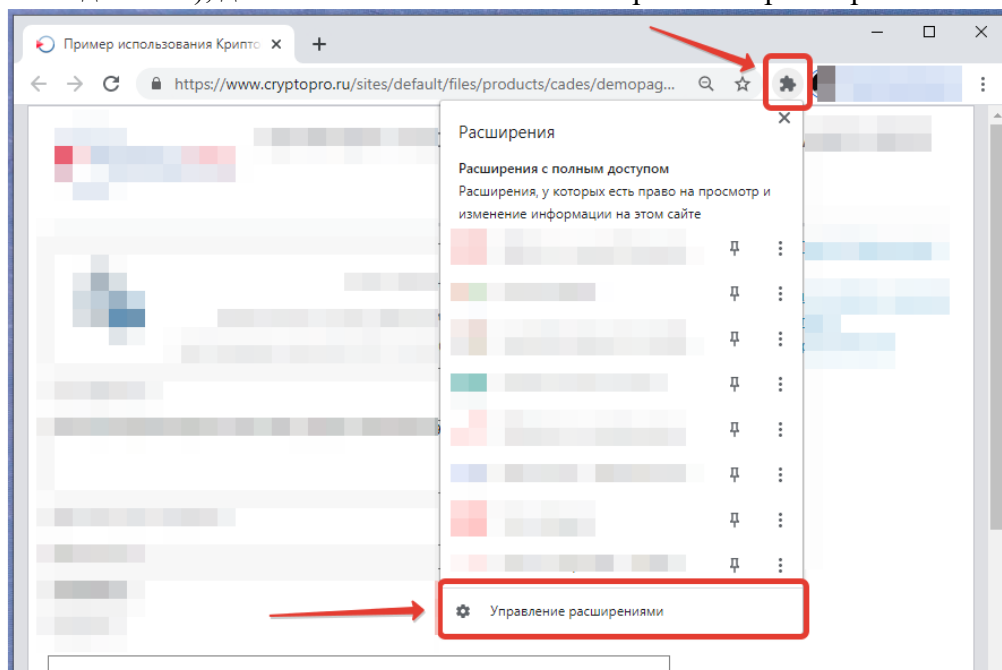
- Необходимо установить или обновить, если устаревшая версия Cades плагин для web-браузера с портала <https://www.cryptopro.ru/products/cades/plugin>, в соответствии с инструкцией по установке <http://docs.cryptopro.ru/plugin/plugin-installation-windows>, см. рисунки



Установка Cades плагин для web-браузера

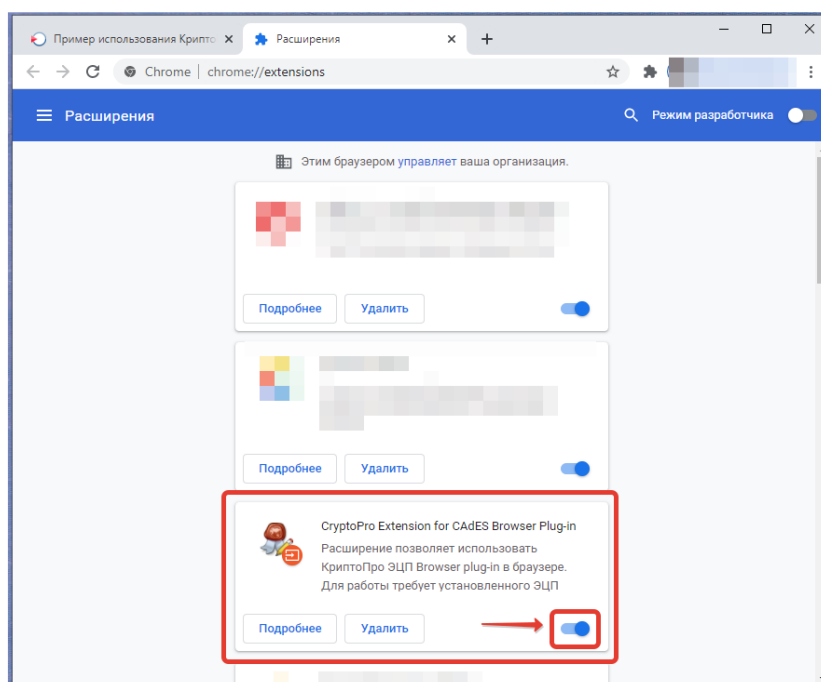
Обязательно: удаляем устаревшую версию Cades плагин, перезагружаем компьютер.

Запускаем установочный файл новой версии Cades плагин и производим установку. После окончания установки необходимо произвести перезапуск браузера. После перезапуска браузера необходимо перейти в настройки расширений в браузере и активировать установленный плагин. На примере браузера Google Chrome производятся следующие действия: В правом верхнем углу окна браузера нажимается кнопка «Расширения» (кнопка в виде пазла), далее нажимается кнопка «Управление расширениями».



Активация расширения

Откроется вкладка с установленными расширениями. После нахождения в списке установленных расширений плагина необходимо активировать его, переведя рычаг вправо.



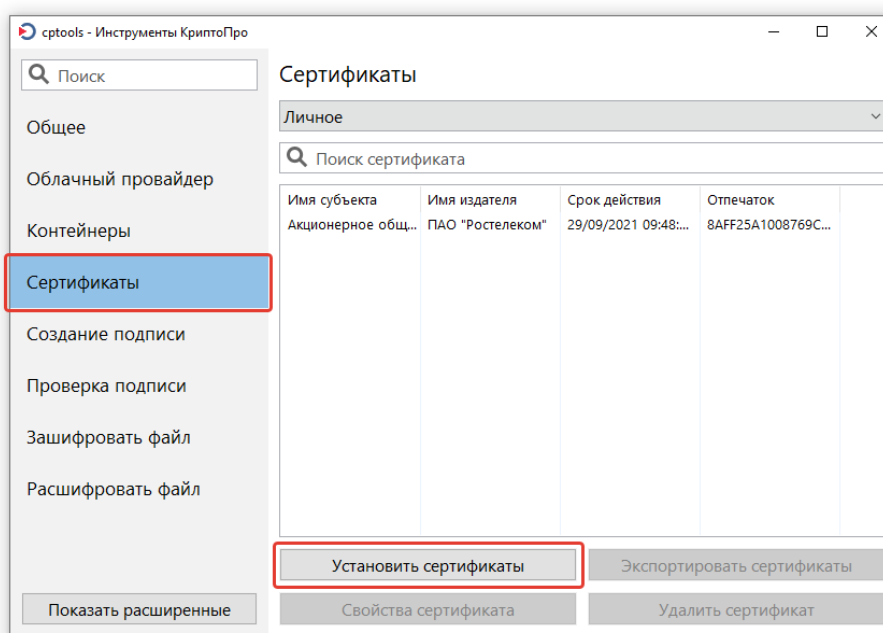
Активация расширения в браузере

После этого рекомендуется зайти в Панель управления – Программы и компоненты – встать на строку КриптоПро CSP и нажать на кнопку «Восстановить», перезагрузить компьютер.

Зайти в браузер в режиме «Инкогнито» или в «Приватном окне», в зависимости от браузера

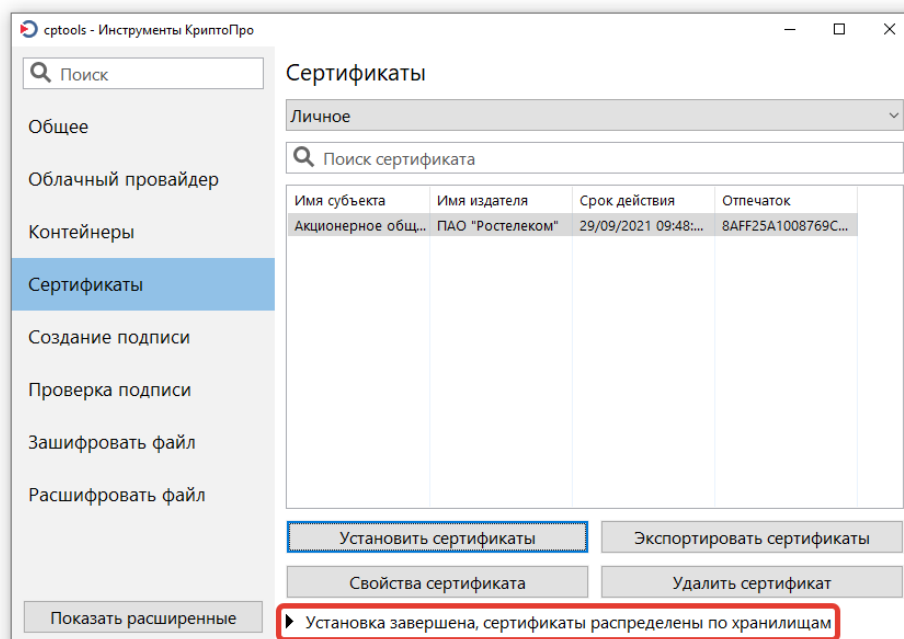
- Установка сертификата (.cer)

Переходим в меню «Пуск» и находим папку «КРИПТО-ПРО». Запускаем в папке приложение «Инструменты КриптоПро». Переходим в раздел «Сертификаты» и нажимаем кнопку «Установить сертификат», в открывшемся окне выбора файла, указываем файл с сертификатом сотрудника и нажимаем кнопку «Открыть».



Установка сертификата

Если установка сертификата прошла успешно, он появится в списке установленных сертификатов, а под кнопкой «Установить сертификат» появится сообщение: «Установка завершена, сертификаты распределены по хранилищам».



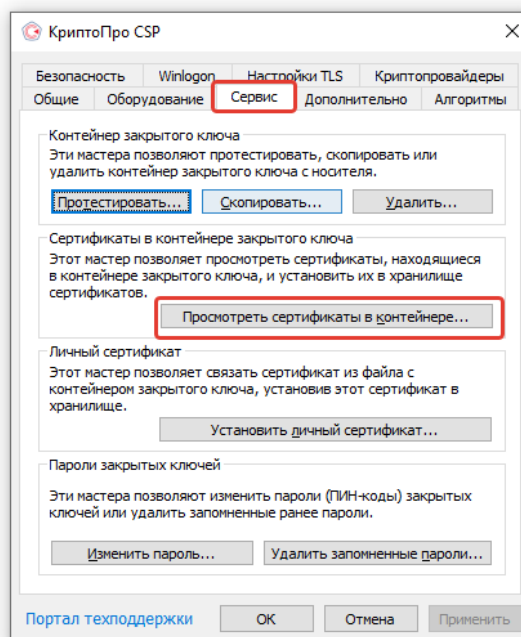
Установка сертификата

Такие же действия необходимо проделать с корневым сертификатом Удостоверяющего центра (УЦ), выдавшего ЭЦП.

■ Установка контейнера закрытого ключа

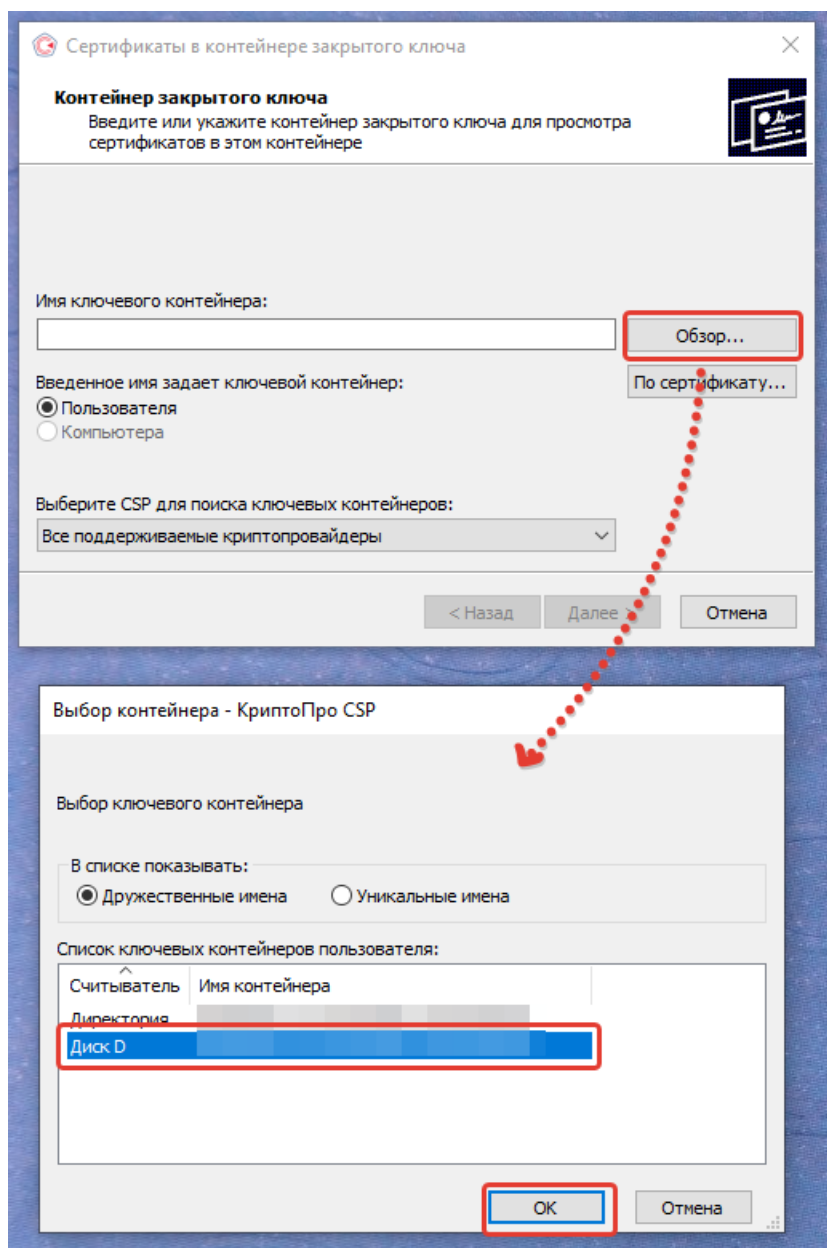
Переходим в меню «Пуск» и находим папку «КРИПТО-ПРО», запускаем в папке приложение «КриптоПро CSP».

В открывшемся окне программы переходим на вкладку «Сервис» и нажимаем кнопку «Просмотреть сертификаты в контейнере».



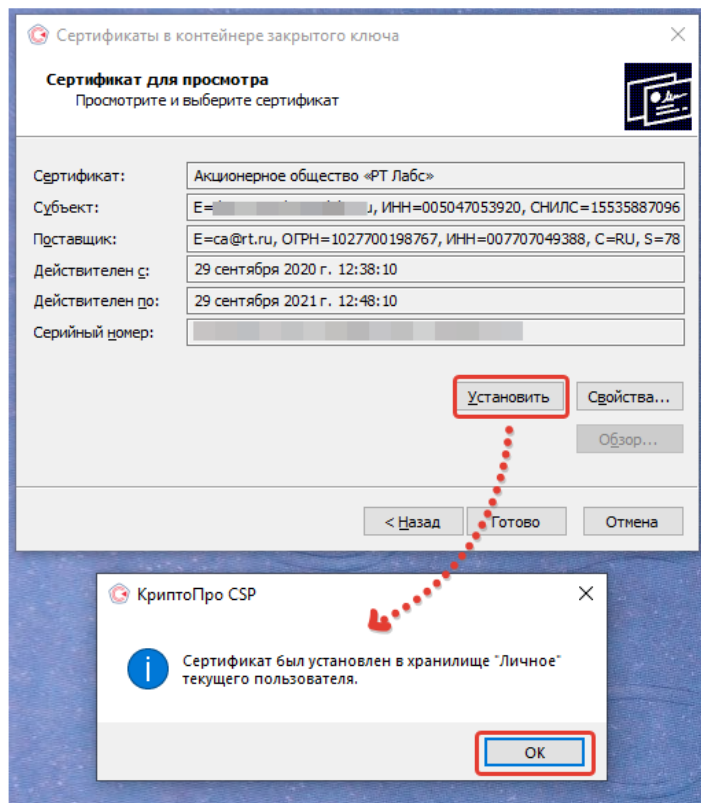
Установка контейнера закрытого ключа

В открывшемся окне нажимаем кнопку «Обзор» и выбираем контейнер с закрытыми ключами (в столбце «Считыватель» указано значение носителя электронной подписи (ЭП). Если такой контейнер отсутствует, необходимо проверить правильность размещения и наименования папки с закрытыми ключами сотрудника на носителе ЭП.



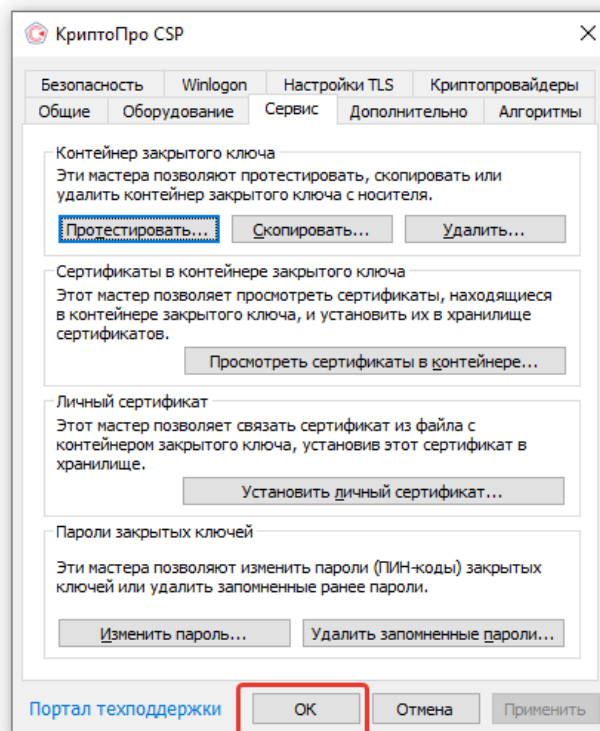
Установка контейнера закрытого ключа

В следующем открывшемся окне отображена информация о сертификате сотрудника. При нажатии на кнопку «Установить» будет получено уведомление о том, что сертификат успешно установлен в личное хранилище. Нажимаем кнопку «Ок».



Установка контейнера закрытого ключа

Далее нажимаем кнопку «Готово», возвращаемся в основное окно КриптоПро CSP и нажимаем кнопку «Ок»



Установка контейнера закрытого ключа

На этом установка всех необходимых компонентов, а также сертификата, завершена.

Если все действия из этого пункта проведены успешно или проверены на корректность, но ошибка подписания сохраняется, то возможна ошибка в некоторых заявлениях со стороны системы. В этом случае рекомендуем вернуться на шаг назад «На доработку» в заявлении и далее продолжить обработку заявки. Если данная ошибка при подписании возникает на этапе первого отказа, то необходимо пройти по пути сначала «Зарегистрировать» заявление, а в конце отказать.