Правительство Санкт-Петербурга
Комитет по информатизации и связи

Санкт-Петербургское государственное
унитарное предприятие
«Санкт-Петербургский
информационно-аналитический центр»

МАИС ЭГУ

Подсистема «Электронный кабинет должностного лица»

Требования к настройке автоматизированных рабочих мест

Санкт-Петербург

2025

Содержание

Термины и определения

В настоящем документе применяются следующие термины с соответствующими определениями (Таблица 1).

Таблица 1. Список примененных терминов

Термин	Определение
1	**2**
Авторизация	Предоставление определенному лицу или группе лиц прав на выполнение определенных действий
Браузер, веб-браузер	Клиентская программа, предназначенная для осуществления навигации в сети Интернет
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Информация	Сведения (сообщения, данные) независимо от формы их представления
Техническая поддержка	Услуги, посредством которых предприятия и организации обеспечивают помощь пользователям при возникновении проблем, связанных с продуктом и/или его использованием

Перечень принятых сокращений и обозначений

В настоящем документе применяются следующие сокращения (обозначения) (Таблица 2).

Таблица 2. Список примененных сокращений

Сокращение (обозначение)	Значение сокращения (обозначения)
1	2
АРМ	Автоматизированное рабочее место
ЕМТС	Государственная информационная система Санкт-Петербурга «Учет ресурсов единой мультисервисной телекоммуникационной сети исполнительных органов государственной власти Санкт-Петербурга»
КЭП	Квалифицированная электронная подпись
МАИС ЭГУ	Межведомственная автоматизированная информационная система предоставления в Санкт-Петербурге государственных и муниципальных услуг в электронном виде
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
ПЭВМ	Персональная электронно-вычислительная машина
СЗИ	Система защиты информации
СПб ГУП «СПб ИАЦ»	Санкт-Петербургское государственное унитарное предприятие «Санкт-Петербургский информационно-аналитический центр»
УЦ	Удостоверяющий центр
ЭКДЛ	Подсистема «Электронный кабинет должностного лица» МАИС ЭГУ
ЭЦП	Электронная цифровая подпись
DOCX (DOC)	Microsoft Office Document – (англ.) текстовый формат файлов для хранения электронных документов пакетов офисных приложений
PDF	Portable Document Format – (англ.) межплатформенный формат электронных документов
USB	Universal Serial Bus – (англ.) последовательный интерфейс для подключения периферийных устройств к вычислительной технике

1 Требования к рабочим станциям

Технические параметры клиентской машины, необходимые для корректной работы АРМ, определяются на основании необходимости работы со следующими приложениями:

функциональное веб-приложение;

ПО, позволяющее создавать и просматривать документы с разрешениями DOC и DOCX (просмотр и редактирование документов) или аналогичное бесплатно распространяемое программное обеспечение;

ПО, позволяющее просматривать отсканированные образы документов в графических форматах и в формате PDF;

ПО, позволяющее осуществлять работу с КЭП.

Минимальные системные требования к рабочим станциям представлены в Таблице 3.

Таблица 3. Минимальные системные требования к рабочим станциям

Наименование	Характеристика
1	2
Процессор	Intel Pentium 4 и выше или аналог
Монитор	Разрешение экрана не менее 1024x768. Диагональ видимой части экрана не менее 19” (данное требование не является обязательным, корректная работа ЭКДЛ не зависит от размера диагонали монитора сотрудника, работающего с АРМ, однако использование мониторов с меньшей диагональю может создавать определённые неудобства при просмотре)
ОЗУ	Не менее 1 Гбайт
Сетевая карта	Скорость передачи данных – не менее 10 Мбит/с
КЭП	См. требования в п.2
Каналы связи	Наличие СЗИ. Наличие доступа в ЕМТС
Порт USB	Один свободный порт USB

Для корректной работы АРМ нет необходимости оборудовать дополнительное рабочее место, оснащенное отдельной ПЭВМ. Программные надстройки могут быть установлены на действующей ПЭВМ без ущерба для работы с иными программными продуктами и информационными системами.

2 Установка программного обеспечения

В целях корректной работы АРМ необходимо обеспечить установку на ПЭВМ пользователя ПО, представленного в Таблице 4.

Таблица 4. Требования к ПО

Наименование	Характеристика
1	2
ОС	Любая ОС, которая позволяет использовать следующие браузеры: актуальные версии браузеров Яндекс.Браузер, Mozilla Firefox поддерживающие плагины NPAPI с включенным установленным расширением «CryptoPro Extension for CAdES Browser Plug-in» для работы с ЭЦП
Браузер	На выбор: Mozilla Firefox версии 52 и выше; Яндекс.Браузер версии 21 и выше; другие браузеры, поддерживающие плагины NPAPI
ПО, позволяющее работать с документами	ПО, позволяющее создавать и просматривать документы с разрешениями DOC и DOCX (в том числе Microsoft Office Reader), Adobe Reader версии 8 и выше
КЭП	Установленное ПО КриптоПро CSP 4.0 и выше (более подробная информация предоставлена по ссылке в сети Интернет https://www.cryptopro.ru/products/csp/compare)
Плагин ЭЦП для браузера	КриптоПро ЭЦП Browser plug-in https://www.cryptopro.ru/products/cades/plugin
ПО для использования модуля сканирования	Dynamic Web TWAIN plug-in для использования модуля сканирования (необходима ОС Windows)

Обращаем Ваше внимание, что всё ПО, за исключением КриптоПро CSP, является свободно распространяемым ПО, поэтому настройка АРМ сотрудника не требует покупки дополнительного ПО.

Перед началом настройки АРМ убедитесь, что на пользовательской ПЭВМ установлено необходимое ПО, указанное в Таблице 4. В случае его отсутствия проведите установку, руководствуясь п.2.1-2.6 настоящего документа.

2.1 Установка браузера

Скачать браузер следует с официальной страницы:

Mozilla Firefox https://www.mozilla.org/ru

Яндекс.Браузер https://browser.yandex.ru/

2.2 Установка Adobe Reader

Для корректной работы АРМ необходимо, чтобы на ПЭВМ пользователя был установлен Adobe Reader версии 8 и выше. Данное ПО можно загрузить с сайта разработчика по ссылке в сети Интернет: http://get.adobe.com/uk/reader/.

2.3 Установка КриптоПро CSP

Программный пакет КриптоПро CSP устанавливается на пользовательскую ПЭВМ сотрудниками УЦ при получении сертификата ЭП.

В результате на ПЭВМ будут установлены: КриптоПро CSP 4.0 и выше; драйвер EToken; сертификаты пользователей; будут настроены носители и считыватели КриптоПро.

В случае если у сотрудника, который уполномочен использовать АРМ, отсутствует сертификат КЭП, необходимо обеспечить её получение. Порядок получения КЭП можно узнать на сайте УЦ СПб ГУП «СПб ИАЦ» по ссылке: http://ca.iac.spb.ru/iogv/iogv.html.

По вопросам оформления заявок на получение КЭП возможно обратиться в УЦ СПб ГУП «СПб ИАЦ» по телефону 8 (812) 764-38-85.

Подтверждением действий сотрудника при работе в ЭКДЛ является КЭП, которая в соответствии с законодательством Российской Федерации приравнивается к обычной подписи сотрудника на бумажных документах.

Работа в ЭКДЛ без КЭП нелегитимна, поэтому сотрудники не могут работать в ЭКДЛ без применения подписи.

2.4 Установка КриптоПро ЭЦП Browser plug-in

Установка КриптоПро ЭЦП Browser plug-in проводится непосредственно в том браузере, который в дальнейшем будет использоваться для работы в ЭКДЛ. Для установки КриптоПро ЭЦП Browser plug-in необходимо загрузить на ПЭВМ архив с файлом-установщиком, размещенным в разделе «Информационные материалы» в блоке «Подсистема «Электронный кабинет должностного лица»:

https://gu.spb.ru/knowledge-base/priem-info/ (в ЕМТС);

http://gu.egu.vpn/knowledge-base/priem-info/ (в сети Интернет).

Для установки необходимо нажать ссылку «Установочный файл плагина КриптоПро ЭЦП Browser plug-in» (Рисунок 1).

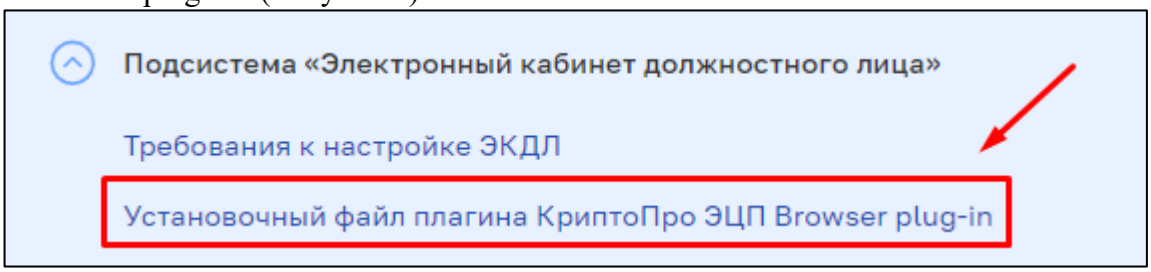

Рисунок 1. Сохранение файла-установщика

Далее извлечь из архива файл-установщик в любую удобную папку (Рисунок 2).

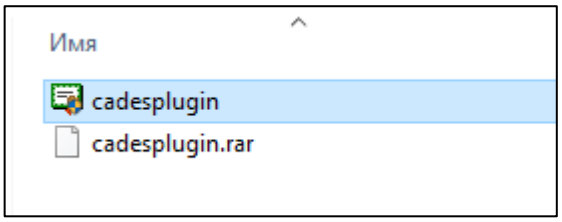

Рисунок 2. Извлечение файла-установщика

После извлечения файла-установщика необходимо кликнуть по нему дважды левой кнопкой мыши для запуска процессе установки (Рисунок 3).

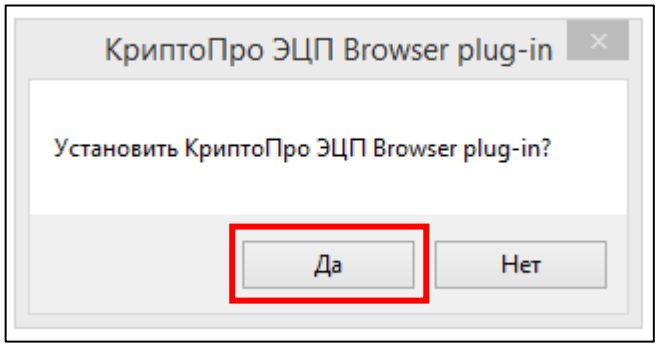

Рисунок 3. Установка КриптоПро ЭЦП Browser plug-in

Программный модуль также можно загрузить с официального сайта КриптоПро по ссылке в сети Интернет:

https://www.cryptopro.ru/products/cades/plugin.

Порядок установки в данном случае не изменится.

По завершении процесса установки КриптоПро ЭЦП Browser plug-in на ПЭВМ пользователя откроется информационное окно с сообщением об успешной установке КриптоПро ЭЦП Browser plug-in и рекомендацией по перезапуску браузера, которую

следует выполнить (Рисунок 4).

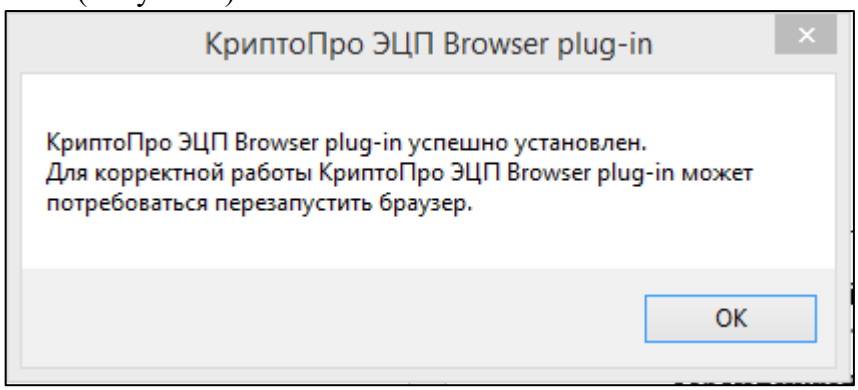

Рисунок 4. Сообщение об успешной установке

После этого необходимо добавить адрес ЭКДЛ в список доверенных в настройках КриптоПро ЭЦП Browser plug-in. Для этого необходимо:

1) Открыть «Настройки ЭЦП Browser plug-in» с помощью того браузера, в котором будет осуществляться дальнейшая работа с ЭКДЛ (Рисунок 5).

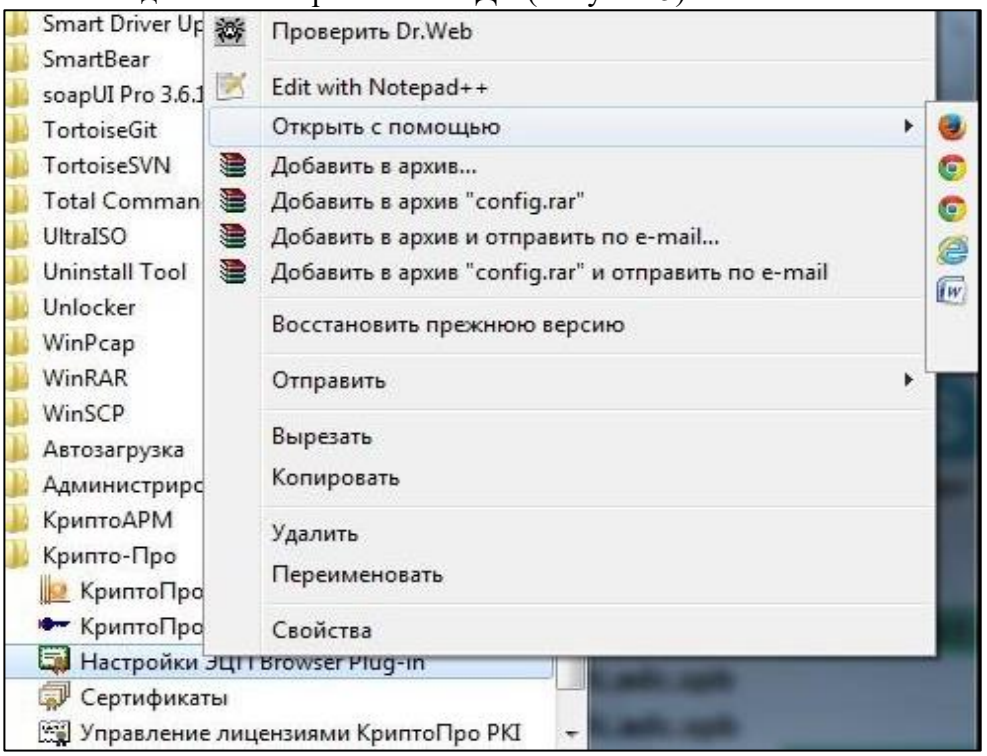

Рисунок 5. Переход к настройкам КриптоПро ЭЦП Browser plug-in

2) Добавить адрес ЭКДЛ http://ekdl2.egu.vpn в список доверенных узлов и нажать кнопку «Сохранить» (Рисунок 6).

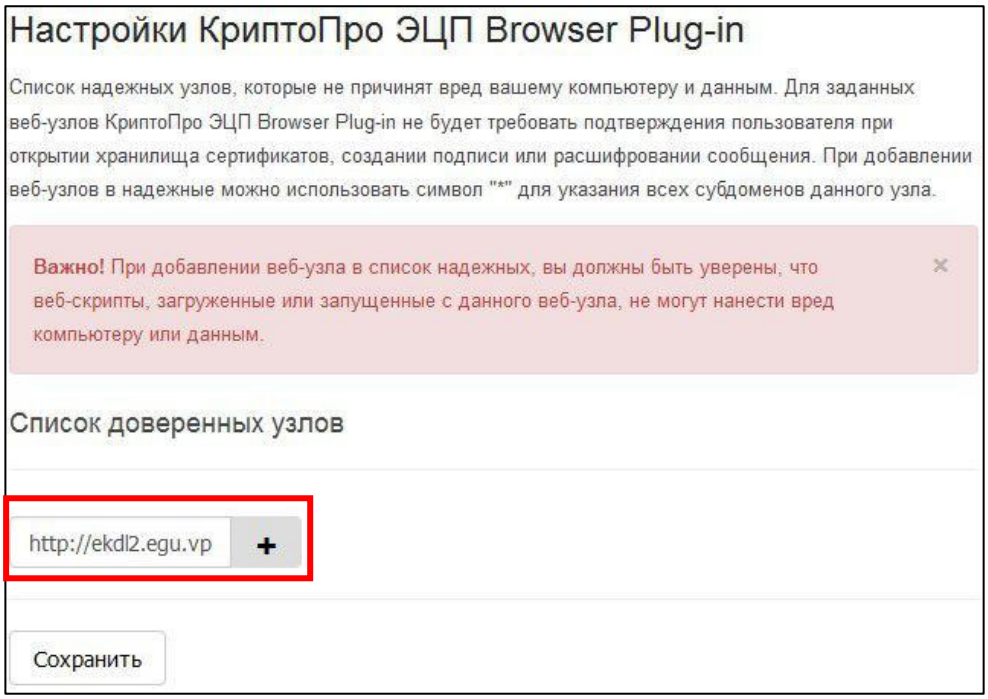

Рисунок 6. Добавление ЭКДЛ в список доверенных узлов

2.5 Проверка корневого сертификата

Далее необходимо проверить установку корневого сертификата УЦ и установить его в случае отсутствия.

Для проверки наличия установленного корневого сертификата необходимо нажать кнопку «Пуск» и в списке программ выбрать «КриптоПРО CSP». В открывшемся окне перейти во вкладку «Сервис» и нажать кнопку «Посмотреть сертификаты в контейнере» (Рисунок 7).

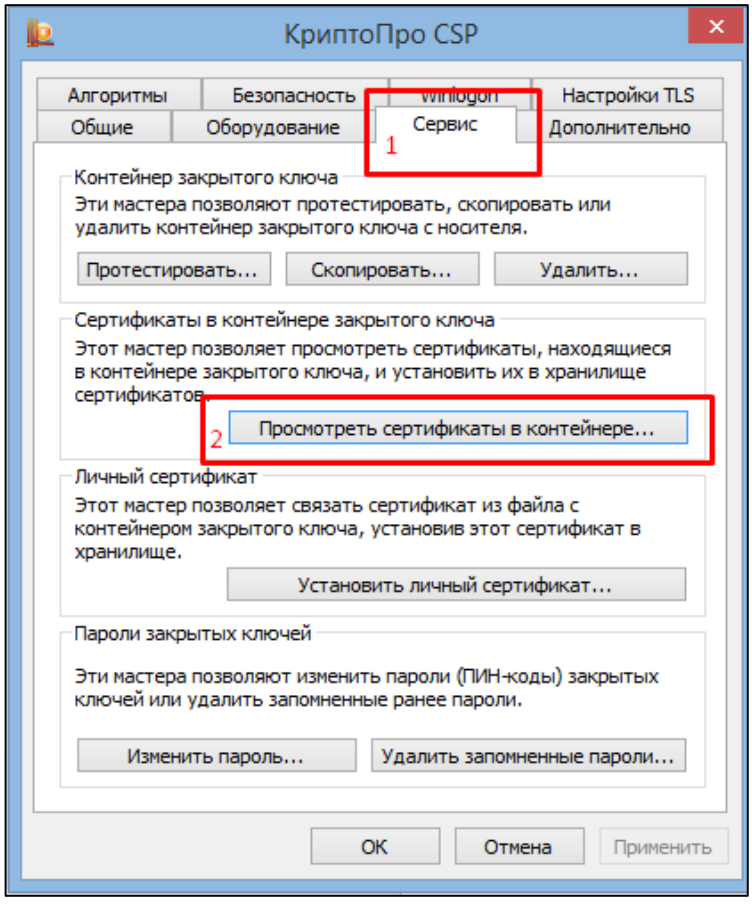

Рисунок 7. Проверка установки корневого сертификата, шаг 1

В открывшемся окне нажать кнопку «Обзор» (Рисунок 8).

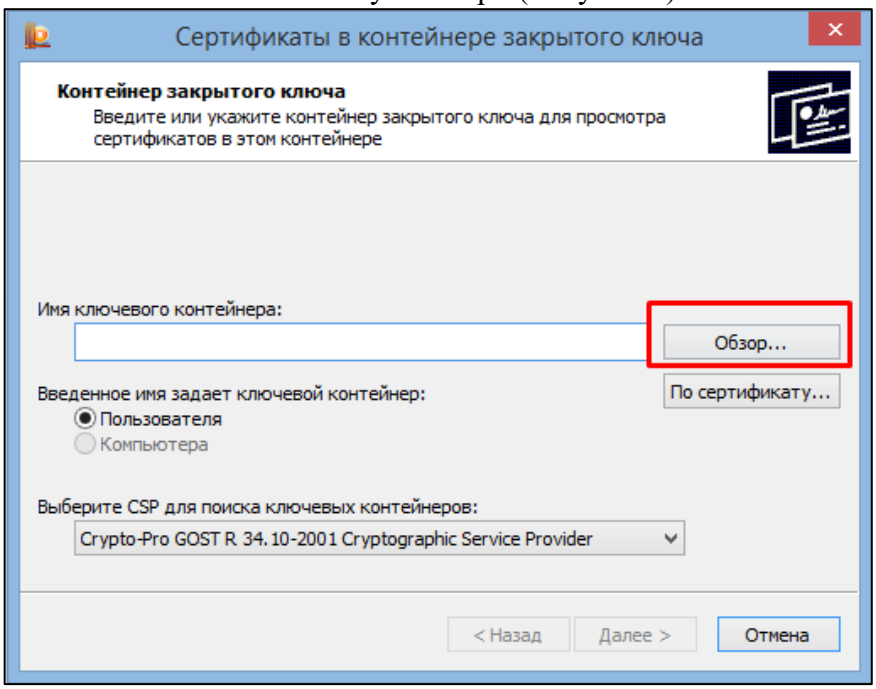

Рисунок 8. Проверка установки корневого сертификата, шаг 2

Далее необходимо выбрать сертификат КЭП, которая будет использоваться при работе в ЭКДЛ, нажать кнопку «ОК» (Рисунок 9).

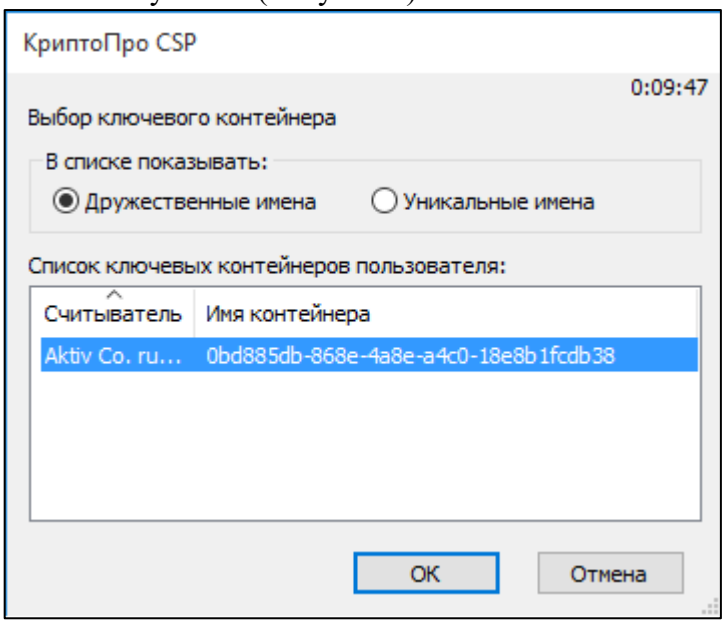

Рисунок 9. Проверка установки корневого сертификата, шаг 3

После выбора сертификата необходимо нажать кнопку «Далее» (Рисунок 10).

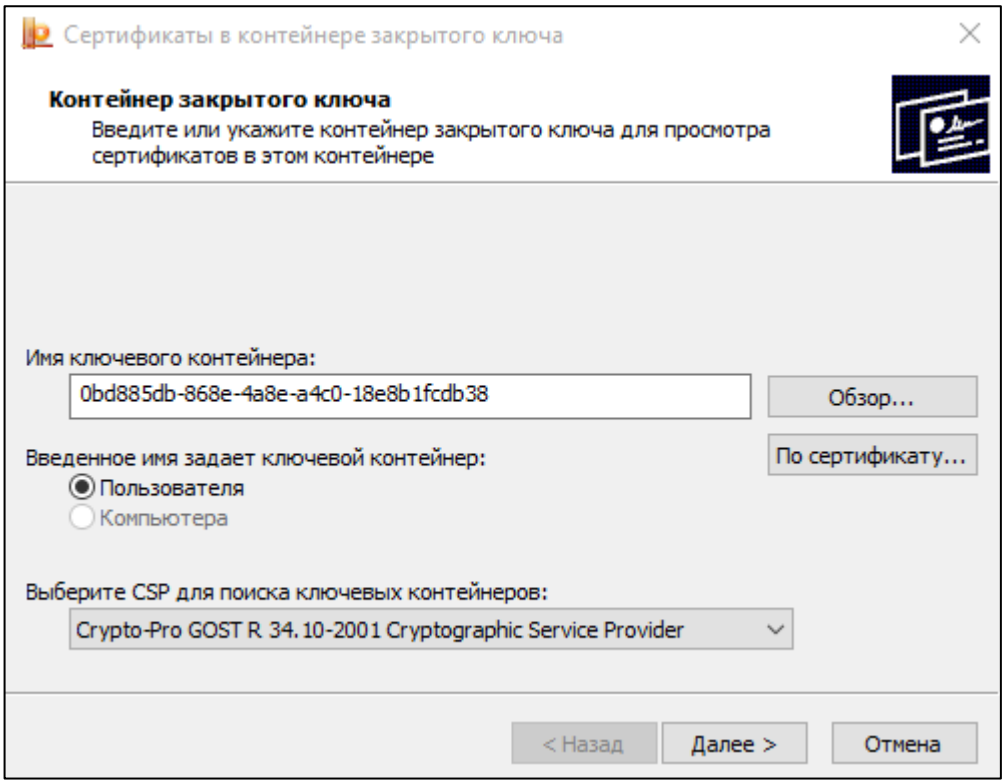

Рисунок 10. Проверка установки корневого сертификата, шаг 4

В открывшемся окне, содержащем информацию о сертификате, необходимо нажать кнопку «Свойства» (Рисунок 11), затем выбрать вкладку «Путь сертификации» и, убедившись, что корневой сертификат УЦ установлен (отображается над личным сертификатом пользователя), нажать кнопку «ОК» (Рисунок 12).

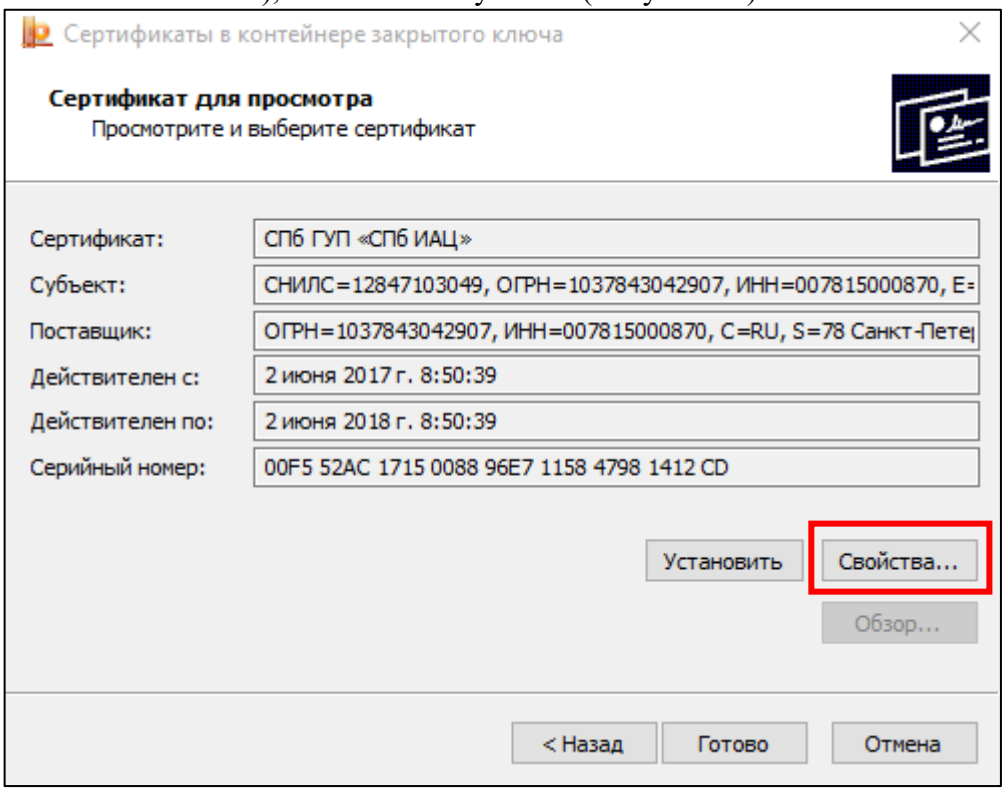

Рисунок 11. Проверка установки корневого сертификата, шаг 5

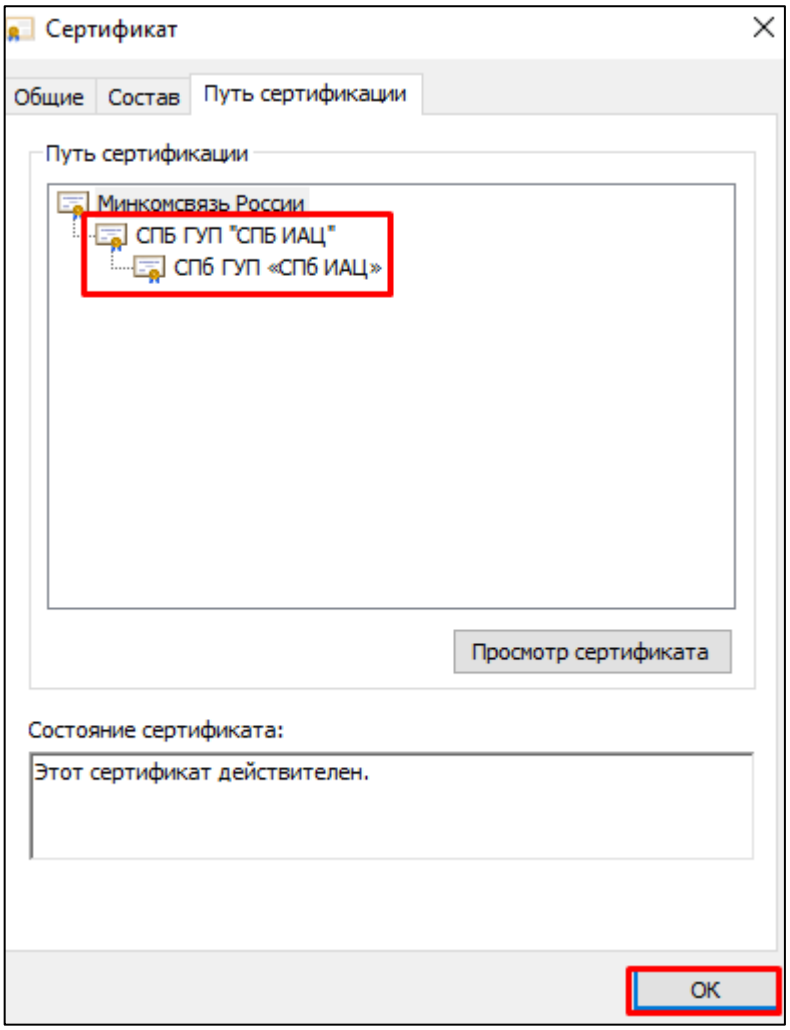

Рисунок 12. Проверка установки корневого сертификата, шаг 6

Проверить корректность установки корневого сертификата на ПЭВМ возможно на демо-странице КриптоПро, расположенной по ссылке: https://www.cryptopro.ru/sites/default/files/products/cades/demopage/simple.html.

Внимание! Для корректной работы сертификата необходимо наличие расширения CryptoPro Extension for CAdES Browser Plug-in во включенном режиме (Рисунок 13).

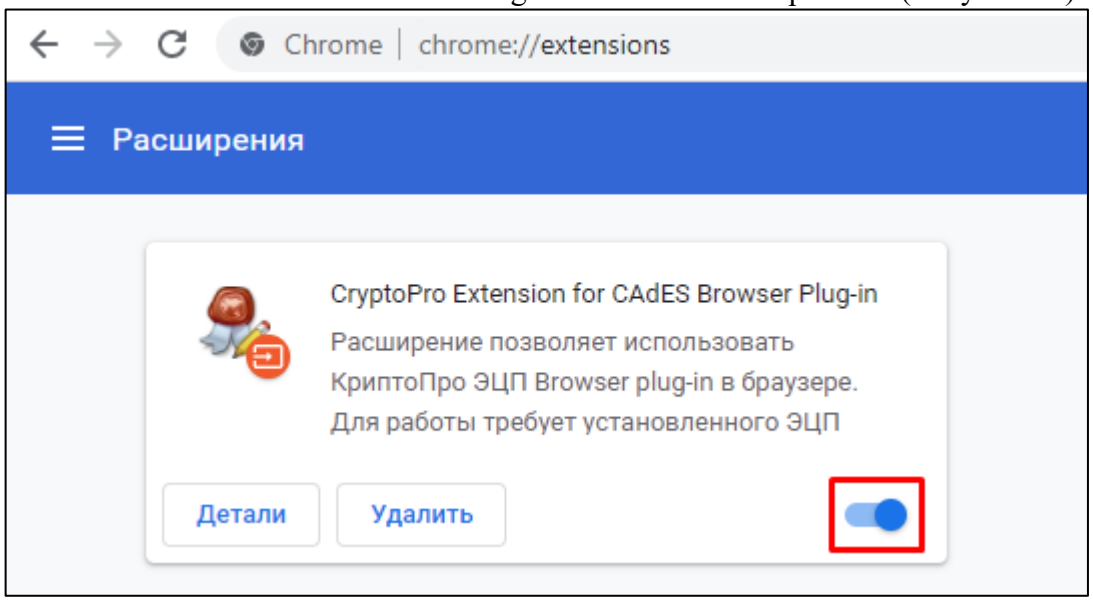

Рисунок 13. Включенное расширение для работы сертификата

Проверить включенность такого расширения можно в настройках браузера («Дополнительные инструменты» – «Расширения»). В случае если данное расширение отсутствует, то его необходимо скачать для используемого браузера. Например, для Mozilla Firefox расширение для браузера можно скачать в магазине дополнений Mozilla Firefox либо по ссылке:
https://www.cryptopro.ru/sites/default/files/products/cades/extensions/firefox_cryptopro_extension_latest.xpi.

Для проверки выполненных настроек работы ЭЦП необходимо на сайте КриптоПро https://www.cryptopro.ru/products/cades/plugin нажать кнопку «Проверить работу плагина» (Рисунок 14).

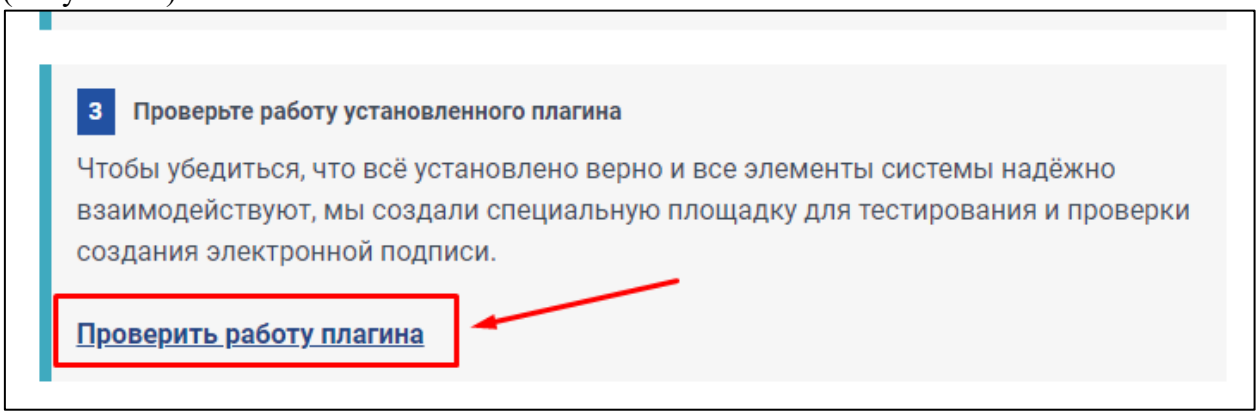

Рисунок 14. Переход на демо-страницу проверки работы установленного плагина

После перехода на демо-страницу появится окно с запросом на подтверждение выполнения операции с КЭП. Необходимо подтвердить, выбрать используемый сертификат, нажать кнопку «Подписать». После описанных действий отобразится результат проверки. В случае успешной проверки отобразится «Подпись сформирована успешно» (Рисунок 15).

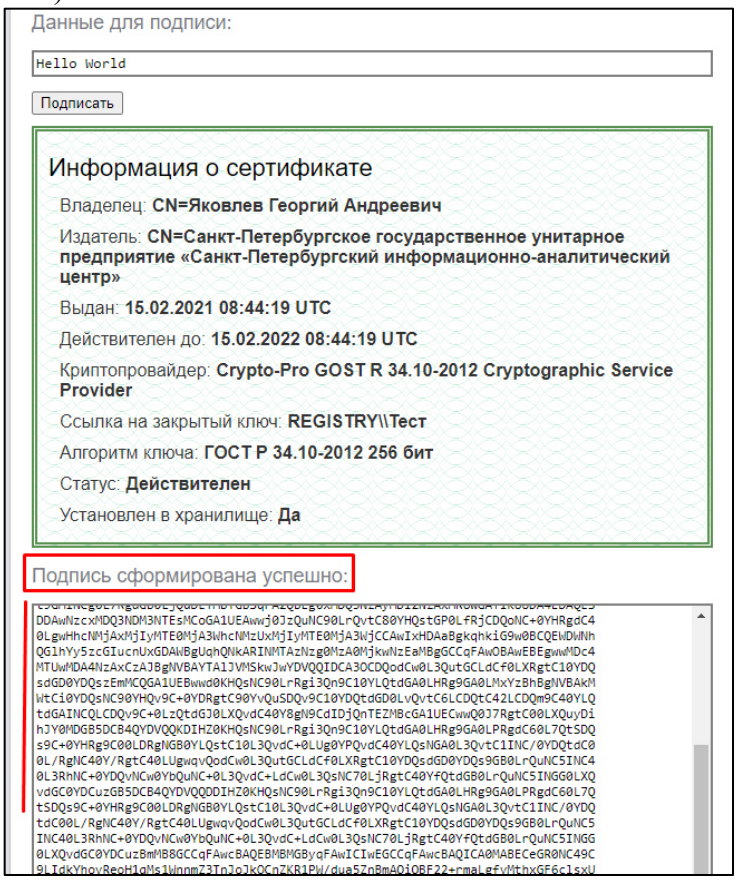

Рисунок 15. «Подпись сформирована успешно»

Если сертификат установлен, появится соответствующее сообщение (Рисунок 16).

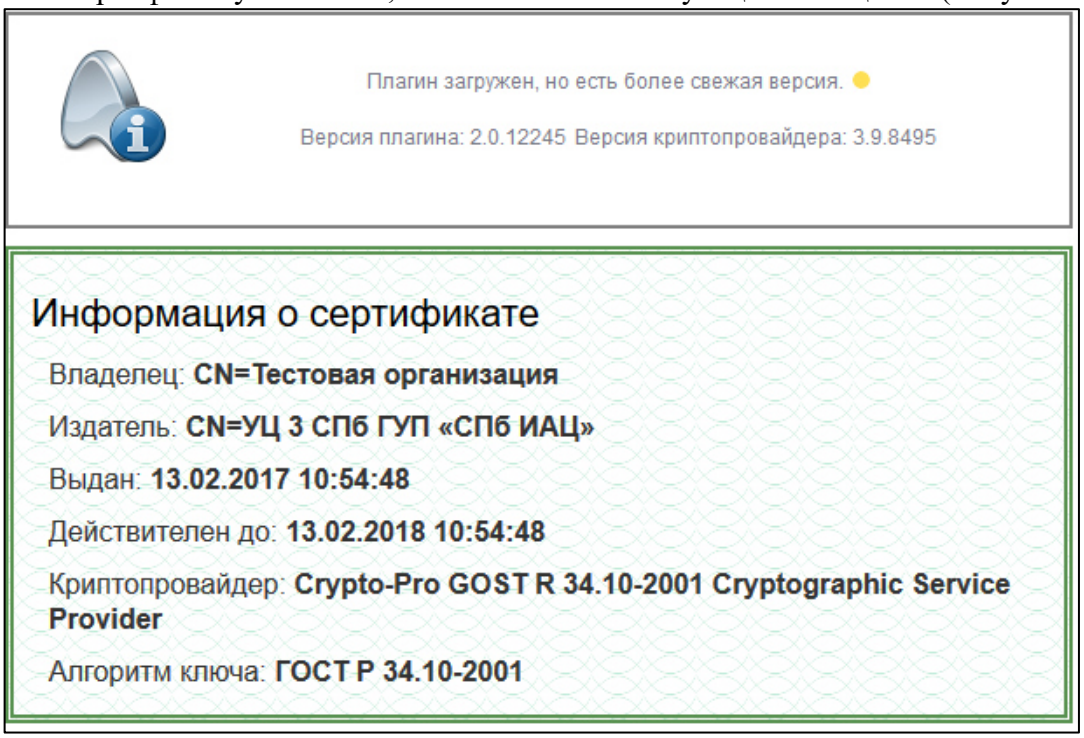

Рисунок 16. Проверка сертификата на демо-странице КриптоПро

2.6 Установка корневого сертификата

В случае если корневой сертификат УЦ не установлен, необходимо выполнить его установку.

Если сертификат КЭП пользователя был выдан УЦ СПб ГУП «СПб ИАЦ», требуется перейти на страницу http://ca.iac.spb.ru/serv/cert.html и установить актуальный корневой сертификат.

В случае если КЭП был выдан до 18.09.2019, необходимо установить первый корневой сертификат (Рисунок 17).

Рисунок 17. Установка корневого сертификата УЦ СПб ГУП «СПб ИАЦ»

В случае, если КЭП выдан после 22.12.2020, необходимо установить второй корневой сертификат (Рисунок 18).

Рисунок 18. Установка корневого сертификата УЦ СПб ГУП «СПб ИАЦ»

Если сертификат выдан не УЦ СПб ГУП «СПб ИАЦ», а иным УЦ, то для получения помощи и консультации рекомендуется обращаться в соответствующий УЦ.

После выбора нужного сертификата начнется загрузка архива. После завершения

загрузки необходимо отрыть архив с инструкцией и файлами для установки (Рисунок 19).

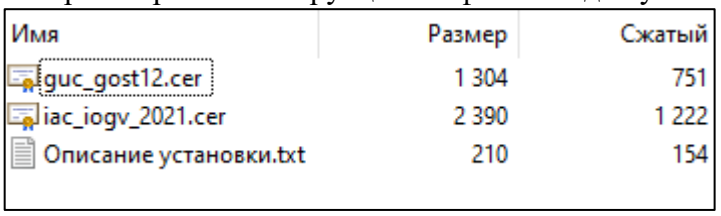

Рисунок 19. Импорт корневого сертификата

Необходимо выбрать первый сертификат с наименованием «guc_gost12.cer» и установить его (Рисунок 20).

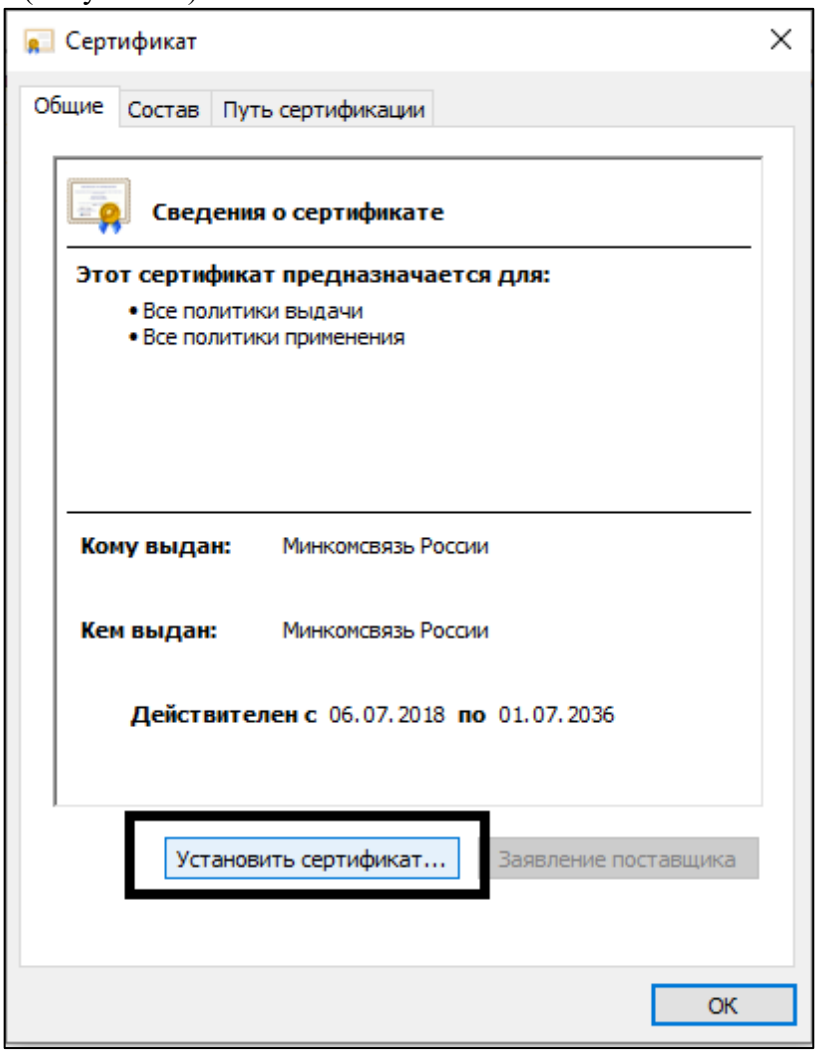

Рисунок 20. Установка корневого сертификата guc_gost12.cer

Далее необходимо осуществить импорт сертификата (Рисунок 21).

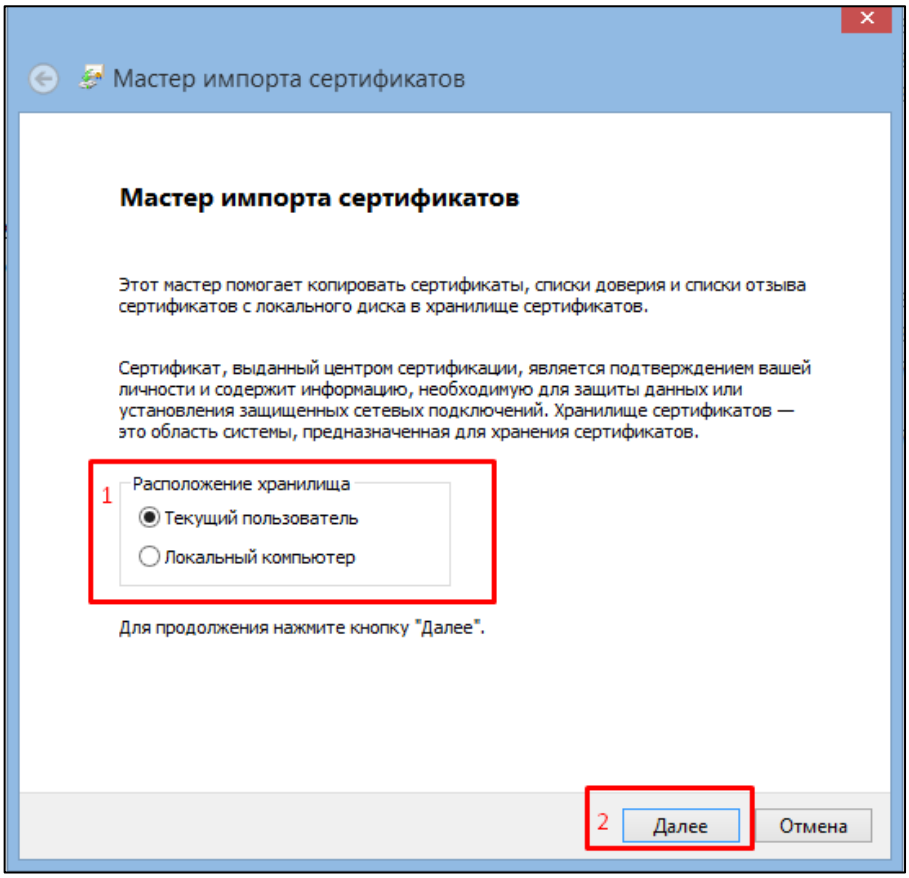

Рисунок 21. Импорт корневого сертификата guc_gost12.cer

После нажатия кнопки «Далее» необходимо выбрать хранилище сертификата. Для этого следует выбрать строку «Поместить все сертификаты в следующее хранилище» и нажать кнопку «Обзор» (Рисунок 22).

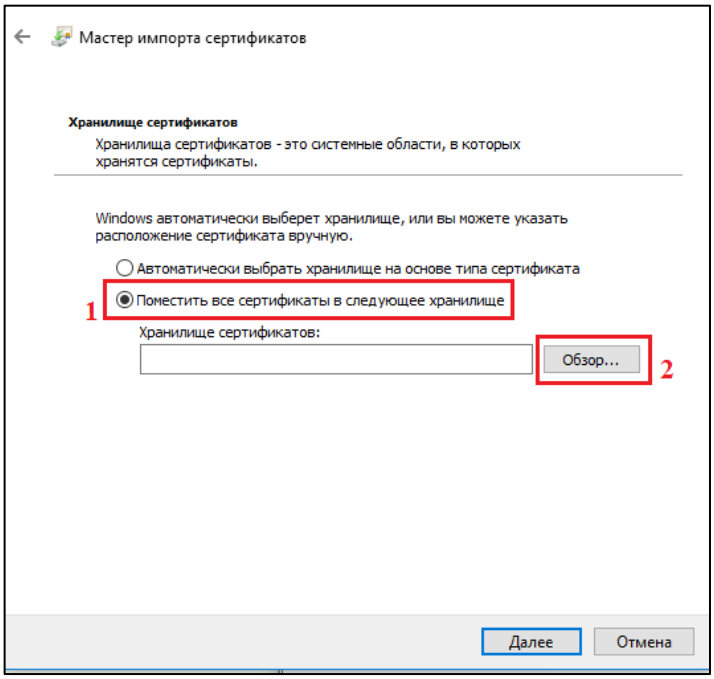

Рисунок 22. Выбор хранилища для сертификата guc_gost12.cer

Необходимо выбрать хранилище «Доверенные корневые центры сертификации» (Рисунок 23).

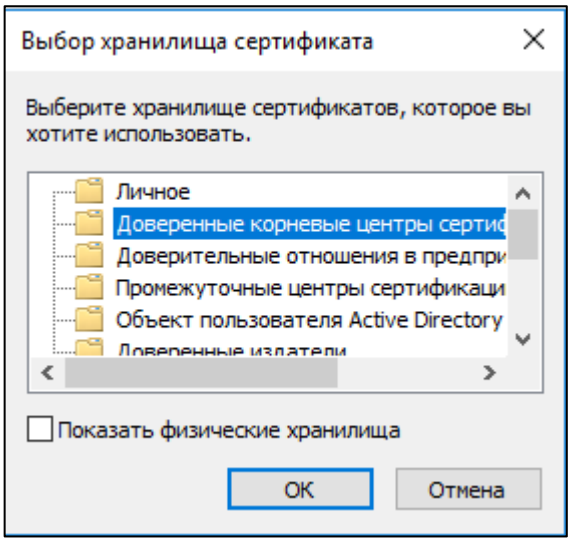

Рисунок 23. Хранилище сертификатов

Далее в открывшемся окне следует нажать кнопку «Готово» (Рисунок 24).

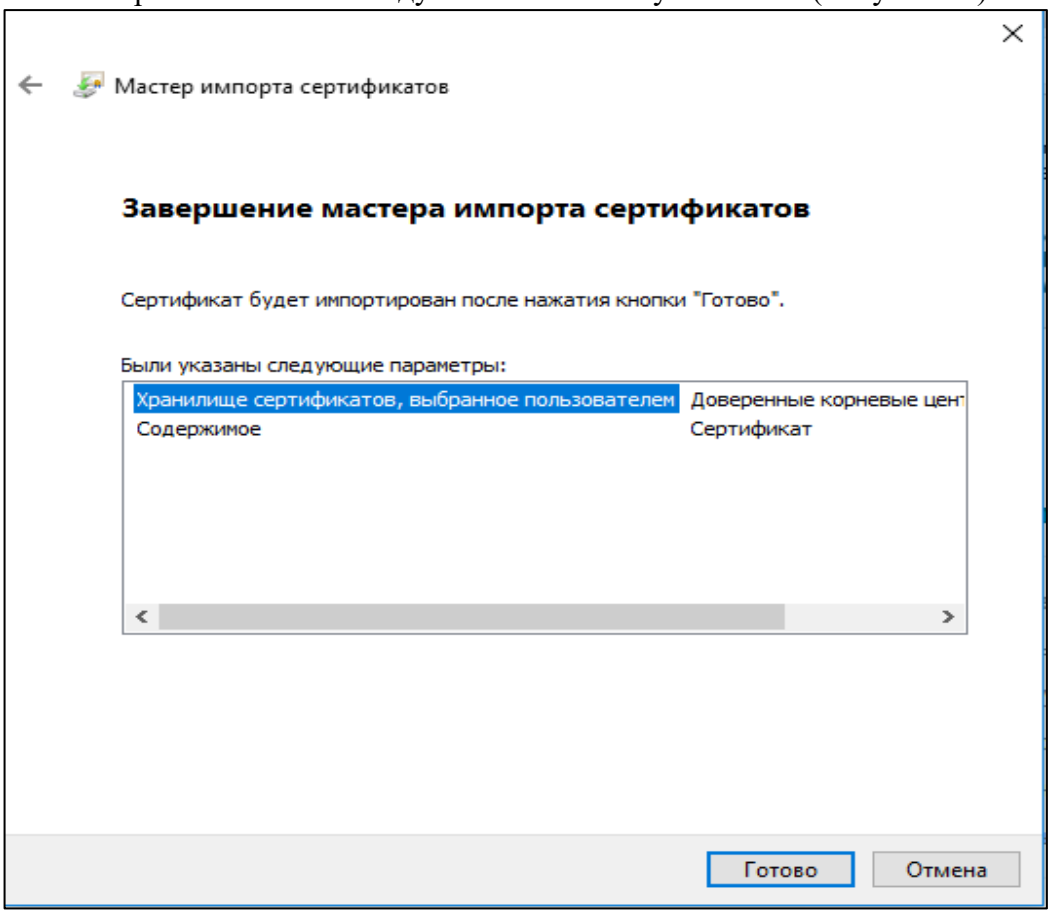

Рисунок 24. Завершение мастера импорта сертификата guc_gost12.cer

В случае успешного импорта сертификата отобразится соответствующее сообщение (Рисунок 25).

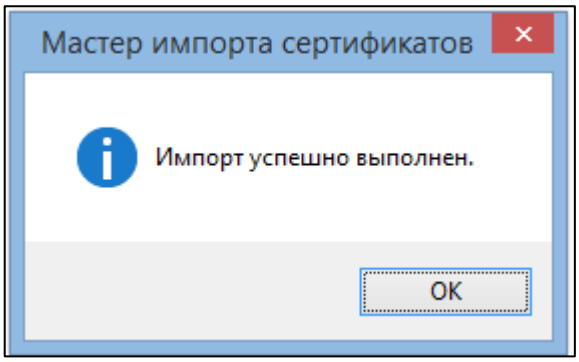

Рисунок 25. Сообщение об успешном импорте корневого сертификата guc_gost12.cer

По аналогии следует совершить импорт второго сертификата iac_iogv_2021. Для этого в открытом ранее архиве с инструкцией и файлами для установки (Рисунок 19) необходимо выбрать второй сертификат с наименованием «iac_iogv_2021» и установить его (Рисунок 26).

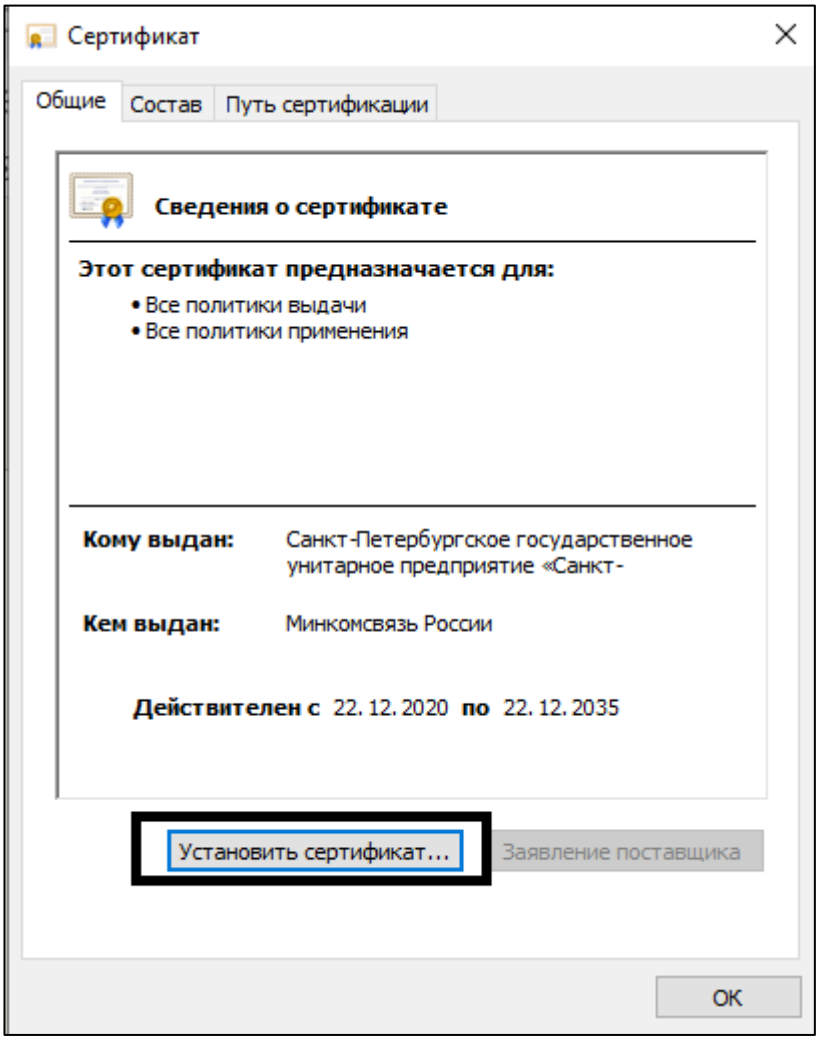

Рисунок 26. Установка корневого сертификата iac_iogv_2021

Далее необходимо осуществить импорт сертификата (Рисунок 27).

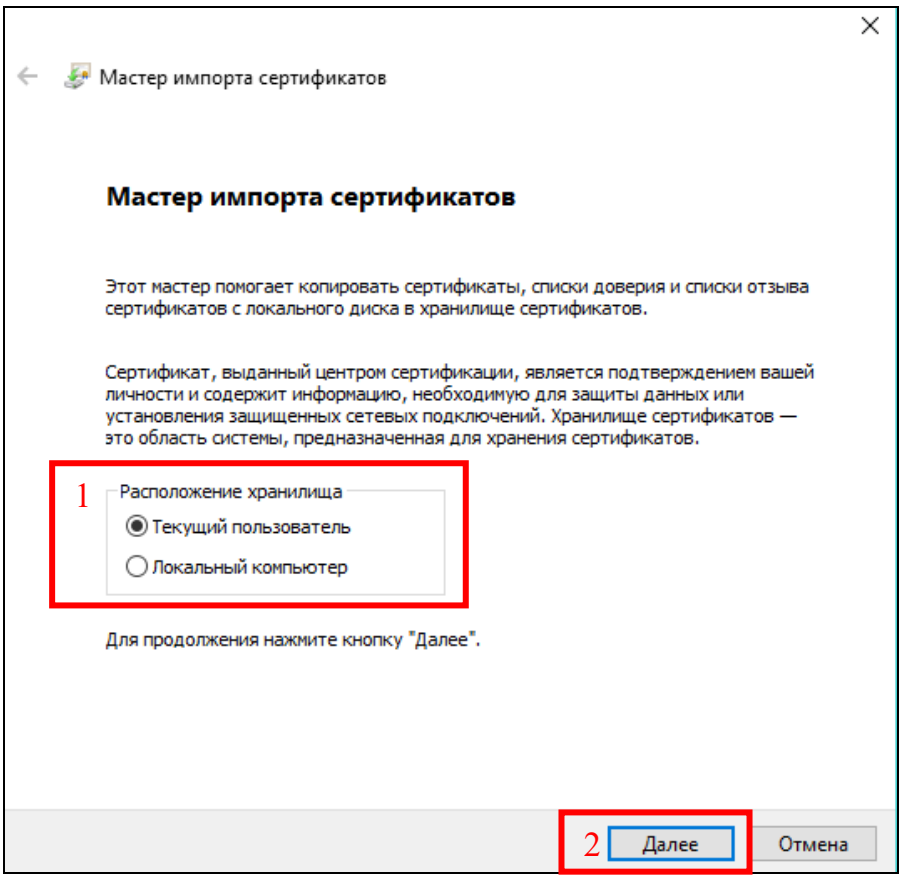

Рисунок 27. Импорт корневого сертификата iac_iogv_2021

После нажатия кнопки «Далее» необходимо выбрать хранилище сертификата. Для этого следует выбрать строку «Поместить все сертификаты в следующее хранилище, нажать кнопку «Обзор» и выбрать хранилище, указанное на скриншоте «Промежуточные центры сертификации» (Рисунок 28).

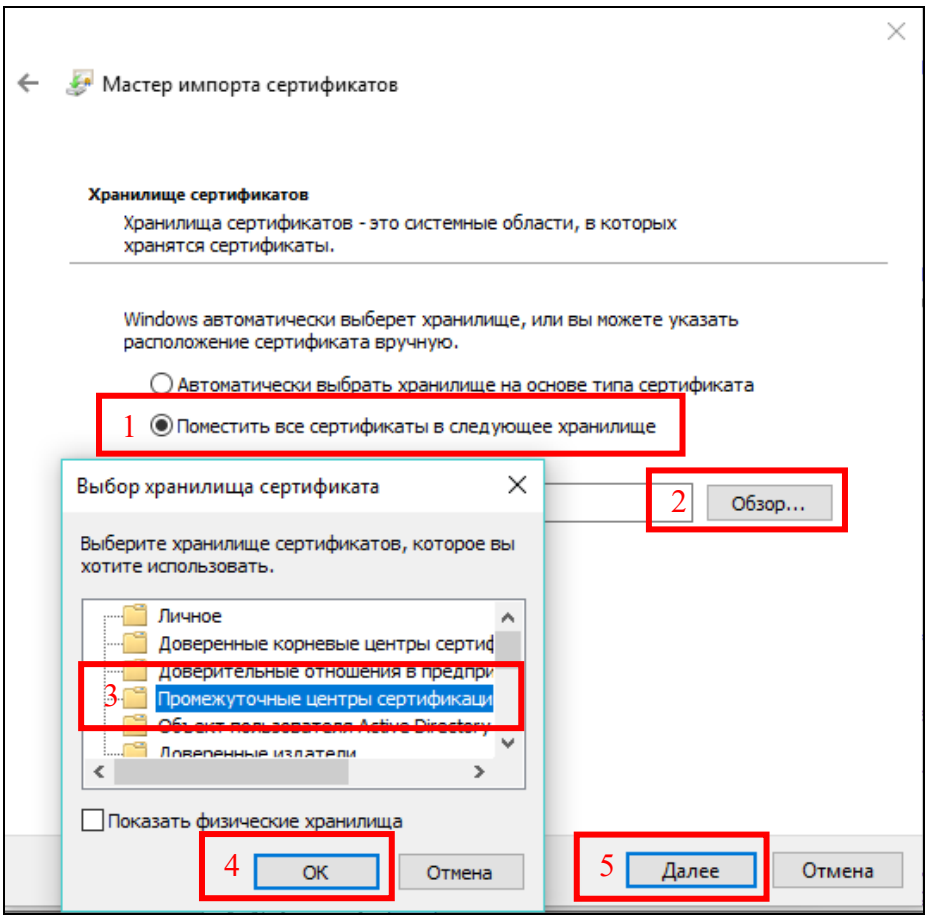

Рисунок 28. Выбор хранилища для сертификата iac_iogv_2021

Далее в открывшемся окне следует нажать кнопку «Готово» (Рисунок 29).

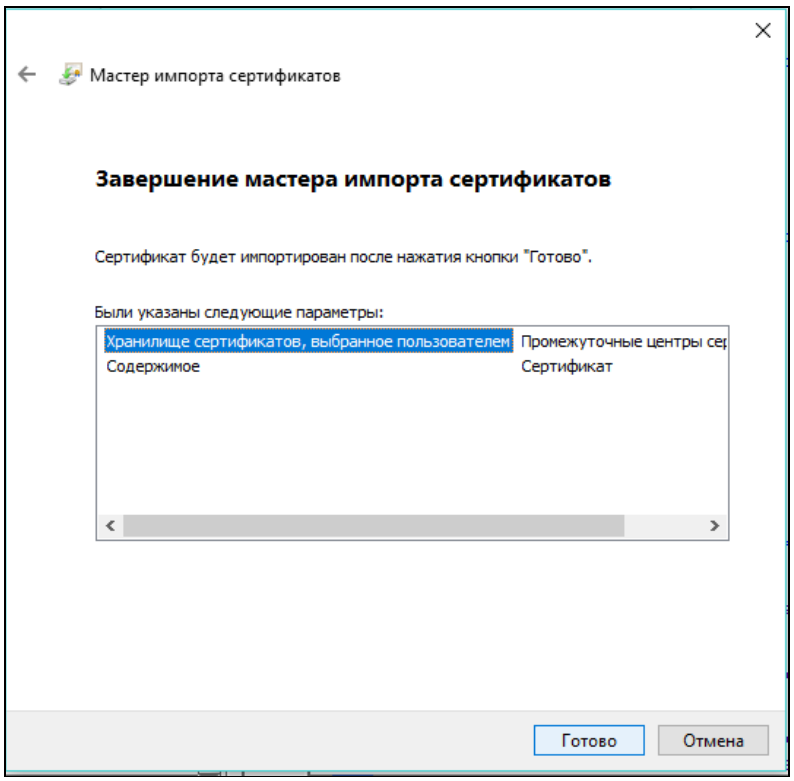

Рисунок 29. Завершение мастера импорта сертификата iac_iogv_2021

В случае успешного импорта сертификата отобразится соответствующее сообщение (Рисунок 30).

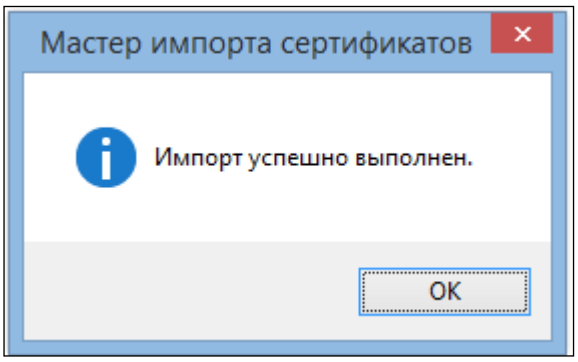

Рисунок 30. Сообщение об успешном импорте корневого сертификата iac_iogv_2021

3 Возможные проблемы при работе с КЭП

3.1 Ошибка создания подписи

Если при попытке использовать КЭП возникают сообщения об ошибке создания подписи (Рисунки 31-32), необходимо добавить корневой сертификат удостоверяющего центра в соответствии с инструкцией, представленной в п.2.6 настоящего документа.

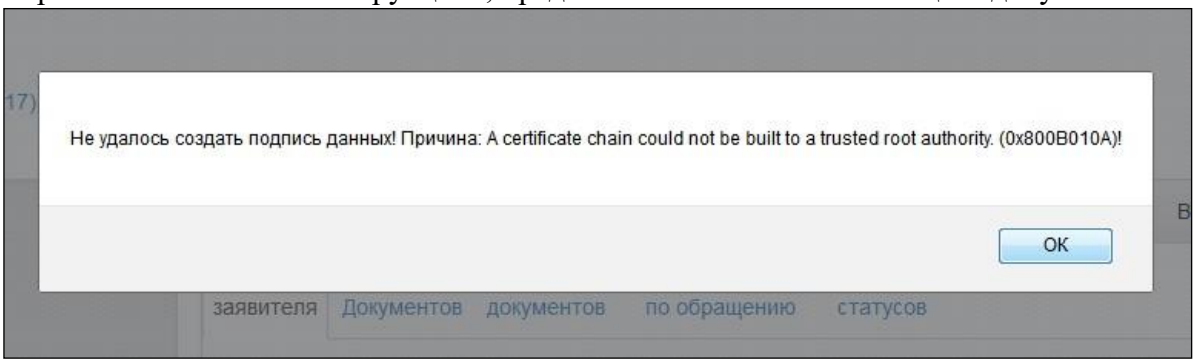

Рисунок 31. Сообщение об ошибке создания подписи

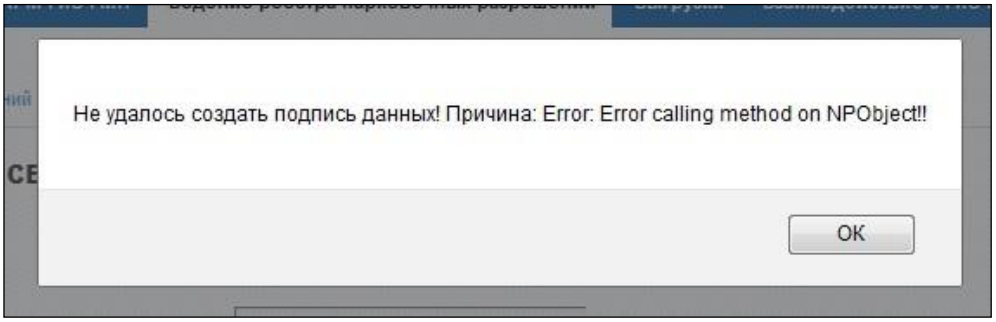

Рисунок 32. Ошибка создания подписи

3.2 Всплывающее окно «мастер-пароль»

В случае если при каждом открытии браузера постоянно всплывает окно «Введите мастер-пароль для доступа в eToken» (Рисунок 33), необходимо выгрузить модуль устройства защиты.

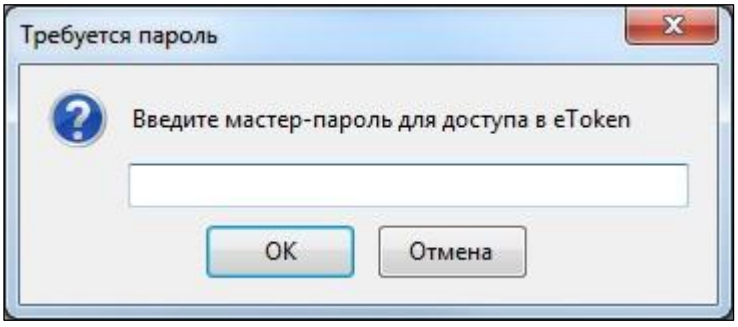

Рисунок 33. Окно для введения пароля

Для выгрузки необходимо (на примере браузера Mozilla Firefox):
открыть меню браузера;
открыть страницу «Настройки»;
выбрать слева вкладку «Дополнительные»;
выбрать в окне вкладку «Сертификаты»;
нажать кнопку «Устройства защиты»;
выбрать eToken и нажать кнопку «Выгрузить»;
перезапустить браузер.

4 Сетевые настройки

Доступ к ЭКДЛ обеспечивается в ЕМТС по адресу: http://ekdl2.egu.vpn. Доступ к ЭКДЛ в сети Интернет невозможен.

При необходимости пользователь может создать ярлык прямого доступа на указанный ресурс. В случае использования браузера Mozilla Firefox это возможно выполнить следующим образом:

ввести в адресной строке браузера адрес, указанный выше;

дождаться загрузки страницы;

нажать на символ слева от адресной строки (Рисунок 34);

зажать левую клавишу мыши и перетащить картинку на рабочий стол;

отпустить левую клавишу мыши.

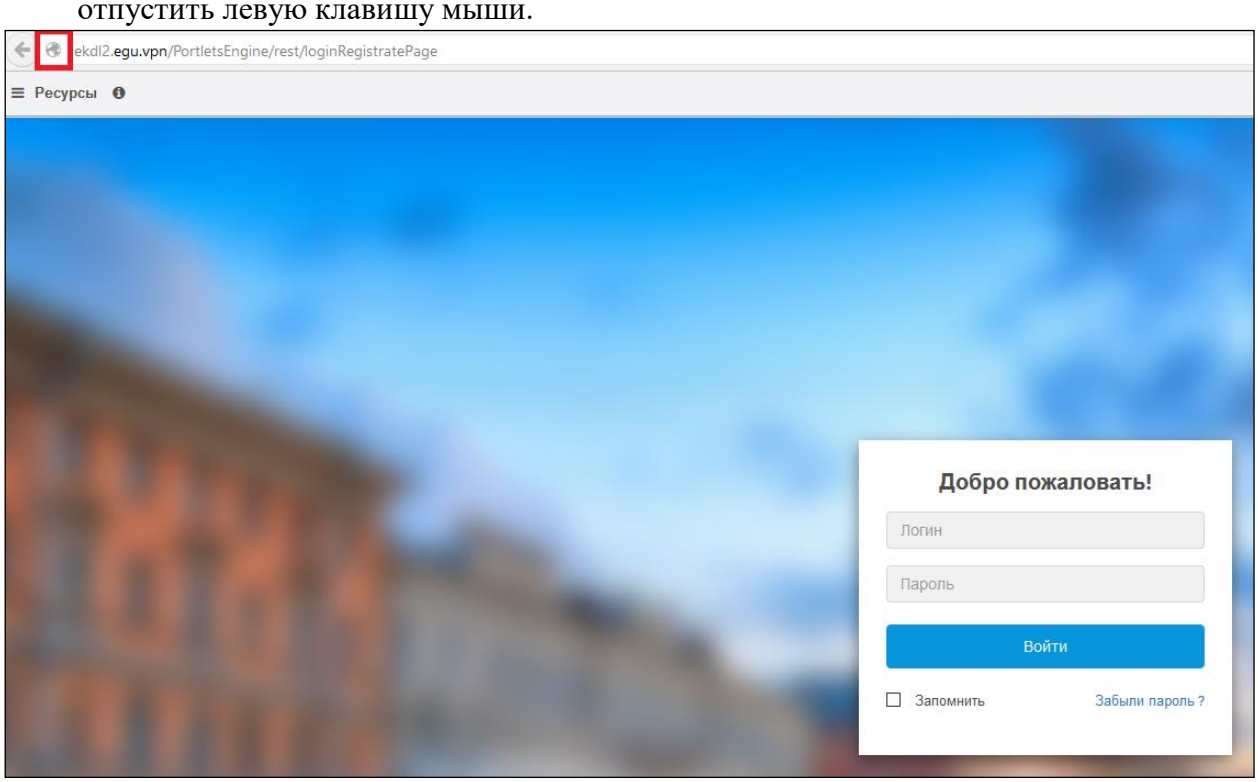

Рисунок 34. Страница для авторизации пользователя

5 Контактные данные

По всем возникающим вопросам использования, а также по вопросам улучшения и доработки ЭКДЛ следует обращаться в Службу технической поддержки Межведомственной автоматизированной информационной системы предоставления в Санкт-Петербурге государственных и муниципальных услуг в электронном виде:

телефон: 8 (812) 246-84-65 (режим работы: с 9:00 до 18:00 по рабочим дням);

e-mail: mais_iogv@sspk.spb.ru.