РУКОВОДСТВО ПО РАБОТЕ С ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСЬЮ

(Обновленное, редакция декабрь 2019)

Содержание

Введение. Причины перехода от старых устройств Рутокен ЭЦП к новому способу хранения ключей подписи

Согласно письму Федеральной службы безопасности Российской Федерации от 07.09.2018 №149/7/6-363 возможность использования схемы электронной подписи по ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (далее – ГОСТ - 2001) для формирования электронных подписей продлевается до 31.12.2019

1 января 2019 года вместо старого стандарта – ГОСТ Р 34.10-2001 вводится в действие новый стандарт формирования усиленной электронной подписи – ГОСТ Р 34.10-2012 (нормативный документ - выписка из документа ФСБ России № 149/7/1/3-58 от 31.01.2014 "О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования").
С 01.01.2020 все сертификаты будут выдаваться только по ГОСТ-2012.

В связи с данными изменениями законодательства удостоверяющий центр СФУ (УЦ СФУ) обязан формировать электронную подпись по новому алгоритму.

Используемые ранее устройства Рутокен ЭЦП не предназначены для хранения электронной подписи, сформированной по данному алгоритму. Федеральный закон №63-ФЗ «Об электронной подписи» не регламентирует требования к устройствам для хранения усиленной неквалифицированной электронной подписи, поэтому подписи данного типа могут храниться на любых носителях, в т.ч. USB-flash-накопителях. В связи с этим, ключевая информация записывается на личное устройство пользователя.

За сохранность ключевой информации отвечает пользователь.

Необходимое программное и аппаратное обеспечение, корневой сертификат

I. Аппаратное обеспечение

1) **USB-флеш-накопитель**

На пользовательское устройство будет записана ключевая информация (контейнер закрытого и открытого ключа) необходимая для работы.

2) **Персональный компьютер** с операционной системой Windows 7 и выше с установленным пакетом .Net Framework 4.5 и выше.

Системные требования ПК:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 512 Мбайт.
- Свободное место на жестком диске — не менее 100 Мбайт.

II. Программное обеспечение

1) **Веб-браузер** — Internet Explorer 10 или более поздней версии, Edge, Google Chrome, Mozilla Firefox, Opera, Яндекс.Браузер, браузер «Спутник» последних версий.

2) **VipNet PKI Client**

ViPNet PKI Client — универсальный программный комплекс, который решает основные задачи пользователя при работе с сервисами использующие:

- заверение документов электронной подписью;
- шифрование файлов;
- аутентификацию пользователей для доступа к веб-сервисам;
- построение защищенных TLS-соединений.

В состав ViPNet PKI Client входят следующие компоненты:

- File Unit – компонент для работы с файлами;
- Web Unit – компонент для работы с данными, передаваемыми браузерами;
- CRL Unit – компонент для обеспечения актуальности требуемых для работы с сертификатами CRL;
- Certificate Unit – компонент для управления жизненным циклом сертификатов, менеджер сертификатов.

- ViPNet CSP - провайдер криптографических функций.

Данный программный продукт имеет **платную** лицензию. Продукт установлен на **кафедральных компьютерах** (которые администрируются системными администраторами корпуса), а также в **деканате.** При необходимости установки данного ПО на личный компьютер можно подать заявку руководителю Удостоверяющего центра.

III. Также для корректной работы на компьютере должен быть установлен актуальный **корневой сертификат**.

Получение и установка корневого сертификата рассмотрена в разделе 2 данного руководства.

Алгоритм действий пользователя после получения ключа и дополнительная информация.

Первоначальный алгоритм действия пользователя:

1) Инициализация контейнера. (Пункт 1 Руководства)
2) Смена пароля доступа к контейнеру (при необходимости). (Пункт 2 Руководства)
3) Работа с ЭЦП в старом знакомом режиме (в некоторых случаях будет необходимо повторно указать путь к контейнеру ключа). Шаги подписания также отражены в руководстве.

После возврата USB-flash-накопителя пользователю на устройстве будет находиться папка **/infotecs/containers**. В ней будет находиться контейнер закрытого ключа. Внутри контейнера находится и открытый ключ, то есть сертификат пользователя. Грубо говоря, эти два файла и представляют собой электронную цифровую подпись (ЭЦП) пользователя.

За сохранность (предотвращение несанкционированного доступа) контейнера **отвечает пользователь**. После получения ЭЦП настоятельно **рекомендуется сменить пароль** доступа к контейнеру.

Внимание! В случае если вы забудете пароль доступа к контейнеру, никто не сможет получить к нему доступ. Администратор не имеет возможности восстанавливать пользовательские пароли по причинам безопасности. Если вы забыли пароль и не имеете возможности его восстановить – необходимо подать заявку на создание нового сертификата.

В случае если произошла компрометация (факт доступа постороннего лица к ЭЦП, а также подозрение на него.) имеется возможность отозвать сертификат (подать соответствующую заявку в УО ИКИТ Сомовой М.В.). Скомпрометированный ключ окажется в списках отзыва, и злоумышленник больше не сможет воспользоваться старой ЭЦП.

1. Инициализация контейнера

Первоначально, каждому пользователю необходимо инициализировать контейнер ключа.

Рассмотрим порядок инициализации контейнера на внешнем накопителе. Контейнер закрытого ключа должен находиться на внешнем USB-flash-накопителе в папке **<том накопителя>:\ infotecs\containers.**

Откройте программу VipNet CSP, нажмите кнопку “Добавить контейнер…”

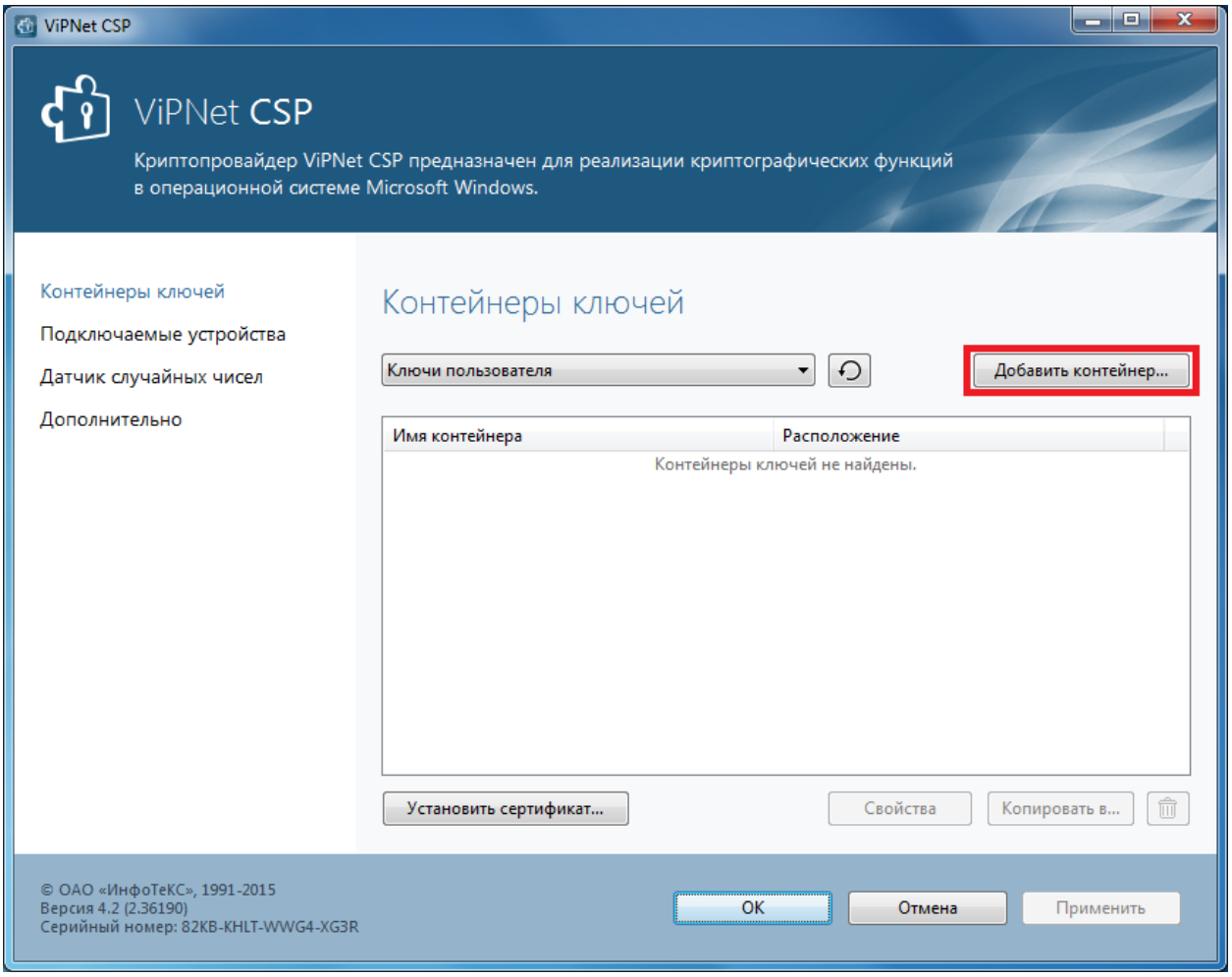

Рисунок 1 – Главное окно программы VipNetCSP, добавление контейнера

После чего откроется окно инициализации контейнера ключей, нажмите кнопку “Обзор…”.

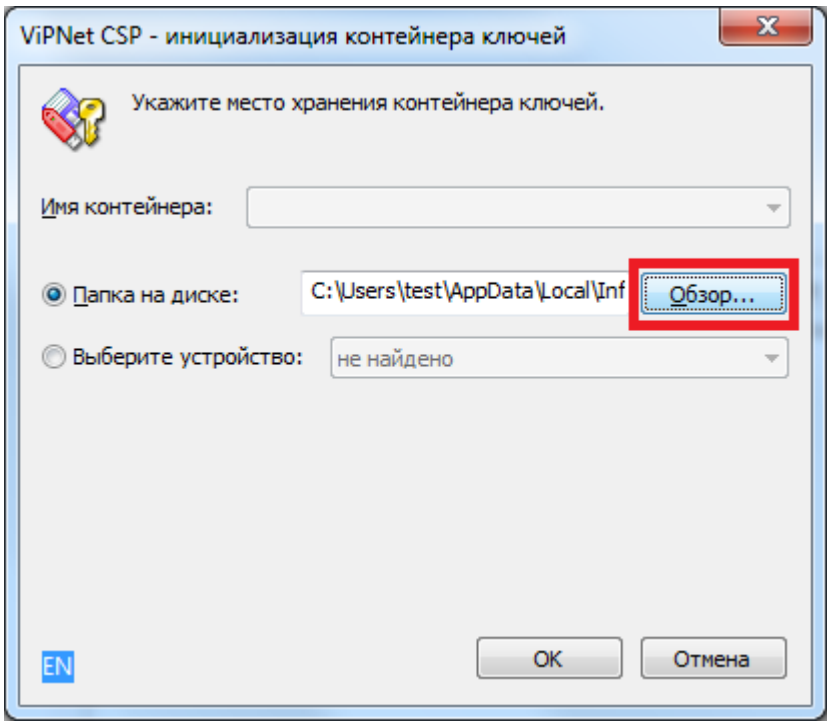

Рисунок 2 – Инициализация контейнера ключей, обзор

Выберите папку на USB-flash-накопителе. Очередной раз обращаем ваше внимание, что контейнер пользователя **должен располагаться по адресу папке <том накопителя>:\infotecs\containers**

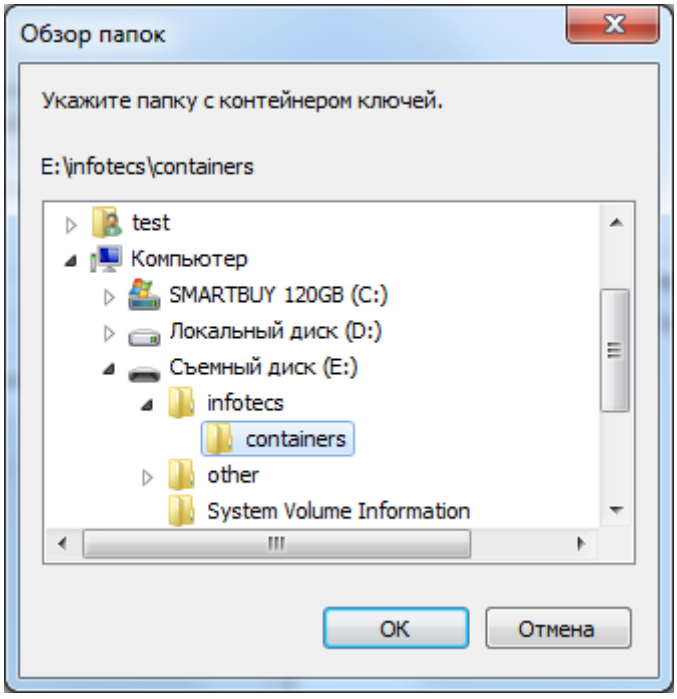

Рисунок 3 – Выбор папки

После того как папка с контейнером была выбрана, нажмите “ОК”.

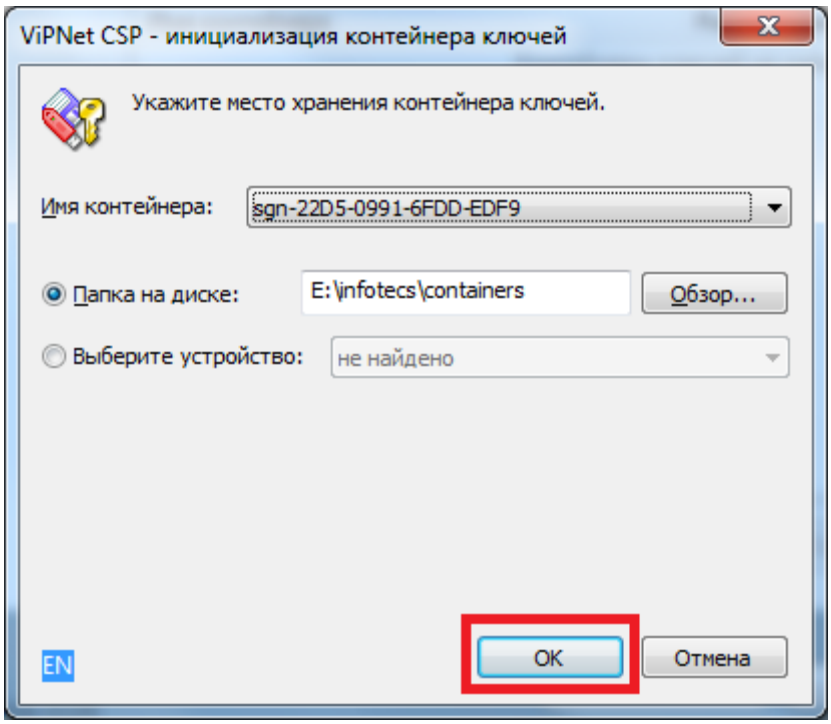

Рисунок 4 – завершение выбора контейнера

После чего вам будет предложено установить сертификат в системное хранилище текущего пользователя, нажмите “Да”.

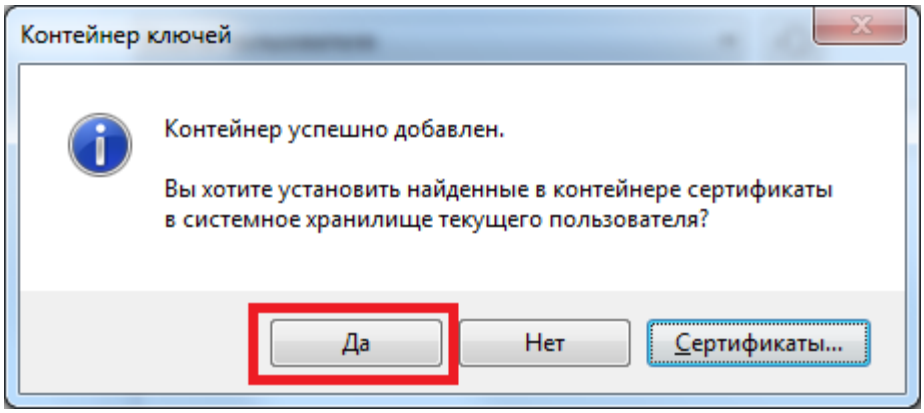

Рисунок 5 – Установка сертификата пользователя в системное хранилище

Дождитесь уведомления об успешном добавлении сертификата.

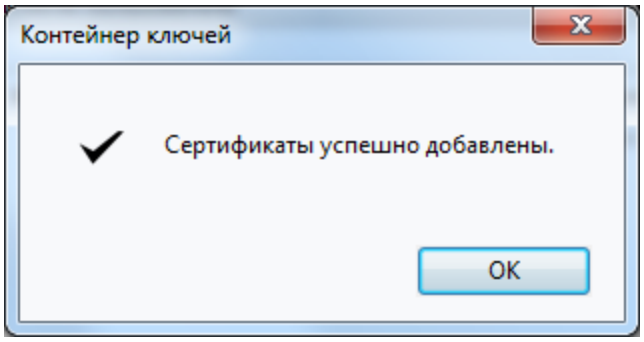

Рисунок 6 – Успешное добавление сертификата

2. Изменение пароля контейнера закрытого ключа

После того как контейнер был проинициализирован, имеется возможность сменить пароль доступа к нему.

Откройте программу VipNet CSP, выберите контейнер и нажмите свойства.

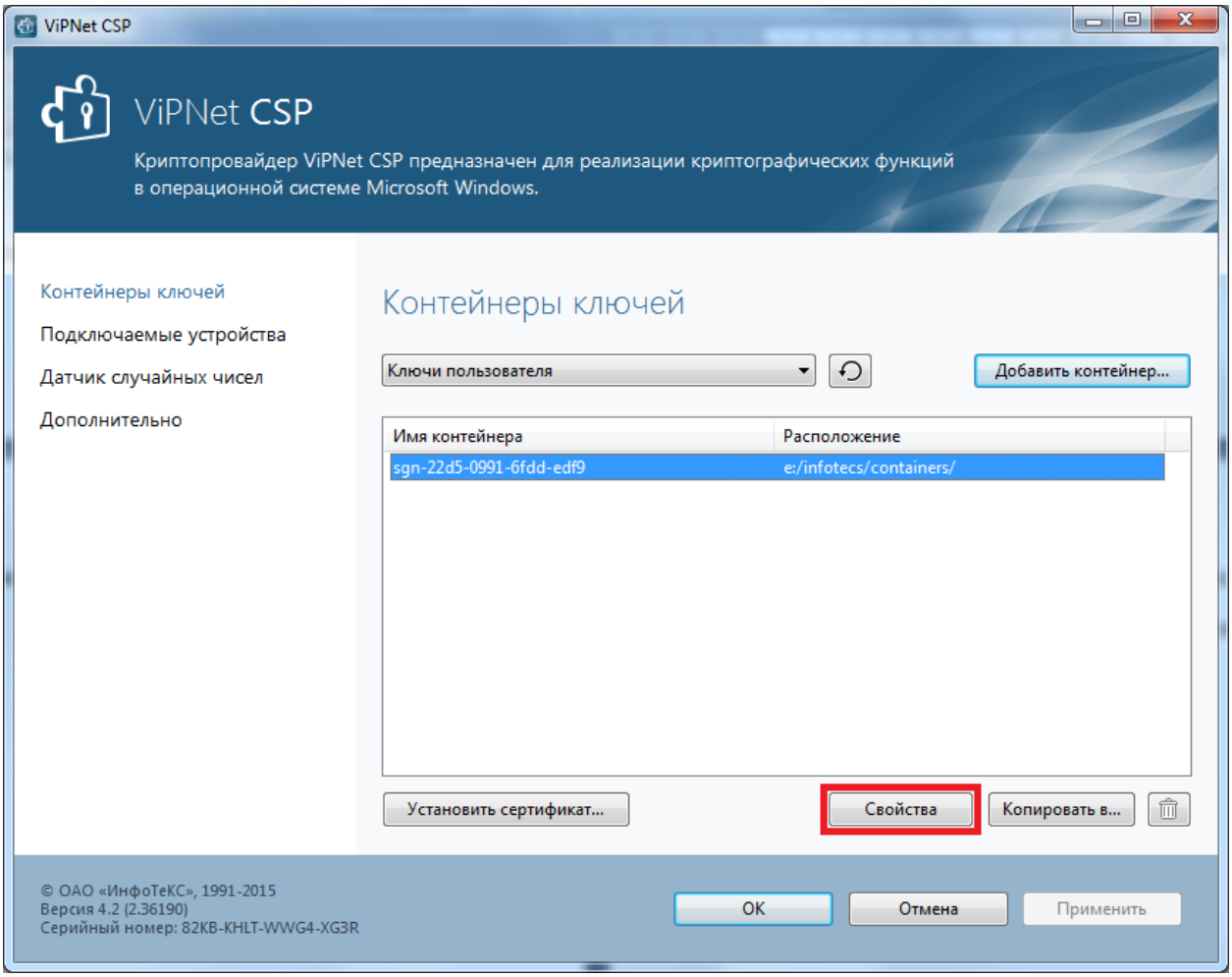

Рисунок 7 – Главное окно программы VipNetCSP, кнопка свойств

В открывшемся окне нажмите кнопку “Сменить…”

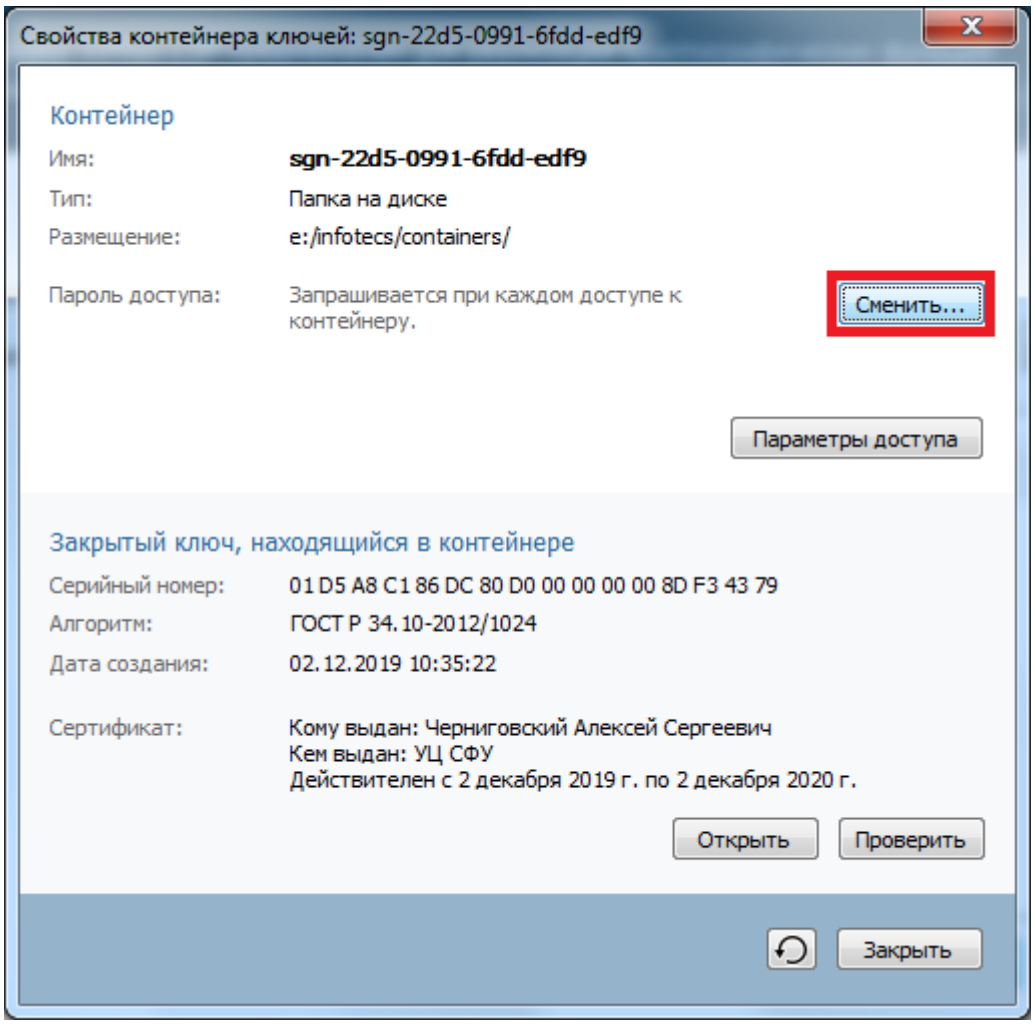

Рисунок 8 – Свойства контейнера ключей, смена пароля доступа

В открывшемся окне введите старый пароль (по умолчанию пароль доступа к контейнеру имеет стандартный пароль доступа **12345678**), после чего введите новый пароль и повторите его. Новый пароль должен быть не короче шести символов, других требований нет. Обратите внимание на язык, на котором вы задаете новый пароль. Сохраните и запомните пароль, в случае если вы его забудете, процедура его восстановления или “сброса” отсутствует. После ввода нажмите “ОК”.

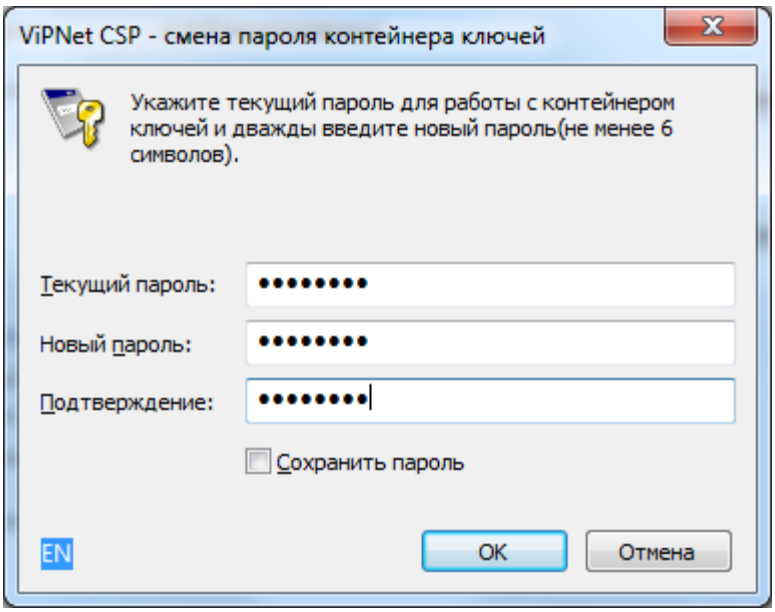

Рисунок 9 – Смена пароля контейнера ключей

После смены пароля закройте окно свойств.

3 Проверка наличия личного сертификата пользователя на компьютере

Перед подписанием документов с помощью ЭЦП необходимо убедиться, что на компьютере уже установлен сертификат проверки электронной подписи в хранилище личных сертификатов. Сделать это можно следующим образом:

Запустите Internet Explorer, выберите “Настройки” (значок шестерёнки) - “Свойства браузера”.

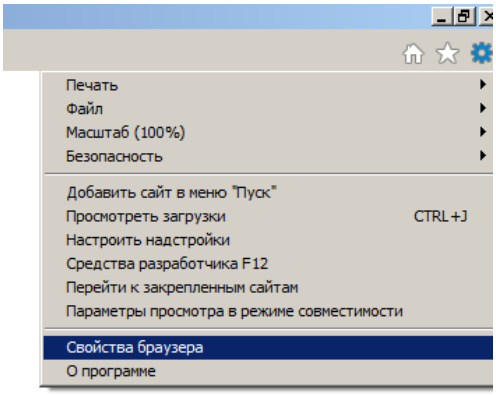

Рисунок 10 – Контекстное меню “Настройки” Internet Explorer

В открывшемся окне выберите вкладку “Содержание” и нажмите “Сертификаты”.

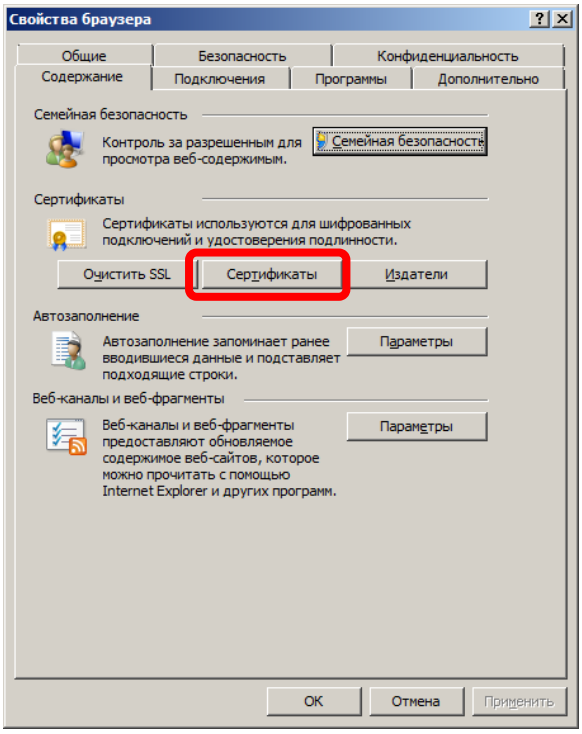

Рисунок 11 – Свойства браузера

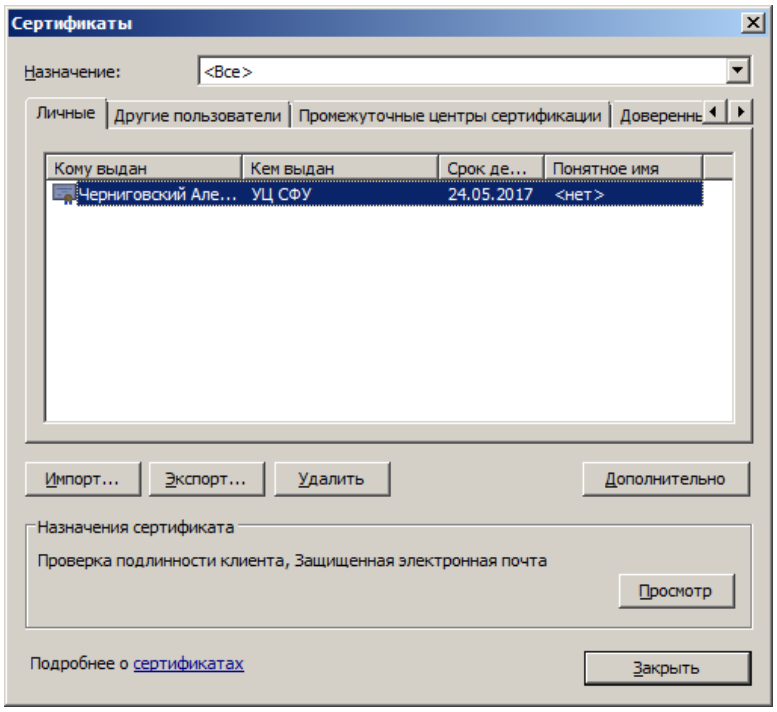

Рисунок 12 – Сертификаты

В открывшемся окне убедитесь, что во вкладке “Личные” находится ваш сертификат. Иначе перейдите к четвертому пункту данного руководства и установите свой личный сертификат в личное хранилище.

4 Установка корневого сертификата

Получите корневой сертификат от администратора или скачайте его самостоятельно.

Для того чтобы найти адрес доступа к корневому сертификату, необходимо через программу VipNetCSP открыть окно свойств сертификата открыть сертификат.

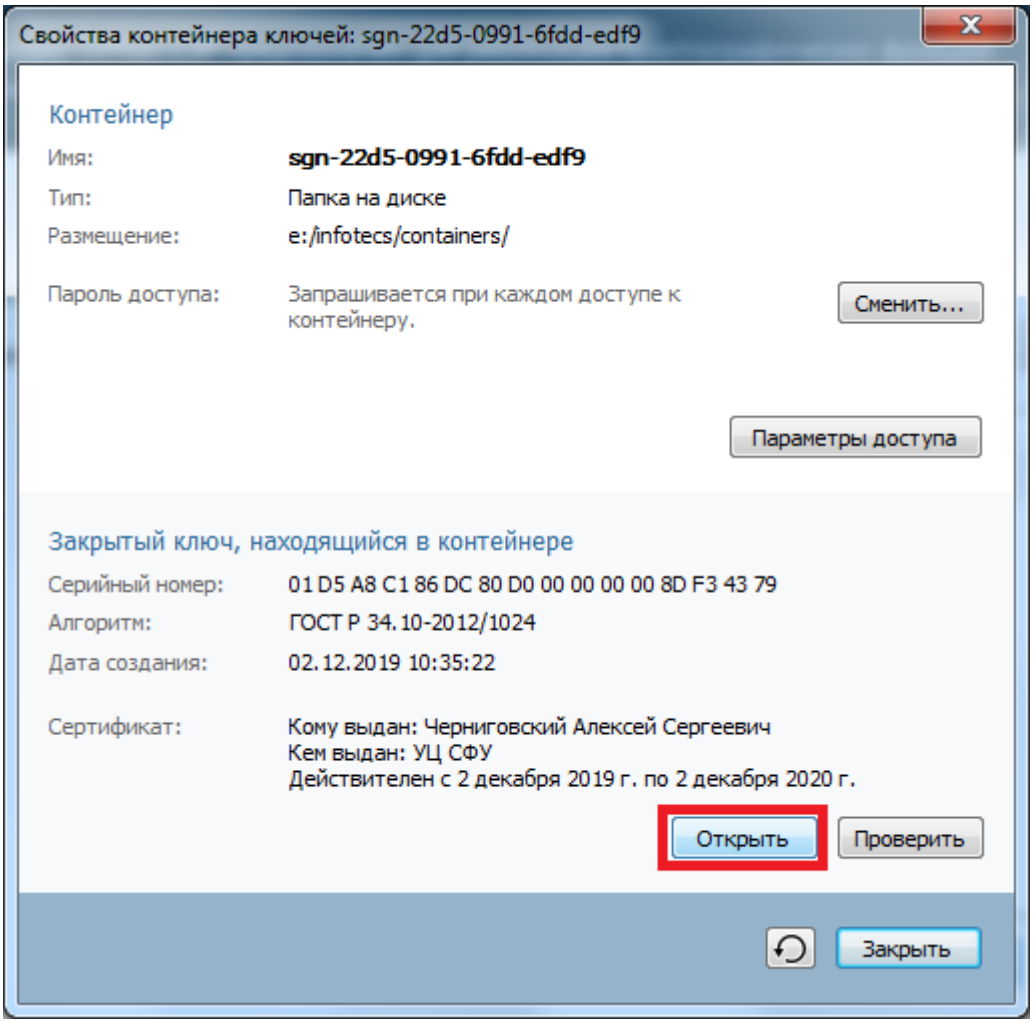

Рисунок 13 – Окно свойств корневого сертификата

Внутри каждого сертификата пользователя существует поле “Доступ к сведениям центра сертификации” (Рис. 14)

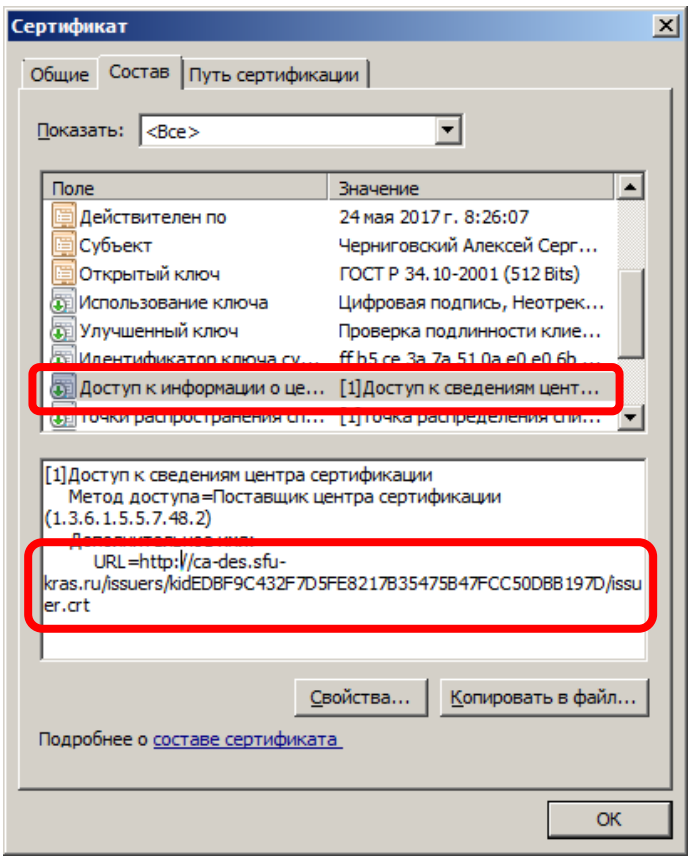

Рисунок 14 – Окно свойств сертификата пользователя

Данное поле содержит URL, после копирования которого в браузерную строку можно скачать корневой сертификат.

Дважды нажимаем на полученный сертификат левой (основной) кнопкой мыши, откроется следующее окно:

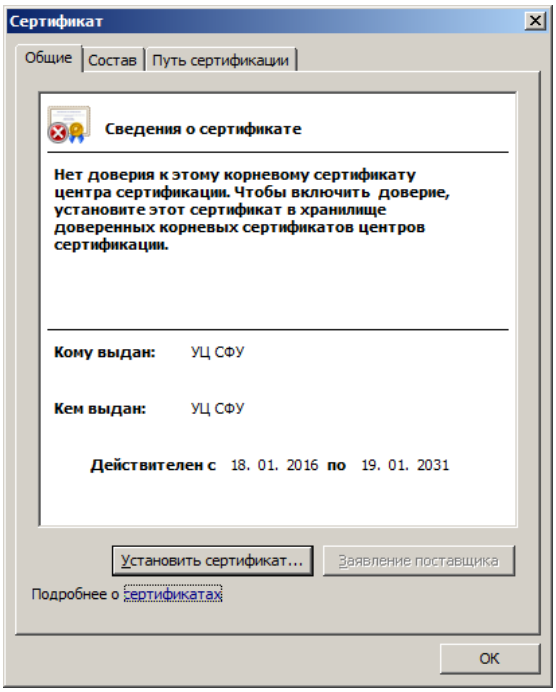

Рисунок 15 – Окно свойств корневого сертификата

Сертификат необходимо поместить в хранилище доверенных сертификатов, сейчас в поле “Сведений о сертификате” мы видим, что ему нет доверия. Включим его в список доверенных. Для этого нажимаем “Установить сертификат…”.

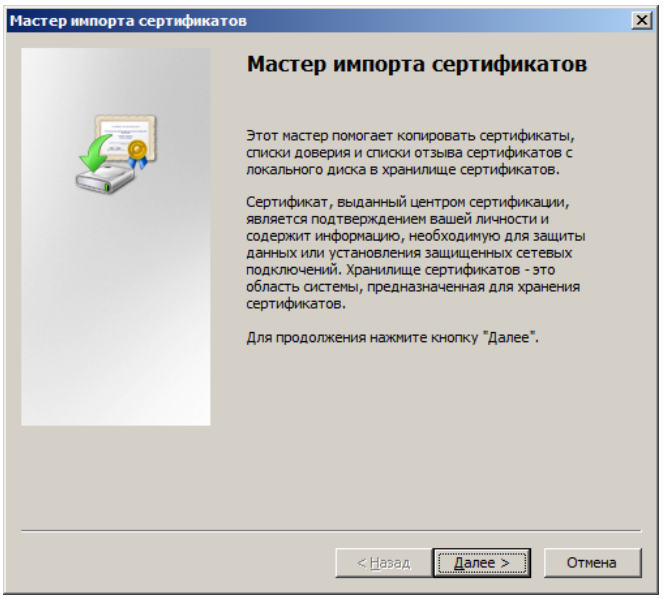

Рисунок 16 – Окно приветствия мастера импорта сертификата

Нажимаем “Далее”.

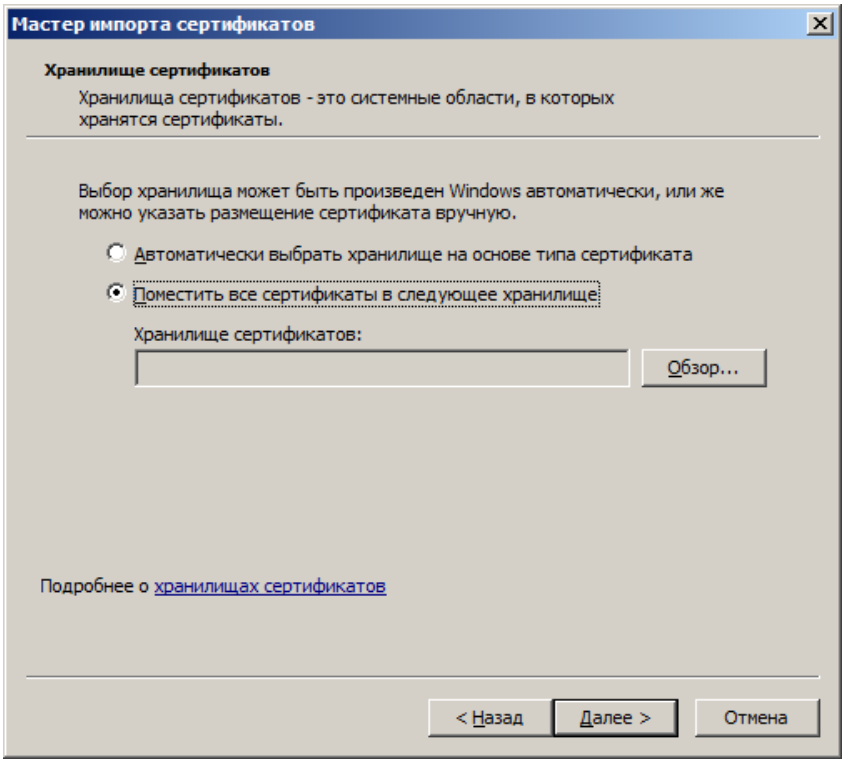

Рисунок 17 – Окно мастера импорта сертификата

Выбираем “Поместить все сертификаты в следующее хранилище” и нажимаем обзор.

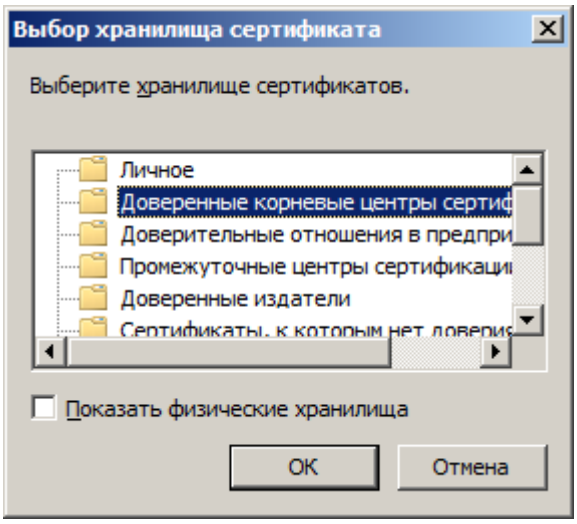

Рисунок 18 – Выбор хранилища сертификата

В открывшемся окне (Рис. 18) выбираем “Доверенные корневые центры сертификации”. Нажимаем “ОК”.

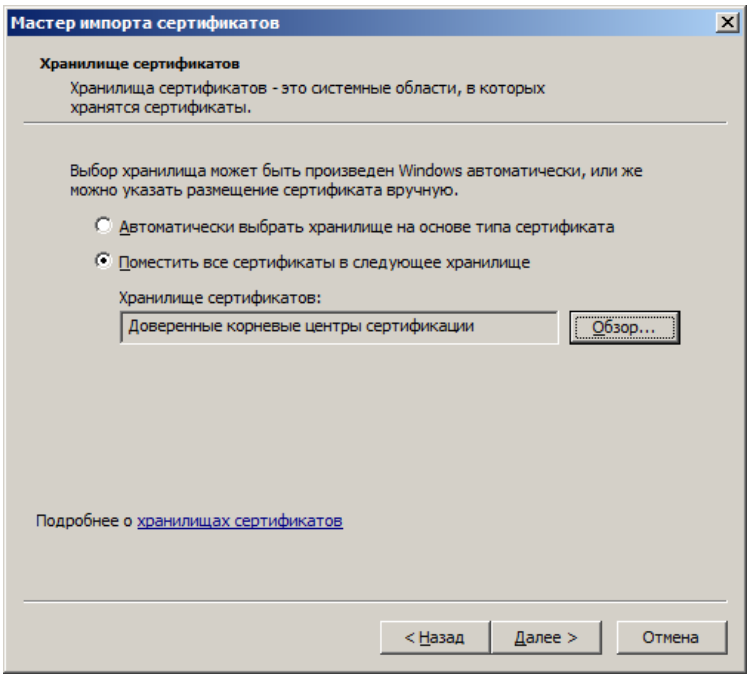

Рисунок 19 – Мастер импорта с выбранным хранилищем

После того, как хранилище выбрано, нажимаем “Далее”.

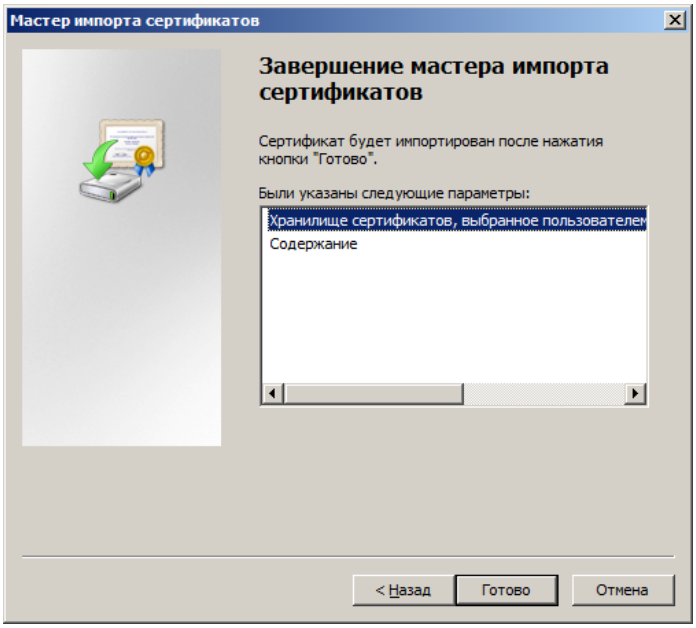

Рисунок 20 – Завершение мастера импорта сертификатов

Откроется окно завершения мастера импорта сертификатов (Рис. 20). Нажимаем “Готово”.

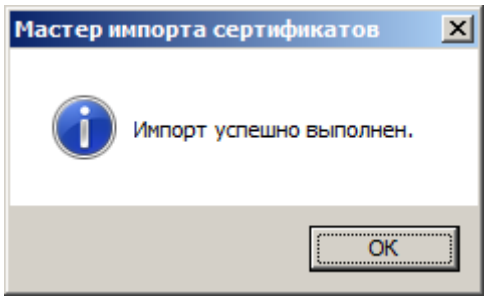

Рисунок 21 – Уведомление об успешном импорте

По окончанию должно появиться уведомление об успешном импорте (Рис. 21).

Снова дважды нажмём на сертификате левой (основной) кнопкой мыши и посмотрим сведения о нём (Рис. 22).

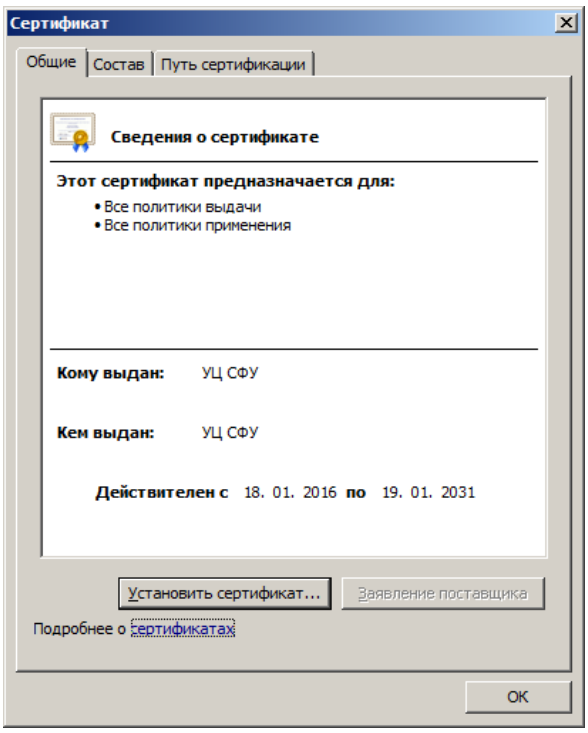

Рисунок 22 – Окно свойств сертификата после помещения в хранилище доверенных корневых сертификатов

Теперь сертификат является доверенным, сообщение о том, что ему нет доверия - отсутствует.

5 Пошаговый пример подписания документа в системе АСУ ИКИТ (dec.sfu-kras.ru/cabinet)

1) В строке ввода web-браузера введите следующий url-адрес:

http://dec.sfu-kras.ru/cabinet/

После загрузки страницы появится окно авторизации:

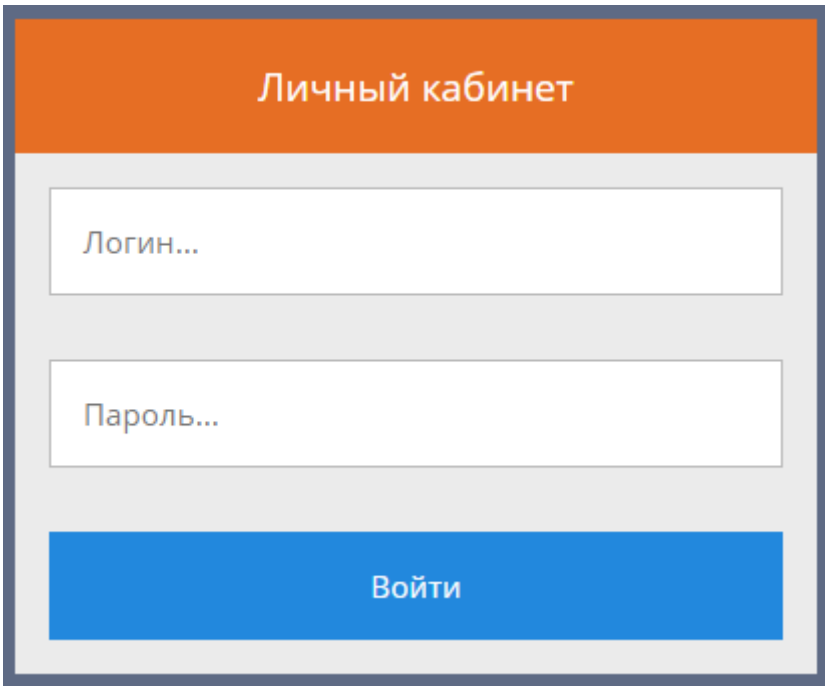

Рисунок 23 – Окно авторизации

2) В появившемся окне авторизации введите ваш логин и пароль аккаунта СФУ (данные для подключения wi-fi и сервисов СФУ).

Проверить состояние аккаунта (возможно заблокирован в связи с необходимостью смены пароля), сменить пароль или получить дополнительную информацию о своем аккаунте СФУ можно по адресу: https://users.sfu-kras.ru/

3) В левом верхнем углу выберите вкладку “Преподаватель” (Рис. 24)

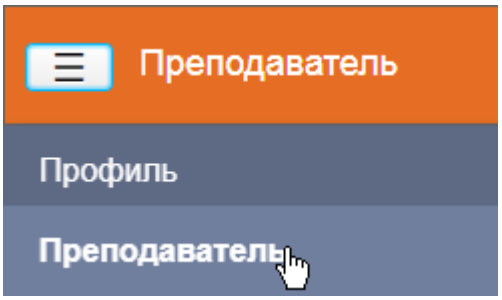

Рисунок 24 – Вкладка преподаватель

4) Выберите ведомость для редактирования и последующего подписания нажав соответствующую кнопку “Ведомость” (Рис 25)

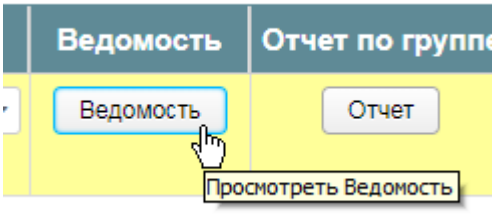

Рисунок 25 – Кнопка просмотра ведомости

5) Проставьте оценки студентам. Тщательно проверьте, верно ли вами заполнены все поля. Нажмите кнопку “Подписать ведомость” в правом нижнем углу (Рис. 26).

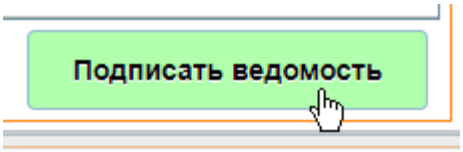

Рисунок 26 – Кнопка подписания ведомости

Появится информационное сообщение, для того чтобы не нажать кнопку случайно.

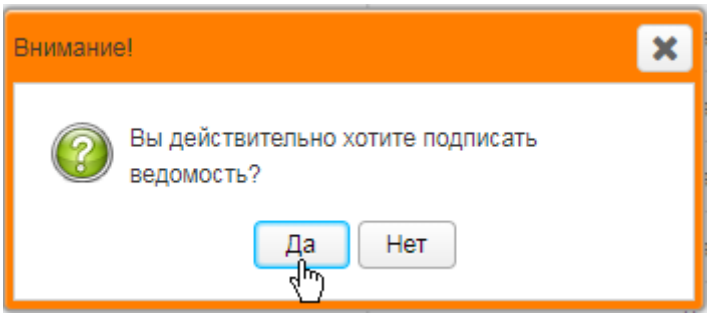

Рисунок 27 – Кнопка подписания ведомости

Подтверждаем, что мы действительно хотим подписать ведомость.

6) После этого будет сформирована печатная версия ведомости - документ формата *.pdf. Тщательно просмотрите документ, при несоответствии печатного документа ранее заполненным данным обратитесь в учебное управление или направьте обращение разработчикам (раздел обратная связь).

В случае верно заполненных данных нажмите кнопку “Подписать” в правом верхнем углу открывшегося окна (Рис. 28).

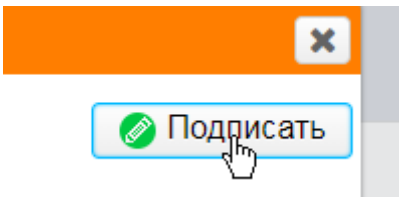

Рисунок 28 – Кнопка подписания документа

7) После чего откроется окно выбора сертифката для подписи программы VipNet PKI Client Web Unit (Рис. 29), которая входит в поставку VipNet PKI Client.

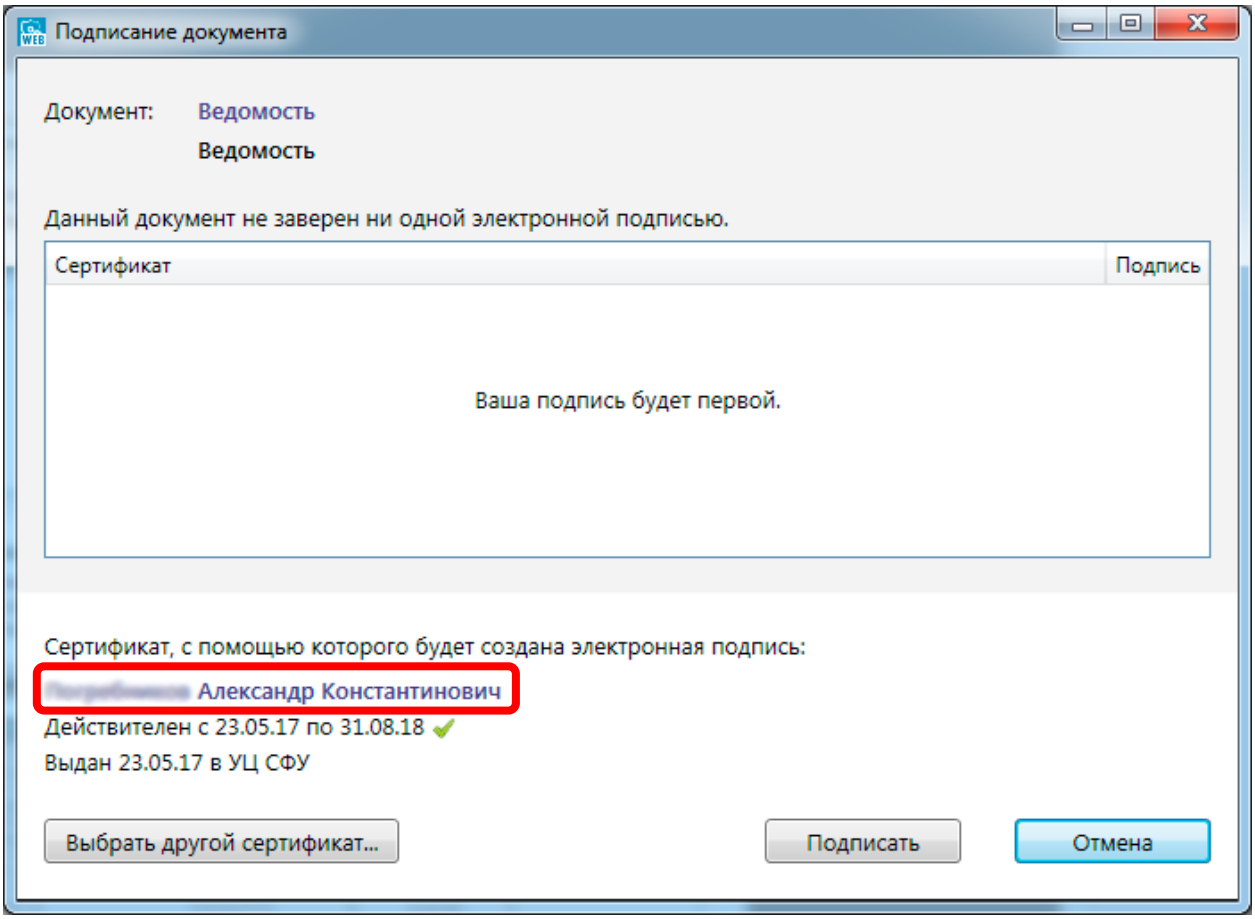

Рисунок 29 – Окно выбора сертификата для подписи

Удостоверьтесь, что выбран Ваш сертификат (Отмечен красной рамкой на Рис. 29) в ином случае нажмите кнопку “Выбрать другой сертификат…”

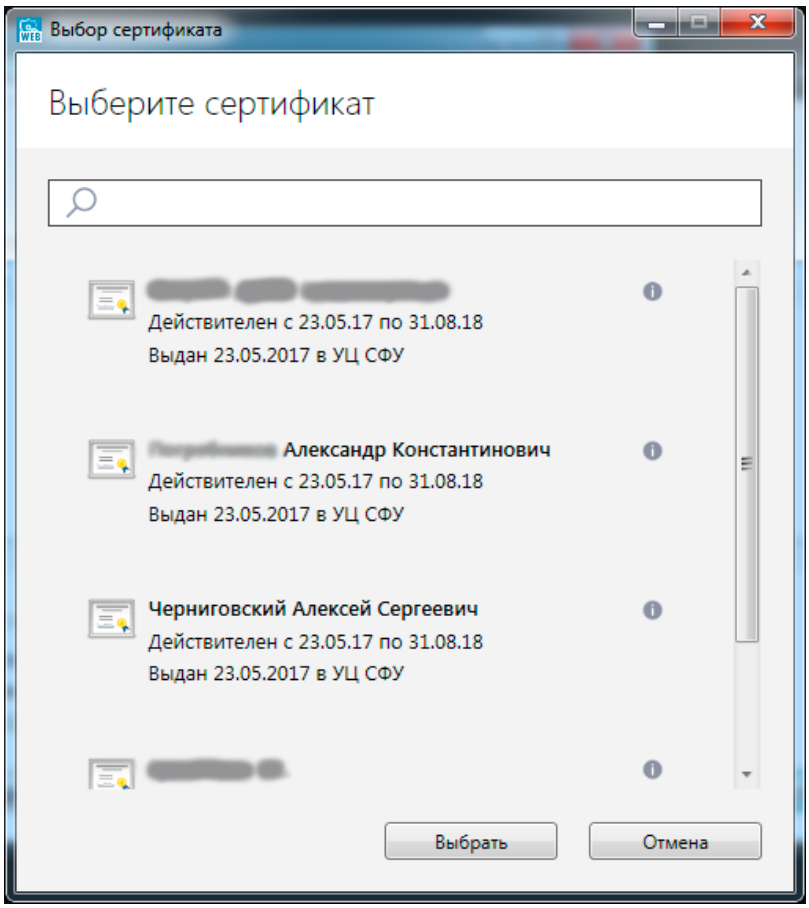

Рисунок 30 – Выбор сертификата

В открывшемся окне найдите свой сертификат (начните печатать свою фамилию в поле ввода и будут выведены совпадения) и нажмите кнопку “Выбрать”.

8) После выбора своего личного сертификата для подписи нажмите кнопку подписать (Рис. 29).

9)* В случае, если сменился том устройства, VipNetCSP может заново запросить путь к контейнеру закрытого ключа.

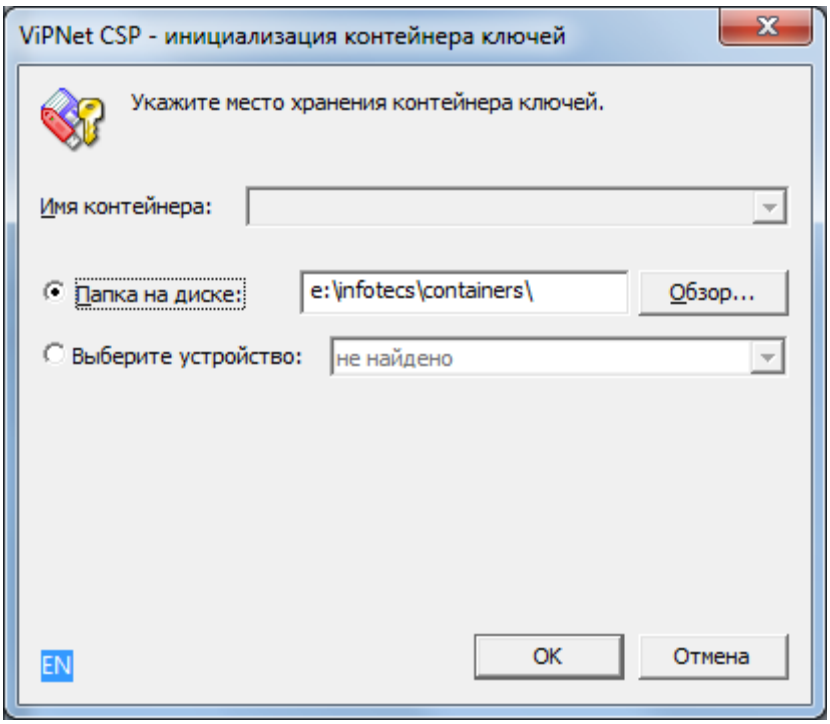

Рисунок 31 – Повторный запрос пути к контейнеру закрытого ключа

Выберите вновь папку /infotecs/containers и нажмите “ОК”. После чего откроется окно ввода пароля контейнера.

Если том устройства не был изменен, то повторный выбор пути к контейнеру не потребуется.

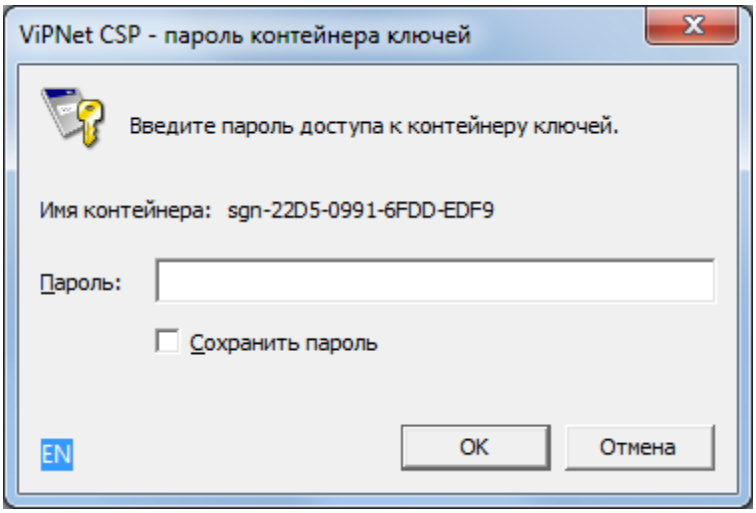

Рисунок 32 – Ввод пароля контейнера закрытого ключа

10) Введите пароль от контейнера на который вы выбрали в пункте 2 настоящего руководства. Если же вы не меняли пароль, то введите пароль по умолчанию – 12345678.

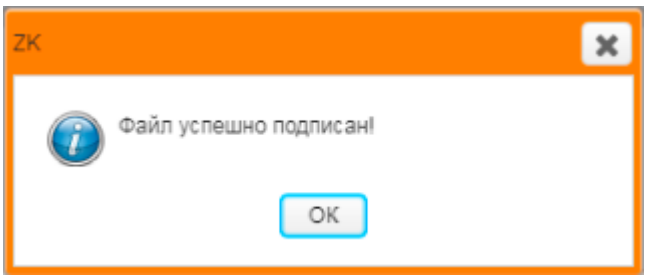

Рисунок 33 – Сообщение об успешном подписании документа

11) В случае успешного подписания документа будет выведено сообщение (Рис. 33). **Не спешите** при подписании, дождитесь данного сообщения.

Часто задаваемые вопросы

1) Моего сертификата нет в списке, после нажатия кнопки “Подписать”.

Решение: Проверьте, присутствует ли ваш сертификат в хранилище личных сертификатов. (Раздел 3 руководства) В ином случае установите его самостоятельно. (Раздел 4 руководства)

2) При подписании выдается сообщение, что мой сертификат не действителен.

Решение: Проверьте, верно ли установлен корневой сертификат. В случае его отсутствия обратитесь к администратору или установите его самостоятельно. (Раздел 2 руководства)

Если при удовлетворении вышесказанных условии ошибка не была исправлена - обратитесь к администратору.

3) При нажатии кнопки подписать выдается сообщение “Ошибка при подписании. Запустите программу для электронной цифровой подписи!”

Решение: **З**апустите вручную компонент программы VipNet PKI Client, который называется VipNet PKI Client Web Unit. Найти его можно в меню “Пуск” - Все программы. После его успешного запуска будет выдано следующее сообщение в системном трее Windows (Рис. 42)

Рисунок 42 – Сообщение об успешном запуске компонента VipNet PKI Client Web Unit

Обратная связь

По вопросам о ЭЦП обращаться по электронному адресу: achernigovskiy@sfu-kras.ru

Просим обратить внимание, что на данный адрес принимаются только технические вопросы, касающиеся подписания документов, установке сертификатов и конфигурации компьютера для подписания.

Все вопросы, касающиеся АСУ ИКИТ (dec.sfu-kras.ru/cabinet) отправляются на адрес разработчиков данного сервиса dec.developers@gmail.com .

По вопросам, касающимся учебного процесса, в частности “отзывам” неверно подписанных ведомостей и открытию новых, просим обращаться в УО ИКИТ к Сомовой М.В.