Инструкция по созданию ключа электронной подписи и запроса на сертификат с помощью ViPNet CSP

Исходные данные: ключевой носитель eToken или Rutoken, персональный компьютер с доступом в Интернет

1 Установка программного обеспечения.

Скачать и установить:

1. Драйверы для ключевого носителя:

eToken – http://www.aladdin-rd.ru/support/downloads/26037/ или

Rutoken – http://www.rutoken.ru/support/download/drivers-for-windows/

Внешний вид eToken

Внешний вид Rutoken

По требованиям безопасности необходимо размещать ключ электронной подписи на защищенном носителе типа eToken или Rutoken.
Если планируется размещать ключ электронной подписи на незащищенном носителе - жестком диске персонального компьютера или флэш-карте, то драйверы устанавливать не требуется.

2. ViPNet CSP 4.x по ссылке

http://infotecs.ru/downloads/product_full.php?id_product=2096

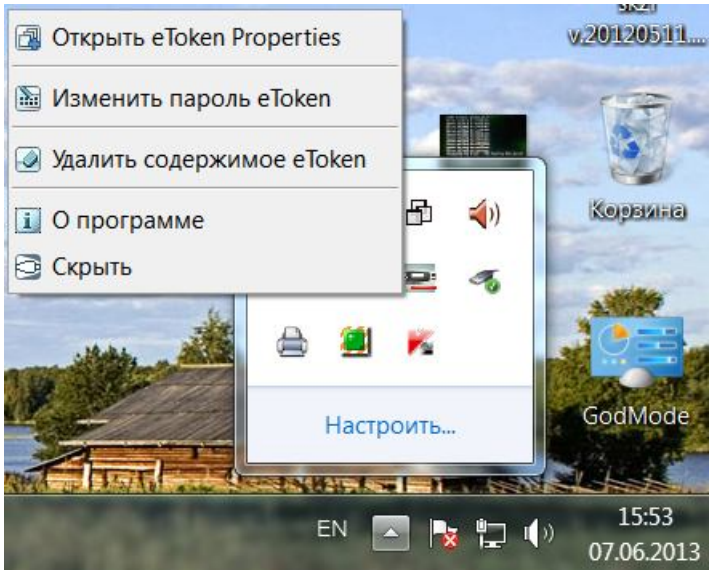
(Установка программного обеспечения осуществляется в соответствии с документацией к ПО. Документация находится на сайтах http://www.aladdin-rd.ru, http://www.rutoken.ru, http://infotecs.ru соответственно).

2 Удаление содержимого ключевого носителя

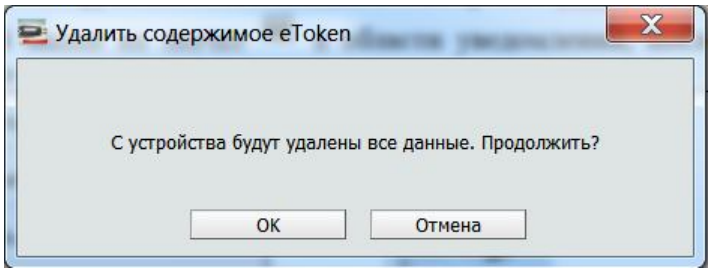
Описание процедуры удаления содержимого eToken приведено в подпункте 1, Rutoken – в подпункте 2.

1. Удаление содержимого eToken

Для удаления содержимого eToken вставьте его в исправный USB порт компьютера. Откройте настройки программы eToken PKI Client, щелкнув правой кнопкой мыши по значку  в области уведомлений, после чего появится меню следующего вида:

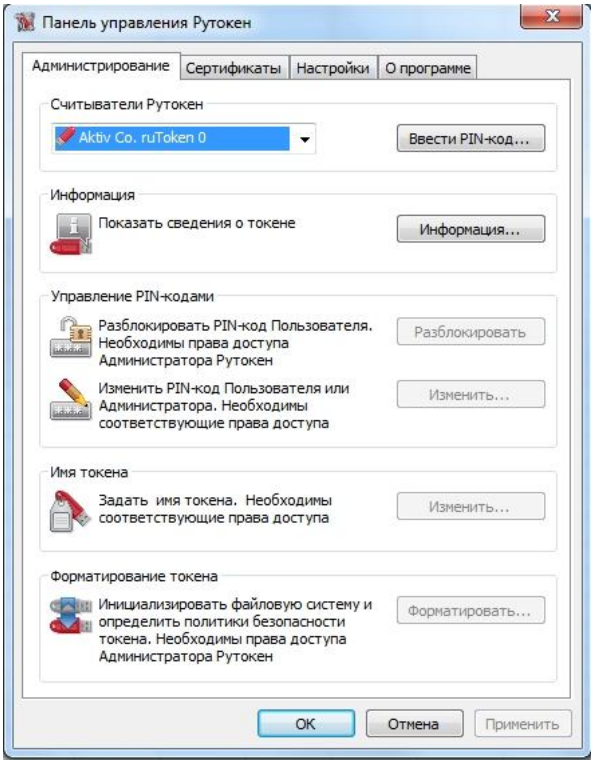


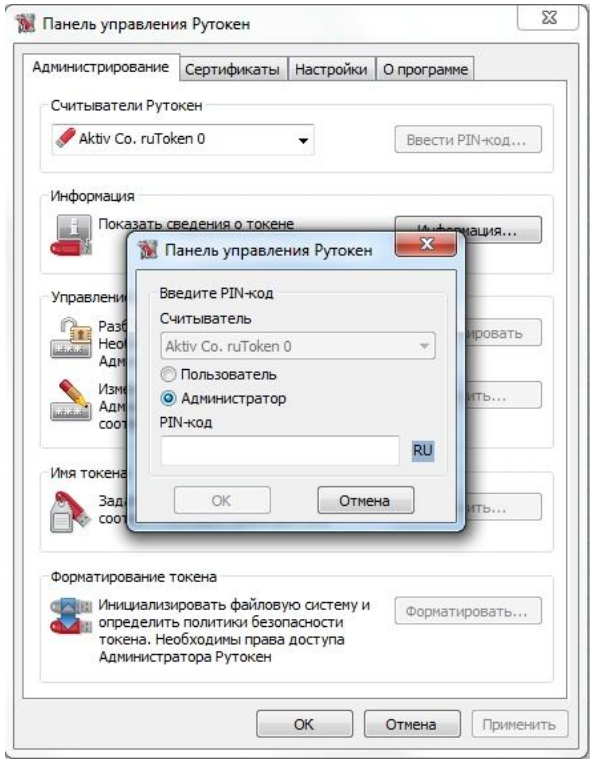
Нажмите «Удалить содержимое eToken». В очередном диалоговом окне подтвердите удаление данных и введите ПИН-код. ПИН-код был выдан при получении сертификата ключа проверки электронной подписи в удостоверяющем центре Правительства Архангельской области.



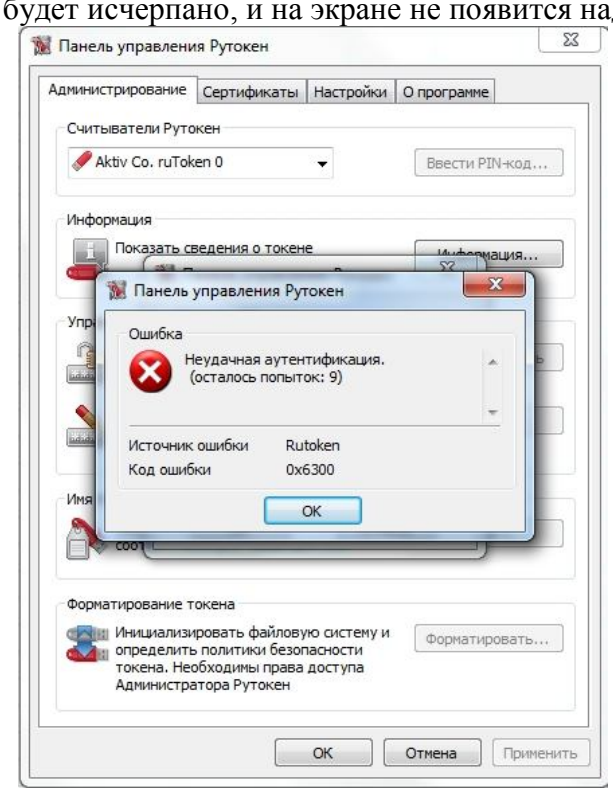
2. Удаление содержимого Rutoken

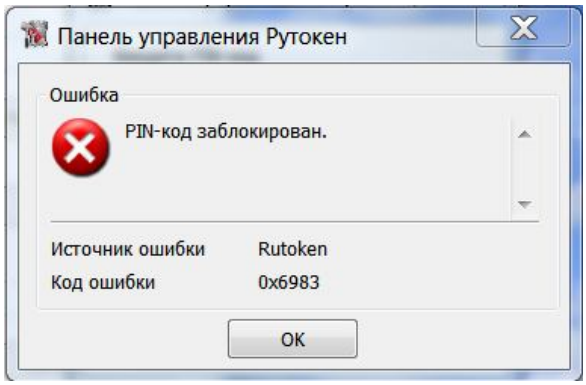
Для удаления содержимого Rutoken вставьте его в исправный USB порт компьютера. Откройте программу для настройки Rutoken – в меню «Пуск» выберите «Все программы» > Rutoken > Панель управления Рутокен. Нажмите кнопку «Ввести PIN-код…» и поставьте переключать в положение «Администратор».



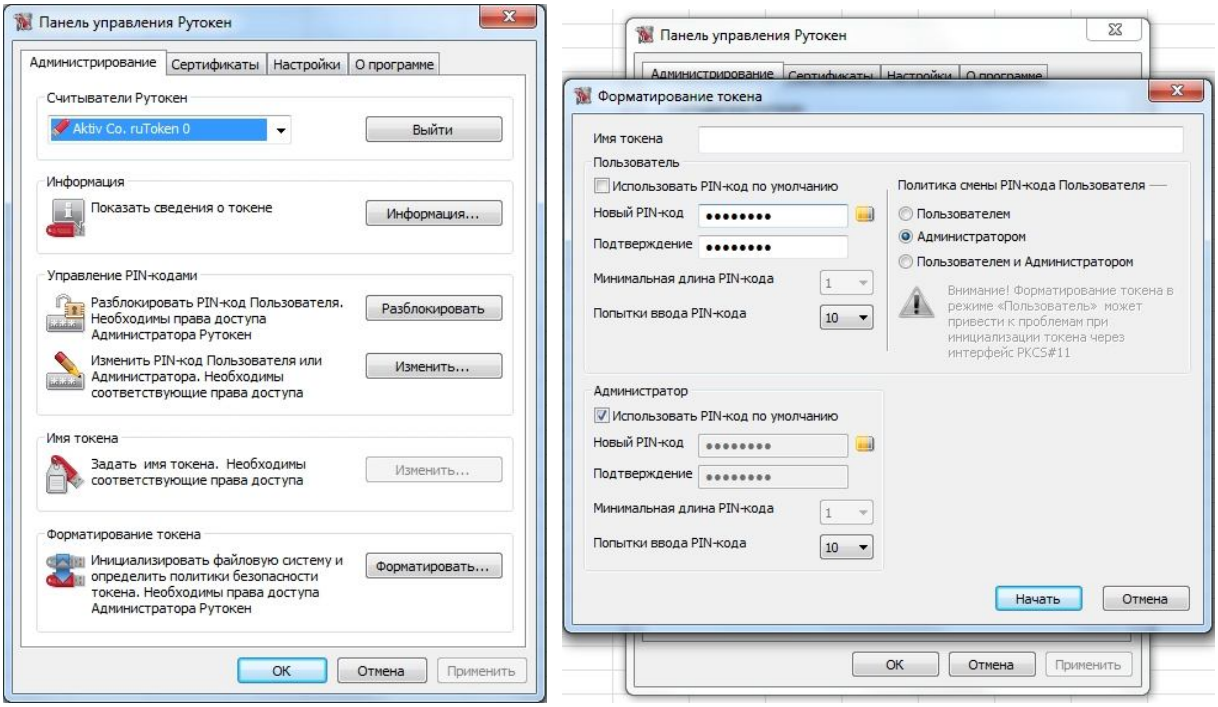


Введите в поле PIN-код цифру 1 и нажмите «ОК». На экран будет выведено сообщение о неудачной аутентификации. Повторите операцию 15 раз, пока количество попыток не будет исчерпано, и на экране не появится надпись PIN-код заблокирован.





Нажмите кнопку «Форматировать…». В поле «Новый PIN-код» и «Подтверждение» введите ПИН-код, который был выдан при получении сертификата ключа проверки электронной подписи в удостоверяющем центре Правительства Архангельской области. Остальные параметры задайте согласно рисунку ниже и нажмите кнопку «Начать».

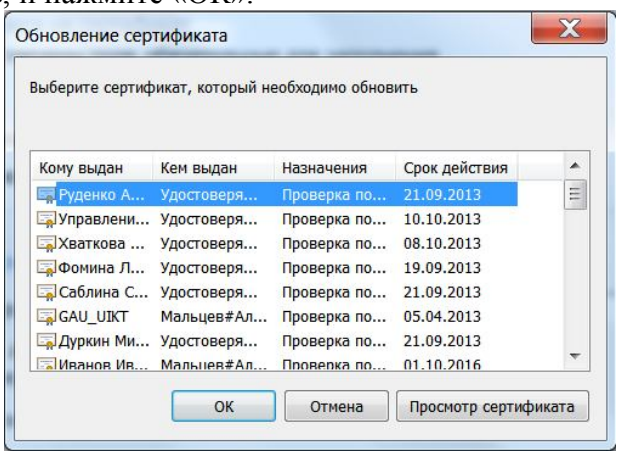


После завершения операции форматирования Панель управления Рутокен необходимо закрыть.

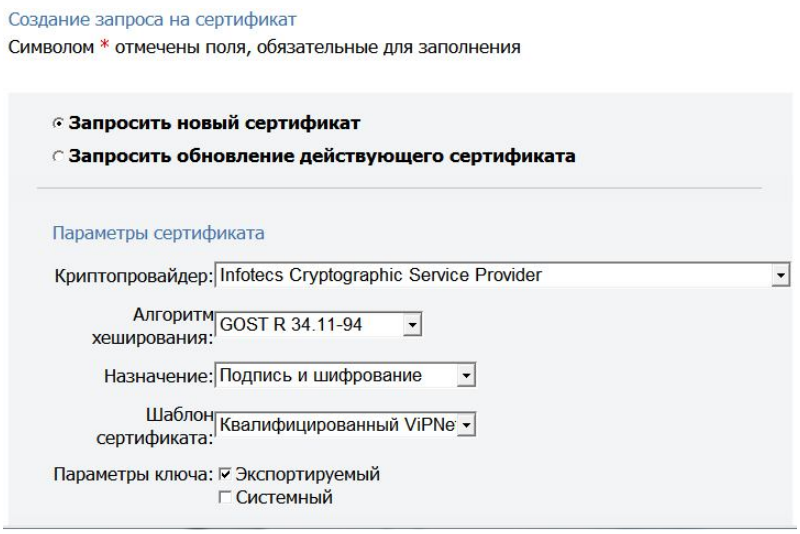
3 Создание запроса на сертификат и ключа электронной подписи

В меню «Пуск» выберите «Все программы» > ViPNet > ViPNet CSP > Создание запроса на сертификат.

В первой части окна создания запроса на сертификат выберите «Запросить новый сертификат», если требуется создать новый сертификат. Если требуется продлить истекающий сертификат, то выберите «Запросить обновление действующего сертификата». В появившемся окне укажите сертификат из списка, который необходимо обновить, и нажмите «ОК».

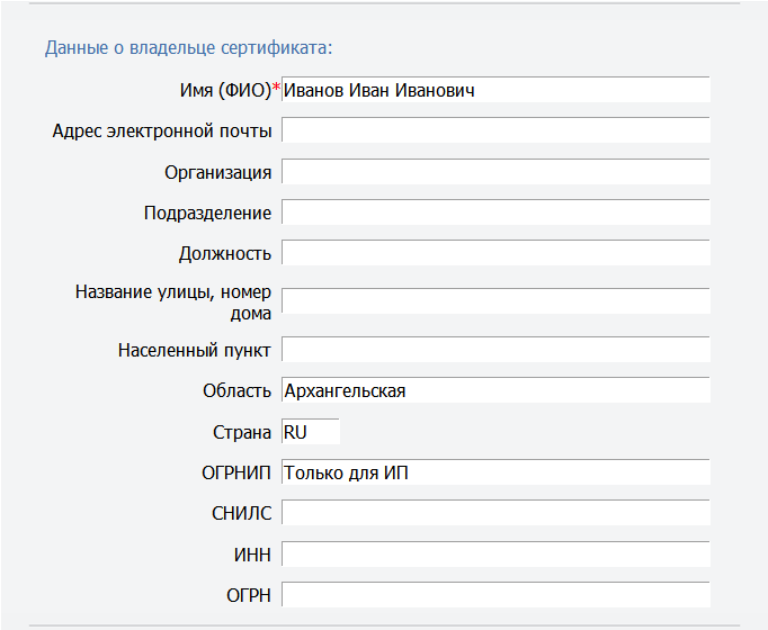


Установите «Параметры сертификата» в соответствии с приведенными ниже:

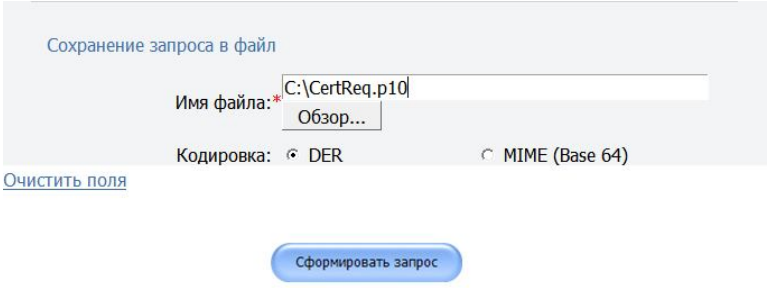


Во второй части окна заполните все данные о владельце сертификата – уполномоченном лице.

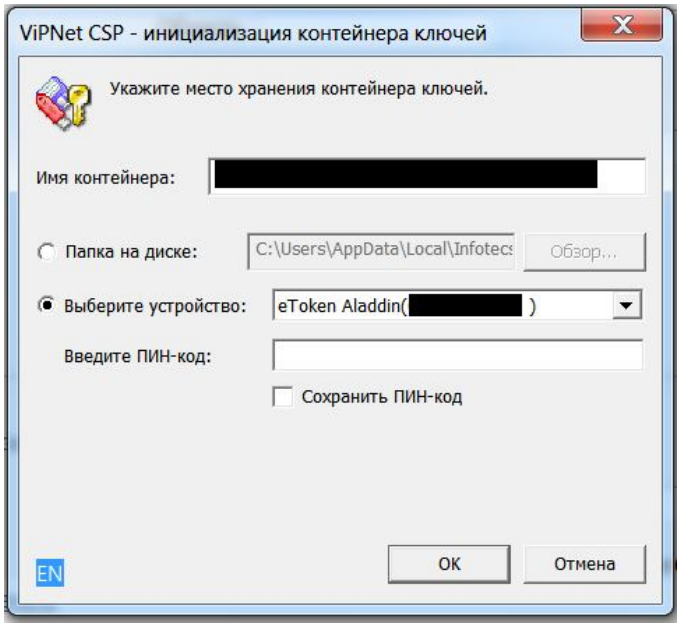
Внимание! Длина поля «Организация» составляет 64 символа. Если полное наименование организации составляет более 64 символов, то необходимо вписать краткое наименование в соответствии с Уставом или Положением.



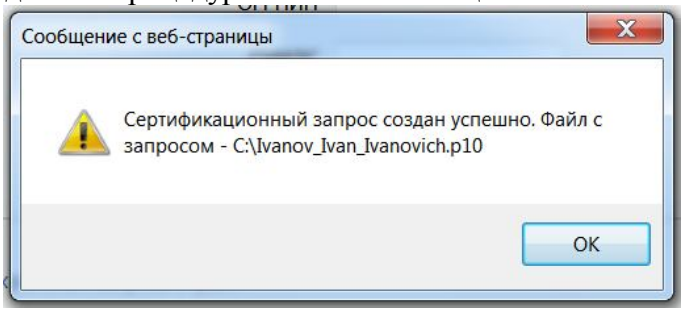
Выберите путь, имя файла для сохранения запроса на сертификат и нажмите «Сформировать запрос».



Укажите местом хранения контейнера ключей папку на диске, либо ключевой носитель eToken/ Rutoken, введите ПИН-код и нажмите «ОК».



При успешно проведенной процедуре появится сообщение.



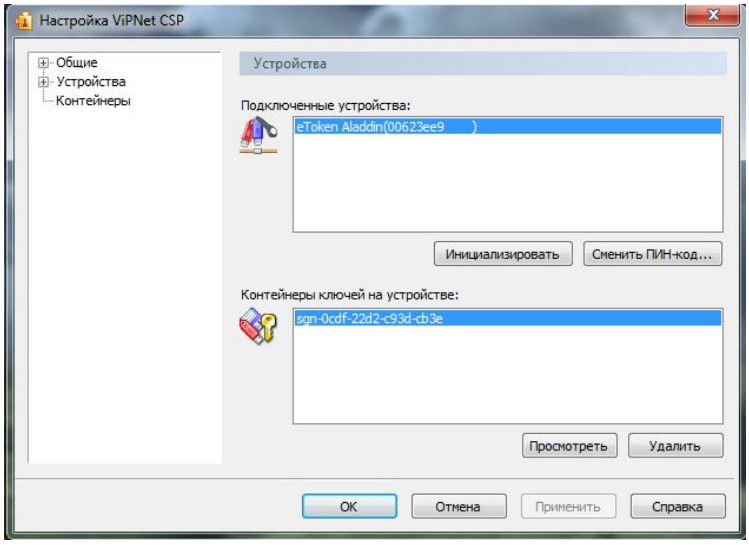
После изготовления ключа электронной подписи необходимо передать файл запроса на сертификат (с расширением *.p10) вместе с документами, описанными регламентом (http://uc2.dvinaland.ru), в удостоверяющий центр Правительства Архангельской области.

Внимание! В заявлении на изготовление сертификата ключа проверки электронной подписи в разделе «Изготовление ключа электронной подписи осуществляется» укажите «Заявителем самостоятельно».

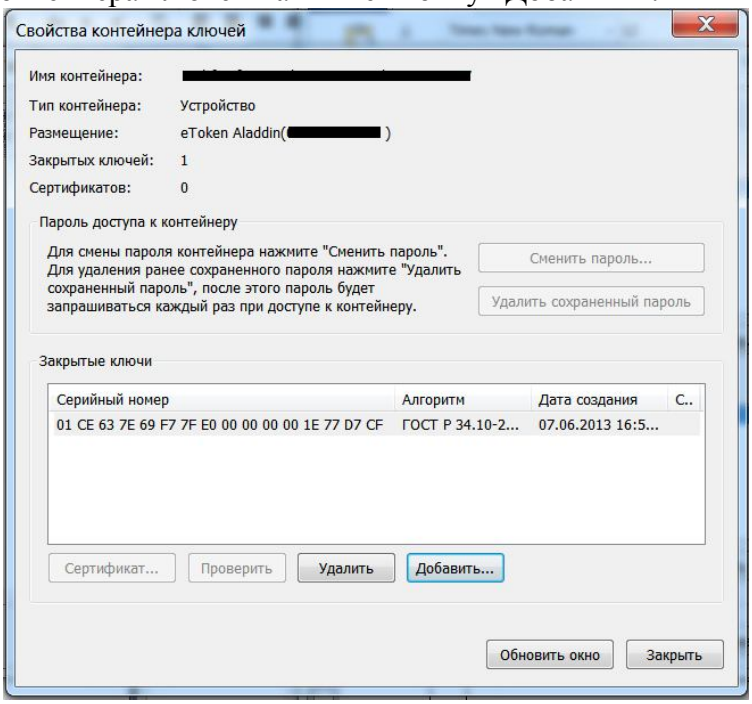
4 Помещение сертификата ключа проверки электронной подписи на ключевой носитель Rutoken/eToken.

На основе запроса на сертификат (файл с расширением *.p10) удостоверяющий центр изготовит сертификат ключа проверки электронной подписи (файл с расширением *.cer). После получения уполномоченным лицом сертификата, его необходимо поместить на ключевой носитель Rutoken/eToken.

Для этого откройте настройки ViPNet CSP («Пуск» > «Программы» > «ViPNet» > «ViPNet CSP» > «Настройка ViPNet CSP»). Выбрать пункт «Устройства». Выбрать подключенный eToken и используемый в нем контейнер ключей. Нажать кнопку «Просмотреть».



В окне свойств контейнера ключей нажмите кнопку «Добавить»:



В окне «Открыть» укажите файл сертификата, который соответствует ключу электронной подписи в контейнере, и нажмите кнопку «Открыть». Если указан верный сертификат, он будет добавлен в контейнер, в противном случае появится сообщение «Ключ не найден».

Чтобы после добавления сертификата увидеть его в окне «Свойства контейнера ключей», нажмите кнопку «Обновить окно».

5 Настройка рабочего места для использования электронной подписи

Для подготовки рабочего места к использованию новой электронной подписи необходимо воспользоваться инструкцией, размещенной в сети Интернет по адресу http://uc.dvinaland.ru (зеркало - http://uc2.dvinaland.ru)