# ИНСТРУКЦИЯ ПО УСТАНОВКЕ КОМПОНЕНТ ЭЛЕКТРОННОЙ ПОДПИСИ

СОДЕРЖАНИЕ

## ИСПОЛЬЗУЕМЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ

| Термин | Описание |
|---|---|
| ЕФРСБ | Единый федеральный реестр сведений о банкротстве |
| ЕФРСФДЮЛ | Единый федеральный реестр сведений о фактах деятельности юридических лиц |
| ПО | Программное обеспечение |
| Система | ЕФРСФДЮЛ (включая ЕФРСБ, являющийся его неотъемлемой частью) |
| УЦ | Удостоверяющий центр. Задача удостоверяющего центра – подтверждать подлинность ключей шифрования с помощью сертификатов ЭП |
| ЭП | Электронная подпись – реквизит электронного документа, предназначенный для защиты данного документа от подделки. Формируется в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи. Позволяет идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в документе |
| ЮЛ | Юридическое лицо |

# 1 Общие сведения

В Едином федеральном реестре сведений о фактах деятельности юридических лиц (далее – ЕФРСФДЮЛ)[1] вход в личный кабинет (ЮЛ, индивидуального предпринимателя, оценщика или нотариуса) осуществляется с использованием сертификата ключа проверки электронной подписи. Кроме того, размещаемые в ЕФРСФДЮЛ сообщения, созданные в личном кабинете пользователя, должны быть подписаны электронной подписью (далее – ЭП). Таким образом обеспечивается

[1] Включая Единый федеральный реестр сведений о банкротстве (далее – ЕФРСБ), являющийся его неотъемлемой частью.

неотрекаемость опубликованных сведений и их целостность (если после подписи данные были изменены, ЭП позволит доказать факт искажения информации).

# 2 Что нужно установить для подписи сведений, вносимых в ЕФРСФДЮЛ, электронной подписью

**На персональном компьютере пользователя должно быть установлено и настроено**:

**1)** Специальное программное обеспечение – средство электронной подписи – шифровальные (криптографические) средства, используемые для авторизации в Системе и создания ЭП сообщений.

Пользователь также должен иметь актуальный сертификат ключа проверки ЭП в виде электронного документа, выданный авторизованным удостоверяющим центром (далее – УЦ) и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП, уполномоченному для работы в Системе.

Инструкции по установке сертификата предоставляются УЦ.

**2)** Криптопровайдер – программное обеспечение, осуществляющее вычисление ЭП: КриптоПро (версий 3.6 - 4.0), VipNet CSP или Signal-COM CSP.

Инструкции по установке криптопровайдера предоставляются УЦ.

**3)** ActiveX-компонент для подписи сообщений и карточек ЭП. Он необходим, чтобы из браузера Internet Explorer или Mozilla Firefox можно было обратиться к криптопровайдеру. Инсталлятор ActiveX-компонента можно скачать здесь.

# 3 Порядок установки ПО, необходимого для создания ЭП

**ВАЖНО!** Для установки программного обеспечения, пользователь должен обладать на компьютере правами локального администратора.

## 3.1 Установка криптопровайдера и сертификата ключа подписи

Возможные варианты действий:

1. Криптопровайдер уже установлен на компьютер пользователя. Сертификат ключа проверки ЭП был получен и установлен, и срок его действия не истек. В этом случае, необходимо выяснить, есть ли удостоверяющий центр, выдавший сертификат, в перечне УЦ, размещенном на сайте ЕФРСФДЮЛ (www.fedresurs.ru/Help). Если УЦ там есть, то необходимо уточнить непосредственно в службе поддержки УЦ, допустимо ли использование данного сертификата в ЕФРСФДЮЛ. В случае положительного ответа на этот вопрос, можно переходить к п. 3.2 настоящей Инструкции.

2. Один из криптопровайдеров (КриптоПро, VipNet CSP или Signal-COM CSP) был ранее установлен, но впоследствии удален. Или истек срок действия сертификата ключа проверки ЭП пользователя.

a. Рекомендуется обратиться в УЦ, в котором ранее были получены криптопровайдер и сертификат, для получения нового сертификата ключа проверки ЭП, а также криптопровайдера, необходимого для вычисления ЭП.

b. Установить и настроить криптопровайдер согласно инструкциям, полученным в УЦ.

3. Криптопровайдер на компьютере установлен не был.

a. Получить криптопровайдер и сертификат ключа проверки ЭП в одном из УЦ, указанных в списке, доступном по адресу www.fedresurs.ru/Help.

b. При установке и настройке криптопровайдера необходимо следовать инструкциям, предоставленным УЦ.

## 3.2 Установка ActiveX-компонента подписи

ActiveX-компонент подписи необходим для вызова криптопровайдера из браузера. Компонент подписи может работать в браузере Internet Explorer (поддерживаются только 32х разрядные версии браузеров), а также в браузере Mozilla FireFox.

В ЕФРСФДЮЛ рекомендуется использовать следующие браузеры:

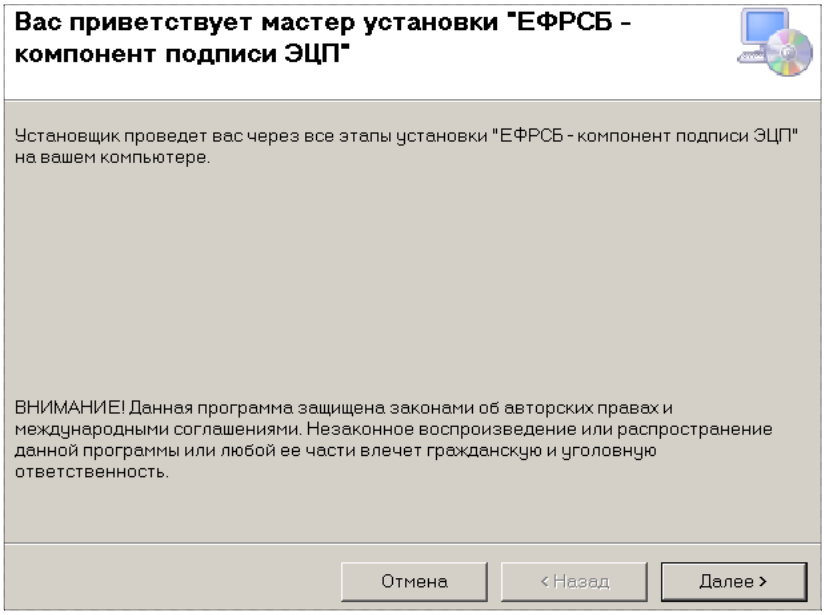
- 32 разрядные версии Internet Explorer 8, 9;
- 32 / 64 разрядные версии Internet Explorer 10, 11;
- Mozilla FireFox 30-х версий и выше.

**Примечание**. В устаревших (неподдерживаемых компанией-разработчиком) версиях веб-браузеров могут некорректно отображаться некоторые формы ввода и просмотра информации.

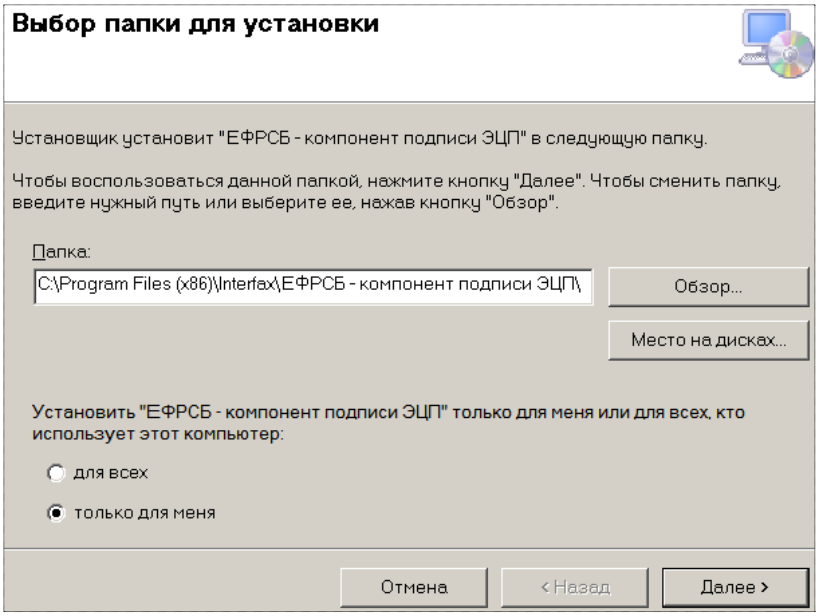
ActiveX-компонент имеет следующий порядок установки:

1. Скачать со страницы «Помощь» сайта ЕФРСФДЮЛ (www.fedresurs.ru/help) инсталлятор cspcomsetup_v2.msi.

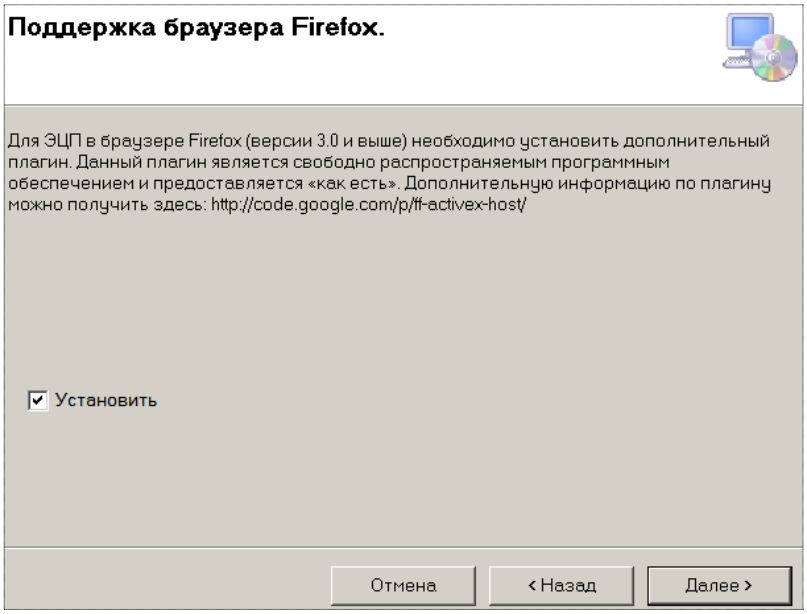
2. Запустить инсталлятор.




3. Нажать кнопку **Далее**. Откроется окно **Выбор папки для установки**:

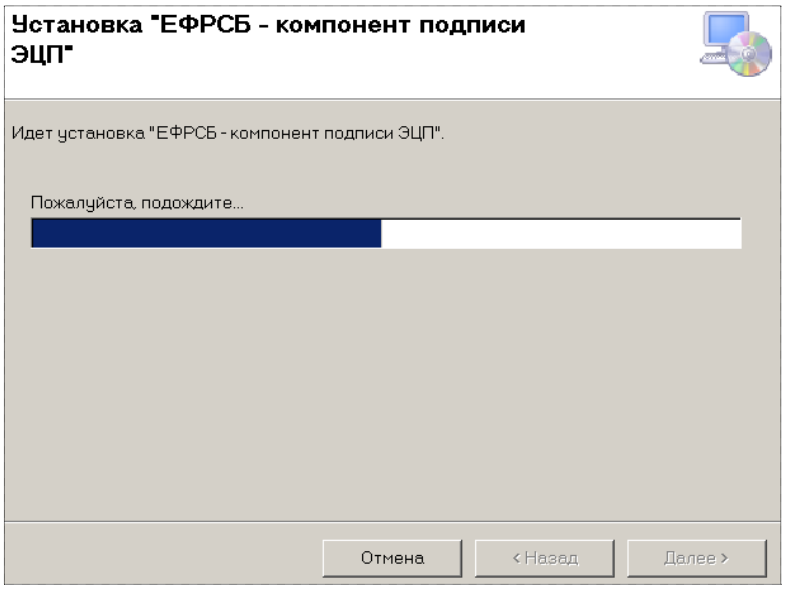



4. Указать папку для установки компонента или оставить папку предлагаемую по умолчанию. Нажать кнопку **Далее**. Откроется дополнительное окно установки плагина для FireFox, позволяющего запускать компонент в этом браузере:

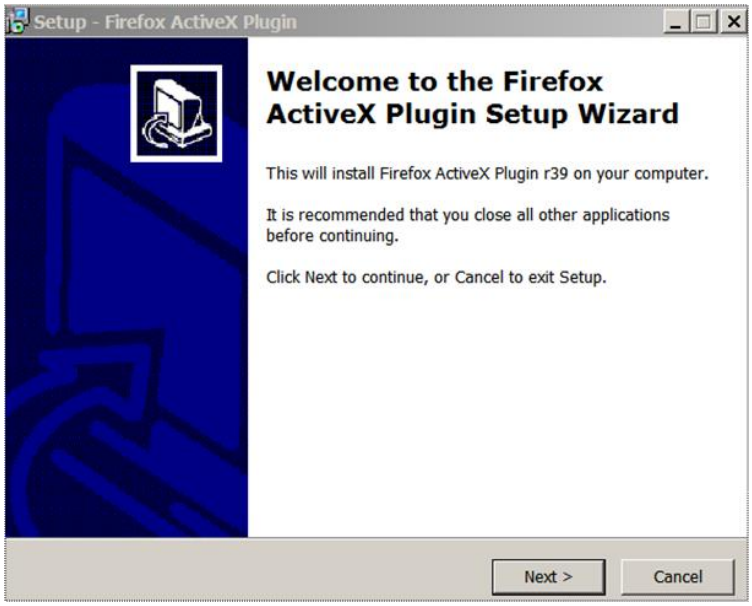



5. Оставить метку **Установить** и нажать кнопку **Далее**. В следующем окне также нажать на **Далее**.

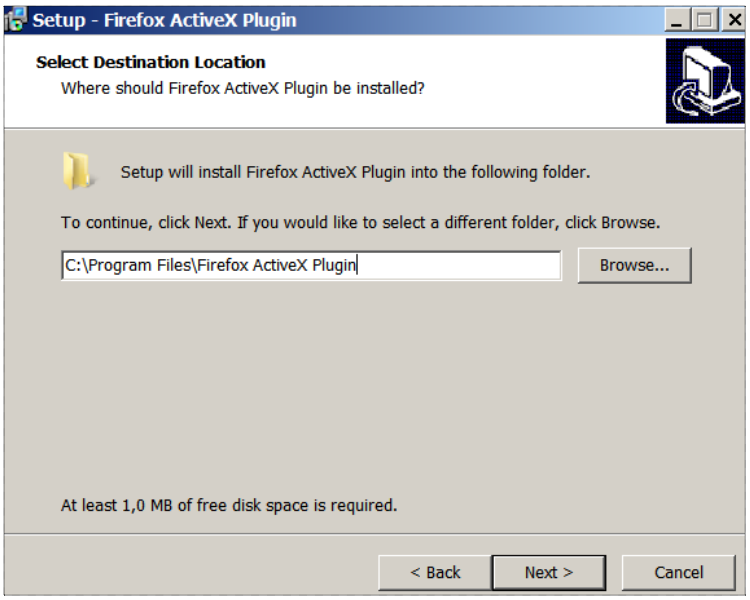
6. Появится окно отображающее ход процесса установки компонента.



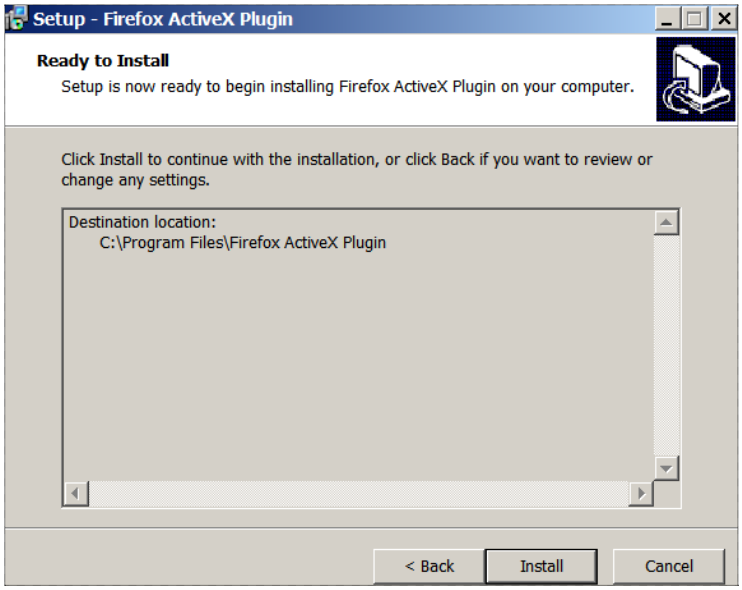

7. Если метка, задающая инсталляцию плагина для FireFox, была оставлена, то параллельно запустится инсталлятор данного плагина:



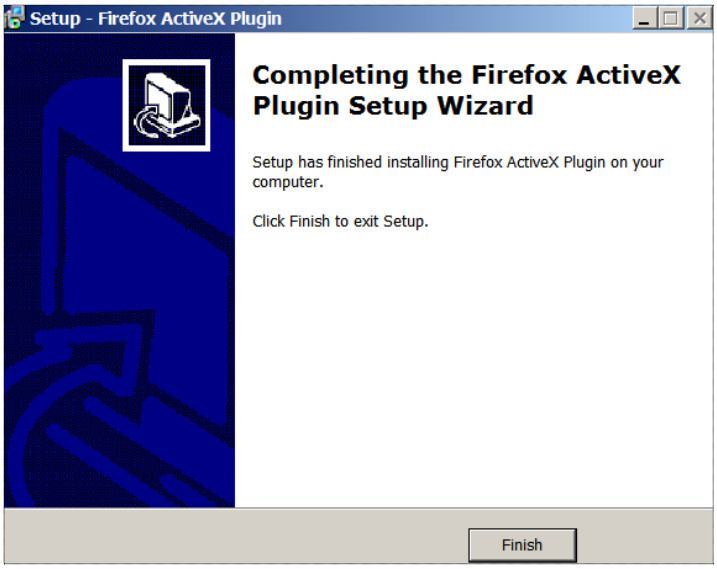

8. Нажать в окне инсталлятора плагина кнопку **Next**. Откроется окно выбора папки для размещения плагина:




9. Указать папку для установки плагина или оставить папку предлагаемую по умолчанию. Нажать кнопку **Next**. Появится окно подтверждения готовности к инсталляции:

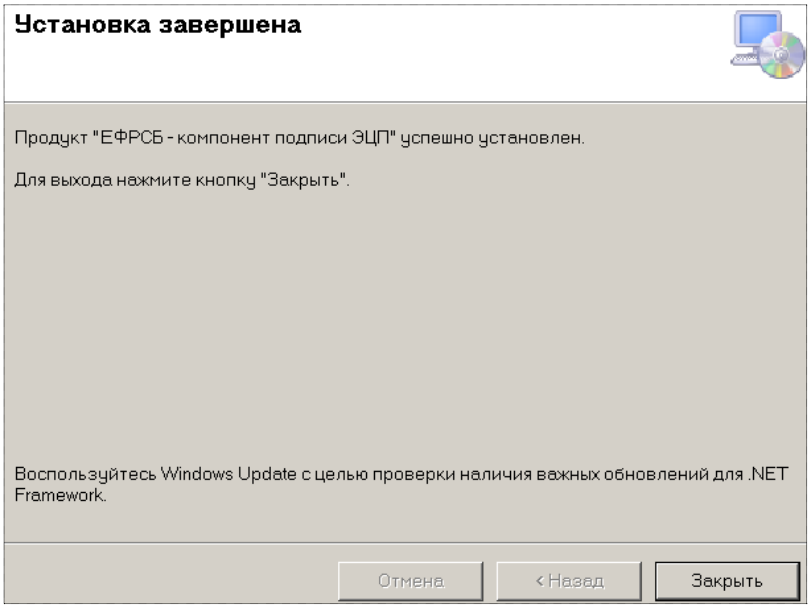



10. Нажать кнопку **Install**. По завершении процедуры инсталляции плагина появится финальное окно:




11. Нажать кнопку **Finish**.

12. Вернуться к окну установки ActiveX-компонента. По завершении процедуры установки компонента появится окно **Установка завершена**:




13. Нажать кнопку **Закрыть**.

# 4 Настройка ПО для возможности подписи

## 4.1 Добавление сертификата в локальное хранилище Windows

Для того чтобы ActiveX-компонент подписи мог обращаться к криптопровайдеру, **сертификат ключа подписи** и **корневой сертификат УЦ** должны быть добавлены в хранилище сертификатов Windows. В настоящем разделе показано, как это сделать для программ-криптопровайдеров КриптоПро, VipNet или Signal-COM.

> **Примечание**. Предполагается, что программа-криптопровайдер установлен. Иначе, необходимо его установить согласно инструкциям, приведенном в п. 3.1.

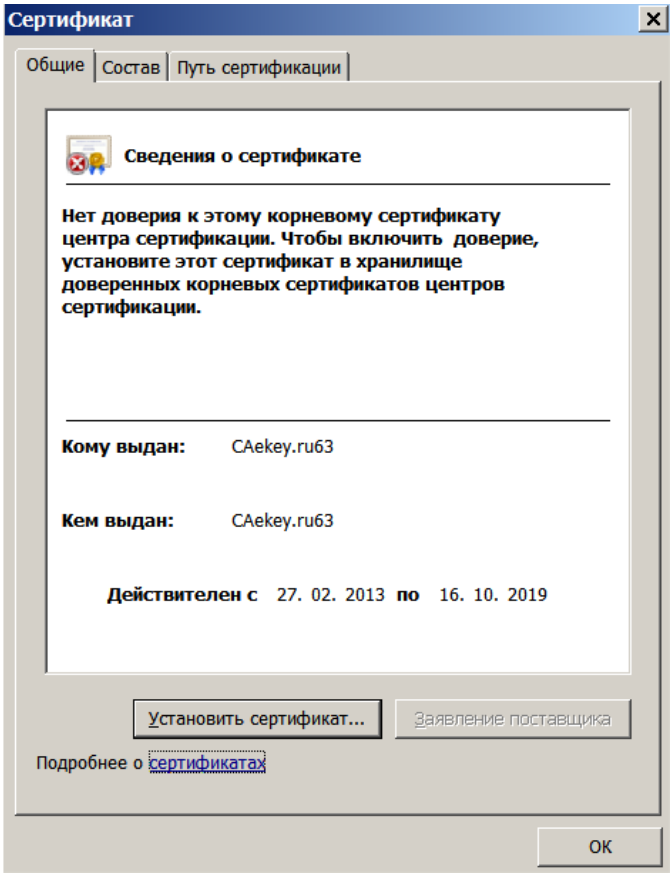
### 4.1.1 Установка корневого сертификата

Если вы получали ЭП в одном из УЦ через Ассоциацию электронных торговых площадок, корневой сертификат можно скачать с сайта aetp.ru (из раздела «Электронная подпись» / «Авторизованные УЦ»). Если вы получали ЭП не через указанную Ассоциацию, обратитесь за корневым сертификатом в ваш УЦ.

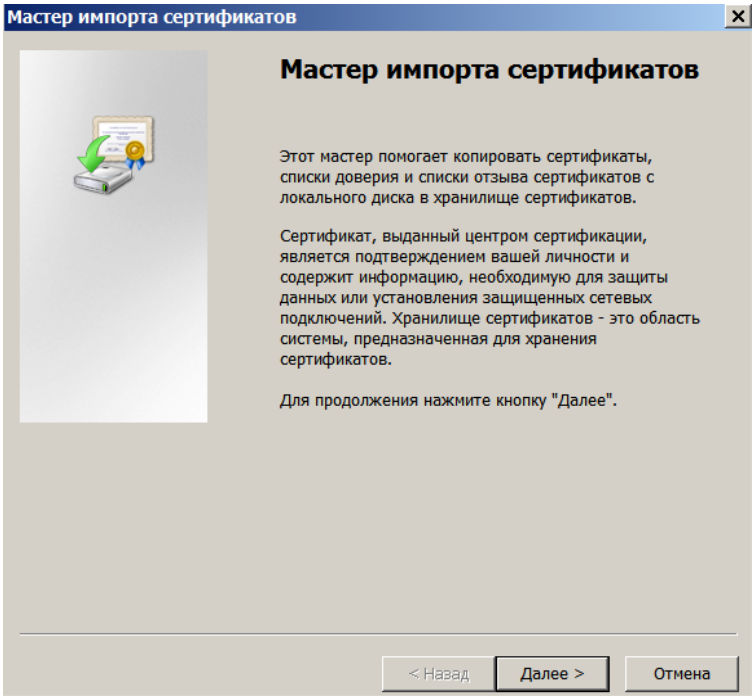
Если вы получали ЭП в УЦ e-Notary, корневой сертификат можно скачать с сайта www.e-notary.ru (из раздела «Корневые сертификаты аккредитованного УЦ e-Notary»).

Откройте ссылку и сохраните файл сертификата на диске.

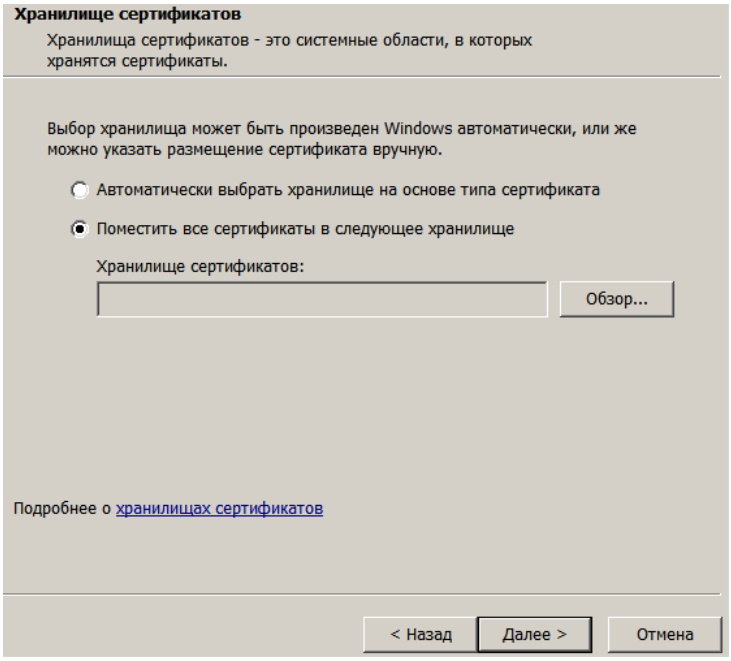
1. Откройте файл сертификата, дважды щелкнув на нем левой кнопкой мыши. Появится окно **Сертификат**:



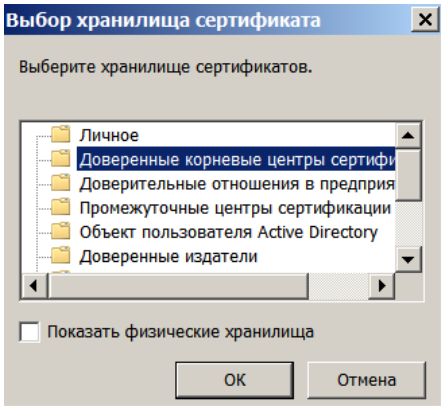

2. Нажмите кнопку **Установить сертификат**. Откроется первое окно мастера импорта сертификатов:



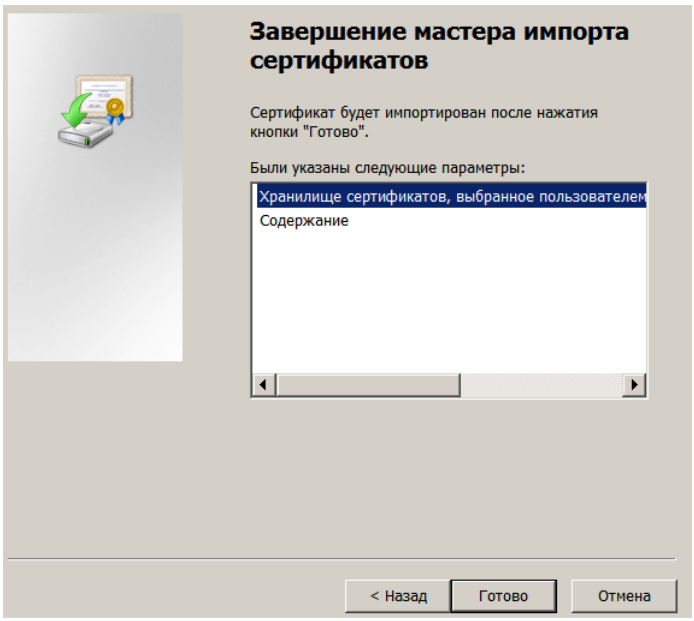

3. Нажмите кнопку **Далее**. Откроется окно выбора хранилища сертификатов. Установите переключатель в позицию **Поместить сертификаты в следующее хранилище**:



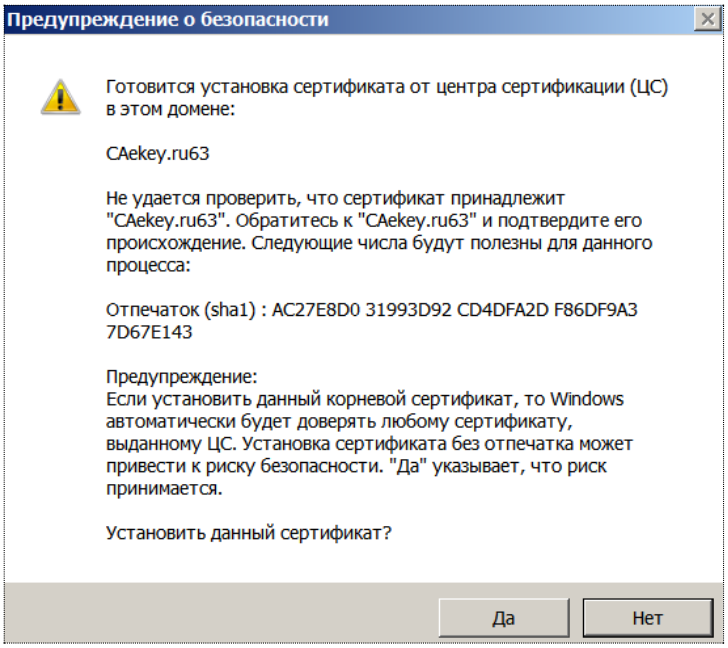

4. Нажмите кнопку **Обзор**. Откроется окно для выбора хранилища:




5. Укажите позицию **Доверенные корневые центры сертификации** и нажмите кнопку **ОК**. Затем нажмите кнопку **Далее**. Откроется окно **Завершение мастера импорта сертификатов**:




6. Нажмите кнопку **Готово**. Появится окно уведомления о готовности установки сертификата:

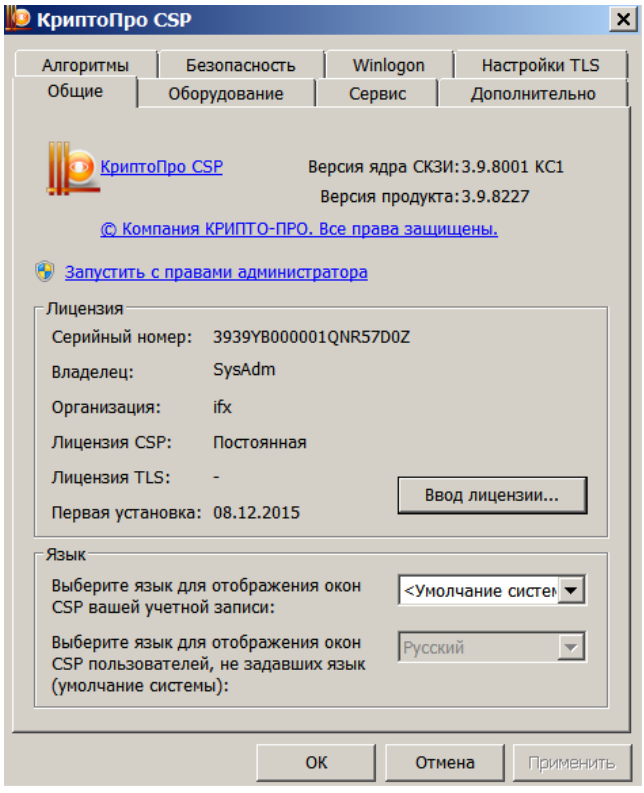



7. Нажмите кнопку **Да**. Сертификат будет установлен.

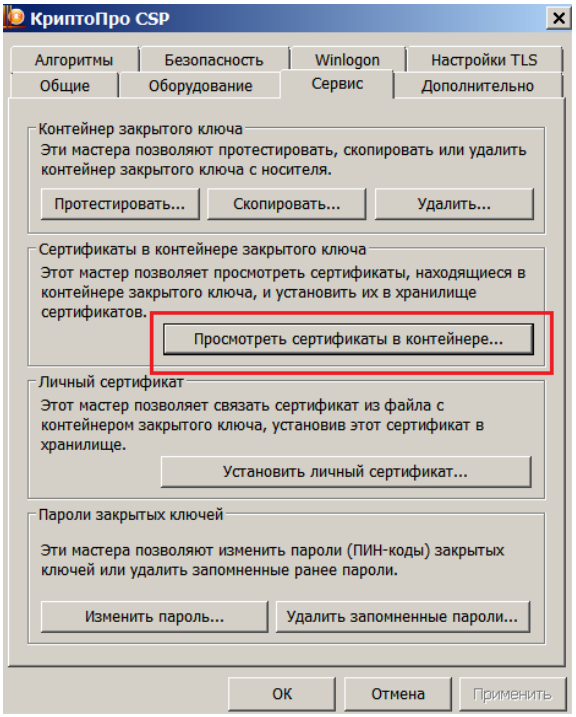
### 4.1.2 Установка личного сертификата при помощи программы КриптоПро

**Примечание**. Если у вас есть открытая часть сертификата (файл с расширением .cer), то в приведенной ниже последовательности действий сразу переходите к шагу 12.

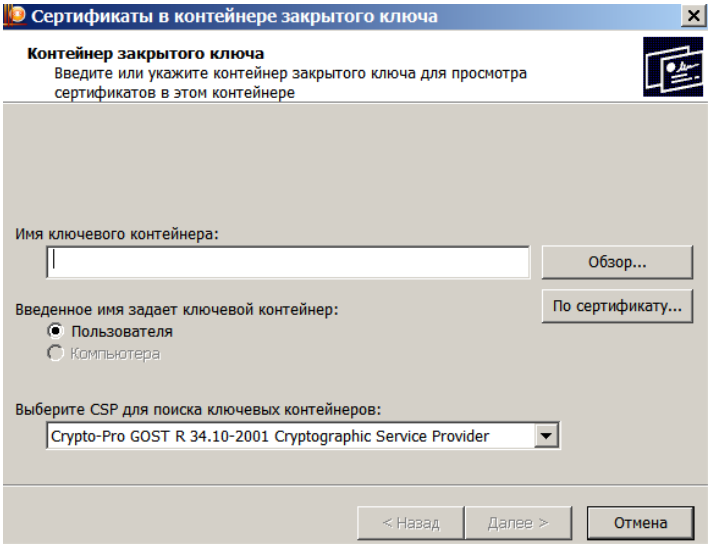
1. Выберите в главном меню Windows пункт **Пуск** / **Все программы** / **КРИПТО-ПРО** / **КриптоПро CSP**. Откроется окно программы КриптоПро CSP:



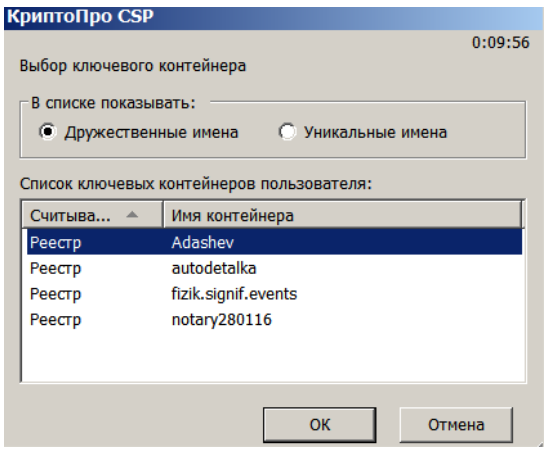

2. Зайдите на вкладку **Сервис** и нажмите кнопку **Просмотреть сертификаты в контейнере**:



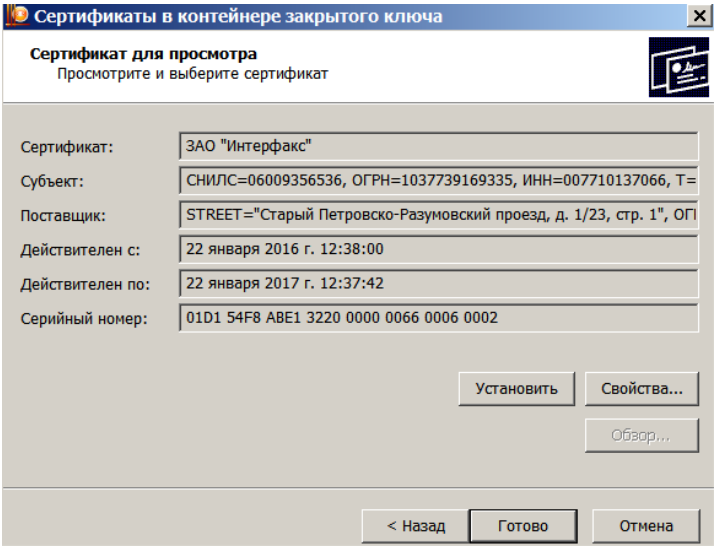

3. Откроется окно **Сертификаты в контейнере закрытого ключа**:



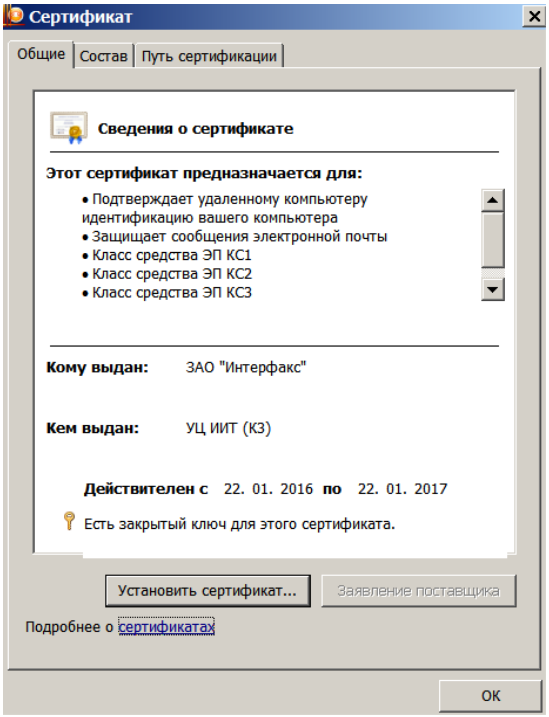

4. Нажмите кнопку **Обзор**. Откроется окно со списком ключевых контейнеров:



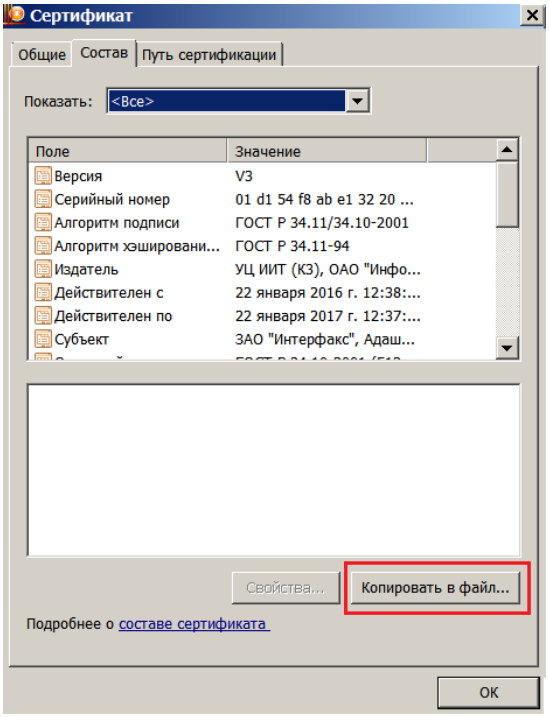

5. Укажите нужный контейнер и нажмите кнопку **ОК**. Затем – нажмите кнопку **Далее**. Откроется окно с информацией о выбранном сертификате:



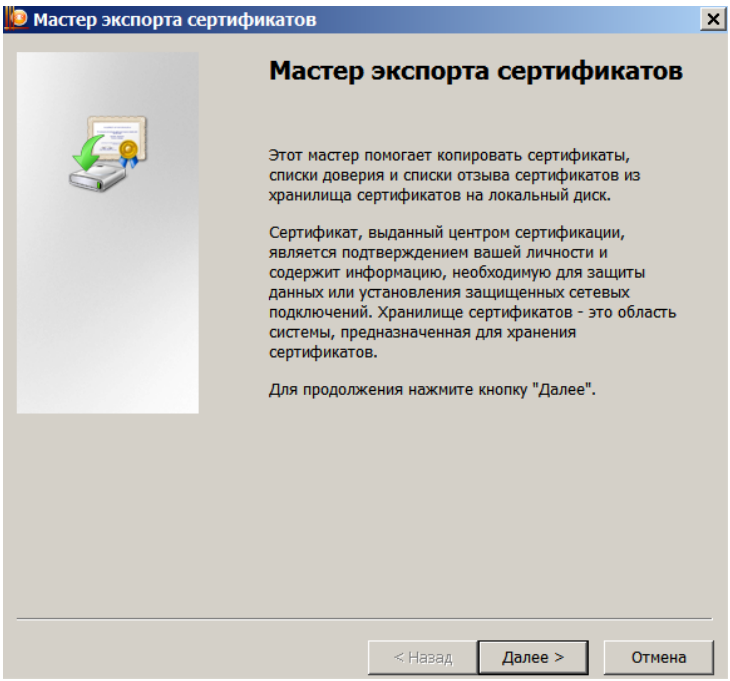

6. Нажмите кнопку **Свойства**. Откроется окно сертификата:



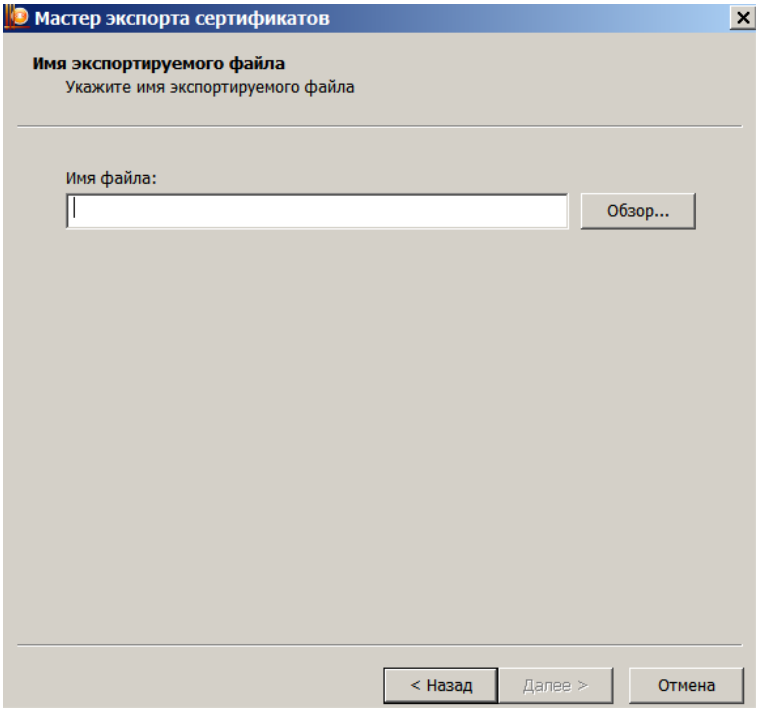

7. Перейдите на вкладку **Состав** и нажмите кнопку **Копировать в файл**:



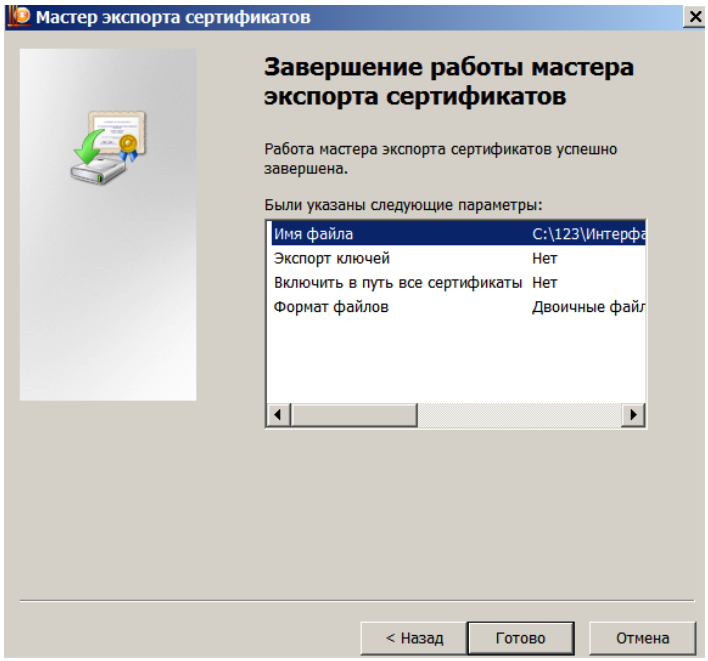

8. Откроется первое окно мастера экспорта сертификатов:




9. В последующих окнах мастера, не внося никаких изменений, просто три раза нажмите кнопку **Далее**. Откроется окно **Имя экспортируемого файла**:

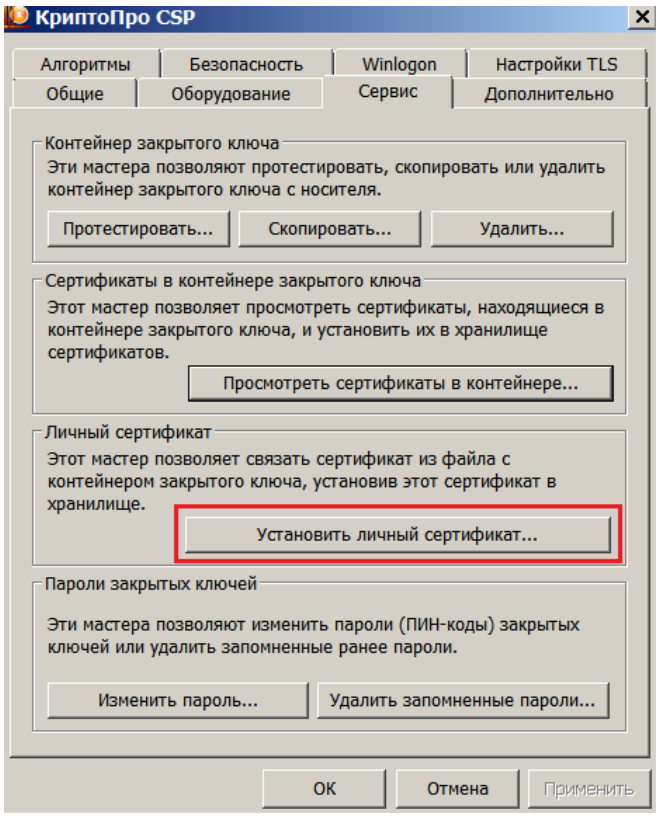



10. Нажмите кнопку **Обзор** и задайте имя файла, а также папку для его сохранения. Затем нажмите кнопку **Далее**. Файл с сертификатом будет сохранен в заданное место. Откроется окно завершения работы мастера:

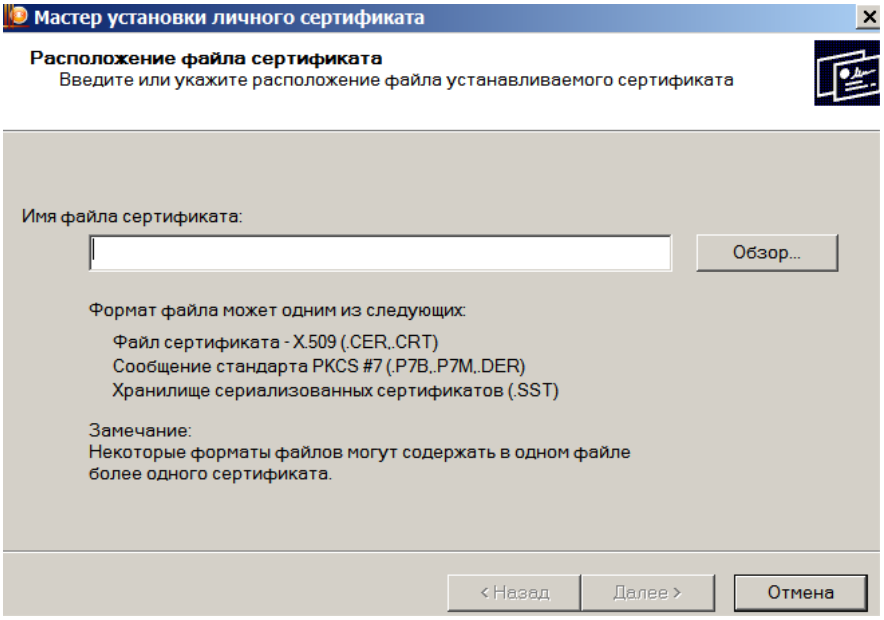



11. Нажмите кнопку **Готово**. В появившемся окне с уведомлением об успешном выполнении экспорта нажмите кнопку **ОК**.

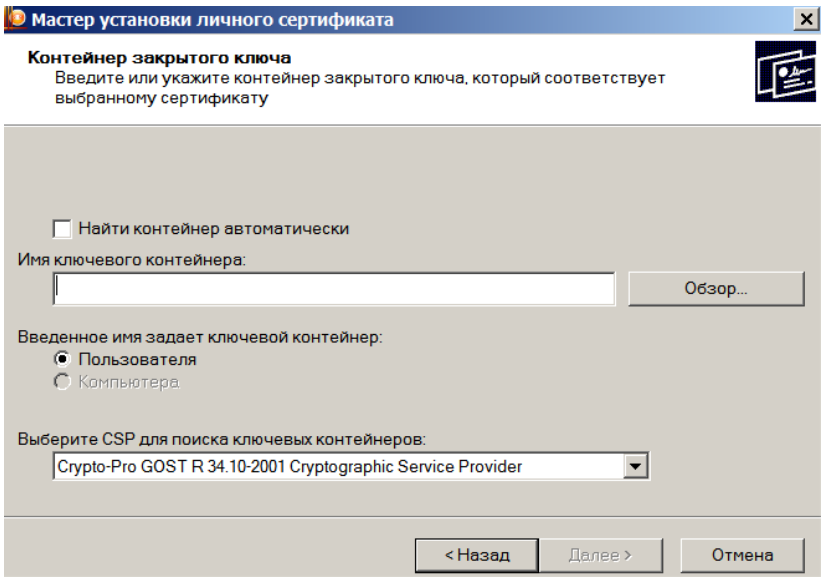
12. Вернитесь к окну программы КриптоПро CSP и вновь перейдите в нем на вкладку **Сервис**.



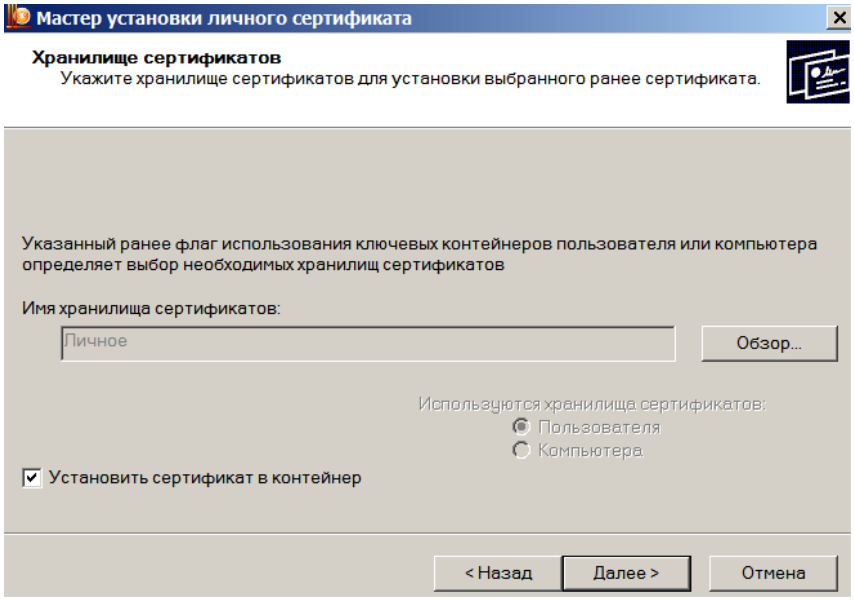

13. На данной вкладке нажмите кнопку **Установить личный сертификат**. Откроется окно **Расположение файла сертификата**:



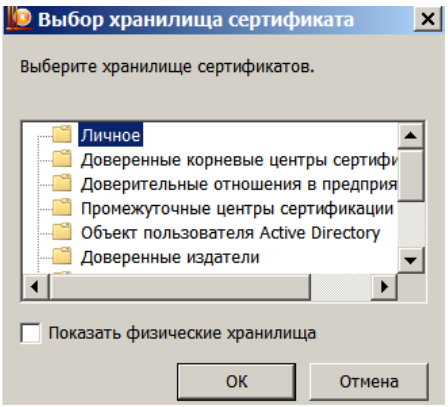

14. Нажмите кнопку **Обзор**. В появившемся стандартном окне выбора файла укажите файл открытой части сертификата и нажмите кнопку **Открыть**. Нажмите кнопку **Далее**. В окне следующего шага, также нажмите на **Далее**. Появится окно **Контейнер закрытого ключа**.



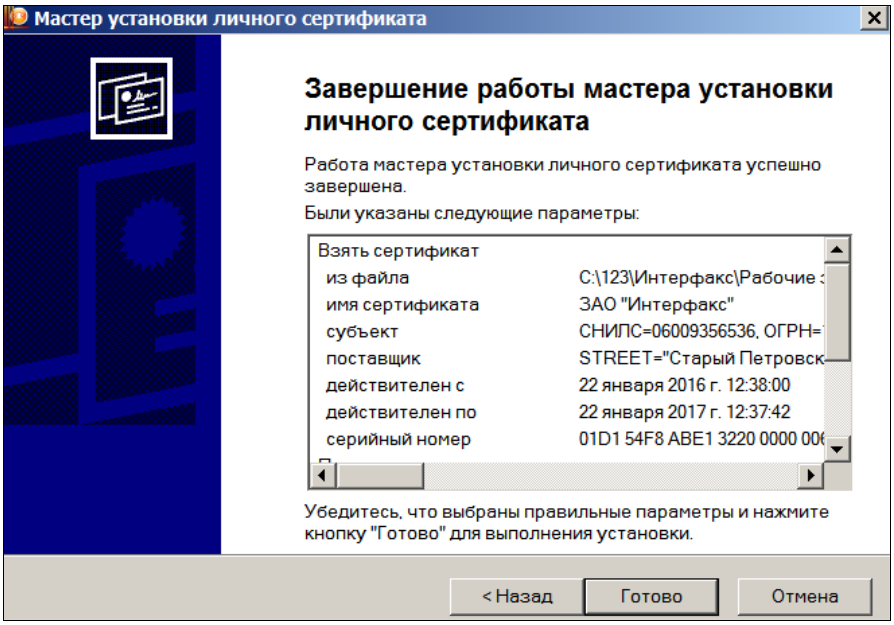

15. Нажмите кнопку **Обзор**. В открывшемся окне со списком ключевых контейнеров укажите нужный контейнер и нажмите кнопку **ОК**. Нажмите кнопку **Далее** – появится окно **Хранилище сертификатов**:




16. Нажмите в нем кнопку **Обзор**. Откроется окно для выбора хранилища сертификатов:

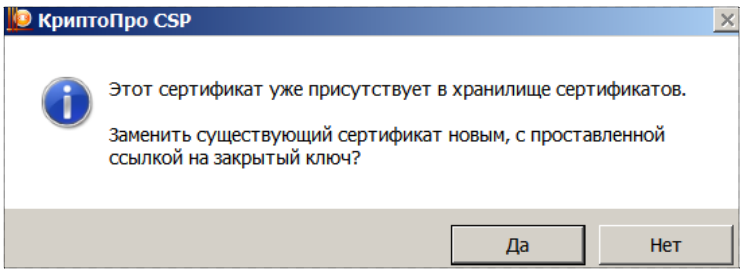



17. Установите метку **Показать физические хранилища**. Затем в древовидной структуре выберите позицию **Личное** / **Реестр**. Нажмите кнопку **ОК**, а затем – кнопку **Далее**. Появится окно завершения работы мастера:




18. Нажмите в нем кнопку **Готово**.

19. Если ранее производилась некорректная установка сертификата, то появится окно уведомления:




20. Нажмите кнопку **Да**. На этом установка личного сертификата завершается.

Перейдите к выполнению инструкций, приведенных в п. 4.2.

### 4.1.3 Установка личного сертификата при помощи программы VipNet CSP

В данном пункте рассмотрена установка корневого и личного сертификатов в хранилище Windows, которую может осуществить пользователь программы VipNet CSP.

В зависимости от используемого Вами носителя ключевой информации следуйте соответствующей инструкции:

- если ключи электронной подписи и сертификат хранятся на ключевом носителе JaCarta LT, следуйте шагам подпункта 4.1.3.1
- если в качестве ключевого носителя используется компакт-диск (CD), следуйте шагам подпункта 4.1.3.2.

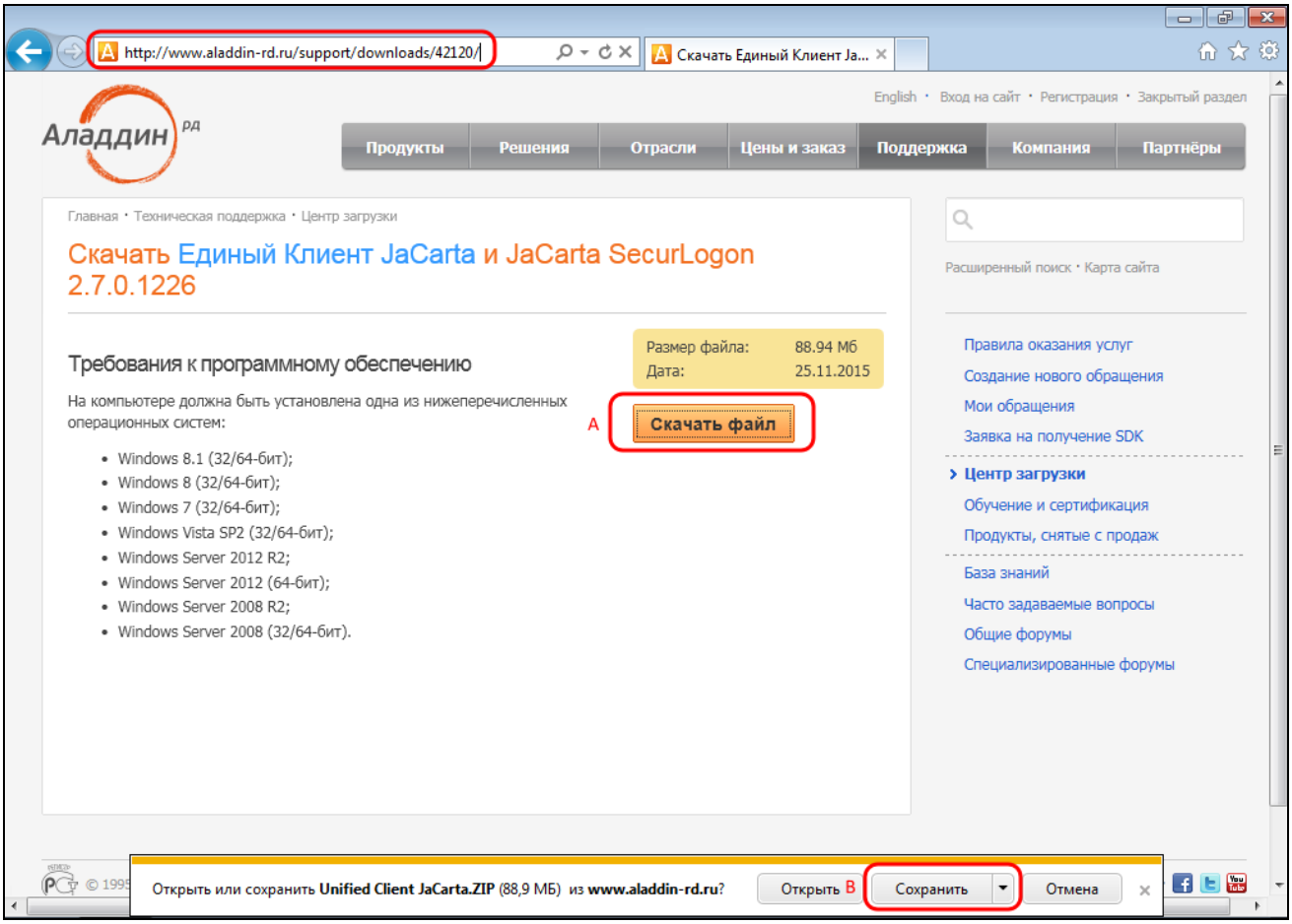
#### 4.1.3.1 Установка личного сертификата с ключевого носителя JaCarta LT

Для корректной работы ключевого носителя JaCarta LT под управлением операционной системы Microsoft Windows необходимо установить программное обеспечение, позволяющее выполнять базовые операции с электронными ключами JaCarta.

1. Для получения данного ПО актуальной версии необходимо скачать архив, доступный по ссылке:

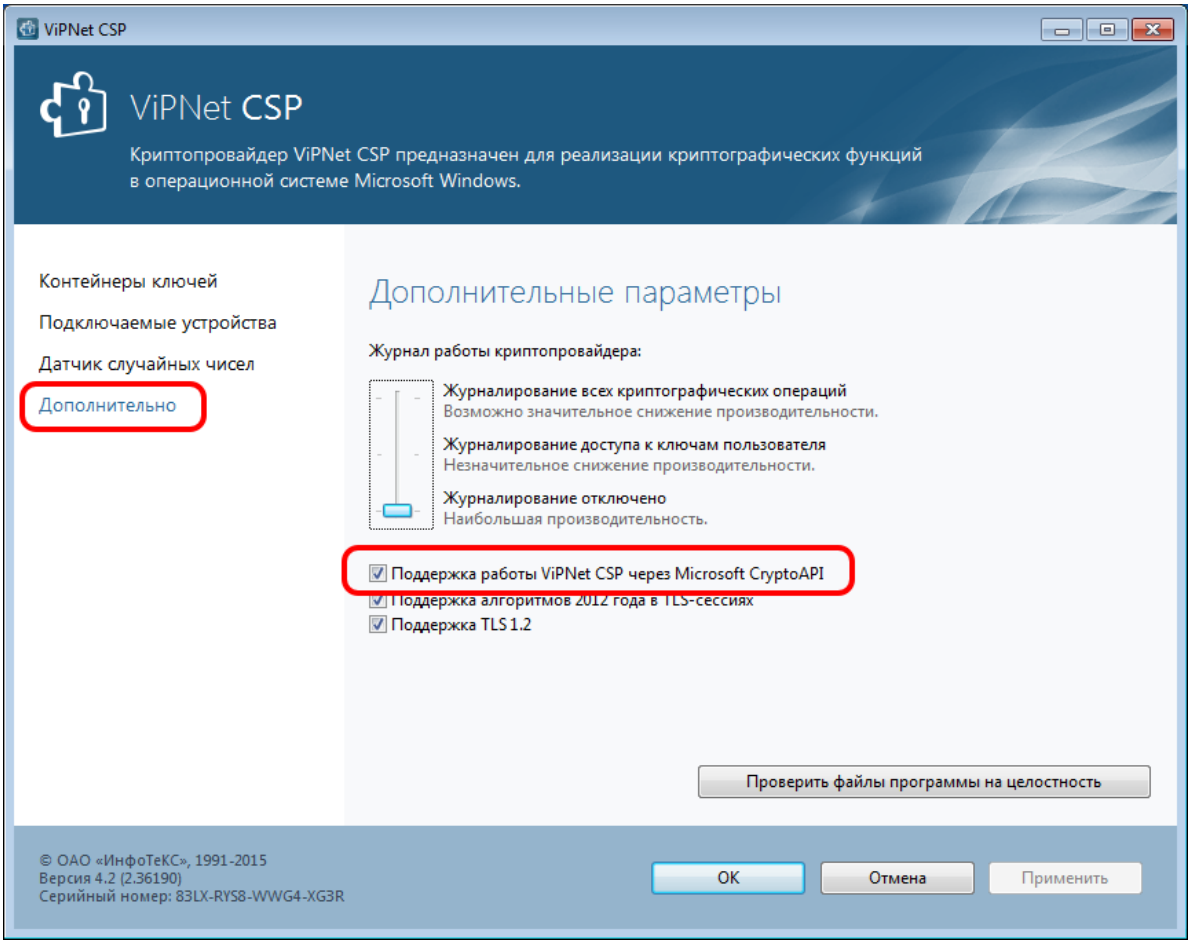
   - при использовании ОС Windows 7 и 8: Единый Клиент JaCarta и JaCarta SecurLogon http://www.aladdin-rd.ru/support/downloads/42120
   - при использовании ОС Windows 10: Единый Клиент JaCarta и JaCarta SecurLogon 2.8.0.1402 http://www.aladdin-rd.ru/support/downloads/43987/

2. На открывшейся странице нажмите кнопку **Скачать файл** (на рисунке ниже – позиция A).

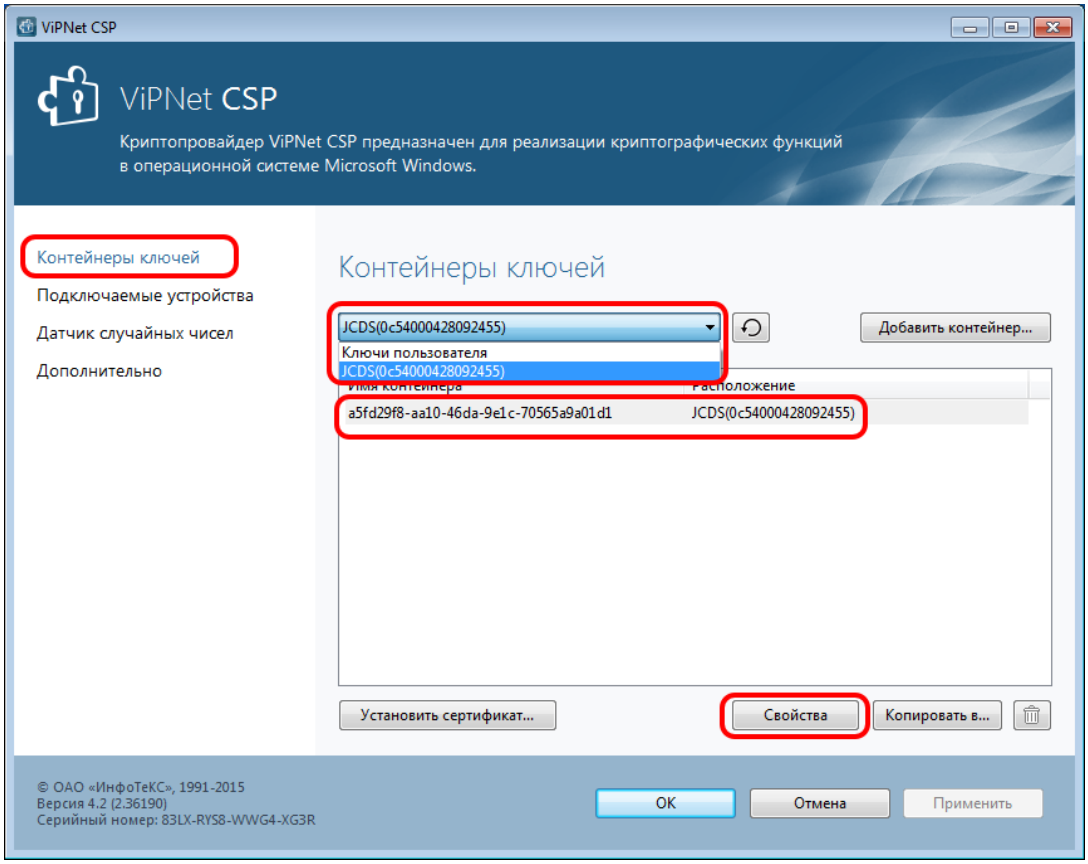



3. Загрузите архив с дистрибутивом в любой каталог Вашего компьютера (на рисунке – позиция B), распакуйте его и запустите установку утилиты. Выполните установку, следуя инструкциям мастера установки.

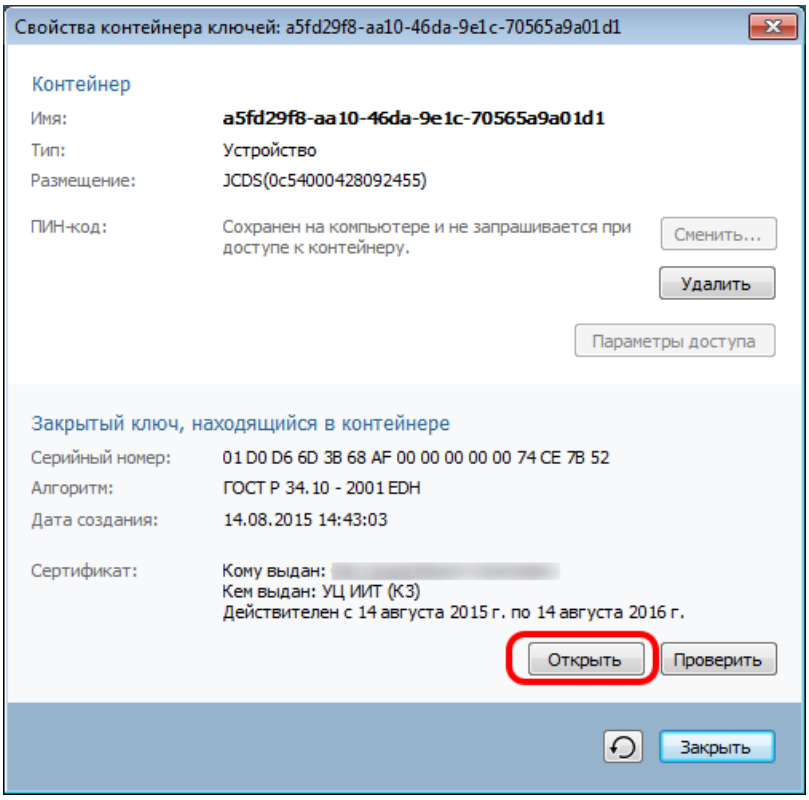
4. Запустите программу ViPNet CSP и убедитесь, что в разделе **Дополнительно** включена опция **Поддержка работы ViPNet CSP через Microsoft CryptoAPI** (см. рисунок ниже):



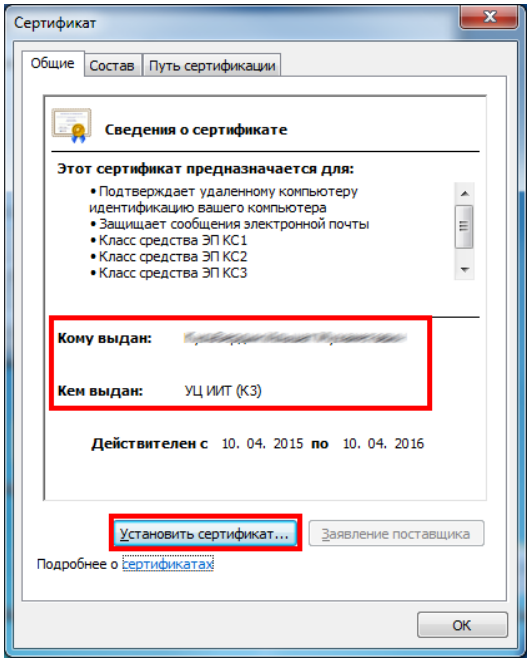

5. Перейдите в раздел **Контейнеры ключей** (см. рисунок ниже). В раскрывающемся списке выберите позицию **JCDS(…)**, а в поле **Имя контейнера** – контейнер ключей «*xxx-xxxx-xxxx-xxxx-xxxx*». Затем нажмите кнопку **Свойства**.




6. В окне **Свойства контейнера ключей** в области **Закрытый ключ, находящийся в контейнере** нажмите кнопку **Открыть**:

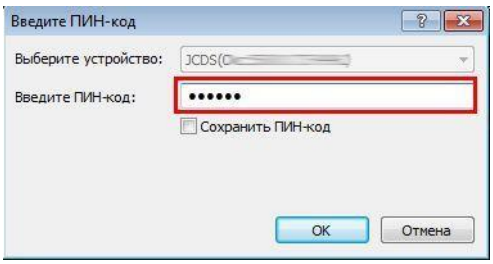



7. В открывшемся окне **Сертификат** убедитесь, что выбран именно тот сертификат, который необходимо использовать, и нажмите кнопку **Установить сертификат**:

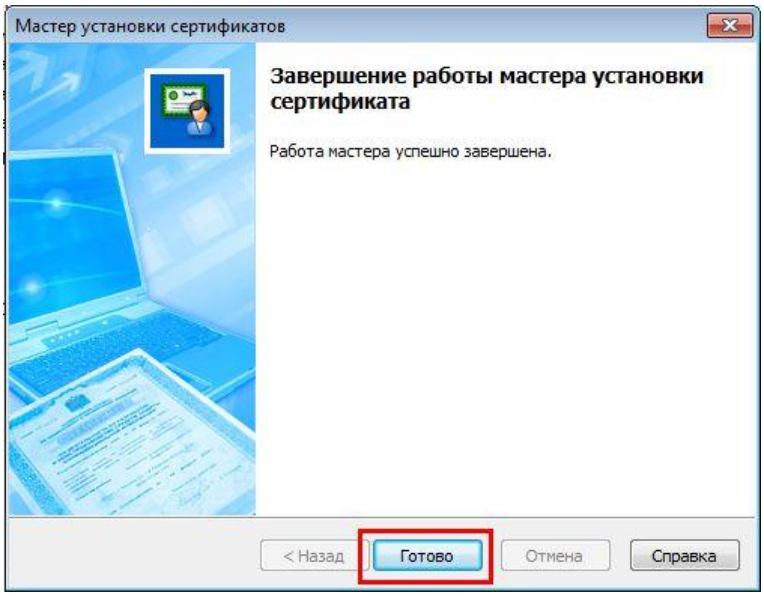



8. Далее следуйте указаниям Мастера установки сертификатов. В ходе установки в окне **Выбор хранилища сертификатов** установите переключатель в позицию **Текущего пользователя**. А в раскрывающемся списке в нижней части окна **Готовность к установке сертификата** – значение «*Указать контейнер с закрытым ключом*».

9. В появившемся на очередном шаге окне введите PIN-код к устройству:




10. В финальном окне Мастера установки сертификатов нажмите кнопку **Готово**. На этом установка личного сертификата завершается:




Перейдите к выполнению инструкций, приведенных в п. 4.2.

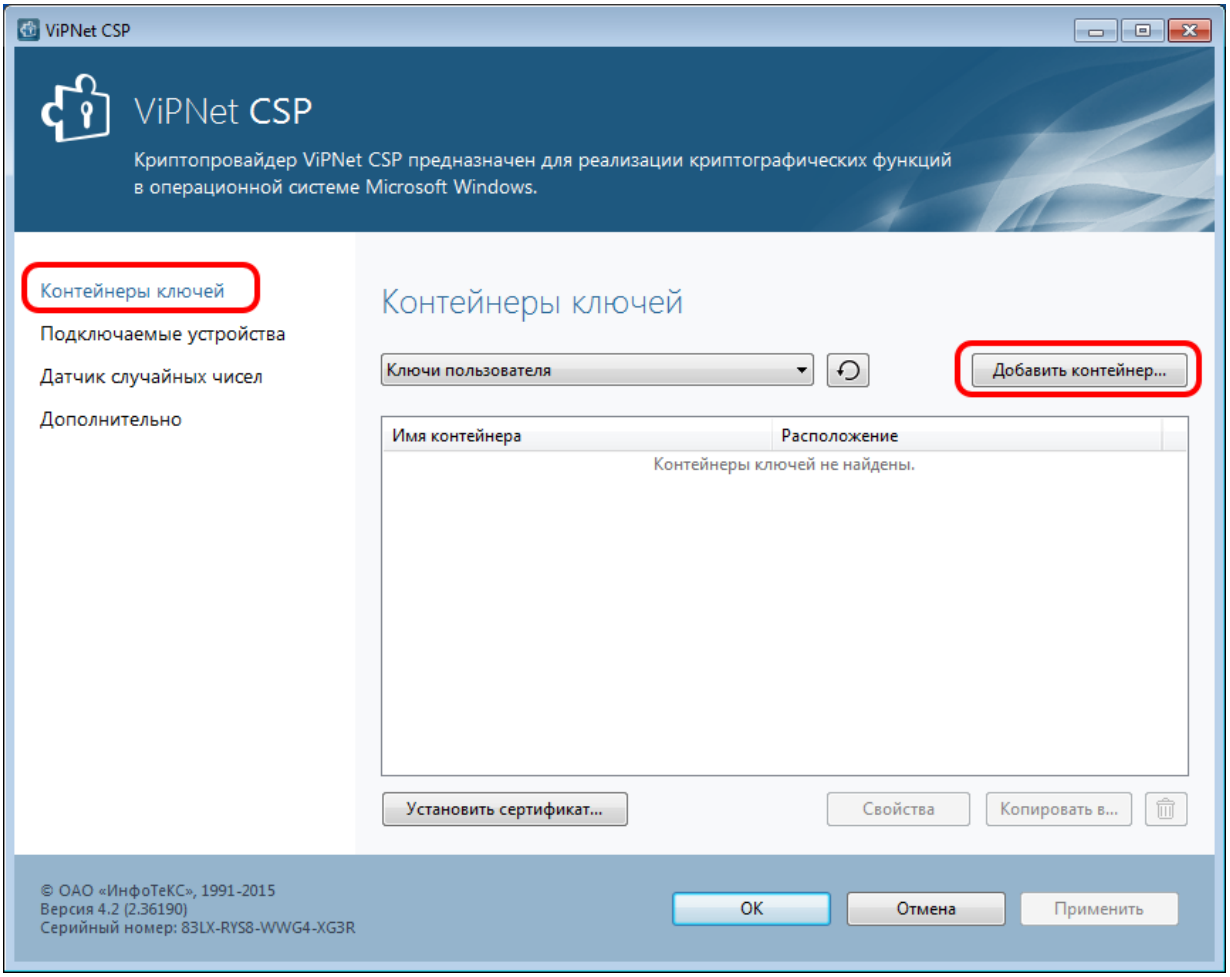
#### 4.1.3.2 Установка личного сертификата с компакт-диска (CD)

В качестве ключевого носителя можно использовать компакт-диск (CD).

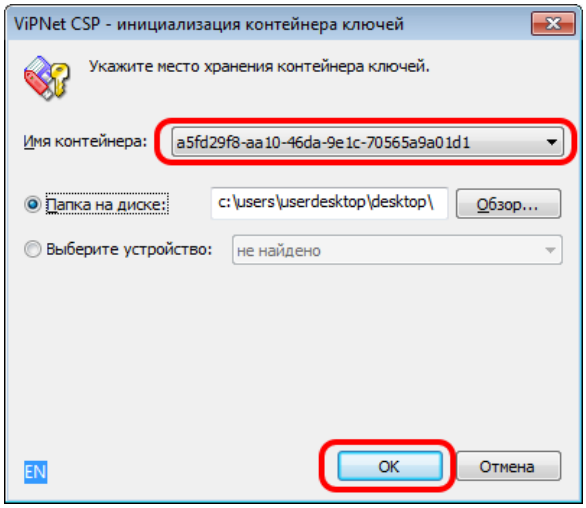
Для установки личного сертификата с компакт-диска выполните шаги рассмотренные ниже:

1. Скопируйте ключевой контейнер (файл с именем *sgn-xxxx-xxxx-xxxx-xxxx*) с компакт-диска в любую директорию жесткого диска компьютера.

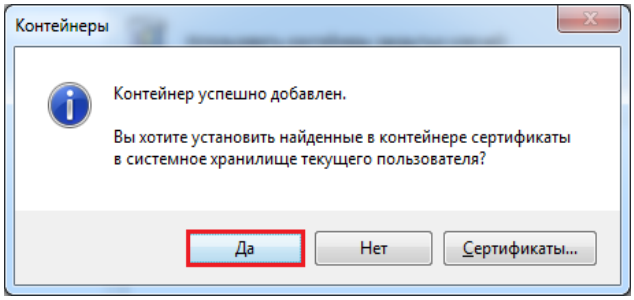
2. Запустите программу ViPNet CSP и перейдите в раздел **Контейнеры ключей**:




3. Нажмите кнопку **Добавить контейнер** (см. рисунок выше). Укажите местоположение ключей и в раскрывающегося списке **Имя контейнера** выберите имя вида «*XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX*» (единственный файл в списке, не имеющий расширения). Затем – нажмите кнопку **OK**:




4. Появится окно с уведомлением «Контейнер успешно добавлен» и вопросом об установке найденных в контейнере сертификатов в системное хранилище. Нажмите в нем кнопку **Да**:




5. **ВНИМАНИЕ!** Выполните физическое уничтожение использованного при данной установке ключевого носителя (компакт-диска).

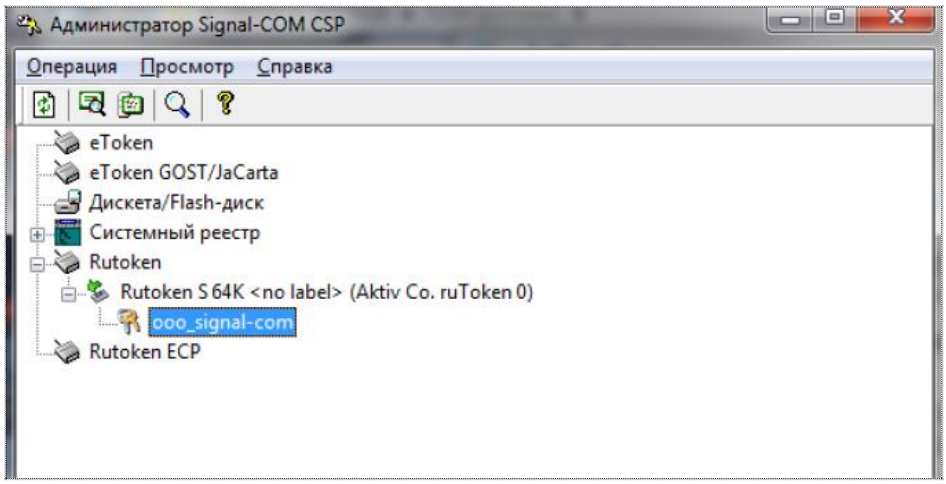
Перейдите к выполнению инструкций, приведенных в п. 4.2.

### 4.1.4 Установка личного сертификата при помощи программы Signal-COM CSP

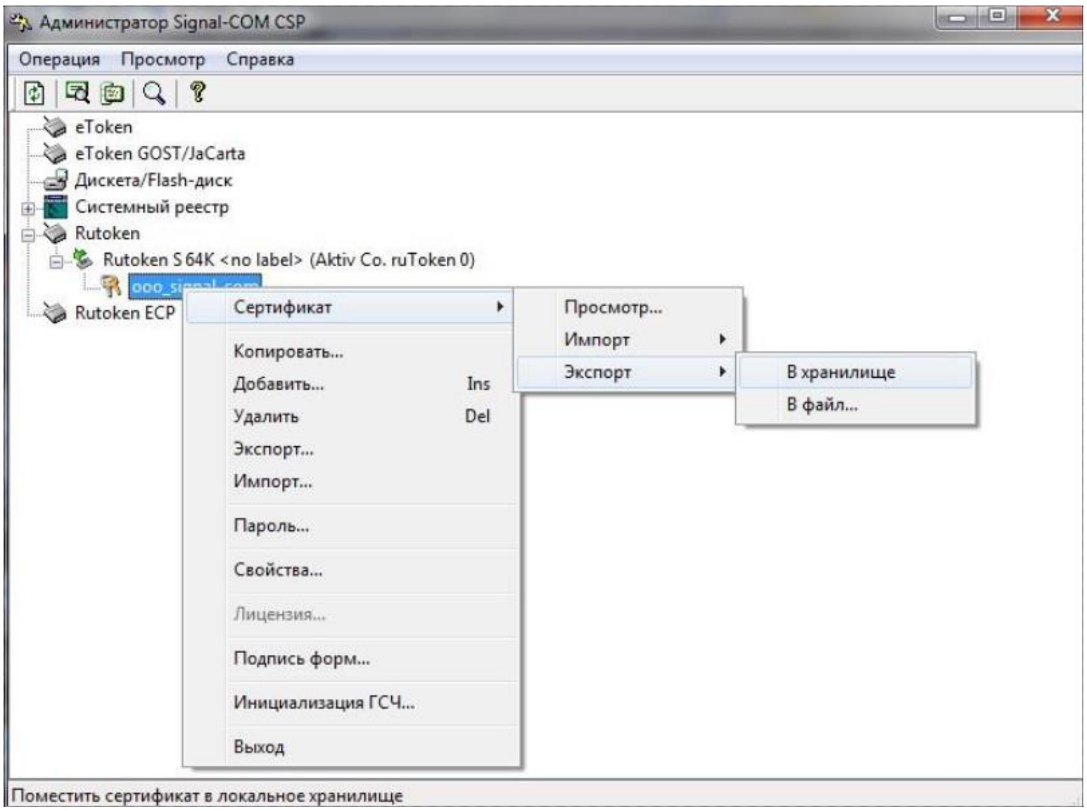
Для установки личного сертификата при помощи программы Signal-COM CSP необходимо выполнить следующие действия:

1. Запустите утилиту «Администратор Signal-COM CSP».

2. В появившемся окне выберите необходимый носитель и укажите ключевой контейнер:




3. Нажмите на ключевом контейнере правой кнопкой мыши и выберите в контекстном меню пункт **Сертификат / Экспорт / В хранилище**:




Перейдите к выполнению инструкций, приведенных в п. 4.2.

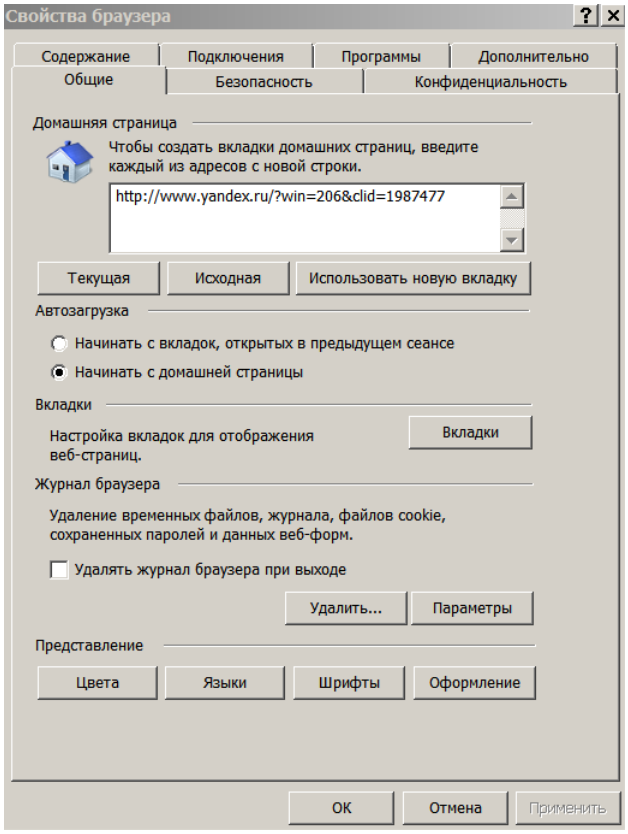
## 4.2 Настройка браузера

### 4.2.1 Добавление сайта ЕФРСФДЮЛ в доверенные узлы Internet Explorer

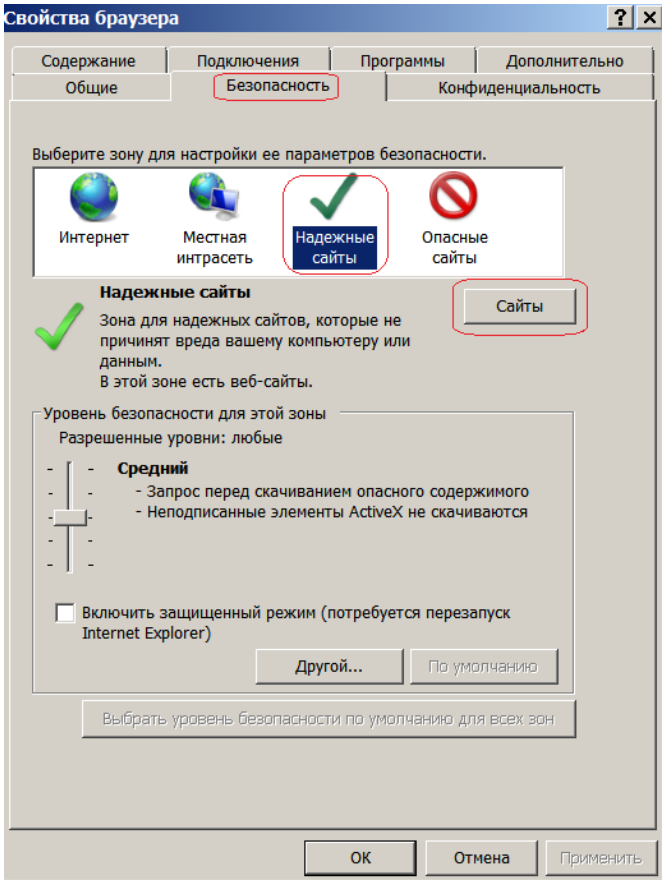
Для возможности запуска ActiveX-компонента в браузере Internet Explorer сайт ЕФРСФДЮЛ (www.fedresurs.ru) должен быть включен в состав доверенных узлов.

Это осуществляется в настройках используемого для работы браузера (ниже дан пример для браузера Internet Explorer 11).

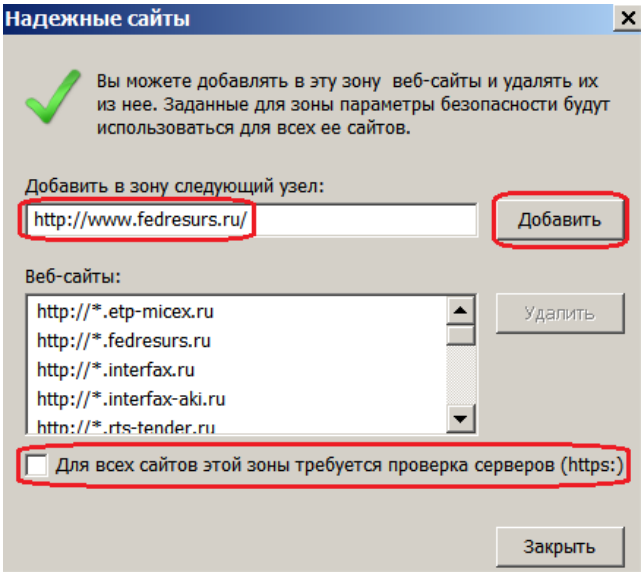
1. Запустить браузер. В правом верхнем углу окна щелкнуть на пиктограмме  и в открывшемся меню выбрать пункт **Свойства браузера**. На экране появится окно **Свойства браузера**:




2. Перейти на вкладку **Безопасность**, выбрать зону для настройки **Надежные сайты** и нажать кнопку **Сайты**:




3. В открывшемся окне убедиться, что флажок **Для всех узлов этой зоны требуется проверка серверов** снят, вписать в поле **Добавить в зону следующий узел** значение *http://www.fedresurs.ru/* и нажать кнопку **Добавить**:



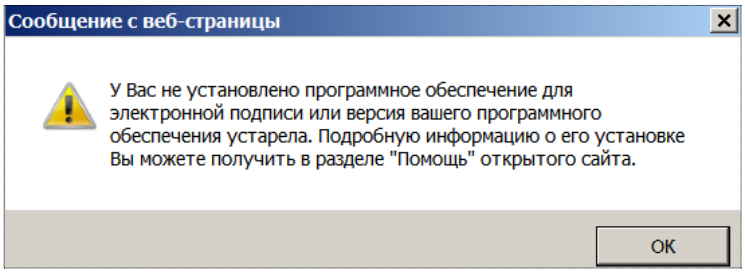

4. Закрыть окно **Свойства браузера**.

### 4.2.2 Разрешение запуска ActiveX-компонента ЭП в браузере Internet Explorer

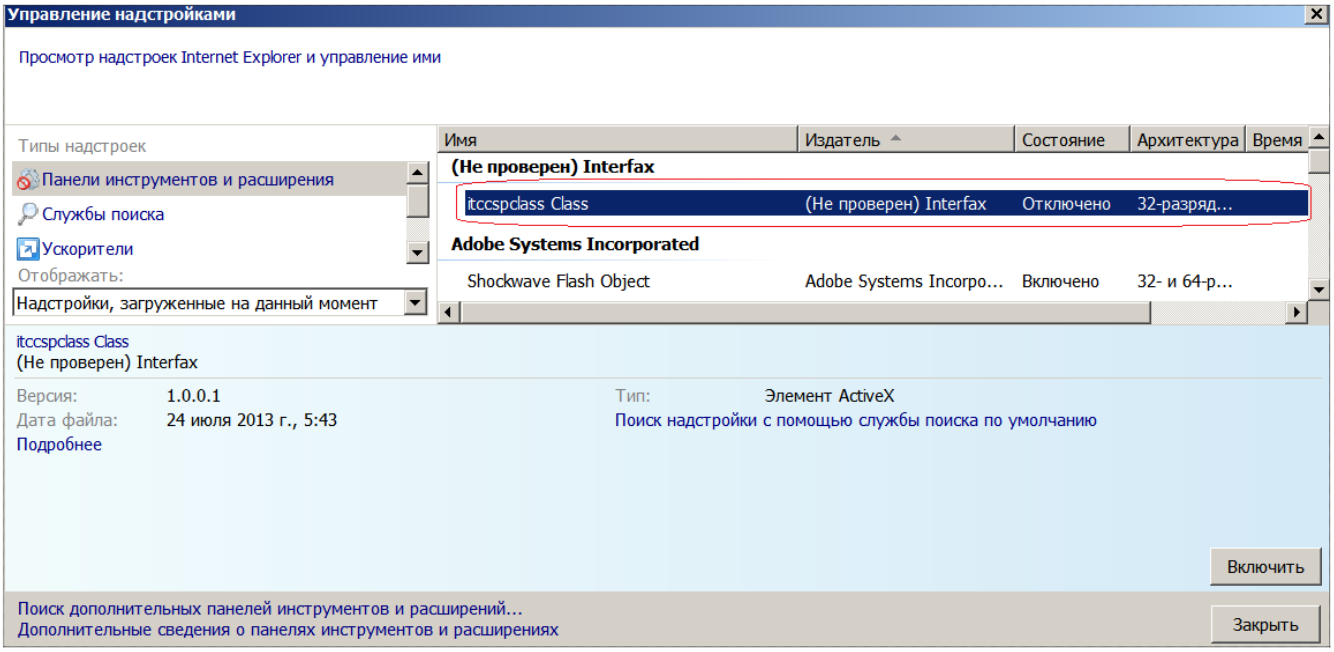
Браузер Internet Explorer блокирует запуск ActiveX-компонентов. Для разрешения запуска, необходимо произвести следующие действия:

1. Зайти на открытом сайте системы в раздел «Помощь» – www.fedresurs.ru/Help. Нажать кнопку **Проверить** в подразделе «Проверка подписи».

2. Если браузер заблокировал запуск ActiveX-компонента, появится окно сообщения:




5. Необходимо в правом верхнем углу браузера щелкнуть на пиктограмме  и в открывшемся меню выбрать пункт **Настроить надстройки**. Появится окно **Управление надстройками**:

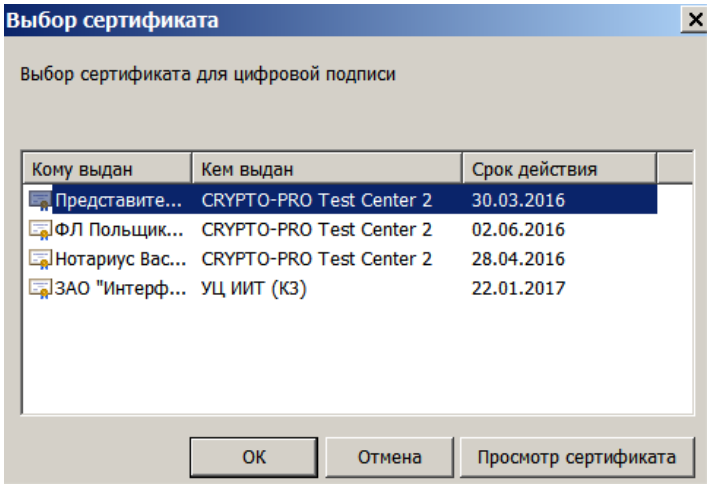



6. Указать в списке запись **itccspclass Class**, щелкнуть на ней правой кнопкой мыши и в появившемся контекстном меню выбрать пункт **Включить**. Закрыть данное окно.

# 5 Проверка системы ЭП

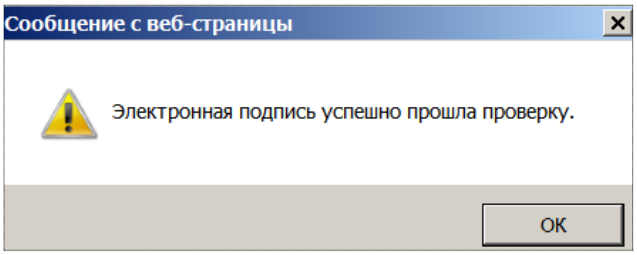
Проверку работоспособности системы ЭП можно осуществить через раздел «Помощь» открытого сайте.

1. Зайти в раздел «Помощь» – www.fedresurs.ru/Help. Нажать кнопку **Проверить** в подразделе «Проверка подписи». Откроется окно **Выбор сертификата**:




2. Выбрать сертификат и нажать кнопку **ОК**. В зависимости от настроек используемого криптопровайдера далее может потребоваться ввод пароля или подключение ключевого носителя.

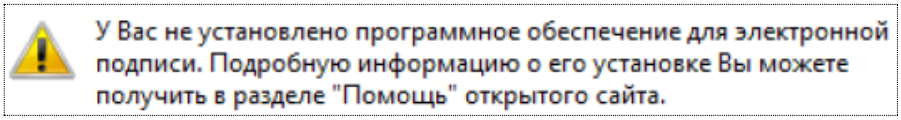
3. Будет произведена проверка подписи на сервере. Если ЭП прошла проверку, появится окно с соответствующим сообщением:




# 6 Разрешение проблем неработоспособности ЭП

## 6.1 Уведомление «Не установлено программное обеспечение …»

Проблема: при проверке подписи после нажатия кнопки **Проверить** в разделе «Помощь» открытого сайта выдается уведомление:



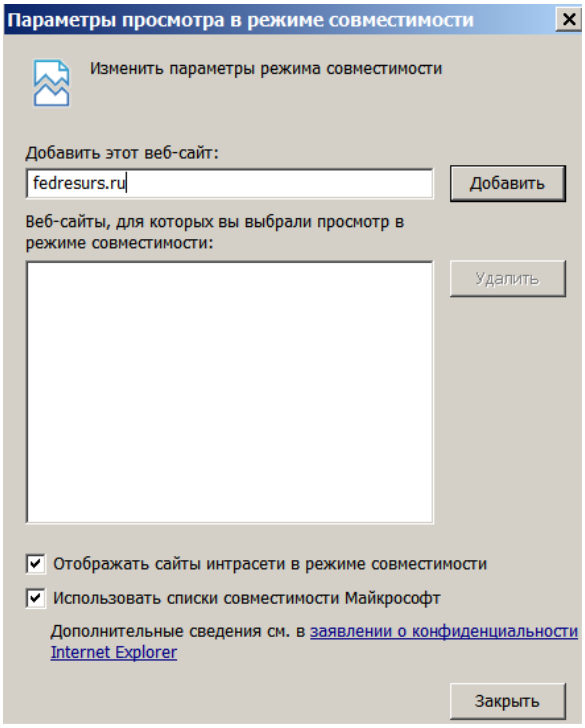

Возможны следующие варианты причин проблемы и методов её устранения:

1. Не установлен ActiveX-компонент подписи. Необходимо произвести его установку в соответствии с инструкцией, приведенной в п. 3.2.

2. В браузере Internet Explorer запрещен запуск ActiveX-компонента подписи. Необходимо разрешить его запуск и выполнение в соответствии с п. 4.2.2.

3. Используется 64 разрядная версия браузера Internet Explorer 8, 9 в операционной системе Windows 7 64-bit (как определить версию Windows см. в п. 7.1). В операционной системе Windows 7 64-bit из-за особенностей системы безопасности ActiveX-компонент подписи может быть запущен только в браузере Mozilla FireFox, 32 разрядной версии Internet Explorer 8, 9 (а также в 32/64 разрядных версиях Internet Explorer 10, 11). Инсталлятор браузера FireFox можно скачать со страницы производителя www.mozilla.com/ru/firefox (рекомендуется использовать версии от 30-х и выше). Данный браузер распространяется бесплатно и полностью поддерживается функционалом АИС.

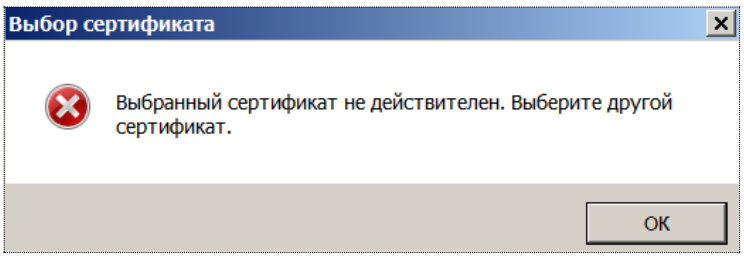
   В версии Internet Explorer 11 сайт *fedresurs.ru* нужно добавить в просмотр в режиме совместимости. Для этого нужно в правом верхнем углу окна браузера щелкнуть на пиктограмме  и в открывшемся меню выбрать пункт **Параметры просмотра в режиме совместимости**. Появится окно **Параметры просмотра в режиме совместимости**:




Вести строку *fedresurs.ru* в поле **Добавить этот веб-сайт**, нажать кнопку **Добавить**, а затем – **Закрыть**.

## 6.2 Уведомление «Выбранный сертификат не действителен»

При авторизации в личном кабинете сертификат электронной подписи не прошел проверку. Появилось окно с уведомлением «Выбранный сертификат не действителен. Выберите другой»:

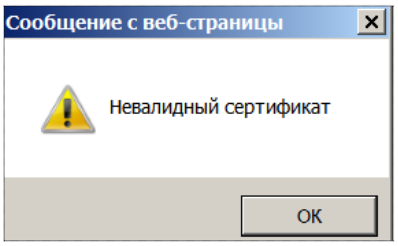



Возможные причины и методы решения проблемы:

- Истек срок действия личного сертификата. Актуализируйте личный сертификат.
- Нарушена целостность личного сертификата. Возможно он поврежден, или изменен. Используйте для авторизации личный сертификат, целостность которого гарантирована.
- Не установлен корневой сертификат. Выполните его переустановку согласно инструкциям в п. 4.1.1.
- Нарушена работоспособность криптопровайдера. Переустановить и настроить криптопровайдер согласно инструкциям, полученным в УЦ. Затем – с помощью данного криптопровайдера выполнить повторную установку личного сертификата (см. п. 4.1.2, 4.1.3 или 4.1.4).

## 6.3 Уведомление «Невалидный сертификат»

При попытке авторизации в личном кабинете сертификат электронной подписи не прошел проверку на соответствие требованиям, предъявляемым к составу содержащихся в нем сведений. Появилось окно с уведомлением «Невалидный сертификат»:




При этом к составу сведений предъявляются следующие требования:

- в поле «Субъект» («Subject») должен присутствовать атрибут «ИНН». Значение атрибута «ИНН» должно быть числовым – длиною в 10 (для ЮЛ) или 12 (для физических лиц) цифр. При этом оно не может состоять только из нулей (например, «0000000000»);
- если в поле «Субъект» («Subject») присутствует атрибут «ОГРН», то его значение должно быть числовым – длиною в 13 цифр. При этом оно не может состоять только из нулей;
- если в поле «Субъект» («Subject») или поле «Дополнительное имя субъекта» («Subject Alternative Name») присутствует атрибут «ОГРНИП», то его значение должно быть числовым – длиною в 15 цифр. При этом оно не может состоять только из нулей;
- если в поле «Субъект» («Subject») присутствует атрибут «СНИЛС», то его значение должно быть числовым – длиною в 11 цифр. При этом оно не может состоять только из нулей.

Необходимо обратиться в службу поддержки пользователей по адресу электронной почты bhelp@interfax.ru.

## 6.4 Уведомление «Сертификат не выбран»

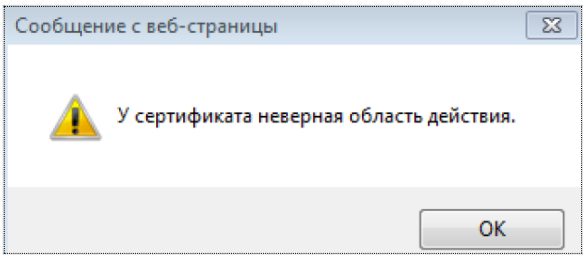
Проблема: при проверке подписи после нажатия кнопки **Проверить** в разделе «Помощь» открытого сайта появляется окно с уведомлением «Сертификат не выбран». При этом окно выбора сертификата не появляется.

Возможная причина проблемы – сертификаты (личный и/или корневой) не были добавлены в локальное хранилище.

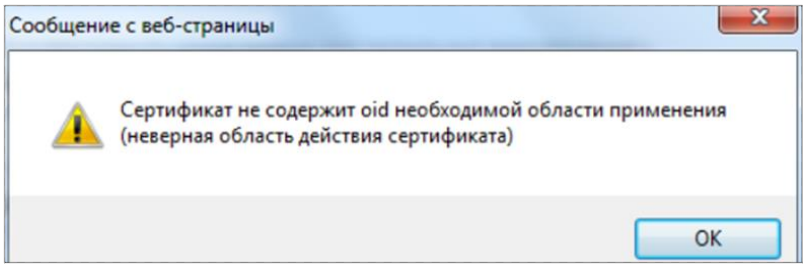
Метод устранения проблемы – необходимо добавить сертификат (сертификаты) в локальное хранилище в соответствии с инструкциями, приведенными в п. 4.1.

## 6.5 Уведомление «У сертификата неверная область действия» или «Сертификат не содержит oid необходимой области применения»

Проблема: при проверке подписи в разделе «Помощь» открытого сайта появляется окно с уведомлением «У сертификата неверная область действия»:




Или при попытке авторизации в личном кабинете появляется окно с уведомлением «Сертификат не содержит oid необходимой области применения (неверная область действия сертификата)»:

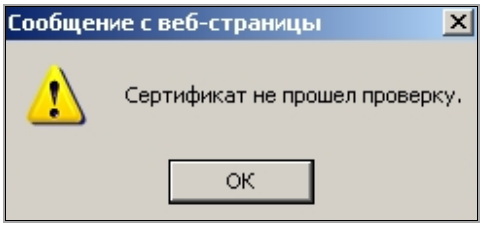



Причина проблемы – сертификат не содержит в расширении Extended Key Usage корректный объектный идентификатор (OID).

Необходимо обратиться в Удостоверяющий центр или в службу поддержки пользователей по адресу электронной почты bhelp@interfax.ru.

## 6.6 Уведомление «Сертификат не прошел проверку»

Проблема: при проверке подписи после нажатия кнопки **Проверить** в разделе «Помощь» открытого сайта появляется окно с уведомлением:



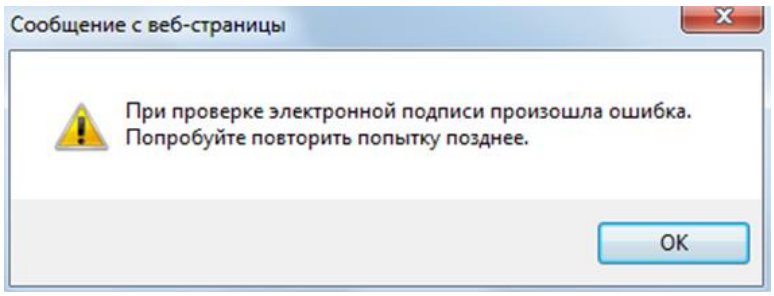

Сообщение выдается в следующих случаях:

- при несовпадении значения атрибута «SN» (SubjectName) поля «Субъект» («Subject») сертификата с переданным значением данного атрибута;
- при ошибке построения цепочки сертификатов:
  - истек срок действия одного из сертификатов;
  - не установлен один из сертификатов цепочки;
  - один из сертификатов цепочки отозван УЦ, выпустившим данный сертификат;
  - отсутствует доверие к корневому или промежуточному сертификату (сертификат не принадлежит доверенному УЦ);
  - один из сертификатов цепочки заблокирован.

Необходимо обратиться в службу поддержки пользователей по адресу электронной почты bhelp@interfax.ru.

## 6.7 Уведомление «При проверке электронной подписи произошла ошибка»

Проблема: при проверке подписи после нажатия кнопки **Проверить** в разделе «Помощь» открытого сайта появляется окно с уведомлением «При проверке электронной подписи произошла ошибка».

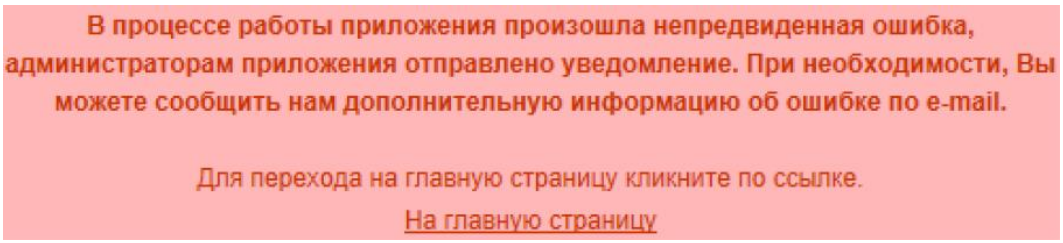



Подобная ошибка возникает при различных видах сбоев, которые могут возникать во время обращения к Системе, например, при проблемах в канале связи.

Проверьте работоспособность канала связи в вашей электронной сети. Если проблема в канале выявлена не будет, то необходимо обратиться в службу поддержки пользователей по адресу электронной почты bhelp@interfax.ru.

## 6.8 При проверке подписи выдается «красная ошибка»

Проблема: при проверке подписи после нажатия кнопки **Проверить** в разделе «Помощь» открытого сайта выдается страница с «красной ошибкой»:

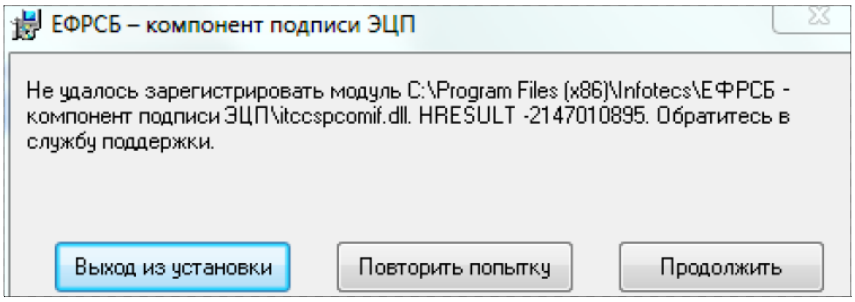



Необходимо обратиться в службу поддержки пользователей по адресу электронной почты bhelp@interfax.ru. При этом в письме следует указать время, когда производилась проверка подписи и название Удостоверяющего центра, в котором был получен сертификат подписи.

Желательно приложить к электронному письму скриншот страницы с сообщением об ошибке (как сделать скриншот см. в п. 7.3).

## 6.9 При установке ActiveX-компонента подписи выдается уведомление «Не удалось зарегистрировать модуль…»

Указанное уведомление об ошибке выглядит следующим образом:




Для устранения данной ошибки необходимо скачать инсталлятор компонента Microsoft Visual C++ 2008 Redistributable Package (x86), доступный по данной ссылке. На открывшейся странице следует нажать кнопку Download. После скачивания – запустить файл vcredist_x86.exe, который выполнит установку этого компонента.

> **Важно!** В Windows 7 необходимо запускать файл vcredist_x86.exe от имени администратора (щелкнуть на файле правой кнопкой мыши и в появившемся контекстном меню выбрать пункт **Запуск от имени администратора**).

# 7 Приложения

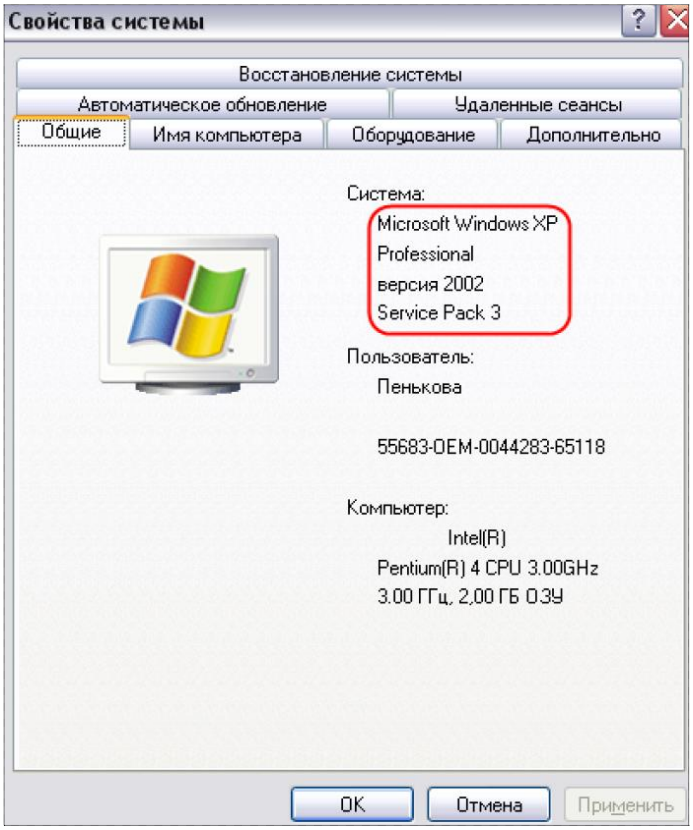
Поведение ActiveX-компонента зависит от того, в какой операционной системе и в каком браузере работает пользователь. При этом для разных операционных систем и браузеров применяются различные методы решения возникающих вопросов.

Имеет значение не только версия операционной системы, но и ее разрядность (64 / 32). Это особенно важно для операционных систем Windows 7 и Vista. Кроме того может иметь значение номер установленного сервисного пакета (SP).

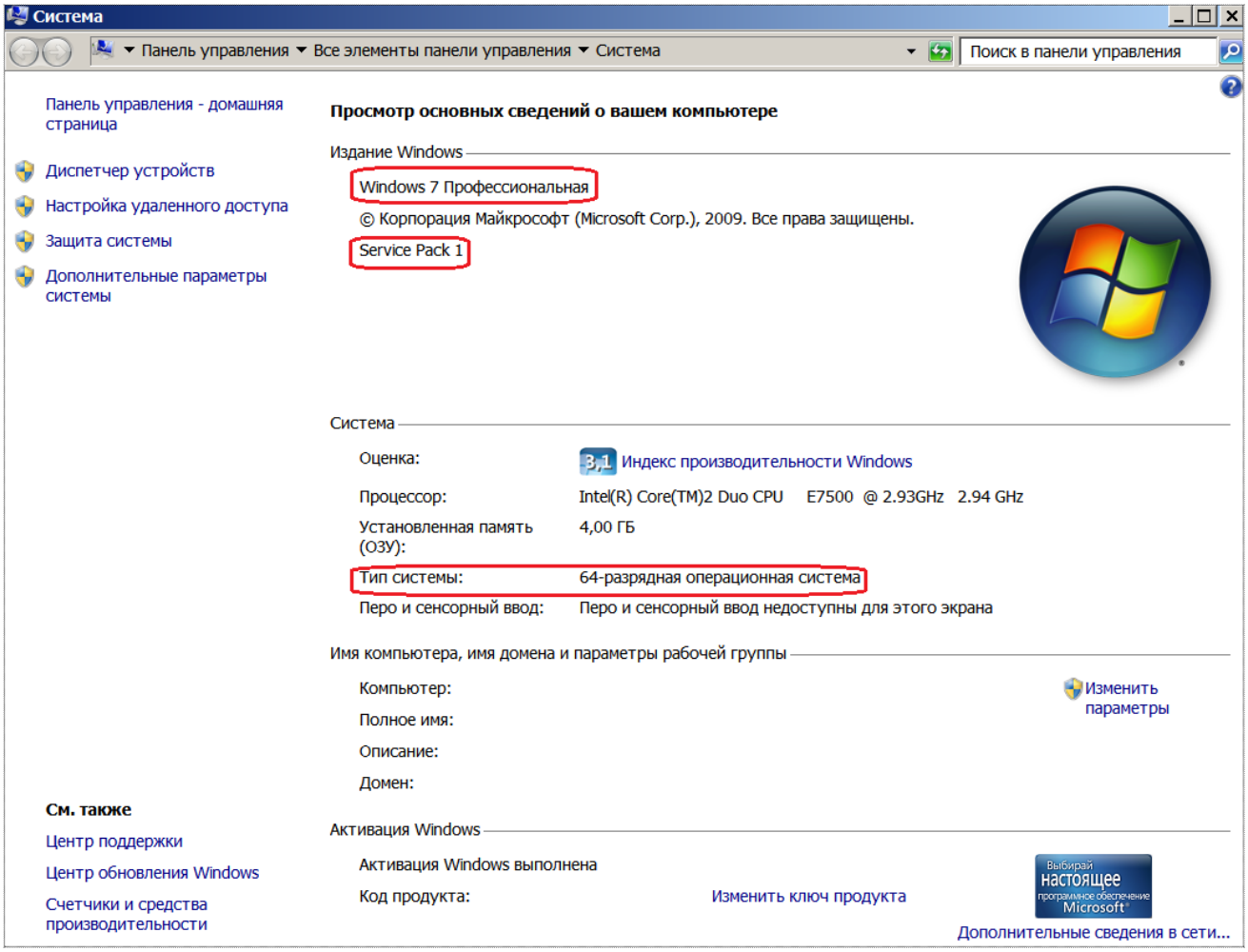
## 7.1 Как определить версию Windows

Для того чтобы определить версию операционной системы Windows необходимо выполнить следующие действия:

1. Нажав кнопку **Пуск** открыть главное меню Windows.
2. Найти пункт меню **Мой компьютер** (в Windows XP) или **Компьютер** (в Windows Vista / 7), щелкнуть на нем правой кнопкой и выбрать в контекстном меню пункт **Свойства**.
3. Откроется окно свойств операционной системы:
   a. в Windows XP окно имеет следующий вид:




b. в Windows 7 или Vista окно имеет следующий вид:

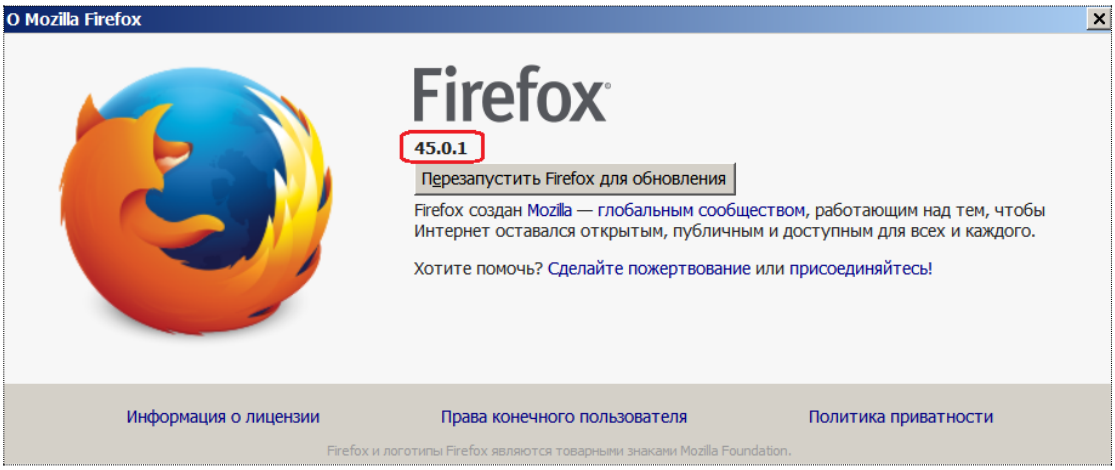


На рисунках выше в окнах выделены сведения, которые необходимо сообщить в службу технической поддержки по запросу или учесть при выполнении некоторых инструкций, приведенных в настоящей документе.

## 7.2 Как определить версию браузера

Для того чтобы определить версию браузера **Internet Explorer** необходимо в правом верхнем углу его окна щелкнуть на пиктограмме  и в появившемся меню выбрать пункт **О программе**. Откроется окно **О программе Internet Explorer**, содержащее атрибут **Версия**:


Для того чтобы определить версию браузера Mozilla Firefox необходимо в правом верхнем углу его окна щелкнуть на пиктограмме  , в появившемся меню щелкнуть на пиктограмме  . В открывшемся контекстном меню пункт **О Firefox**. Появится окно **О Mozilla Firefox**, в котором отображается номер версии вашего браузера:




## 7.3 Как сделать скриншот (снимок экрана)

Скриншот – это «фотография» текущего состояния рабочего стола (снимок экрана). Он часто бывает необходим для более быстрого решения проблем, возникающих при работе с Системой.

Для того чтобы сделать скриншот необходимо выполнить следующие действия:

1. Вывести на экран проблемную страницу (окно) Системы и нажать клавишу **PrtScr** (PrintScreen), расположенную в правой верхней части клавиатуры, рядом с кнопкой F12.
2. Запустить программу Microsoft Word (открыть Word-документ).
3. Нажать сочетание клавиш Ctrl+V – снимок экрана будет вставлен в открытый Word-документ.
4. Описанным способом сделать скриншоты всех страниц (окон) Системы, отражающих суть проблемы.
5. Сохранить Word-документ.
6. Выслать сохраненный Word-документ на адрес электронной почты bhelp@interfax.ru.