

ИНСТРУКЦИЯ ПО УСТАНОВКЕ КОМПОНЕНТ ЭЛЕКТРОННОЙ ПОДПИСИ

(версия 2.3 от 16 марта 2022 года)

На: 40 листах

СОДЕРЖАНИЕ

1	Общие сведения	4
2	Проверка конфигурации системы	5
3	Необходимое программное обеспечение	6
4	Установка ПО, необходимого для создания ЭП.....	7
4.1	Установка криптопровайдера и сертификата ключа подписи.....	7
4.2	Установка компонента "Федресурс. Плагин ЭП"	7
4.3	Установка браузерного расширения и другие настройки браузера	9
4.3.1	Для браузера Firefox	9
4.3.2	Для браузера Chrome или Yandex	11
4.3.3	Возможные настройки браузера Internet Explorer	12
5	Настройка ПО для возможности подписи.....	13
5.1	Добавление сертификата в локальное хранилище Windows.....	13
5.1.1	Установка корневого сертификата.....	14
5.1.2	Установка личного сертификата при помощи программы КриптоПро	17
5.1.3	Установка личного сертификата при помощи программы VipNet CSP	24
5.1.3.1	Установка личного сертификата с ключевого носителя JaCarta LT	24
5.1.3.2	Установка личного сертификата с компакт-диска (CD)	29
5.1.4	Установка личного сертификата при помощи программы Signal-COM CSP	31
6	Проверка работоспособности ЭП.....	32
7	Разрешение проблем неработоспособности ЭП	33
7.1	Уведомление «Не установлено программное обеспечение ...»	33
7.2	Уведомление «Выбранный сертификат не действителен»	33
7.3	Уведомление «Невалидный сертификат».....	33
7.4	Уведомление «Не найдено ни одного сертификата или не установлен криптопровайдер»	34
7.5	Уведомление «У сертификата неверная область действия» или «Сертификат не содержит oid необходимой области применения».....	35
7.6	Уведомление «Сертификат не прошел проверку».....	35
7.7	Уведомление «У компонента недостаточно прав для доступа к сертификатам».....	36
7.8	Уведомление «При проверке электронной подписи произошла ошибка».....	36
7.9	При проверке подписи выдается «красная ошибка»	37
8	Приложения.....	37
8.1	Как определить версию Windows	37

8.2	Как определить версию MacOS	38
8.3	Как определить версию ОС семейства Linux	39
8.4	Как определить версию браузера	39
8.5	Как сделать скриншот (снимок экрана)	40

ИСПОЛЬЗУЕМЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Описание
Федресурс	Единый федеральный реестр юридически значимых сведений о фактах деятельности юридических лиц, индивидуальных предпринимателей и иных субъектов экономической деятельности (ЕФРСФДЮЛ)
ЕФРСБ	Единый федеральный реестр сведений о банкротстве. Составная часть Федресурс.
Плагин	Утилита, обеспечивающая взаимодействие криптопровайдера с веб-браузером
ПО	Программное обеспечение
Система	Федресурс (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

Для полноценной работы с порталом Федресурс¹ необходимо наличие сертификата ключа электронной подписи. Он используется для следующих операций:

- Авторизации в личные кабинеты (исключая личные кабинеты с авторизацией по логину и паролю)

Сертификат ключа электронной подписи позволяет однозначно идентифицировать пользователя и более безопасен, чем вход по логину и паролю.

- Подписи вносимых в реестр данных (сообщения, карточки создаваемых сущностей и т.д.) и электронных документов (счета-фактуры, акты)

Таким образом обеспечивается неотрекаемость опубликованных сведений и их целостность (если после подписи данные были изменены, электронная подпись позволит доказать факт искажения информации).

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

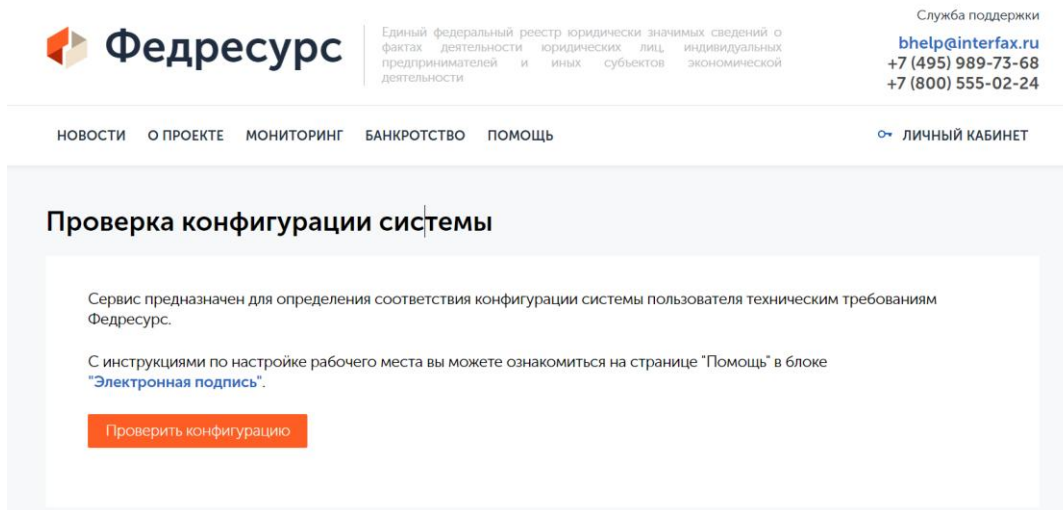
2 Проверка конфигурации системы

Для понимания всего ли Вам хватает для начала работы с системой на портале Федресурс реализован функционал проверки конфигурации системы.

Он расположен по адресу - <https://fedresurs.ru/check>

Иначе его можно найти, перейдя в раздел «Помощь», затем нажав «Проверка конфигурации системы и электронной подписи» в блоке «Электронная подпись».

На странице проверки конфигурации нажмите кнопку «Проверить конфигурацию».



Если у Вас установлено необходимо ПО, то система предложит выбрать сертификат из списка и отобразит результаты проверки.

Результаты проверки:

Операционная система: Windows 10
Браузер: Chrome 98 (98.0.4758.102)
ПО для работы с ЭЦП: Установлено
Адаптер плагина Blitz Smart Card Plugin
Федресурс: Плагин ЭП
Криптопровайдер

Сертификат: Подпись валидна

Для работы в системе сертификат должен выполнять одно из следующих условий:

- пользователь является физическим лицом, в том числе индивидуальным предпринимателем, действующим от своего имени;
- пользователь является лицом, имеющим право действовать от имени юридического лица без доверенности;
- пользователь уполномочен на взаимодействие с Реестром на основе электронной доверенности, внесенной в Реестр;
- сертификат пользователя содержит один из объектных идентификаторов:
OID 1.3.6.1.4.1.40870.1.1.1
OID 1.2.643.2.64.1.1.1
OID 1.2.643.3.5.10.2.12
OID 1.2.643.6.3.2

CN = Общество с ограниченной ответственностью Автодеталь-Сервис тест
GN = Василий Борисович
INN = ██████████
O = ООО Автодеталь-Сервис тест
OGRN = ██████████
SN = Петров
T = сотрудник

В случае отсутствия какого-либо программного обеспечения необходимого для работы с системой или проблем с самим сертификатом, результаты проверки сообщат об этом.

Результаты проверки:

Операционная система: **Windows 10**

Браузер: **Chrome 99 (99.0.4844.51)**

ПО для работы с ЭЦП: **Не установлено**

Федресурс: Плагин ЭП

Не установлено необходимое ПО.

Для работы с ЭП необходимо установить:

1. Криптопровайдер: КриптоПро, Signal-COM CSP, ViPNet CSP
2. Федресурс. Плагин ЭП
3. Расширение для браузера Адаптер плагина Blitz Smart Card Plugin (только для Google Chrome и Mozilla Firefox)

В разделе "[Помощь](#)" представлены ссылки на установщики и инструкция по настройке.

Если проверка показала отсутствие необходимого ПО, то дальнейшая инструкция поможет вам в его установке и настройке.

3 Необходимое программное обеспечение

Для обеспечения взаимодействия криптопровайдера с браузером используются дополнительные утилиты: компонент "Федресурс. Плагин ЭП" (далее – плагин), специальное расширение для FireFox, Chrome, Yandex (далее – браузерное расширение). При этом конкретный вариант развертывания зависит от того, в каком браузере и в какой операционной системе (далее – ОС) Вы работаете. Соответствующая матрица установки представлена в таблице ниже.

Клиентская операционная система	Windows 8.1 и выше	Ubuntu 18, Mint 19, Debian 10	MacOS версии 10.15 и выше
Браузер	Firefox Mozilla актуальной версии (далее – Firefox)		
	Google Chrome актуальной версии (далее – Chrome)		
	Яндекс.Браузер актуальной версии (далее – Yandex)		
	Internet Explorer 11 и выше (далее – IE)		
Криптопровайдер	КриптоПро CSP 4.0 КриптоПро CSP 5.0 Signal-COM CSP 3.0 ViPNet CSP 4.2	КриптоПро CSP 4.0 КриптоПро CSP 5.0	КриптоПро CSP 4.0 КриптоПро CSP 5.0
Плагин	"Федресурс. Плагин ЭП"		
Браузерное расширение	для Firefox, Chrome, Yandex		

Внимание! Работа в серверных версиях данных ОС не поддерживается.

Поддерживаемые средства хранения ЭП: ESMART Token / Token ГОСТ, SafeNet eToken, JaCarta PKI, eToken ГОСТ, Рутокен ЭЦП/ ЭЦП 2.0 / ЭЦП PKI / ЭЦП micro, Рутокен ЭЦП Smart Card, Рутокен S / S micro, Рутокен Lite / Lite micro, Рутокен Lite Smart Card.

Шаги по развертыванию требуемых компонентов приведены в разделе «Установка ПО, необходимого для создания ЭП».

4 Установка ПО, необходимого для создания ЭП

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

4.1 Установка криптопровайдера и сертификата ключа подписи

Возможные варианты действий:

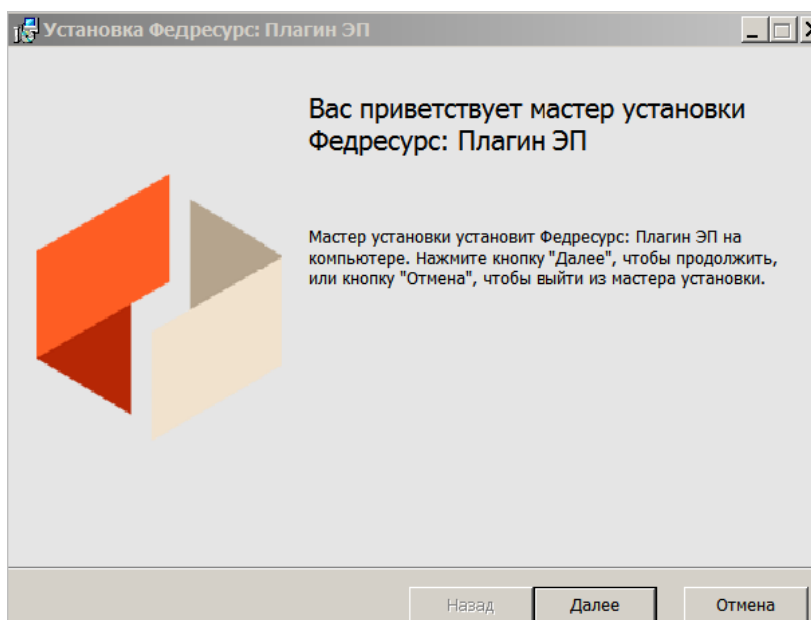
1. Криптопровайдер уже установлен на компьютер пользователя. Сертификат ключа проверки ЭП был получен и установлен, и срок его действия не истек. В этом случае, необходимо выяснить, есть ли удостоверяющий центр, выдавший сертификат, в перечне УЦ, размещенном в разделе **Применение электронной подписи** на странице «Помощь» открытого сайта. Если УЦ там есть, то необходимо уточнить непосредственно в службе поддержки УЦ, допустимо ли использование данного сертификата в Федресурс. В случае положительного ответа на этот вопрос, можно переходить к выполнению действий, описанных в п. 4.2.
2. Один из криптопровайдеров 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 в разделе **Применение электронной подписи** на странице «Помощь»
 - b. При установке и настройке криптопровайдера необходимо следовать инструкциям, предоставленным УЦ.

4.2 Установка компонента "Федресурс. Плагин ЭП"

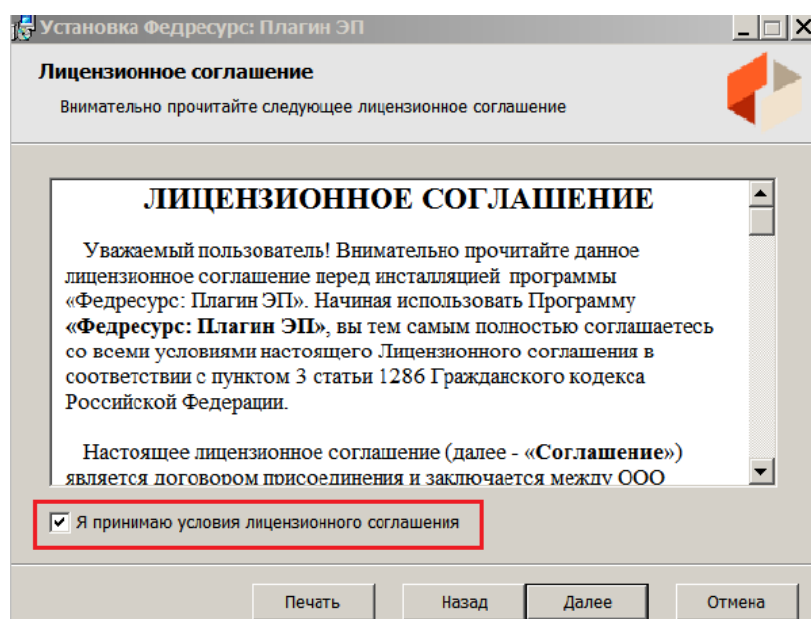
Внимание! Плагин должен быть установлен в локальный профиль пользователя на ПК. Перемещаемые профили не поддерживаются. Каталог установки для пользователя должен иметь вид "C:\Users\User\AppData\Roaming\REAKSOFT\Fedresurs DS Plugin\<версия плагина, например, 1.16.0.2>\"

Для установки компонента "Федресурс. Плагин ЭП" необходимо выполнить следующие действия:

1. Скачать архив с инсталлятором компонента "Федресурс. Плагин ЭП", доступный по ссылке в разделе **Программное обеспечение** на странице «Помощь». Запомнить папку, в которую был скачан архив. Выполнить разархивацию инсталлятора. Ниже приведены форматы имен инсталлятора для различных операционных систем:
 - для Windows: FedresursDSPlugin-x.x.x.x.msi, где x.x.x.x – номер текущей версии
 - для ОС семейства Linux: FedresursDSPlugin-z.z.z.z-x86_64.deb, где z.z.z.z – номер текущей версии
 - для MacOS: FedresursDSPlugin-z.z.z.z.pkg, где z.z.z.z – номер текущей версии
2. Открыть папку, в которую был сохранен файл инсталлятора и запустить его на выполнение. Откроется окно приветствия мастера установки:

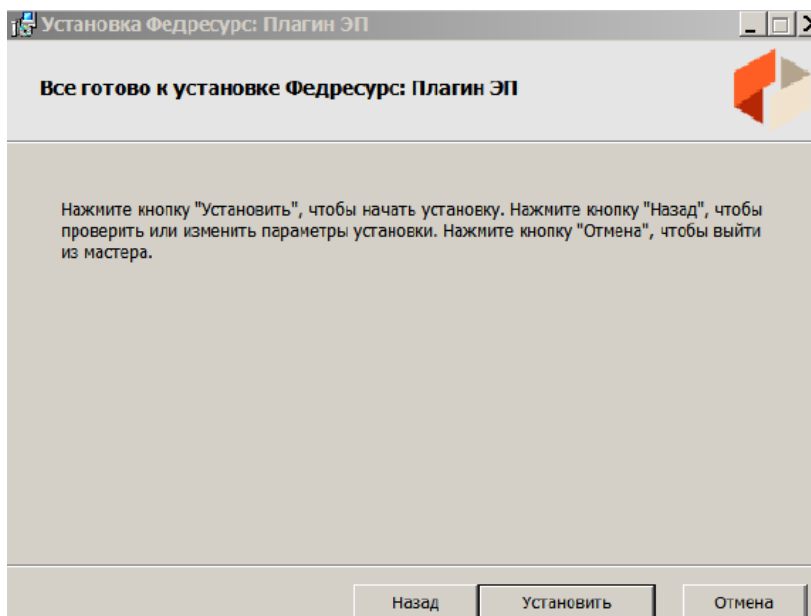


3. Нажать кнопку **Далее**. Откроется окно лицензионного соглашения:

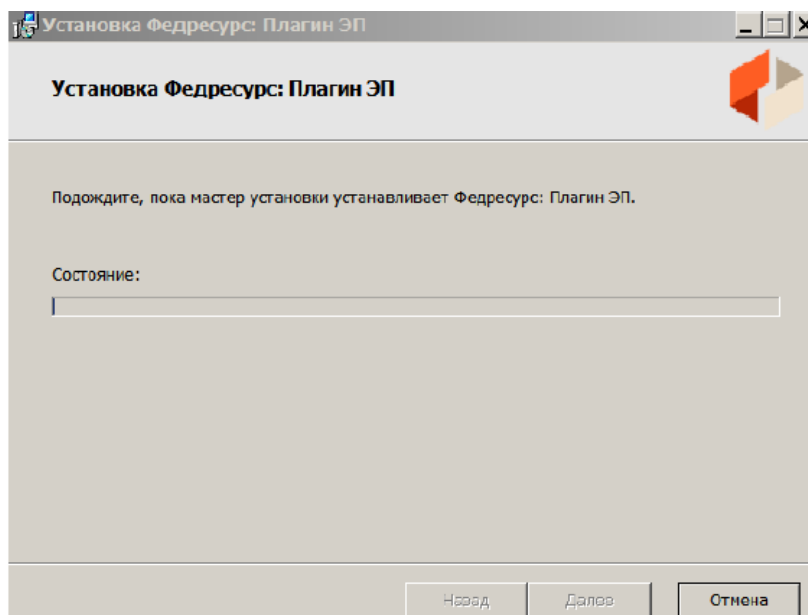


4. Здесь следует включить опцию **Я принимаю условия лицензионного соглашения** и нажать **Далее**. Откроется окно для выбора папки установки компонента. Сменить папку

или оставить папку, предлагаемую по умолчанию. Нажать кнопку **Далее**. Откроется окно с уведомлением о готовности к установке:



5. Нажать кнопку **Установить**. Появится окно отображающее ход процесса установки компонента:



6. По завершении процедуры установки появится окно **Установка завершена**. Нажмите в нем кнопку **Готово**.


4.3 Установка браузерного расширения и другие настройки браузера

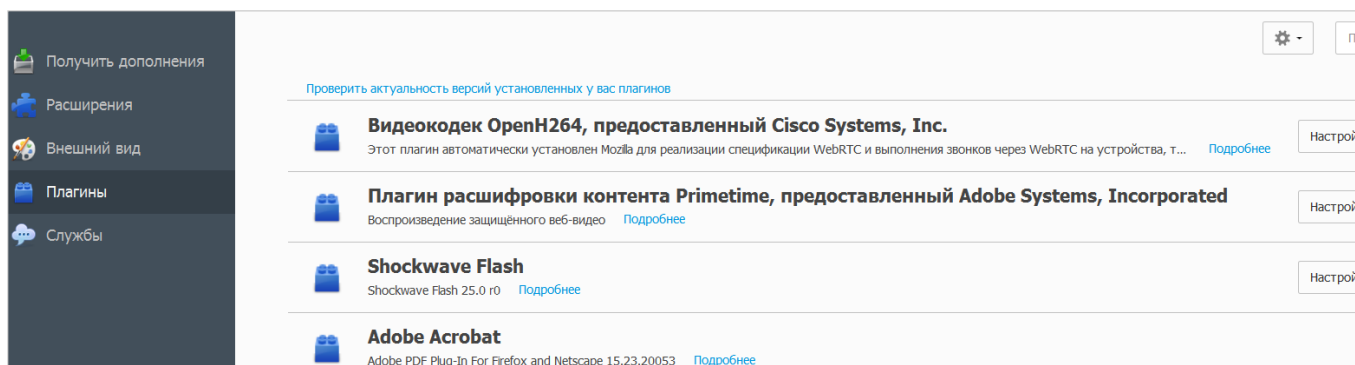
4.3.1 Для браузера Firefox


Если Вы используете браузер FireFox, то в дополнение к установке компонента "Федресурс. Плагин ЭП" (см. п. 4.2) необходимо установить браузерное расширение для FireFox. Для этого нужно выполнить следующие действия:

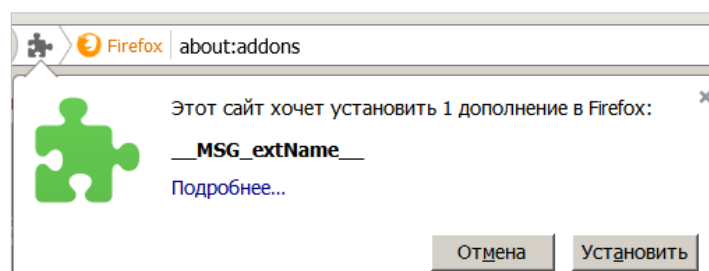
1. Скачать расширение, щелкнув на ссылке **Плагин браузера FireFox для компонента подписи**, расположенную в разделе **Программное обеспечение** на странице «Помощь». Запомнить

папку, в которую был скачан плагин (архив blitz_smart_card_plugin.zip). Распаковать скачанный архив.

2. Открыть браузер FireFox. Нажать в его панели инструментов на кнопку .
3. В появившемся меню выбрать пункт **Дополнения**.
4. В левой части открывшейся страницы браузера выбрать пункт меню **Плагины**. Откроется страница со списком установленных расширений:



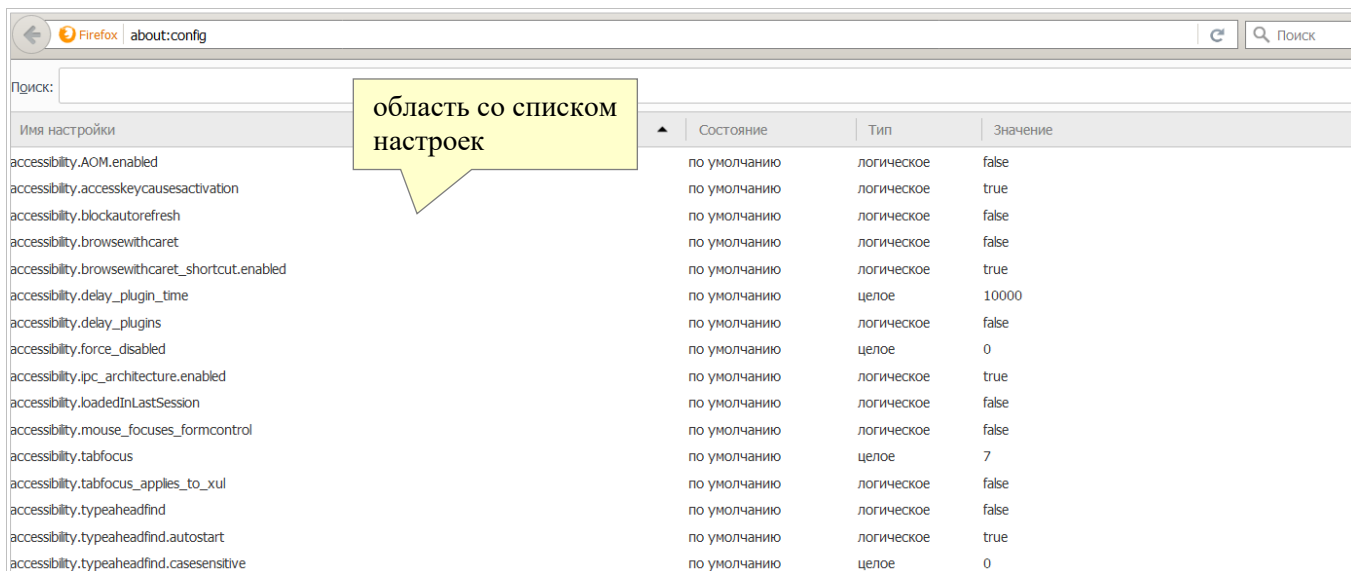
5. Вверху страницы нажать на кнопку  и выбрать в раскрывшемся списке пункт **Установить дополнение из файла**.
6. С помощью открывшегося стандартного окна навигации найти папку, в которую был скачан плагин, открыть её и выбрать файл плагина.
7. В левом верхнем углу окна браузера появится всплывающее уведомление:



8. Нажать кнопку **Установить**.

Если ранее Вы применяли утилиту ActiveX-компонент ЭП, то для переключения на применение компонента "Федресурс. Плагин ЭП" нужно настроить браузер FireFox:

1. Ввести в адресной строке FireFox адрес «about:config» – откроется страница со списком настроек Firefox:



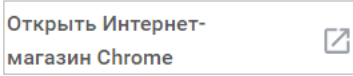
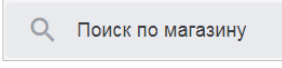


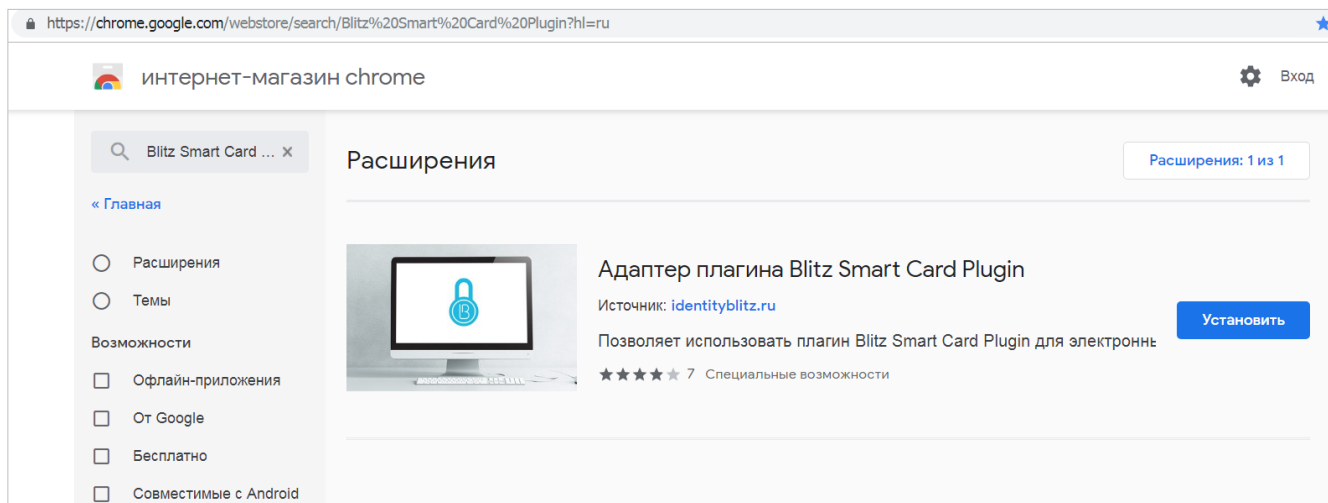
2. Найти в списке настройку *plugin.load_flash_only* (для этого можно ввести данное имя в верхнее поле **Поиск**).
3. Убедиться, что поле **Значение** у найденной записи имеет значение **false**. Если это так, то щелкнуть на записи правой кнопкой мыши и в появившемся меню выбрать пункт **Переключить**. Значение должно смениться на **true**.
4. Перезагрузить браузер (полностью его закрыв).

4.3.2 Для браузера Chrome или Yandex

Если Вы используете браузер Chrome или Yandex, то в дополнение к установке компонента "Федресурс. Плагин ЭП" (см. п. 4.2) необходимо установить специальное расширение для Chrome. Для этого нужно выполнить следующие действия:

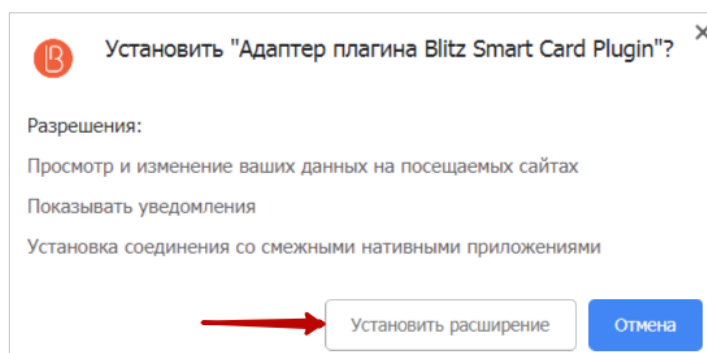
1. Открыть браузер Chrome или Yandex.
2. Введя в адресной строке открытого браузера ссылку <https://chrome.google.com/webstore/search/Blitz%20Smart%20Card%20Plugin?hl=ru>, зайти в интернет-магазин chrome с представленным в нем расширением «Адаптер плагина Blitz Smart Card Plugin»:

Примечание для Chrome. Также можно через меню браузера зайти в интернет-магазин и выполнить поиск требуемого расширения. Для этого нужно нажать в правом верхнем углу браузера кнопку  и выбрать в выпадающем меню пункт **Дополнительные инструменты** | **Расширения**. Далее необходимо в левом верхнем углу страницы **Расширения** нажать кнопку . Затем – в левом нижнем углу – кнопку . На странице магазина можно воспользоваться поисковым полем , введя в него запрос «Blitz Smart Card».




3. Нажать расположенную в правой части страницы кнопку **Установить**.

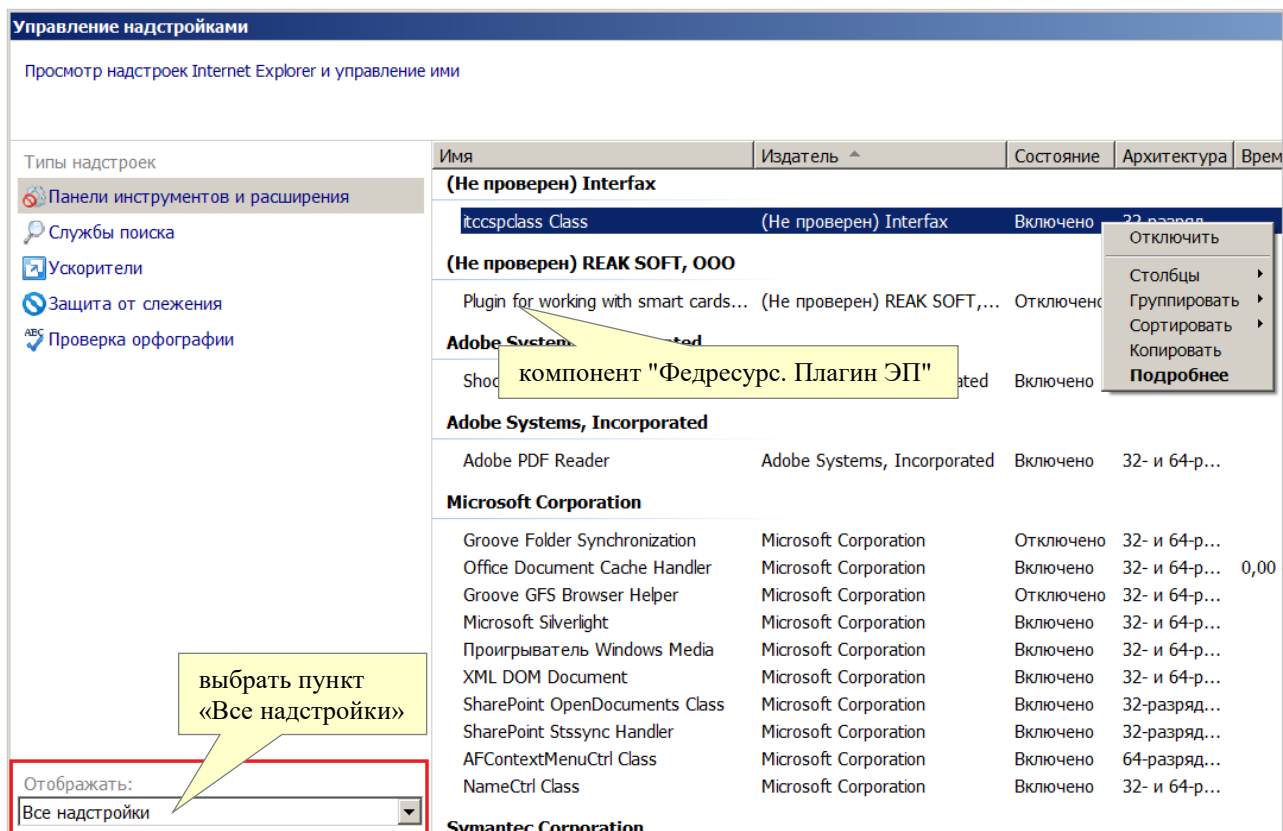
4. Затем – нажать кнопку **Установить расширение** в появившемся всплывающем окне:



4.3.3 Возможные настройки браузера Internet Explorer

Если ранее Вы применяли «старый» плагин (ActiveX-компонент ЭП), то для переключения на применение компонента "Федресурс. Плагин ЭП" нужно выполнить настройку браузера Internet Explorer:

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



2. Выключить устаревший плагин ActiveX-компонент ЭП, указав в списке запись **itccspclass Class**, щелкнув на ней правой кнопкой мыши и в появившемся контекстном меню выбрав пункт **Отключить**
3. Включить компонент "Федресурс. Плагин ЭП". В настройках данный компонент представлен записью **Plugin for working with smart cards** (в группе **REAK SOFT**). Для того чтобы данная запись появилась в списке, может понадобиться в списке **Отображать** в левом нижнем углу окна выбрать пункт **Все надстройки**. Включить компонент, щелкнув правой кнопкой мыши на записи **Plugin for working with smart cards** и в появившемся меню выбрав пункт **Включить**.
4. Перезагрузить браузер (полностью его закрыв).

5 Настройка ПО для возможности подписи

5.1 Добавление сертификата в локальное хранилище Windows

Для того чтобы компонент "Федресурс. Плагин ЭП" 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 и Signal-COM.

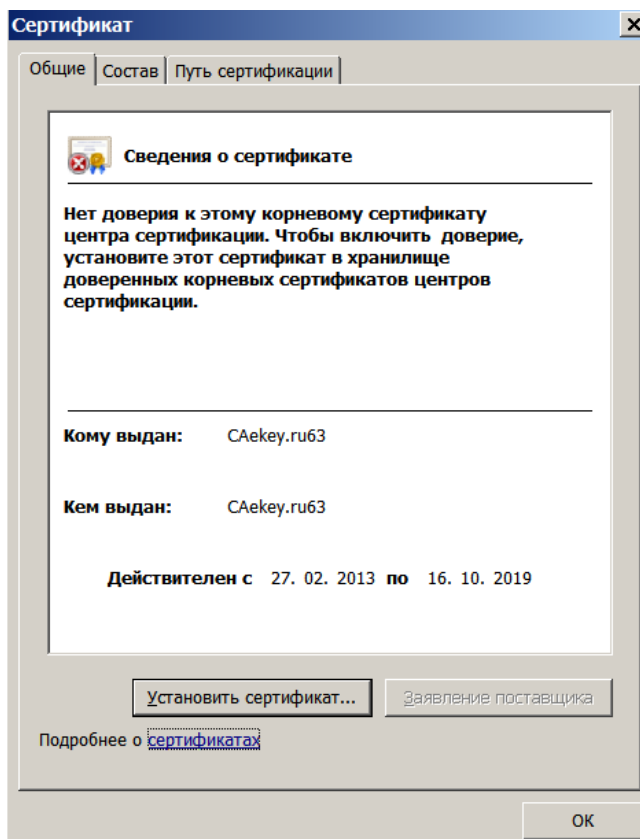
Предполагается, что криптопровайдер установлен. Иначе, необходимо его установить согласно инструкциям, приведенном в п. 4.1.

ВНИМАНИЕ! Для ключевой пары ЭП (закрытого и открытого ключа) свойство Key Specification («KeySpec») обязательно должно иметь значение at_keyexchange.

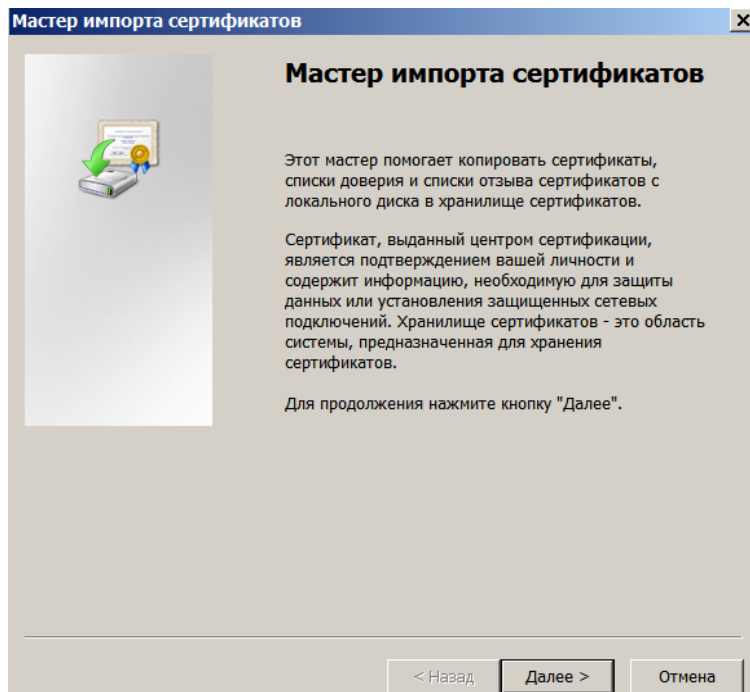
5.1.1 Установка корневого сертификата

Корневой сертификат можно получить на Портале уполномоченного федерального органа в области использования электронной подписи – <http://e-trust.gosuslugi.ru>.

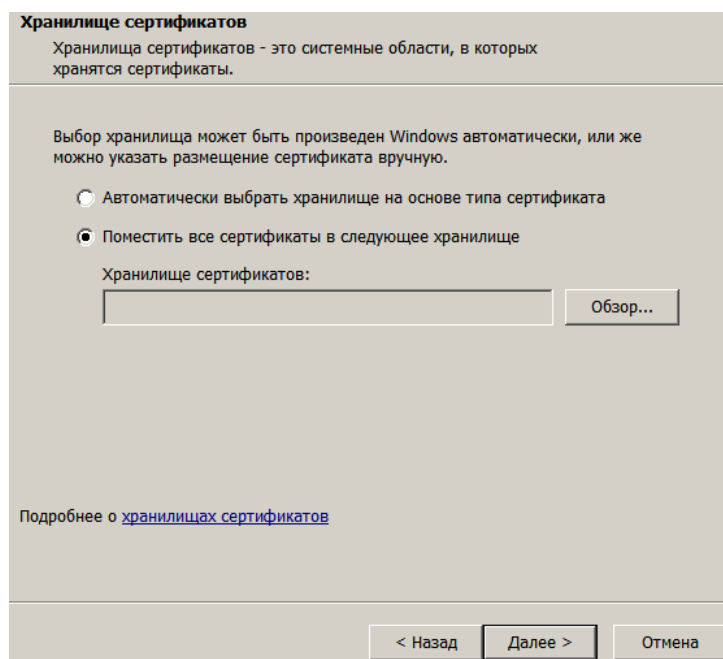
1. Откройте полученный файл корневого сертификата, дважды щелкнув на нем левой кнопкой мыши. Появится окно Сертификат:



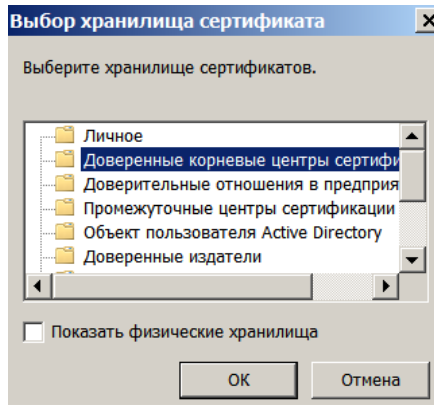
2. Нажмите кнопку **Установить сертификат**. Откроется первое окно мастера импорта сертификатов:



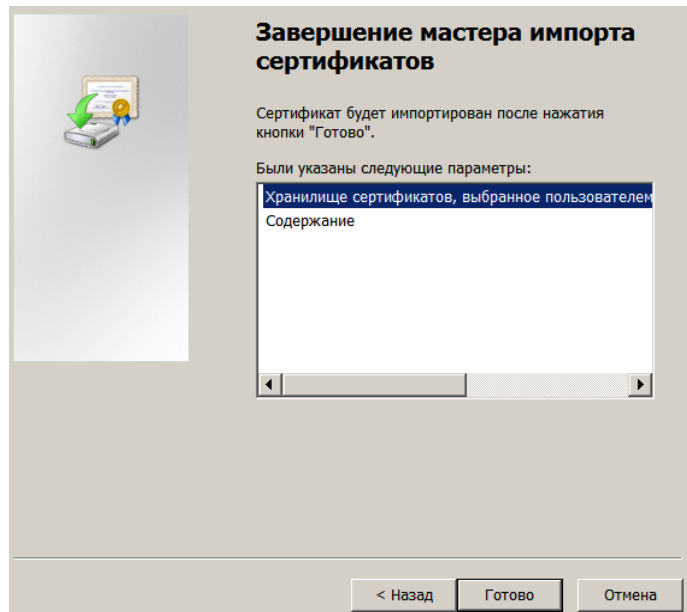
3. Нажмите кнопку **Далее**. Откроется окно выбора хранилища сертификатов. Установите переключатель в позицию **Поместить сертификаты в следующее хранилище**:



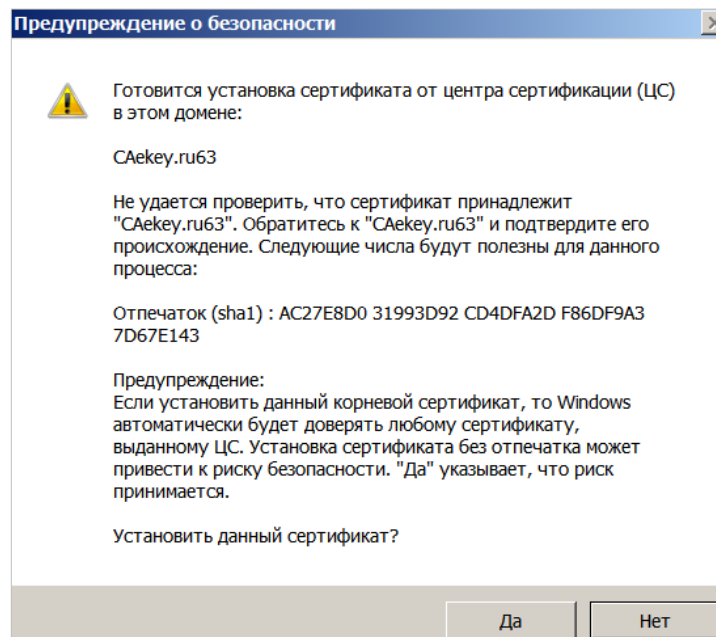
4. Нажмите кнопку **Обзор**. Откроется окно для выбора хранилища:



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:

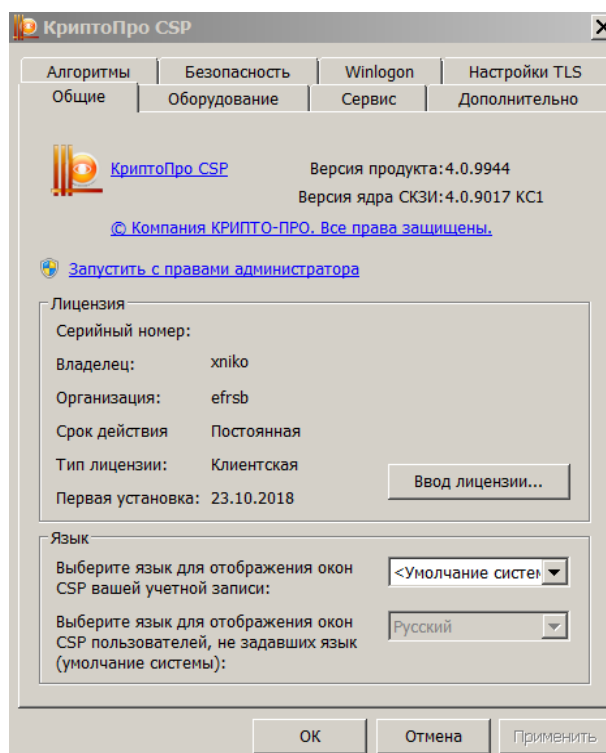


7. Нажмите кнопку **Да**. Сертификат будет установлен.

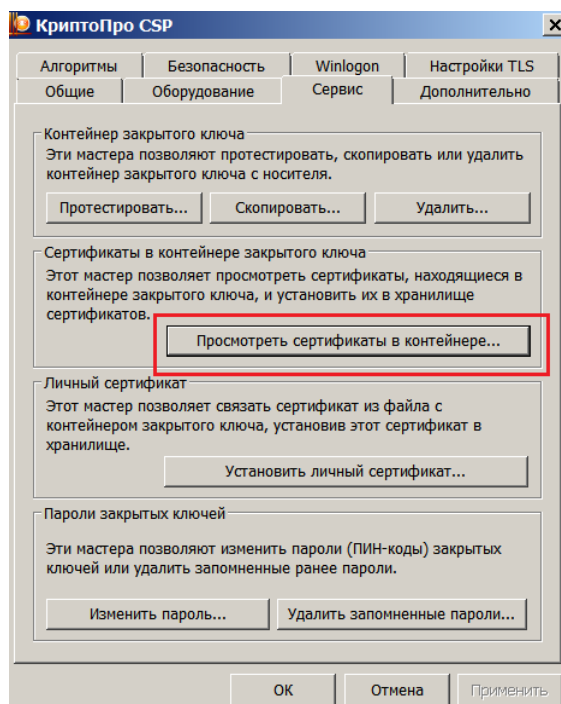
5.1.2 Установка личного сертификата при помощи программы КриптоПро

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

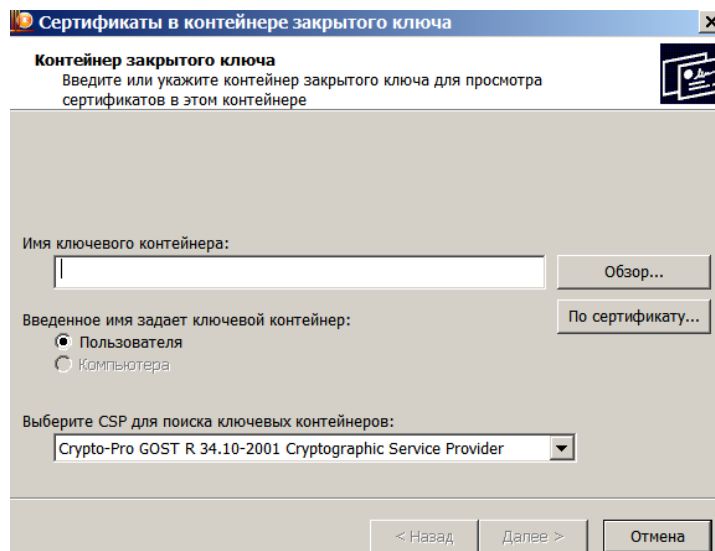
1. Выберите в главном меню Windows пункт **Пуск / Все программы / КРИПТО-ПРО / КриптоПро CSP**. Откроется окно программы КриптоПро CSP:



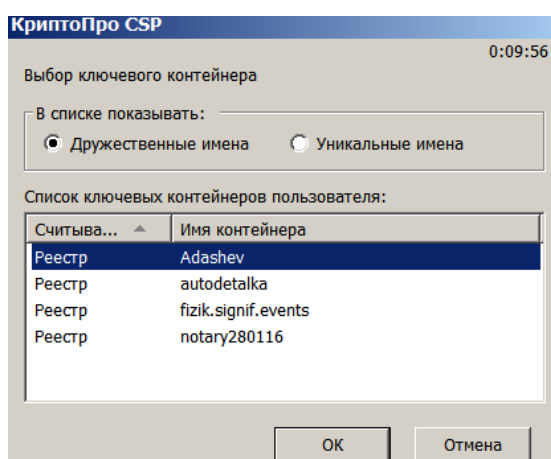
2. Зайдите на вкладку **Сервис** и нажмите кнопку **Просмотреть сертификаты в контейнере**:



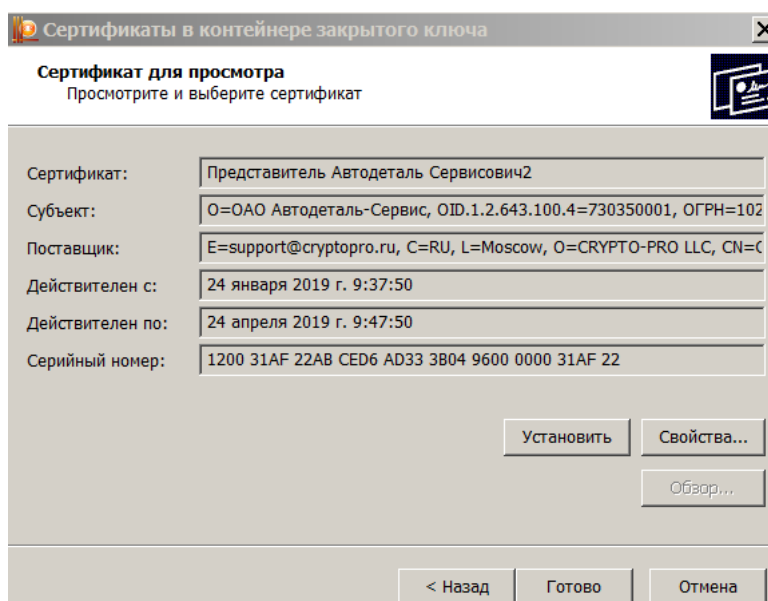
3. Откроется окно **Сертификаты в контейнере закрытого ключа**:



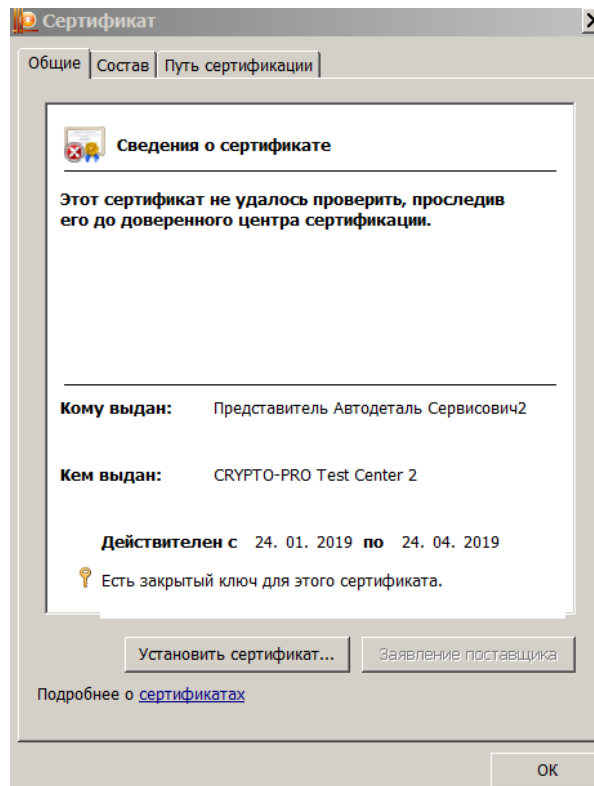
4. Нажмите кнопку **Обзор**. Откроется окно со списком ключевых контейнеров:



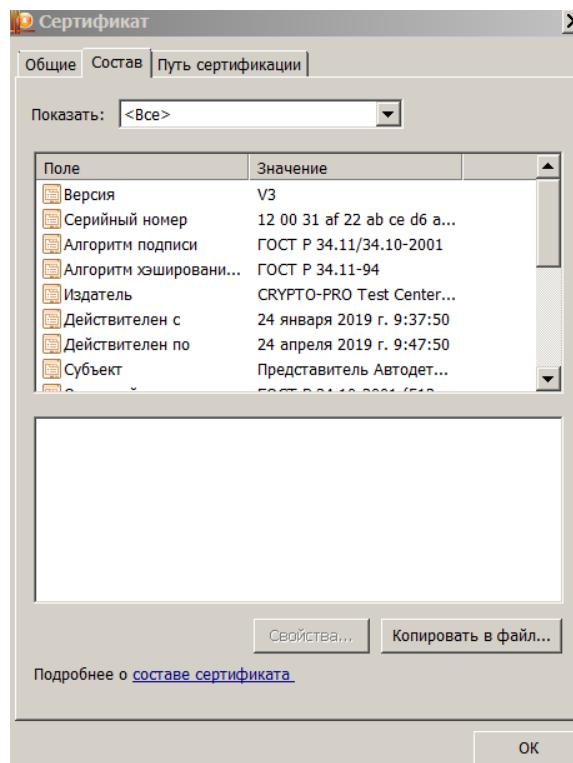
5. Укажите нужный контейнер и нажмите кнопку **ОК**. Затем – нажмите кнопку **Далее**. Откроется окно с информацией о выбранном сертификате:



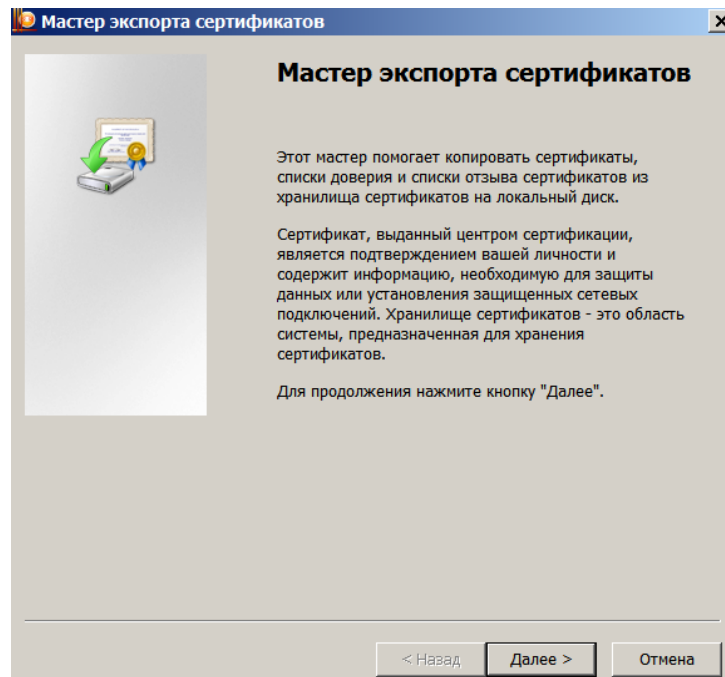
6. Нажмите кнопку **Свойства**. Откроется окно сертификата:



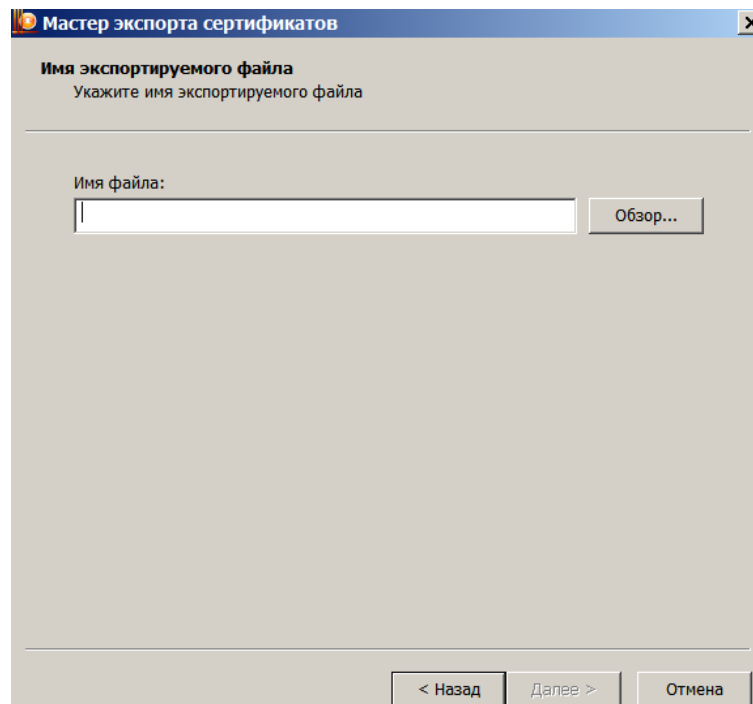
7. Перейдите на вкладку **Состав** и нажмите кнопку **Копировать в файл**:



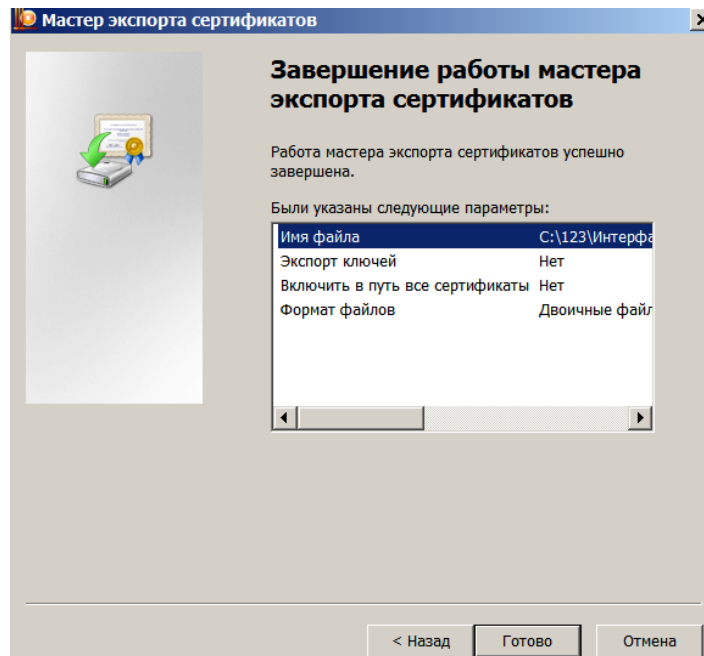
8. Откроется первое окно мастера экспорта сертификатов:



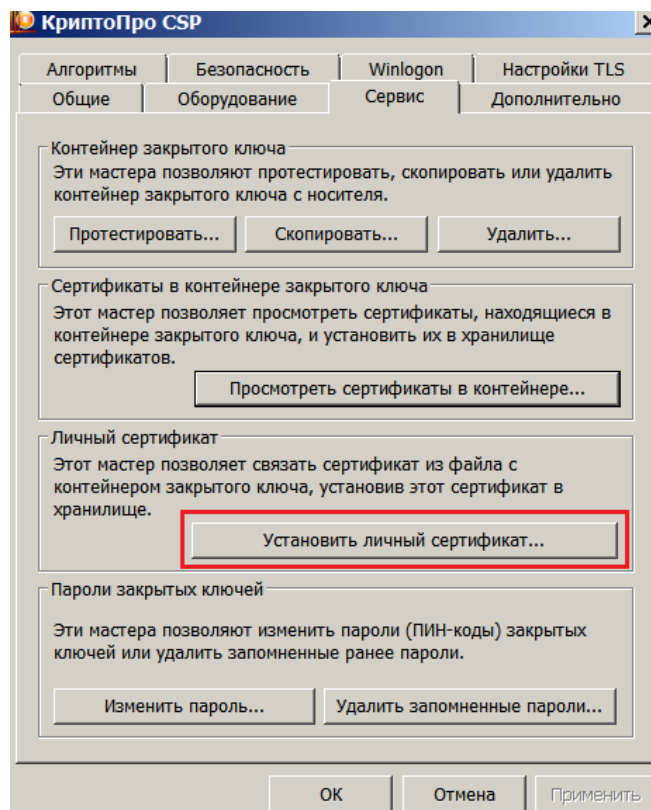
9. В последующих окнах мастера, не внося никаких изменений, просто три раза нажмите кнопку **Далее**. Откроется окно **Имя экспортируемого файла**:



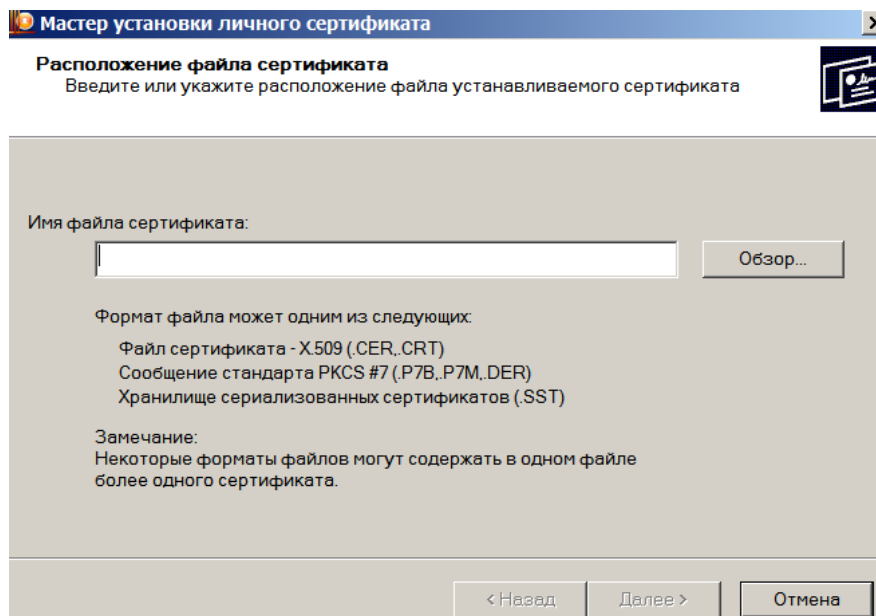
10. Нажмите кнопку **Обзор** и задайте имя файла, а также папку для его сохранения. Затем нажмите кнопку **Далее**. Файл с сертификатом будет сохранен в заданное место. Откроется окно завершения работы мастера:



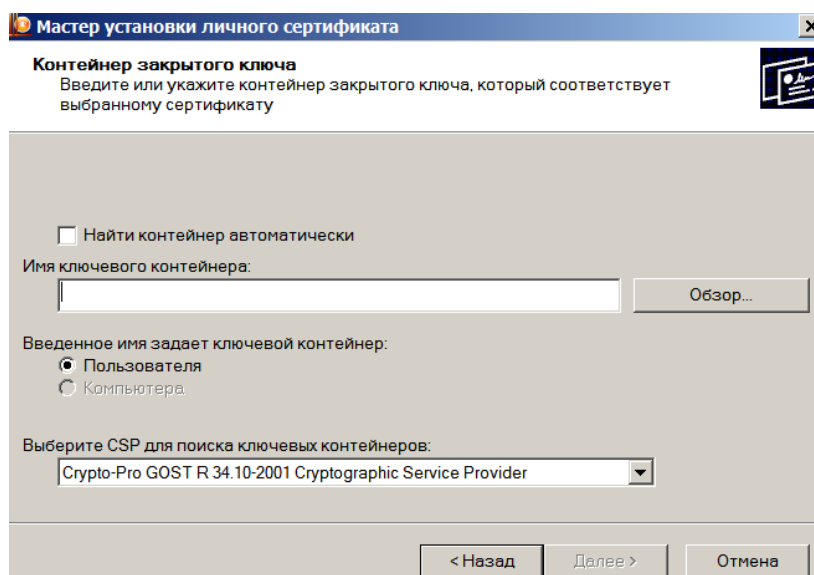
11. Нажмите кнопку **Готово**. В появившемся окне с уведомлением об успешном выполнении экспорта нажмите кнопку **ОК**.
12. Вернитесь к окну программы КриптоПро CSP и вновь перейдите в нем на вкладку **Сервис**.



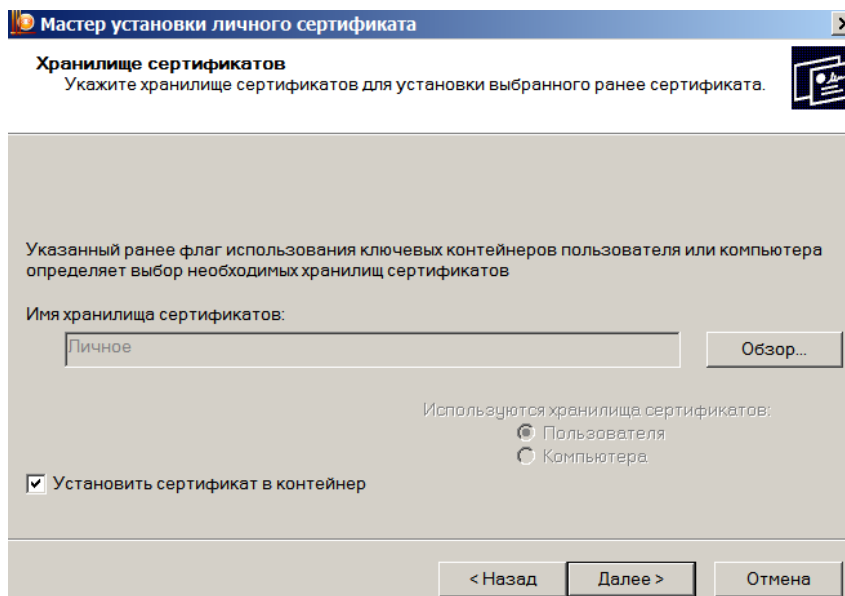
13. На данной вкладке нажмите кнопку **Установить личный сертификат**. Откроется окно **Расположение файла сертификата**:



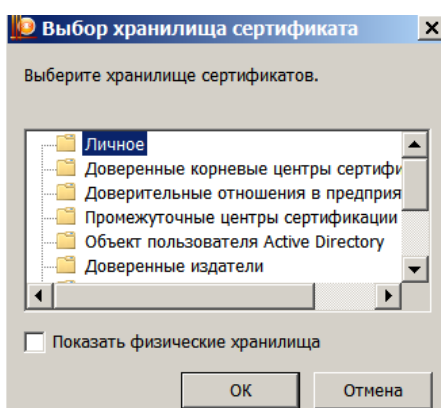
14. Нажмите кнопку **Обзор**. В появившемся стандартном окне выбора файла укажите файл открытой части сертификата и нажмите кнопку **Открыть**. Нажмите кнопку **Далее**. В окне следующего шага, также нажмите на **Далее**. Появится окно **Контейнер закрытого ключа**.



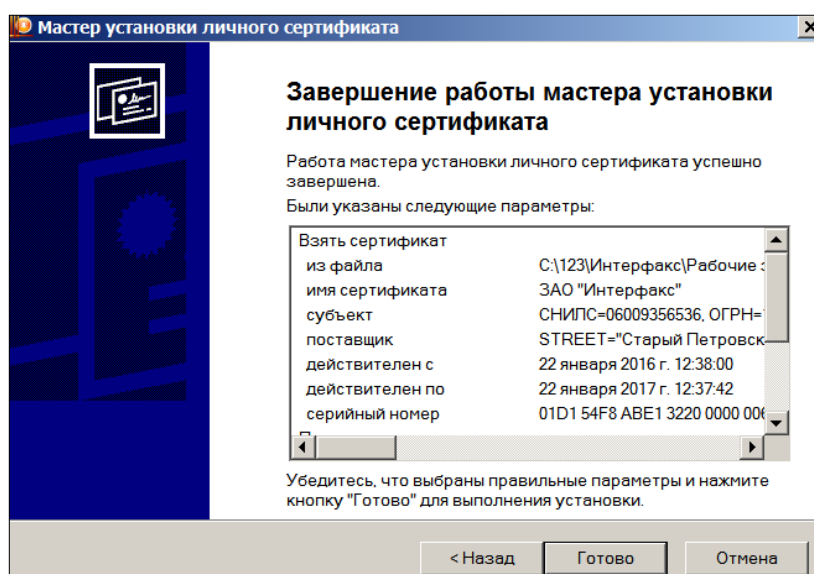
15. Нажмите кнопку **Обзор**. В открывшемся окне со списком ключевых контейнеров укажите нужный контейнер и нажмите кнопку **ОК**. Нажмите кнопку **Далее** – появится окно **Хранилище сертификатов**:



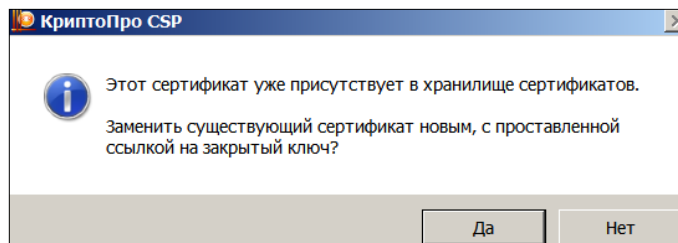
16. Нажмите в нем кнопку **Обзор**. Откроется окно для выбора хранилища сертификатов:



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.

5.1.3 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.

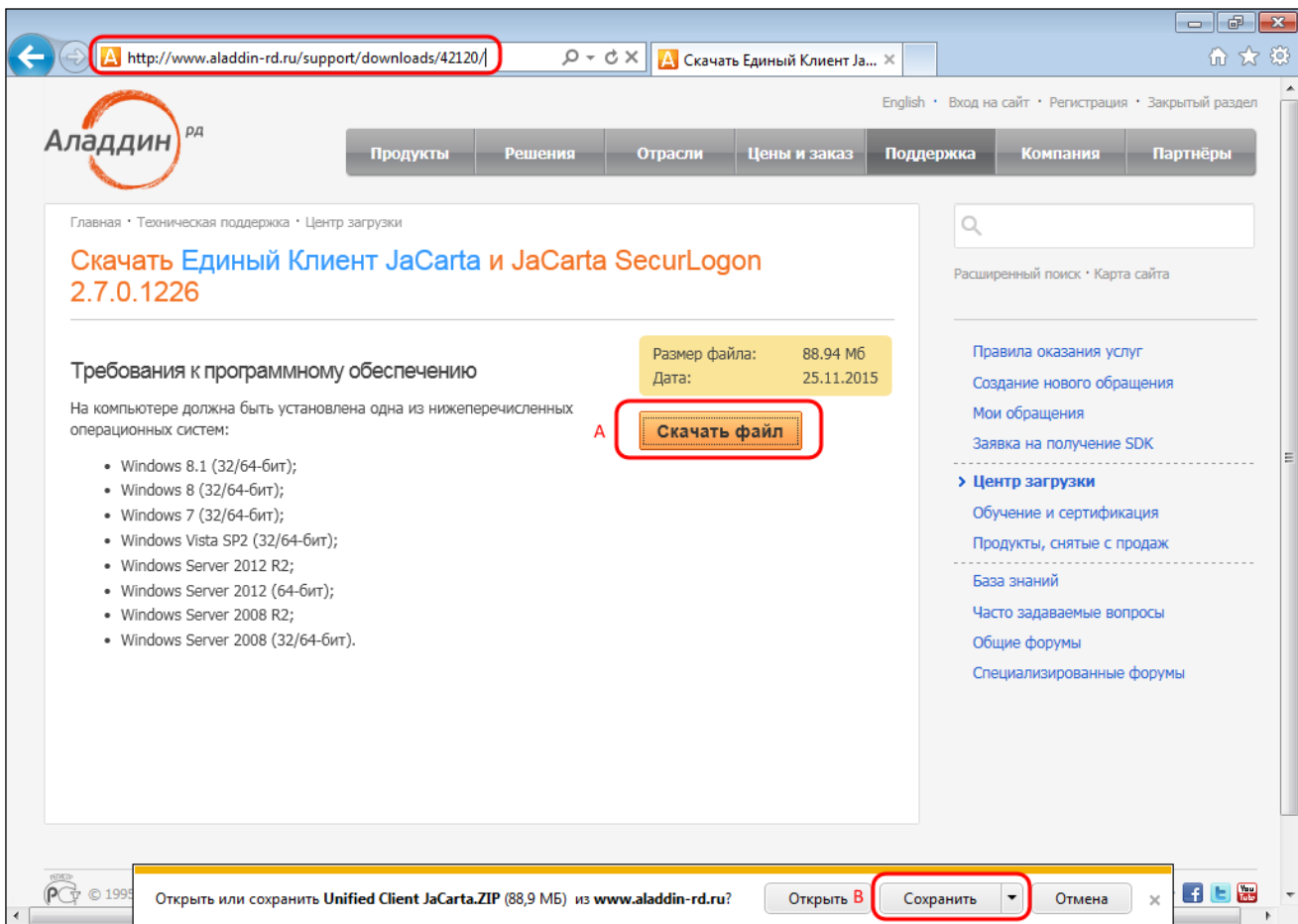
В зависимости от используемого Вами носителя ключевой информации следуйте соответствующей инструкции:

- если ключи электронной подписи и сертификат хранятся на ключевом носителе JaCarta LT, следуйте шагам подпункта 5.1.3.1
- если в качестве ключевого носителя используется компакт-диск (CD), следуйте шагам подпункта 5.1.3.2.

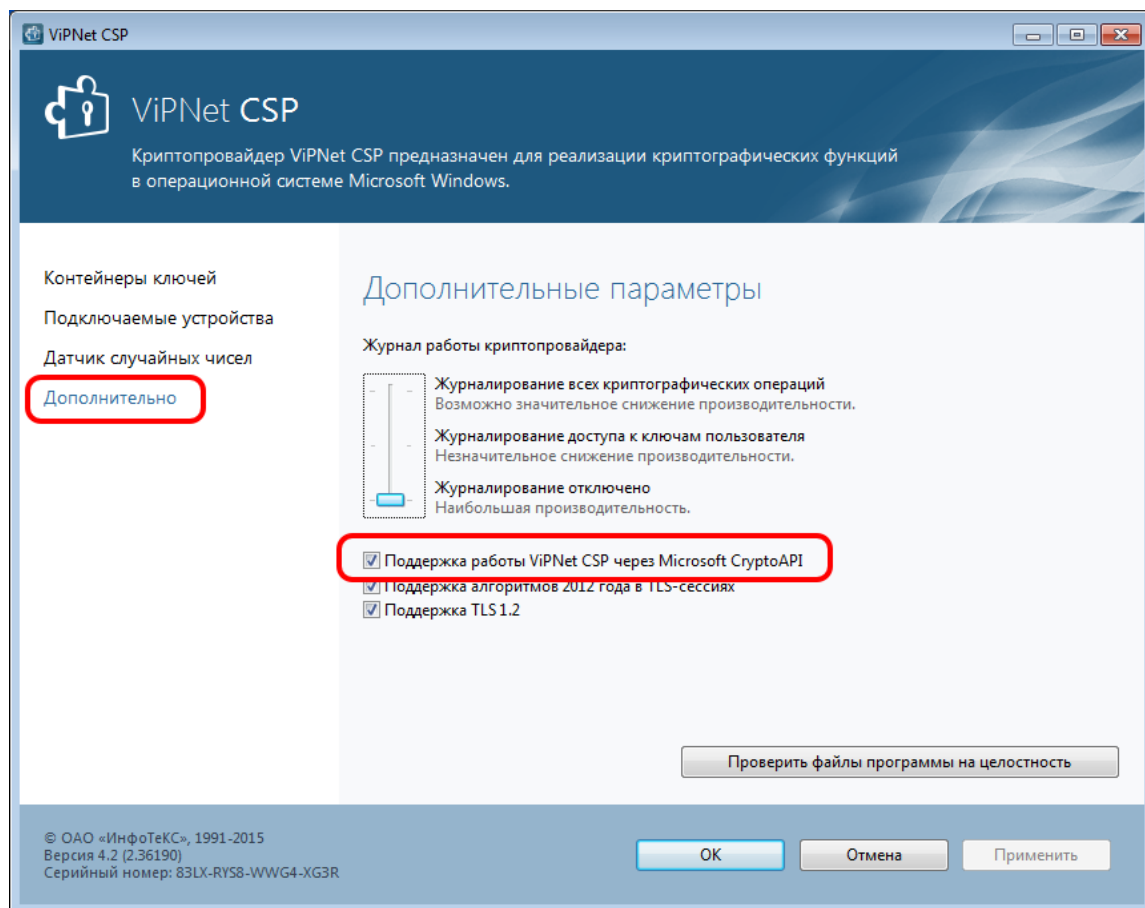
5.1.3.1 Установка личного сертификата с ключевого носителя JaCarta LT

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.

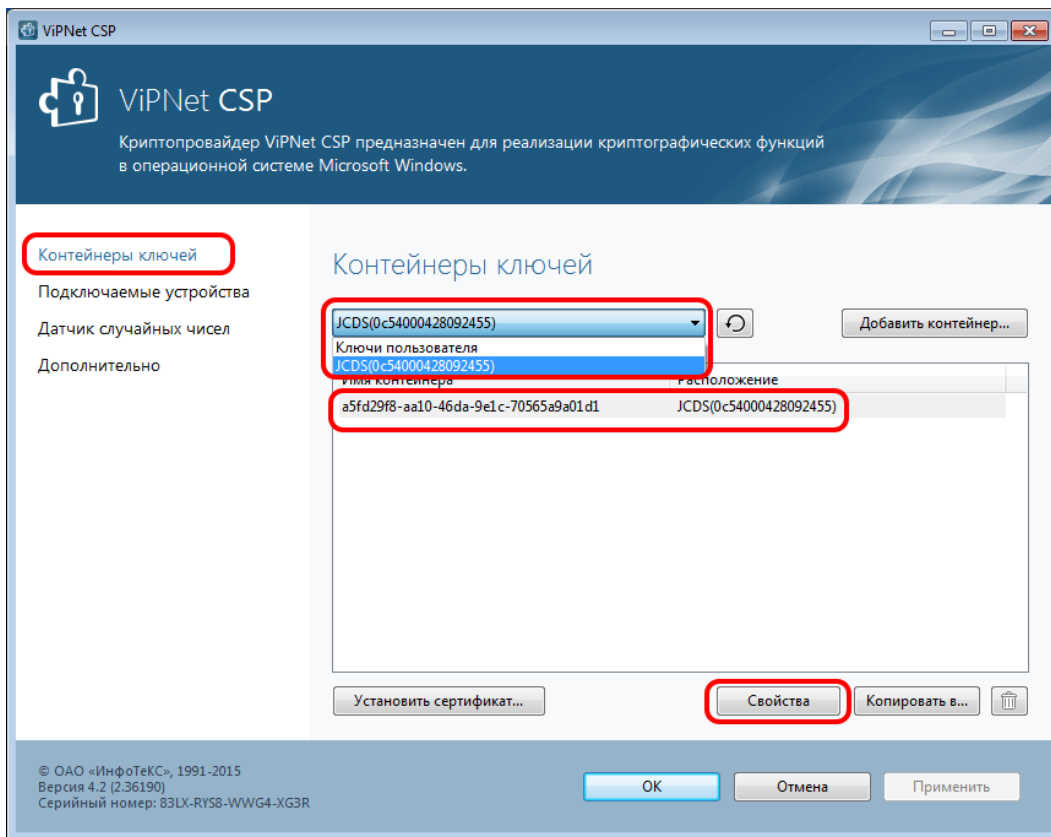
1. Для получения данного ПО актуальной версии необходимо скачать архив, доступный по ссылке:
 - при использовании ОС Windows 7 и 8: Единый Клиент JaCarta и JaCarta SecurLogon <http://www.aladdin-rd.ru/support/downloads/42120>
 - при использовании ОС Windows 10: Единый Клиент JaCarta и JaCarta SecurLogon 2.8.0.1402 <http://www.aladdin-rd.ru/support/downloads/43987/>
2. На открывшейся странице нажмите кнопку **Скачать файл** (на рисунке ниже – позиция А).



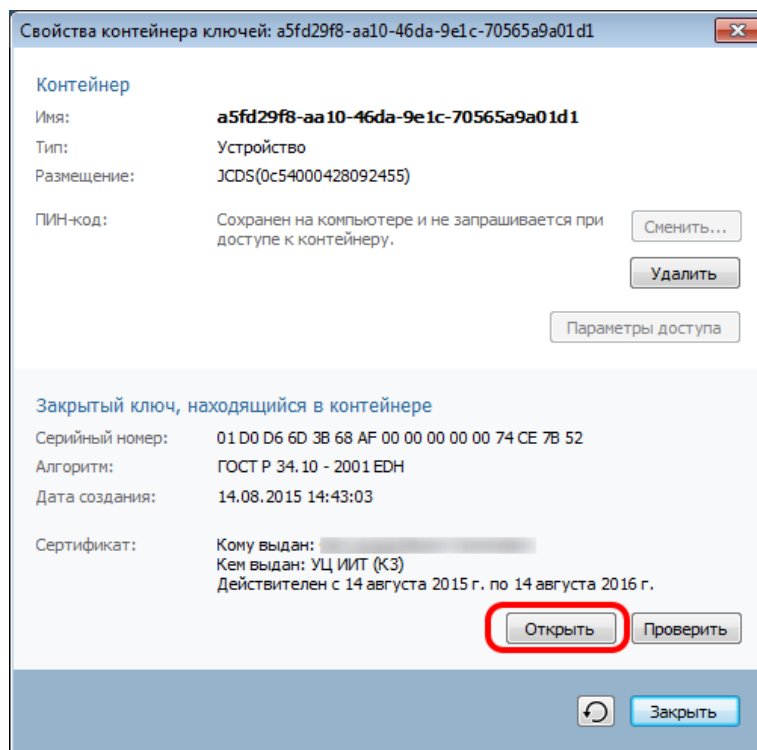
3. Загрузите архив с дистрибутивом в любой каталог Вашего компьютера (на рисунке – позиция В), распакуйте его и запустите установку утилиты. Выполните установку, следуя инструкциям мастера установки.
4. Запустите программу ViPNet CSP и убедитесь, что в разделе **Дополнительно** включена опция **Поддержка работы ViPNet CSP через Microsoft CryptoAPI** (см. рисунок ниже):



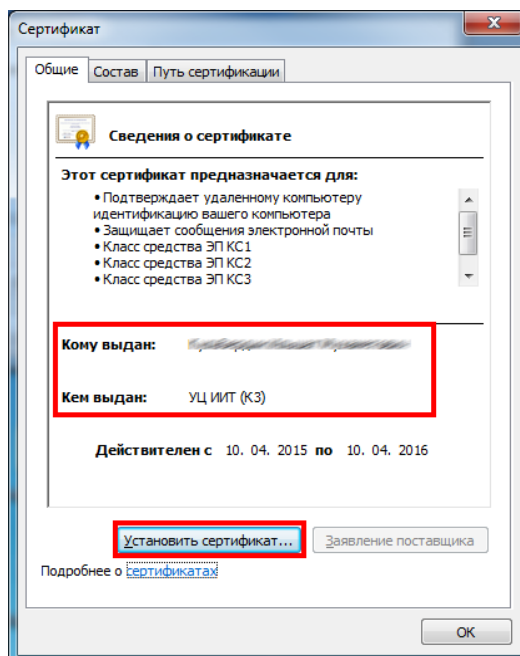
5. Перейдите в раздел **Контейнеры ключей** (см. рисунок ниже). В раскрывающемся списке выберите позицию **JCDS(...)**, а в поле **Имя контейнера** – контейнер ключей «xxx-xxxx-xxxx-xxxx-xxxx». Затем нажмите кнопку **Свойства**.



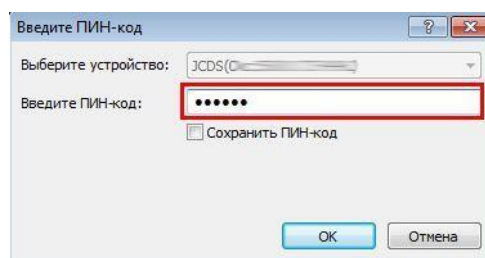
6. В окне **Свойства контейнера ключей** в области **Закрытый ключ**, находящийся в **контейнере** нажмите кнопку **Открыть**:



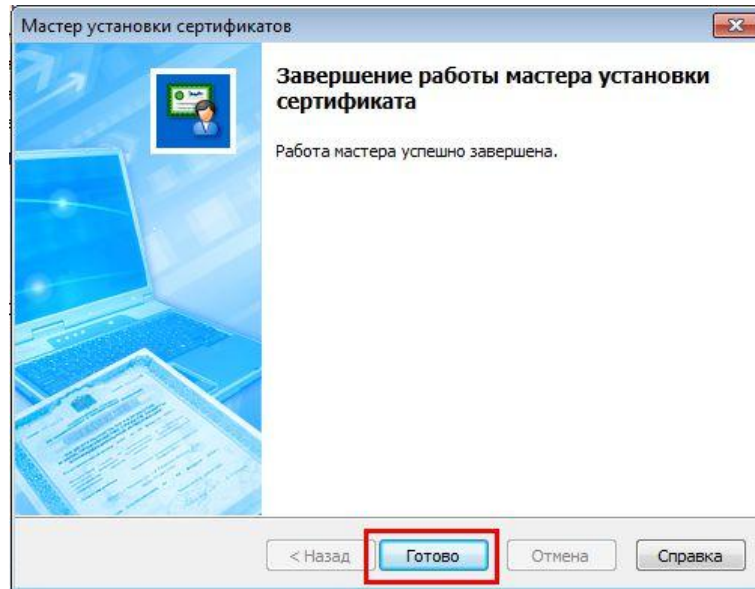
7. В открывшемся окне **Сертификат** убедитесь, что выбран именно тот сертификат, который необходимо использовать, и нажмите кнопку **Установить сертификат**:



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:

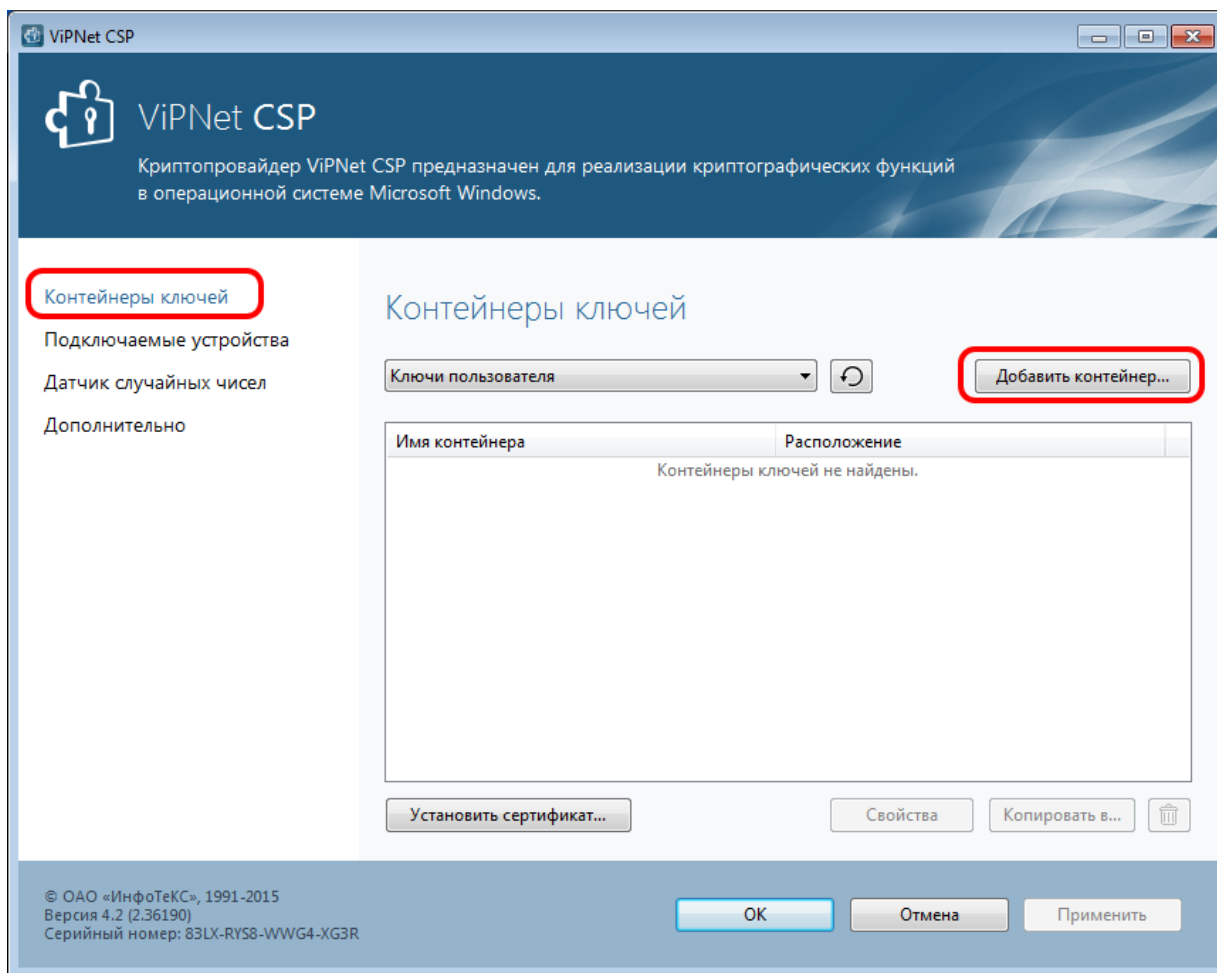


5.1.3.2 Установка личного сертификата с компакт-диска (CD)

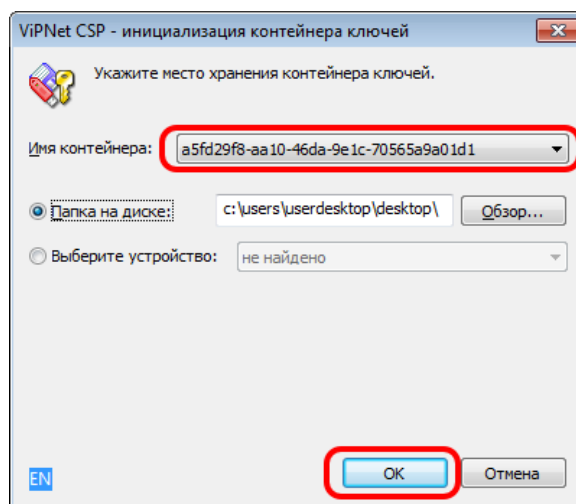
В качестве ключевого носителя можно использовать компакт-диск (CD).

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

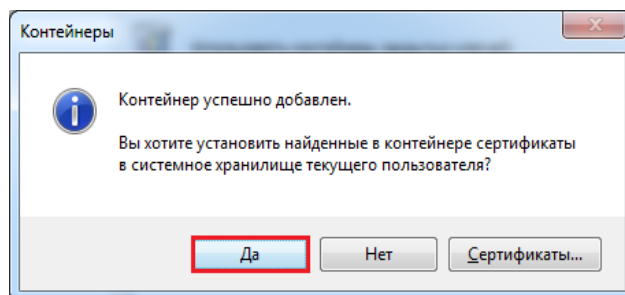
1. Скопируйте ключевой контейнер (файл с именем *sgn-xxxx-xxxx-xxxx-xxxx*) с компакт-диска в любую директорию жесткого диска компьютера.
2. Запустите программу ViPNet CSP и перейдите в раздел **Контейнеры ключей**:



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



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

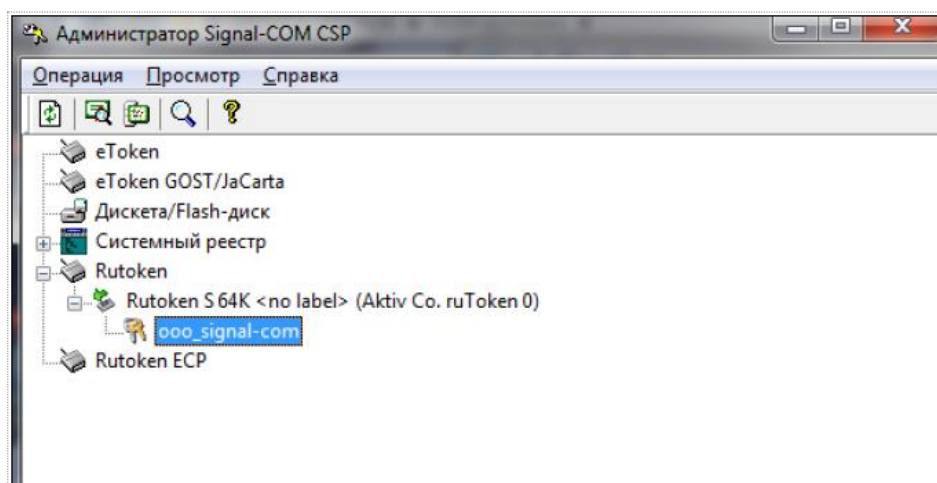


5. **ВНИМАНИЕ!** Выполните физическое уничтожение использованного при данной установке ключевого носителя (компакт-диска).

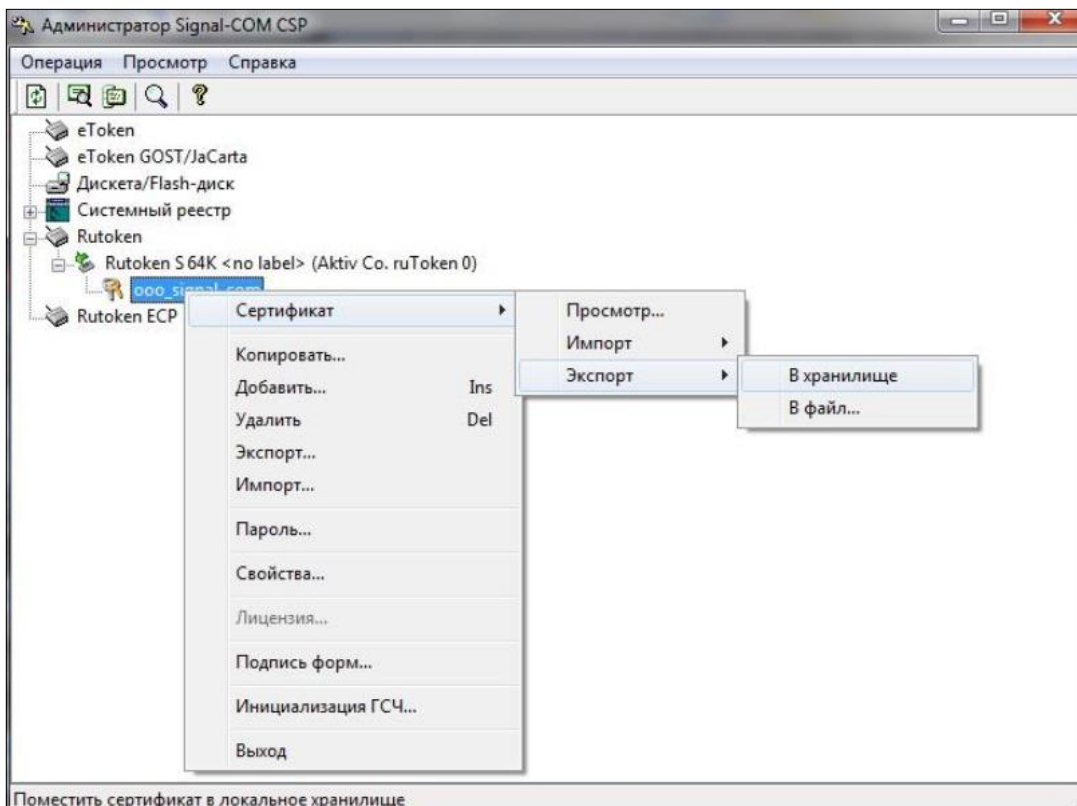
5.1.4 Установка личного сертификата при помощи программы Signal-COM CSP

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:



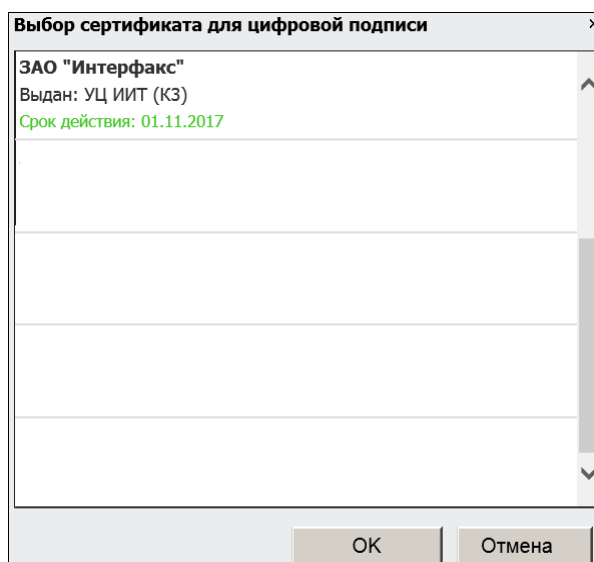
3. Нажмите на ключевом контейнере правой кнопкой мыши и выберите в контекстном меню пункт **Сертификат / Экспорт / В хранилище**:



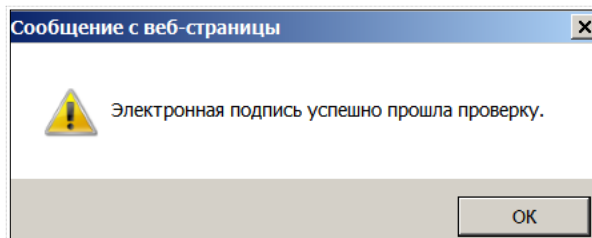
6 Проверка работоспособности ЭП

Проверку работоспособности системы ЭП можно осуществить через страницу «Помощь» открытого сайта.

1. Зайти на страницу «Помощь». Нажать кнопку **Проверить** в подразделе «**Проверка подписи**». Откроется окно выбора сертификата:



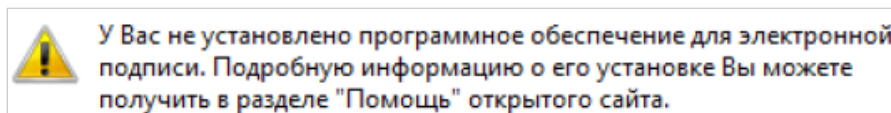
2. Выбрать в списке окна сертификат и нажать кнопку **ОК**. В зависимости от настроек используемого криптопровайдера далее может потребоваться ввод пароля или подключение ключевого носителя.
3. Будет произведена проверка подписи на сервере. Если ЭП прошла проверку, появится окно с соответствующим сообщением:



7 Разрешение проблем неработоспособности ЭП

7.1 Уведомление «Не установлено программное обеспечение ...»

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

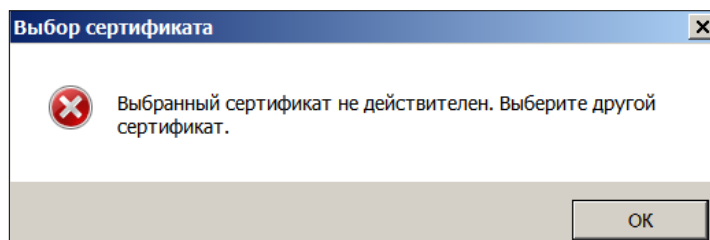


Возможны следующие варианты причин проблемы и методов её устранения:

- не установлен компонент "Федресурс. Плагин ЭП". Необходимо произвести его установку в соответствии с п. 4.2.

7.2 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»:

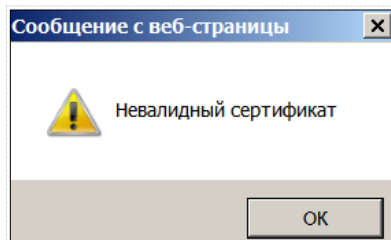


Возможные причины и методы решения проблемы:

- 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. 5.1.1.
- Нарушена работоспособность криптопровайдера. Переустановить и настроить криптопровайдер согласно инструкциям, полученным в УЦ. Затем – с помощью данного криптопровайдера выполнить повторную установку личного сертификата (см. п. 5.1.2, 5.1.3 или 5.1.4).

7.3 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 – длиной в 10 (для ЮЛ) или 12 (для физических лиц) цифр. При этом оно не может состоять только из нулей (например, «0000000000»). В сертификатах компаний-нерезидентов ИНН (10 цифр) должен начинаться с «9909»;
- если в поле «Субъект» («Subject») присутствует атрибут «ОГРН», то его значение должно быть числовым – длиной в 13 цифр. При этом оно не может состоять только из нулей. В сертификатах компаний-нерезидентов ОГРН *должен состоять из одних нулей или отсутствовать*;
- если в поле «Субъект» («Subject») или поле «Дополнительное имя субъекта» («Subject Alternative Name») присутствует атрибут «ОГРНИП», то его значение должно быть числовым – длиной 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 – длиной 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.

7.4 Уведомление «Не найдено ни одного сертификата или не установлен криптопровайдер»

Проблема: при попытке авторизоваться в личном кабинете (нажатии на пиктограмму **ВХОД ПО СЕРТИФИКАТУ** и последующем щелчке на ссылке **Вход**) или проверке работы электронной подписи (нажатии кнопки **Проверить** в разделе «Помощь») появляется окно с уведомлением «Не найдено ни одного сертификата или не установлен криптопровайдер». При этом также на экране появляется окно выбора сертификата, но без списка, содержащего атрибуты сертификатов.

Возможные причины проблемы:

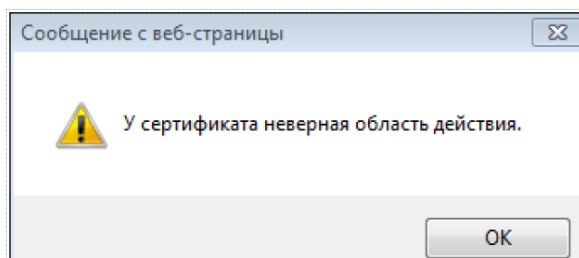
- 1) сертификаты (личный и/или корневой) не были добавлены в локальное хранилище
- 2) не установлен требуемый криптопровайдер

Соответствующие методы устранения данных проблем:

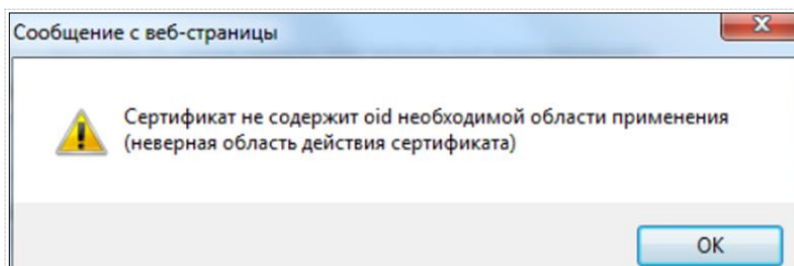
- 1) необходимо добавить сертификат (сертификаты) в локальное хранилище в соответствии с инструкциями, приведенными в п. 5.1
- 2) установить криптопровайдер (см. п. 4.1).

7.5 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)»:



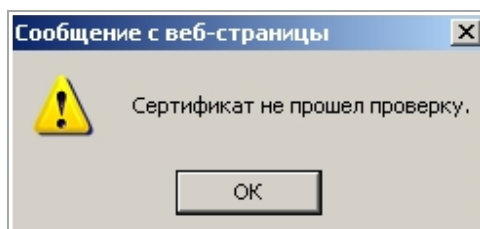
Причина проблемы – сертификат не содержит в расширении Extended Key Usage корректный объектный идентификатор (OID).

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

Также ознакомьтесь с «Регламентом применения электронной подписи в Едином федеральном реестре сведений о фактах деятельности юридических лиц», доступным в разделе «Помощь» открытого сайта.

7.6 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:

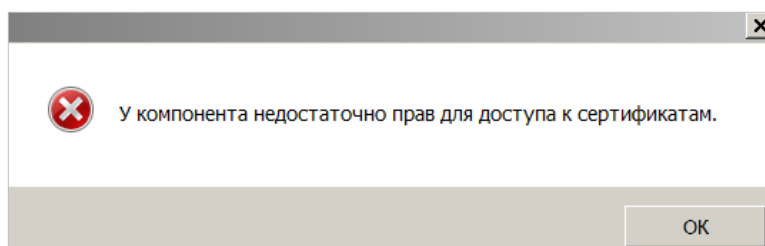
- при несовпадении значения атрибута «SN» (SubjectName) поля «Субъект» («Subject») сертификата с переданным значением данного атрибута;
- при ошибке построения цепочки сертификатов:
 - истек срок действия одного из сертификатов;
 - не установлен один из сертификатов цепочки;

- 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.

7.7 Уведомление «У компонента недостаточно прав для доступа к сертификатам»

Проблема: при попытке авторизоваться в личном кабинете (нажатии на пиктограмму **ВХОД ПО СЕРТИФИКАТУ**) или проверке работы электронной подписи (после нажатия кнопки **Проверить** в разделе «Помощь») появляется окно с уведомлением «У компонента недостаточно прав для доступа к сертификатам».



Данная проблема возникает в случае, когда Вы используете «старый» плагин (ActiveX-компонент ЭП) в связке с браузером Internet Explorer и при этом сайт Федресурс не включен в доверенные узлы Internet Explorer.

Возможные методы устранения проблемы:

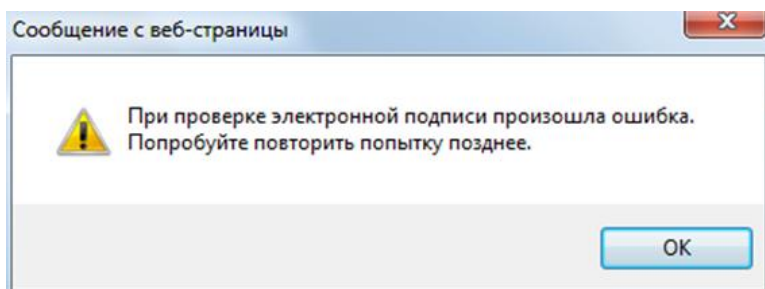
- удалить «старый» плагин (ActiveX-компонент ЭП) и установить вместо него компонент "Федресурс. Плагин ЭП" (см. п. 4.2)

ИЛИ:

- включить сайт Федресурс в состав доверенных узлов Internet Explorer

7.8 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».

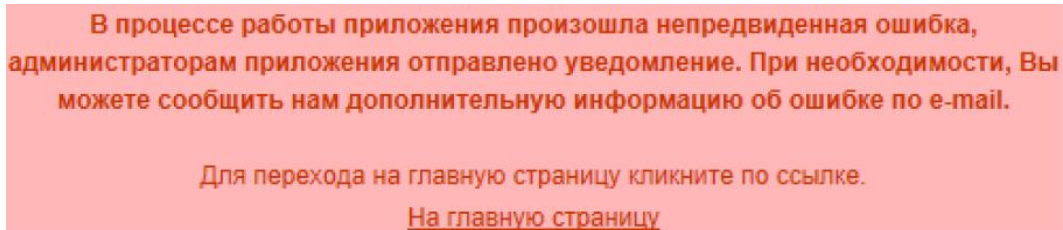


Подобная ошибка возникает при различных видах сбоев, которые могут возникать во время обращения к Системе, например, при проблемах в канале связи.

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.

7.9 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. 8.5).

8 Приложения

Выбор и поведение программного обеспечения для взаимодействия браузера и криптопровайзера зависит от того, в какой операционной системе и в каком браузере Вы работаете. При этом для разных операционных систем и браузеров применяются различные методы решения возникающих вопросов.

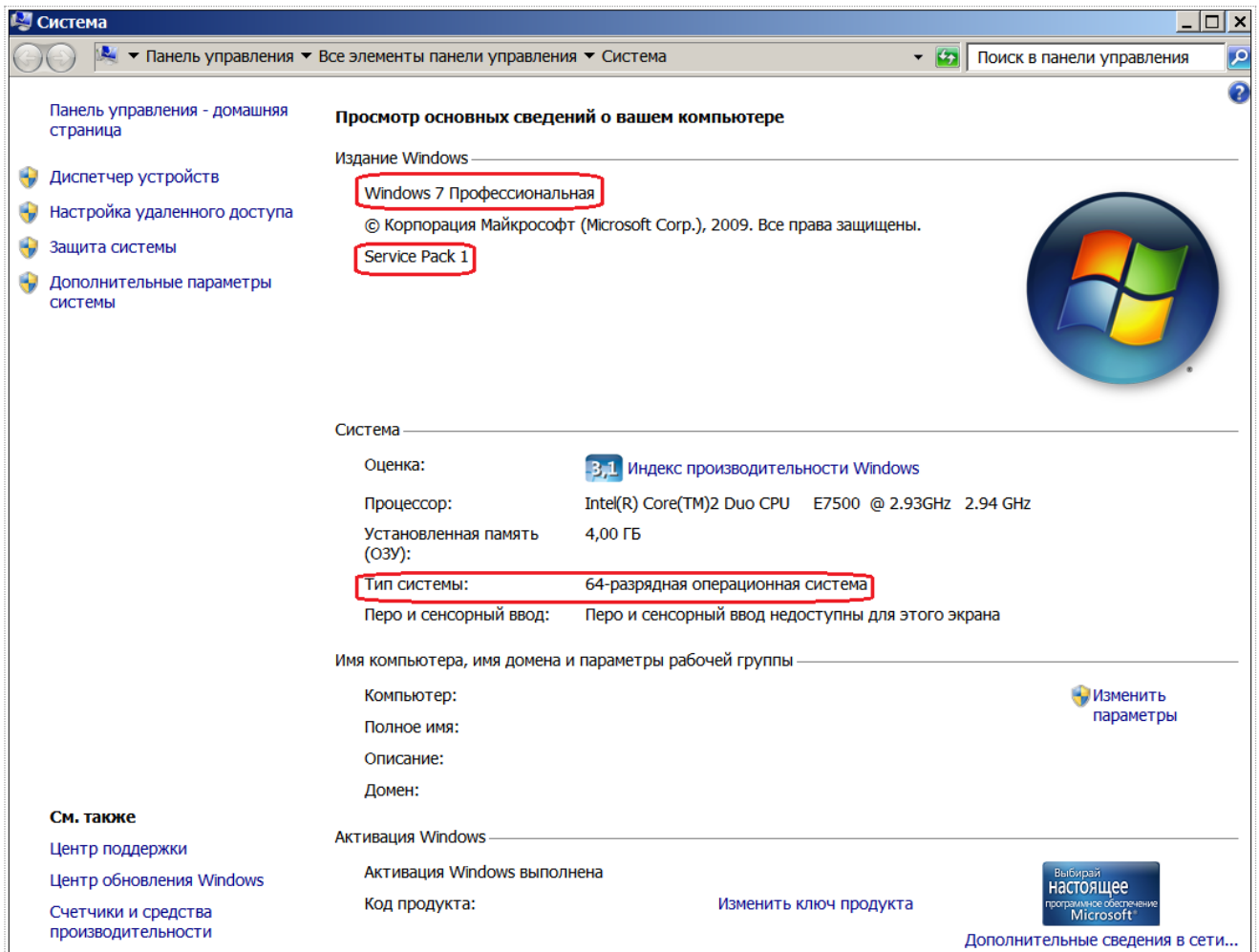
Имеет значение не только версия операционной системы, но и ее разрядность (64 / 32). Это особенно важно для операционных систем Windows 7 и Vista. Кроме того может иметь значение номер установленного сервисного пакета (SP).

8.1 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 **Компьютер**, щелкнуть на нем правой кнопкой и выбрать в контекстном меню пункт **Свойства**.
3. Откроется окно свойств операционной системы:

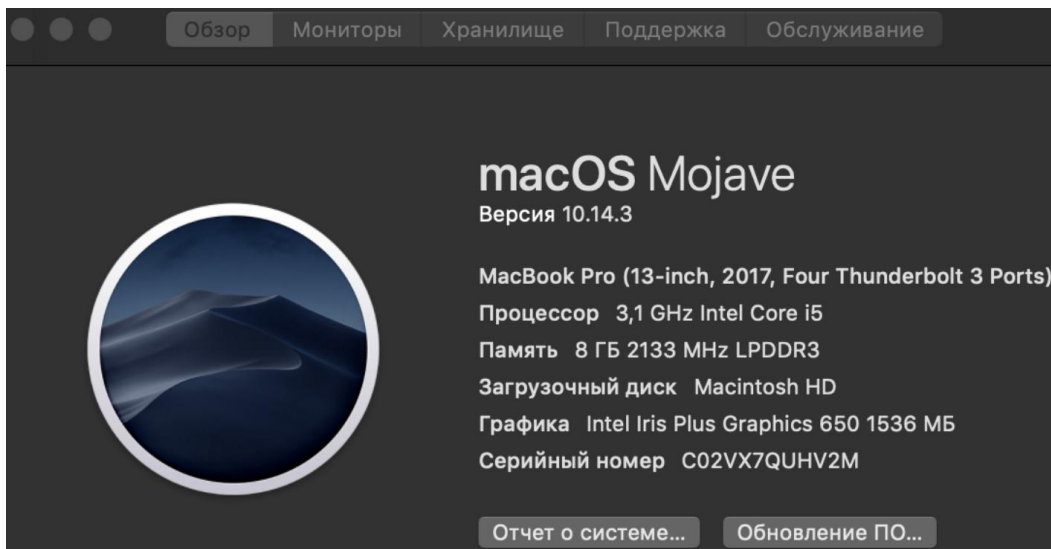
в операционной системе Windows 7 окно имеет следующий вид:



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

8.2 Как определить версию MacOS

Для того чтобы определить версию операционной системы MacOS необходимо в главном меню Мас нажать кнопку  и выбрать пункт **Об этом Мас**. Откроется окно свойств операционной системы:



Версию операционной системы необходимо сообщить (по запросу) в службу технической поддержки.

8.3 Как определить версию ОС семейства Linux


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

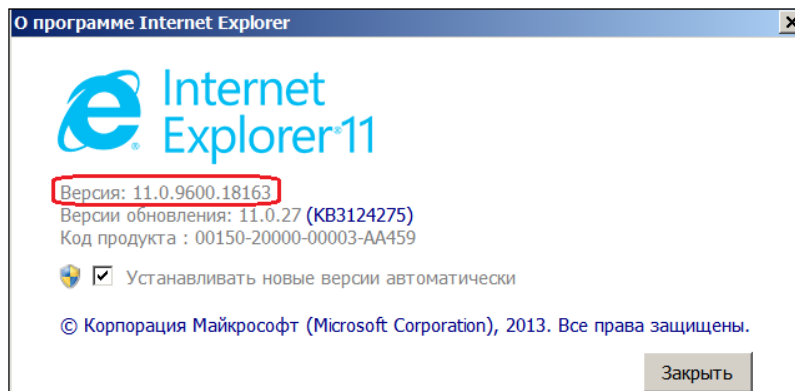
1. Зайти в терминал.
2. Выполнить команду `cat /etc/issue`. Номер версии ОС отобразится в терминале. Пример:



```
Файл  Правка  Вид  Поиск  Терминал  Справка
user@ubuntu:~$ cat /etc/issue
Linux Mint 19.1 Tessa \n \l
```

Версию операционной системы необходимо сообщить (по запросу) в службу технической поддержки.

8.4 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  **Справка**. В открывшемся контекстном меню пункт **О Firefox**. Появится окно **О Mozilla Firefox**, в котором отображается номер версии вашего браузера.

8.5 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.
3. Нажать сочетание клавиш Ctrl+V – снимок экрана будет вставлен в открытый документ Word.
4. Описанным способом сделать скриншоты всех страниц (окон) Системы, отражающих суть проблемы.
5. Сохранить документ Word.
6. Выслать сохраненный документ Word на адрес электронной почты bhelp@interfax.ru.