Инструкция

по установке средств криптографической защиты информации для подачи электронных документов на государственную регистрацию

Содержание:

Начальные условия	1
Установка	2
Шаг 1. Установка драйвера ключевого носителя	2
Шаг 2. Установка СКЗИ	2
Шаг 3. Установка личного КСКПЭП	2
Шаг 4. Установка корневого сертификата УЦ ФНС России	3
Шаг 5. Установка корневого сертификата УЦ ФГУП ГНИЦ ФНС России	3
Шаг 6. Выстраивание цепочки доверия к личному КСКПЭП	3
Шаг 7. Установка узлов https://*.nalog.ru в зону надежных узлов	7
Проверка установки СКЗИ	8
Приложение 1. Установка сертификата в заданную папку	11
Приложение 2. Установка КриптоПро CSP	14
Приложение 3. Установка личного КСКПЭП с помощью КриптоПро CSP	18
Приложение 4. Проверка установки сертификатов	28

Начальные условия.

- 1. Windows XP SP3 или выше (например, Windows 7);
- Internet Explorer 8.0 или выше (при отсутствии Вы можете загрузить с сайта компании Microsoft: <u>http://windows.microsoft.com/ru-RU/internet-explorer/download-ie</u>);
- Квалифицированный сертификат ключа проверки электронной подписи (далее – КСКПЭП) и соответствующий ему ключ электронной подписи, являющиеся действительными на момент подписания электронного документа и на день направления указанных документов в налоговый орган;

КСКПЭП Примечание: должен быть выдан аккредитованным удостоверяющим центром Минкомсвязи России (далее АУЦ), аккредитация которого действительна на день выдачи сертификата. Перечень АУЦ размещен Портале государственных услуг Российской Федерации на (http://etrust.gosuslugi.ru/CA).

Установка.

Шаг 1. Установка драйвера ключевого носителя.

Установите для носителя, на котором размещён ключ электронной подписи, драйвер в соответствии с указаниями разработчика носителя.

Например, если Вы используете ключевой носитель еТокеп разработки компании «Алладин Р.Д.», скачайте драйвер (ПО eToken PKI Client) этого устройства с сайта компании по ссылке <u>http://www.aladdin-rd.ru/support/downloads/26037/</u>, извлеките ключевой носитель eToken из разъема USB компьютера, установите драйвер с настройками по умолчанию и выполните перезагрузку.

Шаг 2. Установка СКЗИ

Установите в соответствии с указаниями разработчика средство криптографической защиты информации (СКЗИ), реализующие следующие требования:

- Авторизация и обеспечение юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки усиленной квалифицированной электронной подписи (ЭП) в соответствии с отечественным стандартом ГОСТ Р 34.10-2001;
- 2) Обеспечение конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89;
- 3) Обеспечение аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS;
- Контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования;
- 5) Управление ключевыми элементами системы в соответствии с регламентом средств защиты.

Примечание: Вы можете использовать сертифицированное СКЗИ **КриптоПро CSP** версии 3.6 или выше. Порядок использования КриптоПро CSP приведен на официальном сайте разработчика: <u>http://www.cryptopro.ru</u> (см. также <u>Приложение 2.</u> <u>Установка КриптоПро CSP</u>.)

Шаг 3. Установка личного КСКПЭП.

Выполните настройку СКЗИ для использования КСКПЭП в соответствии с инструкциями разработчика СКЗИ.

Примечание: Если Вы используете КриптоПро CSP см. <u>Приложение 3. Установка</u> КСКПЭП с помощью КриптоПро CSP.

В результате КСКПЭП должен быть установлен в папку «Личные» хранилища сертификатов текущего пользователя и связан с контейнером ключа электронной подписи.

Шаг 4. Установка корневого сертификата УЦ ФНС России.

Скачайте сертификат Ведомственного УЦ ФНС России по следующей ссылке:

http://uc.nalog.ru/crt/ca_fns_russia.crt

и затем установите его в папку «Доверенные корневые центры сертификации» текущего пользователя. См. <u>Приложение 1. Установка сертификата в заданную папку</u>

Шаг 5. Установка корневого сертификата УЦ ФГУП ГНИЦ ФНС России.

Скачайте сертификат УЦ ФГУП ГНИВЦ ФНС России по следующей ссылке:

http://www.gnivc.ru/uc/gnivc63-2012.crt

и затем установите его в папку «Доверенные корневые центры сертификации» текущего пользователя. См. <u>Приложение 1. Установка сертификата в заданную папку</u>

Шаг 6. Выстраивание цепочки доверия к личному КСКПЭП

Для выстраивания цепочки доверия к личному КСКПЭП, установка которого была осуществлена в соответствии с 3 шагом настоящей инструкции, необходимо установить корневой сертификат Аккредитованного удостоверяющего центра Минкомсвязи России, издавшего личный КСКПЭП.

Корневой сертификат АУЦ, издавшего личный КСКПЭП, Вы можете получить в обратившись в данный АУЦ. Также Вы можете найти сведения о корневом сертификате АУЦ в личном КСКПЭП. Для этого, если Вы используете КриптоПро CSP, в меню «Пуск» выберите Программы -> Крипто-Про -> Сертификаты. Откройте папку «Сертификаты – текущий пользователь» -> Личные -> Реестр -> Сертификаты:



Примечание: Для просмотра сертификатов в хранилище Вы также можете запустить консоль ММС и открыть оснастку сертификаты.

Выберите установленный сертификат, кликнув по нему два раза левой кнопкой мыши. Перейдите на вкладку «Состав»:

бщие Состав Путь сертификации	
<u>о</u> казать: 	
Поле	Значение 4
😈 Идентификатор ключа субъекта	41 5a 36 6a cé
🗊 Идентификатор ключа центра сертификатов	Идентификат
🗊 Точки распространения списков отзыва (CRL)	[1]Точка расп
🗊 Доступ к информации о центрах сертификации	[1]Доступкс
🐺 Использование ключа	Цифровая по,
🔄 Алгоритм отпечатка	sha1
Отпечаток	f9 df 6d 84 5c
 [1] Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификаци (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=<u>http://www.gnivc.ru/uc/GNIVCENSRUS_201</u> [2] Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) 	и 1.crt и
Дополнительное имя: <u>С</u> войства	ровать в файл

Выберите в верхнем окне строку «Доступ к информации о центрах сертификации» и нижнем окне отобразится ссылка на корневой сертификат по протоколу http. По данной ссылке можно скачать корневой сертификат АУЦ.

В случае отсутствия строки «Доступ к информации о центрах сертификации», можно посмотреть издателя личного КСКПЭП на вкладке «Состав», значение в поле «Издатель». В соответствии с указанной в поле «Издатель» информацией Вам следует связаться с АУЦ и получить корневой сертификат АУЦ.

Показать: <Все> ▼		
Поле Значение	*	
ПАЛГОРИТМ ПОДПИСИ ГОСТ Р 34.11/34.10-2001	-	
Палоритм хэширования по ГОСТР 34.11-94 ВИздатель УЦ ФГУП ГНИВЦ ФНС России		
Щинствителен с 5 июля 2013 г. 14:35:00		
Субъект Руководитель, Петров Иван		
Открытый ключ ГОСТ Р 34.10-2001 (512 Bits) Лочишенный ключ Зашишенная электронная п	-	
Свойства Копировать в файл Подробнее о <u>составе сертификата</u>		
	IX.	

Перед установкой сертификата, откройте его (кликнув по нему два раза левой кнопкой мыши), чтобы узнать какой это сертификат: корневой (самоподписанный) или нет. Перейдите на вкладку «Состав».

У корневого (самоподписанного) сертификата поля «Издатель» и «Субъект» на вкладке «Состав» имеют одинаковые значения.

ертификат	X
Общие Состав	Путь сертификации
Показать: <	e> •
оле	Значение
Алгоритм п	FOCT P 34.11/34.10-2001
Издатель	Головной удостоверяющий центр, 0077104743
Действител Действител	20 июля 2012 г. 16:31:14 17 июля 2027 г. 16:31:14
Субъект	Головной удостоверяющий центр, 0077104743
	III FOR THE STORE
V3	
	<u>С</u> войства <u>К</u> опировать в файл
Подробнее о со	таве сертификата
	ОК

Вариант 1

Если сертификат корневой, то его нужно устанавливать в папку «Доверенные корневые центры сертификации». См. <u>Приложение 1. Установка сертификата в</u> заданную папку.

После установки корневого сертификата цепочка доверия к личному КСКПЭП будет выстроена.

Вариант 2

Если у сертификата поля «Издатель» и «Субъект» на вкладке «Состав» имеют различные значения, то данный сертификат необходимо устанавливать в папку «*Промежуточные центры сертификации*». См. <u>Приложение 1. Установка сертификата</u> в заданную папку.

Далее смотрим сведения о следующем сертификате в цепочке. Для этого в хранилище сертификатов откройте папку «Сертификаты – текущий пользователь» -> Промежуточные центры сертификации -> Реестр -> Сертификаты:



Выберите установленный сертификат, кликнув по нему два раза левой кнопкой мыши. Перейдите на вкладку «Состав», где в строке «Доступ к информации о центрах сертификации» и нижнем окне отобразится ссылка на следующий сертификат в цепочке.

Таким образом, необходимо установить все сертификаты, пока не дойдете до корневого сертификата АУЦ. После установки корневого сертификата будет выстроена цепочка доверия к личному КСКПЭП.

Для проверки установки сертификатов см. <u>Приложение 4. Проверка установки</u> сертификатов.

Шаг 7. Установка узлов https://*.nalog.ru в зону надежных узлов.

Зайдите в меню «Сервис» и выберите пункт «Свойства обозревателя». В появившемся окне перейдите на вкладку «Безопасность», выберите «Надежные узлы» и нажмите кнопку «Узлы».



Нажмите «Сайты» и добавьте https://*.nalog.ru в список.

Проверка установки СКЗИ

Для проверки установки и настройки СКЗИ воспользуйтесь сервисом

https://service.nalog.ru/static/gost-test.html?svc=regin

В случае успешной установки СКЗИ все проверки должны быть успешно пройдены (см. Рис.1)

Подача	документов на государственную регистрацию в
электро	нном виде
Проверка у	словий использования сервиса
Будет произведе	на проверка выполнения нижеперечисленных условий использования сервиса. На последнем шаге проверки Вам
будет предложен	ю указать (выбрать) сертификат ключа подписи (СКП) (сертификат CryptoPro), выданный удостоверяющим центром,
аккредитованны	м в сети доведенных удостоведяющих центров ФНС России, и ввести пароль к хранилищу ключей.
 Операционна Интернет обо Возможно за 	ая система - Microsoft Windows озреватель - Microsoft Internet Explorer ащищенное соединение с сервером с использованием алгоритмов ГОСТ 28147-89 и ГОСТ Р 34.10-2001

В случае если средства СКЗИ не установлены или установленные средства СКЗИ не удовлетворяют требованиям к СКЗИ, указанными на Шаге 2, то проверка не будет пройдена (см. Рис. 2).

будет прои будет пред иккредито	ізведена проверка выполнения нижеперечисленных условий использования сервиса. На последнем шаге проверки Вам "пожено указать (выбрать) сертификат ключа подписи (СКП) (сертификат CryptoPro), выданный удостоверяющим центром, ванным в сети доверенных удостоверяющих центров ФНС России, и ввести пароль к хранилищу ключей.
🛛 Onepa	ционная система - Microsoft Windows
🛛 Интери	нет обозреватель - Microsoft Internet Explorer
🛚 Возмо	жно защищенное соединение с сервером с использованием алгоритмов ГОСТ 28147-89 и ГОСТ Р 34.10-2001
🖬 Устано	ивлен сертификат ключа подписи, выданный удостоверяющим центром, аккредитованным в сети доверенных УЦ ФНС России
(!)	Проверка защищенного соединения с сервером с использованием алгоритмов ГОСТ 28147–89 и ГОСТ Р 34.10–2001 К сожалению, проверка возможности защищенного соединения к серверу окончилась неудачно. Это могло случиться по одной из следующих причин:
	На Вашем компьютере не установлены криптосредства, совместимые с КриптоПро (обеспечивающие алгоритмы ГОСТ 28147-89 и ГОСТ Р 34.10-2001).
	➤ На Вашем компьютере нет корневого сертификата УЦ ФНС РФ. Вы можете установить его <u>с сайта УЦ ФНС РФ.</u> Обращаем Ваше викмание, ито с 29 марта 2013 года используется ковый сертификат.

Для устранения этой ошибки выполните Шаг 2. Установка СКЗИ

В случае если КСКПЭП не установлен или КСКПЭП не удовлетворяет установленным требованиям или не удается выстроить цепочку доверия к КСКПЭП, то проверка не будет пройдена (см. Рис. 3).

Проверка условий использования сервиса

Будет произведена проверка выполнения нижеперечисленных условий использования сервиса. На последнем шаге проверки Вам будет предложено указать (выбрать) сертификат ключа подписи (СКП) (сертификат CryptoPro), выданный удостоверяющим центром, аккредитованным в сети доверенных удостоверяющих центров ФНС России, и ввести пароль к хранилищу ключей.

- 🛿 Операционная система Microsoft Windows
- 🗹 Интернет обозреватель Microsoft Internet Explorer
- 🛿 Возможно защищенное соединение с сервером с использованием алгоритмов ГОСТ 28147-89 и ГОСТ Р 34.10-2001
- 🛿 Установлен сертификат ключа подписи, выданный удостоверяющим центром, аккредитованным в сети доверенных УЦ ФНС России

Проверка авторизации с использованием сертификата ключа подписи, выданного удостоверяющим центром, аккредитованным в сети доверенных УЦ ФНС России

К сожалению, проверка возможности авторизации с использованием сертификата ключа подписи окончилась неудачно. Это могло случиться по одной из следующих причин:

- На Вашем компьютере не установлен сертификат ключа подписи, совместимый с КриптоПро (соответствующий ГОСТ 28147-89 и ГОСТ Р 34.10-2001).
- > Срок действия Вашего сертификата ключа подписи истек.
- Используемый Вами сертификат ключа подписи выдан удостоверяющим центром, не аккредитованным в сети доверенных УЦ ФНС России.
- > Ваш сертификат ключа подписи включен в список отозванных.

Рис. 3

Для устранения этой ошибки выполните Шаги 3-6 установки.

Приложение 1. Установка сертификата в заданную папку



Нажмите «Далее».

В следующем окне выберите «Поместить все сертификаты в следующее хранилище»

Мастер импорта сертификатов
Хранилище сертификатов
Хранилища сертификатов - это системные области, в которых хранятся сертификаты.
Выбор хранилища может быть произведен Windows автоматически, или же можно указать размещение сертификата вручную.
Автоматически выбрать хранилище на основе типа сертификата
Поместить все сертификаты в следующее хранилище
Хранилище сертификатов:
<u>630p</u>
Подробнее о хранилищах сертификатов
< <u>Н</u> азад Далее > Отмена

Выберите папку, в которую необходимо установить сертификат». Например, в папку «Доверенные корневые центры сертификации» как показано на рисунке ниже

Выбор хранилища сертификата		
Выберите хранилище сертификатов.		
Личное Доверенные корневые цент Доверительные отношения Доверительные отношения Промежуточные центры сер Объект пользователя Active	ры сертис в предпри отификаци e Directory	
Караланан Каралан Карал Каралан Каралан К	•	
Показать физические хранилища ОК Отмена		



В случае предупреждения системы безопасности подтвердите установку сертификата в указанную папку.



Приложение 2. Установка КриптоПро CSP.

На рабочее место пользователя должно быть установлено сертифицированное средство ЭП КриптоПро версии 3.6 или выше с действующей лицензией.

Если на рабочее место пользователя еще не было установлено программное обеспечение КриптоПро, то рекомендуется установить последнюю сертифицированную версию ПО КриптоПро. Установка аналогична установке версии 3.6.

Если на рабочее место пользователя установлено программное обеспечение КриптоПро 3.6, то рекомендуется обновить до последней сертифицированной версии (<u>http://cryptopro.ru/downloads</u>).

Внимание! Если на рабочее место пользователя установлен несертифицированный криптопровайдер, то рекомендуется его удалить.

Если на рабочее место пользователя установлено программное обеспечение КриптоПро CSP версии 3.0, его необходимо удалить.

Загрузите дистрибутив КриптоПро CSP 3.6 с официального сайта по ссылке <u>http://www.cryptopro.ru/products/csp/overview</u>.

При установке КриптоПро CSP 3.6 следуйте инструкциям мастера установки:

😸 Установка "КриптоПро CS	p"
	Вас приветствует программа установки "КриптоПро CSP (КС1)"
	Программа выполнит установку "КриптоПро CSP" на компьютер. Для продолжения нажмите кнопку "Далее".
Крипто <mark>Про</mark> CSP 3.6	ПРЕДУПРЕЖДЕНИЕ: Данная программа защищена законами об авторских правах и международными соглашениями.
	< Назад Далее > Отмена

😸 Установка "КриптоПро CSP"
Лицензионное соглашение
Пожалуйста, внимательно прочтите следующее лицензионное соглашение.
ВНИМАТЕЛЬНО ОЗНАКОМЬТЕСЬ С ЛИЦЕНЗИОННЫМ СОГЛАШЕНИЕМ НА ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ
1. Термины и определения
 1.1. Настоящее Лицензионное соглашение является общей офертой между ООО "КРИПТО-ПРО" и Пользователем - физическим или юридическим лицом. Настоящее Лицензионное соглашение в случае согласия, выраженного в форме молчания в течение 7 дней с момента приобретения права на использование Изделия, в соответствии со ст. 433 ГК РФ имеет силу договора. 1.2. Под Изделием понимается программа/комплекс программ для ЭВМ, включая носители и документацию, авторские права на которые принадлежат ООО «КРИПТО
 Я принимаю условия лицензионного соглашения Я не принимаю условия лицензионного соглашения
< Назад Далее > Отмена

Сведения о пользователе Укажите сведения о себе. 	😸 Установка "КриптоПро CSP"
Пользователь: admin Организация:	Сведения о пользователе Укажите сведения о себе.
Организация: Серийный номер:	Пользователь: admin
Серийный номер: 	<u>О</u> рганизация:
Введите серийный номер, соответствующий лицензионному соглашению. Без заданного серийного номера срок действия продукта три месяца.	<u>С</u> ерийный номер:
	Введите серийный номер, соответствующий лицензионному соглашению. Без заданного серийного номера срок действия продукта три месяца.
< <u>Н</u> азад Далее > Отмена	< <u>Н</u> азад Далее > Отмена

😸 Установка "КриптоПро CSP"
Вид установки Выбор наиболее подходящего вида установки.
Выберите вид установки.
 Обычная Будет установлен стандартный набор компонент.
Выборочная Выбор необходимых компонентов программы и папки, в которой они будут установлены. Рассчитана на опытных пользователей.
< <u>Н</u> азад Далее > Отмена

В блоке «Требуемые библиотеки поддержки» необходимо выбрать все опции:

😸 Установка "КриптоПро CSP"
Последние приготовения к установке программы
Программа готова к началу установки.
Выберите требуемые библиотеки поддержки (можно настроить позже):
Зарегистрировать считыватель "Реестр"
🔽 Зарегистрировать считыватель смарт-карт
📝 Зарегистрировать считыватель съемных носителей
Нажмите кнопку "Установить", чтобы начать установку.
Чтобы просмотреть или изменить параметры установки, нажмите кнопку "Назад". Нажмите кнопку "Отмена" для выхода из программы.
< <u>Н</u> азад <u>У</u> становить Отмена

1	🛃 Установк	а "КриптоПро CSP"	J
	Установк	ка "КриптоПро СЅР"	
	Устанав	ливаются выбранные компоненты программы.	
	1 1	Дождитесь окончания установки "КриптоПро CSP". Это может занять несколько минут.	
		Состояние:	
		< <u>Н</u> азад Далее > Отмена	

🛃 Установка "КриптоПро CSP	
	Программа установки "КриптоПро CSP" завершена
	Установка "КриптоПро CSP" успешно завершена. Нажмите кнопку "Готово" для выхода из программы.
Крипто <mark>Про</mark> CSP 3.6	< Назад Готово Отмена

После завершения установки обязательно перезагрузите компьютер.



Приложение 3. Установка личного КСКПЭП с помощью КриптоПро CSP.

Подключите ключевой носитель с личным КСКПЭП и ключем ЭП (дискету, eToken или т.п.) к компьютеру.

В меню «Пуск» выберите Программы -> Крипто-Про -> КриптоПро CSP:



Вариант установки 1 (с носителя КСКПЭП):

На вкладке «Сервис» нажмите «Посмотреть сертификаты в контейнере...»:

	Алгоритмы	Безопасно	ость	Winlogo
Общие	Оборудов	ание		Сервис
Контейнер закрыт	ого ключа			
Эти мастера позво	ляют протестиро	вать, скопир	овать и	ли
удалить контейне	р закрытого ключ	а с носителя		
Про <u>т</u> естировать.		ать	<u>У</u> дал	ить
Сертификаты в ко	нтейнере закрыт	ого ключа		
Этот мастер позво	ляет просмотреть	сертификат	ы, нахо	дящиеся
в контейнере закр	ытого ключа, и у	становить их	в хран	илище
сертификатов.				
	просмотреть се	ртификаты в	контей	нере
Личный сертифика	т			
Этот мастер позво	ляет связать сер	гификат из ф эновив этот (айла с гертифі	Wat P
хранилище.	sitoro tono da, yen		cprinφi	ikar b
	Установить	личный серт	ификат	
	клюцей			
Пароли закрытых	101104201			
Пароли закрытых п Эти мастера позво ключей или удали	ляют измененить ть запомненные р	пароли (ПИН анее пароли	-коды)	закрытых

Нажмите «Обзор...» рядом с полем «Имя ключевого контейнера»:

📴 Сертификаты в контейнере закрытого ключа	x
Контейнер закрытого ключа Введите или укажите контейнер закрытого ключа для просмотра сертификатов в этом контейнере	14. 14.
Имя ключевого контейнера:	
<u> </u>	
Введенное имя задает ключевой контейнер: © Пользователя © Компьютера	
Выберите CSP для поиска ключевых контейнеров:	
Crypto-Pro GOST R 34. 10-2001 Cryptographic Service Provider	
< <u>Н</u> азад Далее > Отмена	

Выберите ключевой контейнер, соответствующий подключенному носителю электронной подписи:

K	риптоПро CSP		
	Выбор ключево	о контейнера	0:09:55
	 <u>В</u> списке пока: <u>Ф</u>ружестве 	енные имена 💿 <u>У</u> никальные име	на
	Список ключевы	их контейнеров пользователя:	
	Считыватель	Имя контейнера	
	Реестр	Petrov_container	
	Реестр	Иванов	
	Реестр	Сергеев	
		ОК	Отмена

Нажмите «ОК».

После того, как имя контейнера отобразится в поле «Имя ключевого контейнера», нажмите «Далее».

Внимание! Если при выборе ключевого контейнера появляется окно с предупреждением о том, что истек срок действия лицензии КриптоПро CSP, то необходимо обновить лицензию, иначе работа с сервисом будет невозможна.

Нажмите «Установить»:

Сертификат:	Петров Иван Сергеевич
С <u>у</u> бъект:	OID. 1.2.643.3.131.1.1=7707083861, E=0, C=RU, S=77 Москва, L=г.
Поставщик:	Е=ucinfo@gnivc.ru, C=RU, L=Москва, О=ФГУП ГНИВЦ ФНС России, О
Действителен <u>с</u> :	30 октября 2012 г. 16:44:00
Действителен <u>п</u> о:	30 октября 2013 г. 16:53:00
Серийный <u>н</u> омер:	35D4 278C 0001 0000 6C51
	<u>У</u> становить <u>Св</u> ойства О <u>б</u> зор

Нажмите «ОК»:



При необходимости введите пароль/пин-код, заданный для доступа к ключу ЭП на ключевом носителе.

Вариант установки 2 (из файла сертификата):

Для установки понадобится файл сертификата (файл с расширением .cer). Он может находиться, например, на дискете или на жестком диске компьютера (если Вы делали копию сертификата или Вам присылали его по электронной почте). Также файл сертификата можно экспортировать из хранилища Личные.

На вкладке «Сервис» нажмите кнопку «Установить личный сертификат...»:

цополнительно	Алгоритмы	Безопасност	ъ Winlogo
Общие	Оборудов	ание	Сервис
Контейнер закрыт	ого ключа		
Эти мастера позво	ляют протестиро	вать, скопиров	ать или
удалить контейне	р закрытого ключ	а с носителя.	
Протестировать.	Скопирова	ать	<u>У</u> далить
Сертификаты в ко	нтейнере закрыт	ого ключа	
Этот мастер позво	ляет просмотреть	сертификаты,	находящиеся
в контейнере закр сертификатов.	ытого ключа, и у	становить их в	хранилище
	Просмотреть се	отификаты в ко	онтейнере
Личный сертифика	т		
этот мастер позво контейнером закр хранилище.	ыляет связать серт ытого ключа, уста	гификат из фаи ановив этот сер	ла с отификат в
	Установить	<u>л</u> ичный сертиф	рикат
Пароли закрытых	ключей		
Эти мастера позво ключей или удали	ляют измененить ть запомненные р	пароли <mark>(</mark> ПИН-ка анее пароли.	оды) закрытых
	роль Уд	алить запомнен	ные <u>п</u> ароли

В окне «Мастер установки личного сертификата» нажмите кнопку «Обзор» рядом с полем «Имя файла сертификата», чтобы выбрать файл сертификата:

📴 Мастер установки личного сертификата
Расположение файла сертификата Введите или укажите расположение файла устанавливаемого сертификата
<u>И</u> мя файла сертификата: Обзор
Формат файла может одним из следующих: Файл сертификата - X.509 (.CER,.CRT) Сообщение стандарта РКСЅ #7 (.P7B,.P7M,.DER) Хранилище сериализованных сертификатов (.SST) Замечание: Некоторые форматы файлов могут содержать в одном файле более одного сертификата.
< <u>Н</u> азад Далее > Отмена

Укажите путь к сертификату (файл с расширением .cer) и нажмите на кнопку «Открыть»:

🖻 Открыть	an (19		- Augur	×
😋 🔵 🗢 📔 « Локальнь	и Кертификат Петров	► - 4 ₇	Поиск: Сертификат	م
Упорядочить 🔻 Нова	я папка		111	
🔆 Избранное	Имя		Дата изменения	Тип
〕 Загрузки	鷆 Petrov.000		24.07.2013 12:19	Папка с фа
🕮 Недавние места	🔄 Петров		05.07.2013 14:44	Сертифика
詞 Библиотеки				
🌉 Компьютер				
🏭 Локальный диск (С				
👝 Локальный диск (D				
🗣 Сеть				
	•	III		•
<u>И</u> мя с	файла: Петров	•	Certificate Files (*.cer;*.c	rt) 🔻

В поле «Имя файла сертификата» отобразится выбранный сертификат, нажмите «Далее».

Pacr	толожение файла сертификата Зведите или укажите расположение файла устанавливаемого сертификата
<u>И</u> мя фа	айла сертификата:
	D:\Сертификат Петров\Петровcer Обзор
	Формат файла может одним из следующих:
	Файл сертификата - X.509 (.CER,.CRT) Сообщение стандарта PKCS #7 (.P7B,.P7M,.DER)
	Хранилище сериализованных сертификатов (.SST)
	Замечание:
	Некоторые форматы файлов могут содержать в одном файле более одного сертификата.

В окне «Сертификат для установки» кликните по кнопке «Далее».

Сертификат для Просмотрите	и выберите сертификат для установки
Сертификат:	Петров Иван Сергеевич
С <u>у</u> бъект:	OID.1.2.643.3.131.1.1=7707083861, E=0, C=RU, S=77 Москва, L=г.
П <u>о</u> ставщик:	Е=ucinfo@gnivc.ru, C=RU, L=Москва, О=ФГУП ГНИВЦ ФНС России, С
Действителен <u>с</u> :	30 октября 2012 г. 16:44:00
Действителен <u>п</u> о:	30 октября 2013 г. 16:53:00
Серийный <u>н</u> омер:	35D4 278C 0001 0000 6C51
	Свойства
	О <u>б</u> зор
	< <u>Н</u> азад Далее > Отмена

Выберите «Обзор», чтобы указать соответствующий контейнер закрытого ключа.

🛛 Мастер установки личного сертификата	×
Контейнер закрытого ключа	
Введите или укажите контейнер закрытого выбранному сертификату	ключа, который соответствует
Найти контейнер автоматически Имя ключевого контейнера:	О <u>б</u> зор
Оправление имя задает ключевой контейнер.	
Компьютера	
Выберите CSP для поиска ключевых контейнеров	8:
Crypto-Pro GOST R 34.10-2001 Cryptographic S	ervice Provider 🔹
	< Назад Далее > Отмена

Установите опцию «Найти контейнер автоматически» или выберите нужный ключевой контейнер через кнопку «Обзор». Нажмите «ОК».

Kŗ	оиптоПро CSP			
	0:09:55			
	В списке показывать:			
	© pp////cerbe			
	Список кл <u>ю</u> чевь	іх контейнеров пользователя:		
	Считыватель Имя контейнера			
	Реестр	Petrov_container		
	Реестр	Иванов		
	Реестр	Сергеев		
		ок	тмена	

После того, как имя контейнера отобразится в поле «Имя ключевого контейнера», нажмите «Далее».

Примечание: Если в списке нет Вашего ключевого контейнера, например, если Вы используете eToken, то выполните Шаг 1. Установка драйвера носителя КСКПЭП.

Ko	тейнер закрытого ключа
	Введите или укажите контейнер закрытого ключа, который соответствует выбранному сертификату
	Найти контейнер автоматически
<u>И</u> мя н	лючевого контейнера:
F	'etrov_container O <u>6</u> 30p
Введе	нное имя задает ключевой контейнер:) <u>П</u> ользователя) <u>К</u> омпьютера
Выбе	оите CSP для поиска ключевых контейнеров:
	Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider ▼
0	

В окне «Выбор хранилища сертификатов» кликните по кнопке «Обзор».

це сертификатов	
те хранилище сертификатов д сертификата.	ля установки в него выбранного
анее флаг использования клк	чевых контейнеров пользователя или
определяет выбор необходим	ых хранилищ сертификатов
ща сертификатов:	Oбзор
ща сертификатов:	Обзор
ща сертификатов:	Обзор Используются <u>х</u> ранилища сертификатов:
ща сертификатов:	Обзор Используются <u>к</u> ранилища сертификатов: () <u>Пользователя</u> () <u>К</u> омпьютера
ща сертификатов: гь сертификат в контейнер	Обзор Используются <u>х</u> ранилища сертификатов: () Пользователя () <u>К</u> омпьютера
ща сертификатов: ть сертификат в контейнер	Обзор Используются <u>х</u> ранилища сертификатов: () Пользователя () <u>К</u> омпьютера
ща сертификатов: гь сертификат в контейнер	Используются <u>х</u> ранилища (© <u>Пользовател</u> <u>Компьютера</u>

Выберите хранилище «Личное» и нажмите «ОК».

🖻 Выбор хранилища сертификата			
Выберите <u>х</u> ранилище сертификатов.			
Личное Доверенные корневые центры сертиф Доверительные отношения в предпри Промежуточные центры сертификаци Объект пользователя Active Directory Ловеренные излатели Промежиточные излатели			
🔲 Показать физические хранилища			
ОК Отмена			

После выбора хранилища нажмите на кнопку «Далее».

Укажите хранилище с ранее сертификата.	сертификатов для установки в него выбранного
казанный ранее флаг испо омпьютера определяет вы мя хранилища сертификат	ользования ключевых контейнеров пользователя или бор необходимых хранилищ сертификатов ов:
Личное	Обзор

Затем нажмите на кнопку «Готово».

Мастер установки лично	 Мастер установки личного сертификата Завершение работы мастера установки личного сертификата Работа мастера установки личного сертификата успешно завершена. Были указаны следующие параметры: 		
	Взять сертификат из файла имя сертификата субъект поставщик действителен с действителен по серийный номер < Убедитесь, что выбраны п нажлите кнопку, "Готово"	D:\Сертификат Петров Петров Иван Сергеевич OID.1.2.643.131.1.1=7700 E=ucinfo@gnivc.ru, C=RL 30 октября 2012 г. 16:44 30 октября 2013 г. 16:53 35D4 278C 0001 0000 6C! ▼ равильные параметры и лля выполнения установки	
 Казад Готово Отмена 			

После нажатия на кнопку «Готово» может появиться такое сообщение: «Этот сертификат уже присутствует в хранилище сертификатов. Заменить существующий сертификат новым, с проставленной ссылкой на закрытый ключ?». В таком случае необходимо выбрать «Да».

КриптоПро CSP Этот сертификат уже присутствует в хранилище сертификатов.		
	Заменить существующий сертификат новым, с проставленной ссылкой на закрытый ключ?	
	Да <u>Н</u> ет	

В сообщении об успешной установке нажмите «ОК». Если у Вас отобразилось сообщение «Этот сертификат уже присутствует в хранилище сертификатов. Заменить существующий сертификат новым, с проставленной ссылкой на закрытый ключ?», то сообщение «Сертификат был установлен в хранилище «Личные» текущего пользователя» может не появиться.



Внимание! Если при установке личного КСКПЭП в хранилище сертификатов «Личные» появляется сообщение «Закрытый ключ на указанном контейнере не

соответствует открытому ключу в сертификате. Выберите другой ключевой контейнер», или выберите опцию «Найти контейнер автоматически». При повторном появлении сообщения Вам потребуется перейти в закладку «Сервис» и нажать кнопку «Удалить запомненные пароли...», в появившемся окне «Удаление запомненных паролей» проставить галки для пунктов «Удалить все запомненные пароли закрытых ключей:», «Удалить информацию об использованных съемных носителях:» и нажать «ОК». Далее повторить действия по установке личного КСКПЭП.

- 1. Запустите редактор реестра (Пуск/ввести в поисковую строку "regedit"/ ввод).
- Перейдите в следующую ветвь редактора реестра: HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings\USERS, найдите ветку с названием S-1-5-21-887842899-779666540-1964827887-17186 (где S-1-5-21-887842899-779666540-1964827887-17186- SID пользователя).
- 3. Зайдите в KeyDevices и удалите там passwords.
- 4. Удалите содержимое папки C:\Documents and Settings\имя пользователя \Application Data\Microsoft\SystemCertificates\My\Keys.
- 5. Установите заново сертификат.

Если выполнение описанных выше действий, не решило Вашу проблему, обратитесь в Аккредитованный удостоверяющий центр, издавший личный КСКПЭП.

Приложение 4. Проверка установки сертификатов

Откройте хранилище сертификатов. Для этого если Вы используете КриптоПро CSP в меню «Пуск» выберите Программы -> Крипто-Про -> Сертификаты или запустите консоль Пуск->Выполнить ММС и откройте оснастку «Сертификаты».

Далее откройте папку «Сертификаты – текущий пользователь» -> Личные -> Реестр -> Сертификаты:



Выберите установленный сертификат, кликнув по нему два раза левой кнопкой мыши. Перейдите на вкладку «Путь сертификации»:

Сертификат	x
Общие Состав Путь сертификации	
Путь сертификации	
Головной удостоверяющий центр Ц 1 ИС ГУЦ Ц 0ГУП ГНИВЦ ФНС Росси Петров Иван Сергеез	и ич
	Просмотр сертификата
<u>С</u> остояние сертификата:	
Этот сертификат действителен.	
Подробнее о <u>путях сертификации</u>	
	ОК

На вкладке «Путь сертификации» должна отображаться цепочка сертификатов, с помощью которых устанавливается доверие. Верхний сертификат должен быть корневым.

В поле «Состояние сертификата» должно отображаться сообщение о действительности сертификата.

Корневой сертификат «УЦ ФГУП ГНИВЦ ФНС России», корневой сертификат Ведомственного УЦ ФНС России и корневой сертификат АУЦ, выдавшего личный КСКПЭП, будут размещаться в хранилище сертификатов «Доверенные корневые центры сертификации»:

🗐 Сертификаты			
Файл Действие Вид Окно Справка			
🗢 🔿 📶 🤞 🖏 🗙 🖼 😖 🛛 🖬			
📔 Корень консоли 🔺	Кому выдан	Кем выдан	
Сертификаты - текущий пользов Пичное	🛱 GNIVC FNS RUS	GNIVC FNS RUS	
🔺 🗎 Доверенные корневые центрі	🔄 УЦ ФГУП ГНИВЦ ФНС России	УЦ ФГУП ГНИВЦ ФНС России	
 Реестр Сертификаты Оскальный компьютер 			
 Бальный компьютер Смарт-карта 			
Доверительные отношения в			
Промежуточные центры серт			
Объект пользователя Active D			
Доверенные издатели			
Сертификаты, к которым нет			
Сторонние корневые центры — Сторонние корневые центры —			
 доверенные лица Другие пользователи 			
Запросы заявок на сертифика •			
	<	Þ	
Хранилище Реестр содержит сертификато	в.		

Остальные сертификаты цепочки будут размещаться в хранилище сертификатов «Промежуточные центры сертификации»:

