

ФАКТОР-ТС

Абонентский пункт ЭЦП

DiSignCA

Руководство пользователя

НКБГ. 501430.773И6

МОСКВА

Разработчик: ООО «ФАКТОР-ТС»

*Коммерческая поставка **DiSignCA** и других программных продуктов технологии **ДИОНИС** производится ООО «ФАКТОР-ТС»*

*Е-mail адрес разработчиков: **factor@factor-ts.ru***

© ООО «ФАКТОР-ТС», 2008

*Все вопросы, замечания и пожелания по настоящему руководству и другой документации ООО «**ФАКТОР-ТС**» присылайте по указанному выше адресу с заголовком **Документация***

Содержание

1. Общие сведения	6
1.1. Наименование программы	6
1.2. Назначение и область применения программы	6
1.2.1. Основные функции программы	7
1.2.2. Интеграция с MS Word.....	9
2. Основные понятия.....	10
2.1. Электронная цифровая подпись	10
2.2. Криптосистема	10
2.3. Закрытый ключ ЭЦП	10
2.4. Открытый ключ ЭЦП	11
2.5. Сертификат ключа	11
2.6. Удостоверяющий центр	11
2.7. Цепочка доверия УЦ.....	12
3. Правила использования программы.....	14
3.1. Подготовительные действия.....	14
3.2. Ключевая информация и ключевой носитель	14
3.2.1. Получение ключевого носителя	15
3.2.2. Состав ключевой информации	15
3.3. Хранение сертификатов	16
3.4. Настройка криптосистемы	16
4. Условия применения программы	18
4.1. Требования к оборудованию и операционной среде.....	18
4.2. Требования к ключевым носителям и ключевой информации	18
4.3. Состав ПО DiSignCA	19
4.4. Инсталляция ПО DiSignCA	19
4.4.1. Инсталляция основного ПО	19
4.4.2. Инсталляция дополнительного ПО.....	21
4.5. Проверка контрольных сумм.....	23
5. Настройка программы DiSignCA.....	24
5.1. Начальная настройка и инициализация криптосистемы	25
5.1.1. Занесение личного сертификата в хранилище	26
5.1.2. Занесение сертификатов УЦ и СОС в хранилища	28
5.2. Продолжение настройки криптосистемы.....	30
5.2.1. Установка личного сертификата пользователя	30
5.2.2. Защита хранилища доверенных УЦ.....	30
5.2.3. Работа с хранилищами сертификатов.....	31
5.2.4. Установка параметров сообщения	31
5.3. Инициализация криптосистемы	32
5.4. Работа с хранилищами	33
5.4.1. Хранилище Сертификаты	34

					НКБГ. 501430.773И6	Лист
						4
Изм.	Лист	№ документа	Подпись	Дата		

5.4.2. Хранилище Списки отзыва.....	37
5.4.3. Хранилище Доверенные УЦ.....	38
5.5. Рабочие папки.....	39
5.6. Протоколирование работы программы.....	40
5.7. Файл инициализации.....	40
6. Работа с программой.....	43
6.1. Запуск программы.....	43
6.2. Формирование ЭЦП.....	44
6.3. Проверка ЭЦП.....	46
6.4. Извлечение исходного файла.....	47
7. Работа с макросами в Microsoft Word.....	49
7.1. Формирование ЭЦП при помощи макроса.....	49
7.2. Проверка ЭЦП при помощи макроса.....	50
8. Входные и выходные данные.....	51
8.1. Входные данные.....	51
8.1.1. Исходные файлы.....	51
8.1.2. Формат информации на ключевом носителе.....	52
8.1.3. Открытые ключи и сертификаты ключей.....	52
8.1.4. Сертификаты и списки отозванных сертификатов доверенных УЦ.....	52
8.2. Выходные данные.....	53
Приложение 1. Макрос для Microsoft Word 2007.....	54
Приложение 2. Список терминов.....	56

1. Общие сведения

В данном разделе приведена информация о назначении, основных функциях и возможностях программы.

1.1. Наименование программы

Полное наименование программного обеспечения – **Абонентский пункт ЭЦП DiSignCA.**

Условное обозначение **DiSignCA.**

Разработчик: ООО “Фактор-ТС”, 123290, Москва, Первый Магистральный проезд, дом 11, тел. (495) 644-31-30, e-mail: factor@factor-ts.ru.

1.2. Назначение и область применения программы

Программа **DiSignCA** («Абонентский пункт ЭЦП» технологии **ДИОНИС**) предназначена для формирования и проверки **электронной цифровой подписи (ЭЦП)** при информационном обмене электронными документами, представленными в виде файлов произвольного формата операционной системы WINDOWS.

Программа **DiSignCA** обеспечивает формирование и проверку ЭЦП для одного или нескольких файлов, размещенных в локальных или сетевых директориях файловой системы компьютера.

Результатом работы программы **DiSignCA** является один (в случае, если ЭЦП помещается в тот же файл) или два (ЭЦП помещается в отдельный файл) файла, помещенные в заданные при настройке программы директории.

Программа **DiSignCA** обеспечивает формирование ЭЦП для уже подписанного документа (добавление подписи пользователя к уже существующей). Программа **DiSignCA** проверяет все полученные с проверяемым электронным документом ЭЦП.

Программа **DiSignCA** может (при соответствующих настройках) при генерации ЭЦП добавлять к ней информацию, необходимую для проверки получателем электронного документа (сертификат ключа пользователя **DiSignCA**, формирующего ЭЦП для документа и список отзыва Удостоверяющего центра, выдавшего сертификат пользователя). Программа **DiSignCA** может (при соответствующих настройках) при проверке ЭЦП сохранять полученную с ЭЦП дополнительную информацию, используемую для проверки (сертификат ключа участника электронного обмена документами, подписавшего документ, и список отзыва Удостоверяющего центра, выдавшего сертификат этого участника).

					НКБГ. 501430.773И6	Лист
						6
Изм.	Лист	№ документа	Подпись	Дата		

Программа **DiSignCA** формирует и проверяет ЭЦП в соответствии с криптографическими алгоритмами ГОСТ 34.10-2001, ГОСТ 34.11-94. Ключевая система использует инфраструктуру открытых ключей. Форматы цифровых сертификатов, списков отзыва, подписанных сообщений соответствуют рекомендациям RFC 4490, RFC 4491, RFC 4357.

1.2.1. Основные функции программы

Программа **DiSignCA** выполняет две основные функции:

1. **Формирует ЭЦП** для электронного документа (файла) и либо помещает ЭЦП в отдельный файл, либо упаковывает исходный файл и ЭЦП в один файл в формате **PKCS#7**.

Формирование ЭЦП выполняется посредством криптографического преобразования информации в соответствии с алгоритмом электронной цифровой подписи с использованием **закрытого ключа**, записанного на **ключевом носителе** пользователя ПО **DiSignCA**.

2. **Проверяет ЭЦП** для электронного документа. При положительном результате проверки помещает исходный файл (электронный документ) в предназначенную для этого директорию. Проверка выполняется как для случая, когда подпись (подписи) находится в том же файле (файл формата **PKCS#7** с расширением **p7m**), так и для случая, когда подпись (подписи) находится в отдельном файле (с расширением **p7s**). В последнем случае должно выполняться условие, что файл ЭЦП находится в той же директории, что и подписанный документ.

Проверка ЭЦП выполняется при помощи **сертификата ключа** лица, подписавшего файл. В процессе проверки ЭЦП решается вопрос доверия **сертификату ключа**, то есть проверяется подлинность и актуальность сертификата, при этом проверяются сертификаты и Списки отозванных сертификатов (СОС) Удостоверяющих центров, входящих в *цепочку доверия* (о цепочках доверия см. раздел 2.7, стр. 12).

При отрицательном результате проверки или при невозможности проверить ЭЦП программа предоставляет возможность извлечения электронного документа из файла, находящегося в формате **PKCS#7**, и помещает извлеченный файл в предназначенную для этого директорию.

Примечание. Решение проблем доставки, размещения, взаимной увязки файлов, а также выполнение действий с документами, для которых получен отрицательный

					НКБГ. 501430.773И6	Лист
						7
Изм	Лист	№ документа	Подпись	Дата		

абонента (**S** на рисунке). Результатом работы программы является файл в формате PKCS#7, содержащий и исходный файл, и ЭЦП (расширение имени файла – **p7m**). Упакованный файл отправляется получателю документа (на АРМ 2-го абонента).

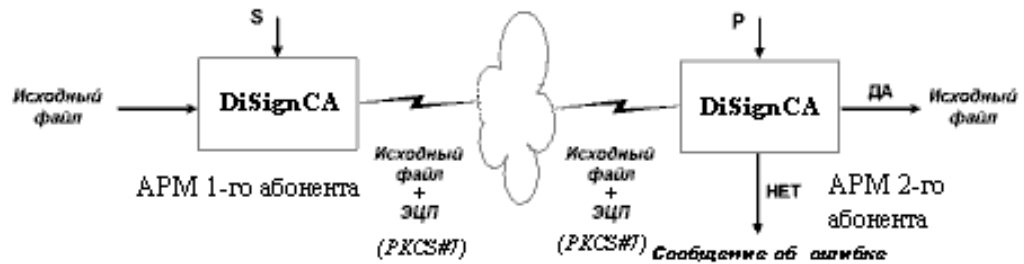


Рис. 1-2

Программа **DiSignCA**, установленная на рабочем месте получателя, получает упакованный файл и проверяет его с помощью открытого ключа отправителя документа (**P** на рисунке). Если ЭЦП верна (информация в исходном файле не подвергалась искажению и ЭЦП была сформирована именно отправителем документа), то **DiSignCA** извлекает исходный файл из упакованного и переносит его в директорию писем, прошедших проверку (направление **ДА** на рисунке). В противном случае **DiSignCA** выдает сообщение об ошибке проверки ЭЦП и оставляет упакованный файл в директории писем, не прошедших проверку (направление **НЕТ** на рисунке).

Примечание. В последнем случае **DiSignCA** по команде пользователя может извлечь исходный файл из полученного упакованного файла без проверки ЭЦП и перенести его в директорию «извлеченных писем». Сам упакованный файл остается в директории «непроверенных писем».

1.2.2. Интеграция с MS Word

Для удобства пользователей, работающих с документами в программе Microsoft Word, реализована возможность интеграции **DiSignCA** в Microsoft Word с помощью специального макроса Microsoft Word («макрос ЭЦП»). Это позволяет для текущего документа сформировать ЭЦП и проверить ЭЦП, не выходя из Microsoft Word.

					НКБГ. 501430.773И6	Лист
						9
Изм	Лист	№ документа	Подпись	Дата		

2. Основные понятия

В данном разделе приведена информация о терминологии, используемой в электронном документообороте с использованием ЭЦП, а также в данном документе для описания функционирования программы.

2.1. Электронная цифровая подпись

Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, предназначенный для удостоверения источника данных (идентификации отправителя электронного документа) и защиты данного электронного документа от подделки. Использование ЭЦП основано на применении криптографической системы (**криптосистемы**) асимметричного шифрования, в которой для формирования ЭЦП и ее проверки используется пара ключей (ключевая пара): **открытый ключ ЭЦП** и **закрытый ключ ЭЦП**.

2.2. Криптосистема

Криптосистема в общем случае представляет собой набор криптографических функций (программных модулей), реализующих криптографические преобразования открытой информации при помощи алгоритмов шифрования, имитозащиты, электронной цифровой подписи. В криптосистеме программы **DiSignCA** реализуются только алгоритмы электронной цифровой подписи и имитозащиты (для защиты хранилищ сертификатов).

Перед выполнением заданных функций **криптосистема** должна быть инициализирована, то есть, настроена на использование в криптографических функциях ключевой информации пользователя. Инициализация криптосистемы выполняется при изменении ее настроек, а также автоматически при запуске программы. Пользователь также может в некоторых ситуациях выполнить инициализацию криптосистемы.

2.3. Закрытый ключ ЭЦП

Закрытый ключ ЭЦП принадлежит участнику информационного обмена электронными документами. Он формируется на ключевом носителе средствами генерации ключей (программой **Модуль Генерации Ключей**) и должен храниться участником информационного обмена в тайне.

Закрытый ключ используется для формирования ЭЦП электронного документа (формирования ЭЦП).

					НКБГ. 501430.773И6	Лист
						10
Изм.	Лист	№ документа	Подпись	Дата		

2.4. Открытый ключ ЭЦП

Открытый ключ ЭЦП однозначно соответствующий **закрытому ключу**, доступен всем участникам информационного обмена и либо размещается в общедоступном месте, либо пересылается вместе с документом. Закрытый и открытый ключ образуют так называемую **несимметричную ключевую пару**.

Открытый ключ используется для проверки ЭЦП полученного документа.

Подлинность **открытого ключа** подтверждается электронно-цифровой подписью доверенной организации. Такая организация называется **Удостоверяющий центр (УЦ)**.

Примечание. ЭЦП отправителя и получателя документов могут быть подтверждены как одним, так и разными Удостоверяющими центрами.

Открытый ключ входит в состав **Сертификата ключа**.

2.5. Сертификат ключа

Сертификат ключа имеет следующую структуру: открытый ключ, электронная цифровая подпись **Удостоверяющего центра**, выдавшего этот сертификат, и сопроводительная информация.

В состав сопроводительной информации входят следующие данные:

- реквизиты владельца ключа (имя, почтовый адрес и т. п.);
- период действия закрытого ключа;
- реквизиты УЦ, выпустившего сертификат;
- параметры использования закрытого ключа (только ЭЦП или ЭЦП и шифрование, а также указание, для каких систем предназначен - Электронная почта, аутентификация на WEB-сервере и т. п.);
- серийный номер сертификата;
- другая служебная информация.

2.6. Удостоверяющий центр

Главной задачей Удостоверяющего центра является выдача гарантированно подлинных сертификатов владельцам ключевой пары (закрытого и открытого ключей).

УЦ ведет архив и отслеживает актуальность выданных им сертификатов. УЦ по запросам пользователей генерирует для них закрытые ключи.

Для выполнения этих задач Удостоверяющий центр выполняет следующие действия.

1. УЦ формирует сертификаты ключей пользователей, сформированным самим центром, а также ключей, сформированным пользователями, приславшими запрос на

					НКБГ. 501430.773И6	Лист
						11
Изм	Лист	№ документа	Подпись	Дата		

сертификат. УЦ заверяет сертификаты своей электронной цифровой подписью, подтверждая тем самым принадлежность сертификата конкретному пользователю и гарантируя неизменность данных, внесенных в сертификат.

- УЦ выпускает и поддерживает список отозванных сертификатов, т.е. тех сертификатов, которые должны быть изъяты из обращения по тем или иным причинам (например, в случае компрометации закрытого ключа).
- УЦ формирует свой закрытый ключ. Формирует сертификат ключа и либо заверяет этот сертификат своей ЭЦП - «самоподписанный» сертификат (такой УЦ называется корневым доверенным УЦ), либо направляет соответствующий запрос в вышестоящий УЦ.

При наличии в организации нескольких УЦ, а также в случае необходимости межведомственного обмена электронными документами между организациями, обслуживаемыми различными УЦ, появляется необходимость работы с сертификатами, заверенными различными Удостоверяющими центрами.

Для успешного обмена каждому участнику необходимо иметь полный набор сертификатов и списков отозванных сертификатов промежуточных и корневых доверенных УЦ, необходимых для построения цепочки доверия (см. следующий раздел) для сертификата абонента, подписавшего документ.

Сертификаты корневых доверенных УЦ должны быть доставлены по надежным каналам связи всем участникам обмена и храниться в условиях, исключающих их подмену.

Программа **DiSignCA** использует сертификаты промежуточных УЦ и сертификаты корневых доверенных УЦ во время проверки ЭЦП документа для определения достоверности сертификатов ключей участников обмена.

2.7. Цепочка доверия УЦ

Цепочка доверия УЦ – это последовательность всех УЦ, участвующих в проверке одного сертификата.

Когда программа **DiSignCA** получает подписанный документ, она должна, в первую очередь, решить, «доверяет» ли она сертификату автора. Решить вопрос доверия означает проверить подлинность и актуальность сертификата.

- Сертификат считается подлинным, если для него верна ЭЦП, сформированная удостоверяющим центром, выпустившим данный сертификат.

					НКБГ. 501430.773И6	Лист
						12
Изм.	Лист	№ документа	Подпись	Дата		

2. Сертификат считается актуальным, если у него не истек срок действия (указывается в самом сертификате) и если он не отозван выпустившим его Удостоверяющим центром (проверяется путем анализа списка отозванных сертификатов).

Вопрос доверия сертификату в программе **DiSignCA** решается построением для этого сертификата цепочки доверия УЦ:

- программа **DiSignCA**, получив подписанный документ, идентифицирует автора и извлекает из своего локального хранилища его сертификат (*сертификат 1*);
- определяет, какой УЦ выдал этот сертификат, извлекает из локального хранилища сертификат этого УЦ (*сертификат 2*) и проверяет с его помощью ЭЦП под сертификатом автора (*сертификатом 1*);
- если оказывается, что сертификат УЦ (*сертификат 2*) подписан вышестоящим УЦ, то повторяется проверка для него и так вплоть до корневого УЦ - того УЦ, сертификат которого подписан им самим;

Примечание. Вместе с проверкой ЭЦП на всех этапах программа проверяет актуальность соответствующего сертификата.

- проверяется наличие корневого УЦ в списке корневых доверенных УЦ в специальном хранилище **DiSignCA**.

Все УЦ, участвующие в проверке сертификата, образуют цепочку доверия для этого сертификата. В частном случае, цепочка доверия может содержать один корневой УЦ.

Программа **DiSignCA** «доверяет» сертификату, если он подписан или корневым УЦ, или каким-то УЦ из цепочки, заканчивающейся корневым УЦ, причем корневой УЦ содержится в списке корневых УЦ на рабочем месте абонента.

					НКБГ . 501430.773И6	Лист
						13
Изм	Лист	№ документа	Подпись	Дата		

3. Правила использования программы

В данном разделе приведена информация, необходимая для правильной подготовки программы к работе - исходные данные для настройки и использования (раздел 3.1), в том числе, подготовка ключевых носителей, получение и ввод данных (сертификатов и списков отзыва сертификатов), необходимых для проверки подлинности ЭЦП (раздел 3.3), а также действия по настройке криптосистемы (раздел 3.4).

3.1. Подготовительные действия

Подготовительные действия, которые необходимо выполнить перед началом работы с программой, состоят во вводе в систему всех необходимых для создания и проверки ЭЦП исходных данных – ключевой информации пользователя, его сертификата, сертификатов других участников обмена и доверенных УЦ, а также списков отозванных сертификатов.

Для участия в обмене документами, защищенными ЭЦП, каждый участник обмена должен иметь свой закрытый ключ ЭЦП и свой сертификат ключа ЭЦП.

Для того чтобы два участника могли обмениваться подписанными файлами, каждый из них должен иметь:

- свой закрытый ключ ЭЦП и свой сертификат ключа для того, чтобы подписать документ;
- сертификат ключа того участника обмена, который подписал документ, для того, чтобы проверить ЭЦП.

Если участников обмена несколько, то каждый из них должен иметь:

- свой закрытый ключ ЭЦП и свой сертификат;
- сертификаты ключей ЭЦП всех участников обмена, с которыми он будет обмениваться подписанными файлами.

Кроме того, каждый из участников обмена должен иметь сертификаты и списки отозванных сертификатов (СОС) всех УЦ, необходимых для построения цепочек доверия.

Все эти данные необходимо ввести в программу на этапе ее настройки (см. раздел 5, стр. 24).

3.2. Ключевая информация и ключевой носитель

Закрытый ключ ЭЦП (и необходимая для его использования информация) должен обязательно храниться на съемном ключевом носителе. Для удобства пользователей на этом же носителе могут размещаться все (или часть) сертификаты и все списки отозванных сертификатов, но возможно хранение сертификатов отдельно на другом носителе.

					НКБГ. 501430.773И6	Лист
						14
Изм.	Лист	№ документа	Подпись	Дата		

3.2.1. **Получение ключевого носителя**

Ключевой носитель пользователь **DiSignCA** может получить от УЦ (по надежному каналу связи) или сформировать самостоятельно на своем рабочем месте.

1. В первом случае Удостоверяющий центр, используя программу **Модуль генерации ключей**, сгенерирует закрытый ключ для пользователя и запишет его на ключевой носитель вместе с необходимой служебной информацией. На этот же носитель (если это не eToken или ruToken) УЦ может поместить необходимые пользователю сертификаты: сертификат ключа пользователя, сертификат ключа своего УЦ и всех УЦ из *цепочки доверия*, сертификаты ключей участников обмена, а также списки отозванных сертификатов всех УЦ из *цепочки доверия*.
2. Во втором случае пользователь с помощью той же программы **Модуль генерации ключей** генерирует закрытый ключ и формирует запрос на выдачу сертификата ключа. Посылает этот запрос на УЦ. УЦ формирует требуемый сертификат ключа и передает его пользователю. Вместе с ним УЦ может передать все остальные сертификаты и списки отозванных сертификатов.

Замечание 1. В обоих случаях информация на ключевом носителе может быть закрыта паролем.

Замечание 2. Сертификаты участников обмена и списки отозванных сертификатов могут быть опубликованы в месте, доступном для всех участников обмена.

3.2.2. **Состав ключевой информации**

На ключевом носителе всегда содержатся два файла (заключенные в «контейнер»):

- <идентификатор_ключа>.pvt – закрытый ключ ЭЦП;
- <идентификатор_ключа>.hdr – дополнительная информация, необходимая для использования закрытого ключа.

Основную часть имени файлов (<идентификатор_ключа>) задает программа **Модуль Генерации ключей**, указанные расширения имен являются обязательными.

Кроме этого, на все ключевые носители, кроме eToken и ruToken, УЦ может разместить файлы, содержащие следующие сертификаты и списки отозванных сертификатов.

1. Сертификаты пользователей - как правило, находятся в файлах, имена которых имеют расширение **cer**.

Файл с расширением **cer** может содержать только один сертификат.

					НКБГ. 501430.773И6	Лист
						15
Изм	Лист	№ документа	Подпись	Дата		

2. Сертификаты удостоверяющих центров - как правило, находятся в файлах, имена которых имеют расширение **p7b**. В этот же файл УЦ, как правило, помещает списки отозванных сертификатов.

Файл с расширением **p7b** может содержать как один, так и несколько сертификатов, а также списки отозванных сертификатов.

3. Кроме того, списки отозванных сертификатов могут находиться в файлах, имена которых имеют расширение **cr1**.

Если используются ключевые носители eToken или ruToken, то указанные сертификаты и списки отозванных сертификатов УЦ размещает в другом доступном пользователю месте.

На ключевой носитель записывается также ссылка на текущий сертификат, создаваемая в процессе настройки криптосистемы **DiSignCA** (см. раздел 5.1, стр. 25).

3.3. Хранение сертификатов

Для хранения действующих сертификатов и списков отозванных сертификатов в **DiSignCA** используется набор из трех хранилищ.

1. Хранилище **Сертификаты** - предназначено для хранения сертификата ключа пользователя **DiSignCA**, сертификатов участников обмена и сертификатов УЦ, в том числе, корневых.
2. Хранилище **Списки отзыва** - предназначено для хранения списков отозванных сертификатов всех УЦ, необходимых для построения *цепочки доверия*.
3. Хранилище **Доверенные УЦ** - предназначено для хранения сертификатов корневых УЦ (эти сертификаты продублированы в первом хранилище).

3.4. Настройка криптосистемы

Для работы с программой **DiSignCA** необходимо произвести настройку криптосистемы, то есть:

- ввести ключевую информацию пользователя (включая его сертификат ключа);
- ввести данные во все три типа хранилищ (сертификаты и списки отзыва сертификатов);
- выполнить инициализацию криптосистемы.

Настройка криптосистемы может быть выполнена только для **ОДНОГО** ключевого носителя, ключевая информация с которого используется для инициализации криптосистемы и последующего формирования ЭЦП и имитозащиты хранилищ. Назначение **текущего**

					НКБГ. 501430.773И6	Лист
						16
Изм.	Лист	№ документа	Подпись	Дата		

ключевого носителя выполняется во время процедуры установки **текущего** сертификата пользователя (см. п. 5.2.1, стр. 30). При перезапуске программы автоматически выполняется поиск заданного при настройке ключевого носителя и инициализация криптосистемы.

Во время этой же процедуры (установки текущего сертификата пользователя) может быть осуществлено заполнение хранилищ соответствующей информацией. Ввод новых сертификатов УЦ и списков отзывов возможен также при помощи процедуры работы с хранилищами (см. п. 5.2.3, стр. 31 и п. 5.4. стр. 33) .

При настройке криптосистемы также можно указать местоположение **хранилища сертификатов корневых УЦ**. При размещении его на съемном магнитном носителе (например, НГМД) следует придерживаться правил защиты от несанкционированного использования данного носителя. При размещении данного хранилища на жестком магнитном диске компьютера пользователя необходимо защитить его средствами криптосистемы (имитовставкой).

При изменении места расположения хранилища сертификатов корневых УЦ необходимо выполнить следующие действия:

1. Снять защиту (имитовставку) с хранилища сертификатов корневых УЦ (раздел 5.2.2, стр. 30).
2. Указать новое местоположение.
3. Установить новый текущий сертификат пользователя (раздел. 5.2.1 стр. 30).
4. Установить защиту хранилища (раздел 5.4.3, стр. 38).

					НКБГ. 501430.773И6	Лист
						17
Изм	Лист	№ документа	Подпись	Дата		

4. Условия применения программы

Программа **DiSignCA** обеспечивает выполнение решаемых ею задач при соблюдении требований к операционной среде (раздел 4.1), требований к используемым ключевым носителям и ключевой информации (раздел 4.2), соблюдении правил ее инсталляции (раздел 4.4), корректной настройке ПО (раздел 5, стр. 24), а также при соблюдении правил контроля целостности ПО (проверка контрольных сумм) (раздел 4.5, стр. 23).

При работе с программой **DiSignCA** необходимо соблюдать правила, изложенные в предыдущем разделе.

4.1. Требования к оборудованию и операционной среде

Программное обеспечение **DiSignCA** устанавливается на IBM-совместимом компьютере с операционной системой семейства Microsoft WINDOWS (версии 2000/2003/XP/Vista).

Компьютер должен быть оснащен устройством для считывания съемных носителей (НГМД, USB-порт и проч.).

Для работы с макросом ЭЦП требуется установленная программа Microsoft Word (версии 2000/2002/2003/2007).

4.2. Требования к ключевым носителям и ключевой информации

Для работы с ПО **DiSignCA** пользователь должен иметь ключевой носитель с записанной на нем информацией (см. раздел 3.2.2, стр. 15), а также собственный сертификат (на этом же или на другом носителе).

В качестве ключевых носителей могут быть использованы любые носители, которые ОС WINDOWS может определить как съемные и перезаписываемые (НГМД, Flash - накопители, ZIP Drive и т.п.). В качестве ключевых носителей также могут использоваться устройства ruToken или eToken.

Ключевой носитель содержит закрытую информацию. Пользователь ДОЛЖЕН обеспечить его надежное хранение. КАТЕГОРИЧЕСКИ запрещается модифицировать содержимое ключевого носителя. В то же время на носителе не должна быть установлена защита от записи.

					НКБГ. 501430.773И6	Лист
						18
Изм.	Лист	№ документа	Подпись	Дата		

4.3. Состав ПО DiSignCA

Программное обеспечение **DiSignCA** поставляется в виде дистрибутивного пакета на одном носителе (гибком магнитном диске или на компакт-диске). Дистрибутивный пакет содержит:

- программу установки ПО **DiSignCA SETUP.EXE**;
- директорию, содержащую файлы установки ПО поддержки носителей eToken и ruToken.

Программное обеспечение **DiSignCA** состоит из следующих компонент:

- программа **DiSignCA** (Абонентский пункт ЭЦП);
- программа проверки целостности ПО **CheckWin** и файл **checksum.txt**;
- программа удаления ПО - **Uninstall DiSignCA**;
- справка **DiSignCA**;
- конфигурационный файл **DiSignCA.ini**;
- библиотеки программных модулей (***.dll**).

4.4. Инсталляция ПО DiSignCA

Для инсталляции ПО **DiSignCA** пользователь должен обладать правами администратора ОС WINDOWS.

Если на компьютере уже установлена программа **DiSignCA**, то ее необходимо предварительно деинсталлировать с помощью программы **Uninstall DiSignCA** (ярлык программы находится в той же рабочей группе меню «**Программы**», что и ярлык для запуска программы **DiSignCA**).

Инсталляция состоит из установки основного ПО (собственно ПО **DiSignCA**) и, при необходимости, установки дополнительного программного обеспечения поддержки носителей eToken и/или ruToken.

Внимание! Если на ПЭВМ пользователя установлена программа Microsoft Word 2007 и предполагается использование макроса ЭЦП, то перед инсталляцией **DiSignCA** необходимо выполнить некоторые специальные настройки в Microsoft Word 2007. Эти настройки и использование макроса ЭЦП для Microsoft Word 2007 описаны в **Приложении 1**.

4.4.1. Инсталляция основного ПО

Начинается установка с выдачи информации о версии устанавливаемого ПО и предупреждающего сообщения о необходимости закрыть все приложения.

					НКБГ. 501430.773И6	Лист
						19
Изм	Лист	№ документа	Подпись	Дата		

Для инсталляции ПО **DiSignCA** необходимо пройти через последовательность шагов, отвечая на задаваемые вопросы.

В процессе инсталляции запрашивается директории для установки, по умолчанию предлагается поддиректория в стандартной системной директории: **<Системный диск>\Program Files\DiSignCA**.

В процессе инсталляции программа запрашивает название рабочей группы в меню **Пуск** ⇒ **Программы**, в которую будут помещены ярлыки для запуска Абонентского пункта ЭЦП **DiSignCA**, а также ярлыки служебных программ: программы проверки контрольных сумм **CheckWin** и программы удаления Абонентского пункта ЭЦП **Uninstall DiSignCA**.

По умолчанию предлагается название

FACTOR Applications\Абонентский пункт ЭЦП DiSignCA.

В процессе инсталляции будет выдан запрос, позволяющий установить в Абонентский пункт ЭЦП **DiSignCA** дополнительную функцию – макрос для MS Word.

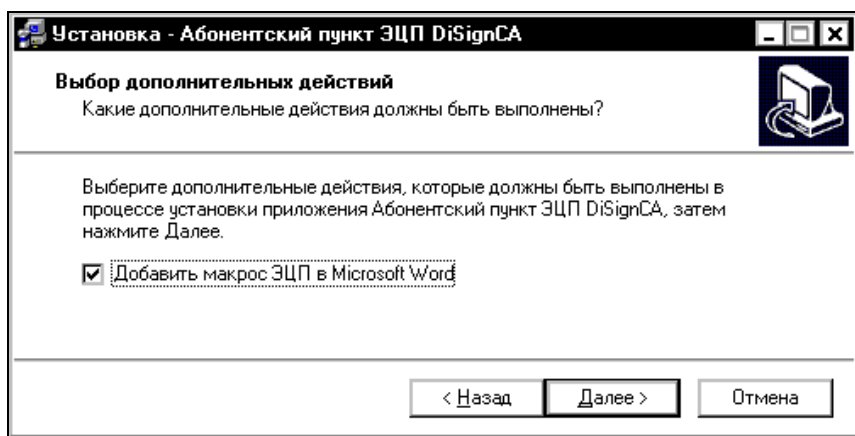


Рис. 4-1

При установке флажка **Добавить макрос ЭЦП в Microsoft Word** в процессе инсталляции ПО **DiSignCA** на экран будет выведено окно с именем директории, которая зарегистрирована в реестре ОС Windows как директория установки Microsoft Word, и запросом:

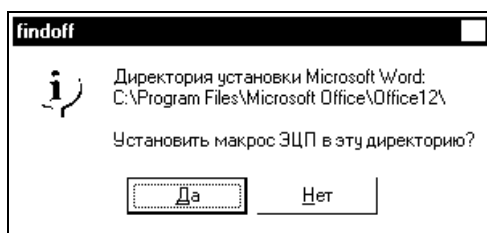


Рис. 4-2

В том случае, если найденная директория установки Microsoft Word совпадает с директорией, в которую желательно установить макрос, следует нажать кнопку **Да**.

Выбор другой директории может понадобиться, если в системе установлено несколько программ Microsoft Word. В этом случае необходимо нажать кнопку **Нет** и в появившемся окне выбора директорий найти место установки нужной программы Microsoft Word. При необходимости установки макроса для всех версий Microsoft Word следует после окончания инсталляции **DiSignCA** вручную скопировать в директорию **<Директория программ Windows>\Microsoft Office\OfficeXX\StartUP** (или в любую другую директорию установки MS Office) файл **disign.dot** (Здесь **xx** – номер версии MS Office).

Если в системе не установлена программа Microsoft Word, то программа инсталляции сообщит об ее отсутствии и невозможности установки макроса.

Замечание. Особенности работы с макросами в Microsoft Word 2007 рассмотрены в **Приложении 1** к настоящему документу.

После нажатия кнопки **Далее** (Рис. 4-1) на экран будет выведено окно с перечнем выбранных пользователем параметров, и после их подтверждения будет выполнена инсталляция. По окончании инсталляции будет запущена программа проверки контрольных сумм **checkwin**.

4.4.2. **Инсталляция дополнительного ПО**

Если предполагается работа с носителями eToken и ruToken, на ПЭВМ пользователя должно быть установлено ПО поддержки (драйверы) этих носителей.

Для удобства пользователей мы включили в дистрибутивный пакет **DiSignCA** ПО драйверов устройств eToken и ruToken. Им можно воспользоваться, если требуемое ПО на ПЭВМ не установлено.

Примечание. ООО «Фактор-ТС» не является разработчиком ПО поддержки носителей eToken и ruToken, а только обеспечивает возможность их использования в качестве ключевых носителей.

ПО поддержки носителей EToken и RuToken располагается в директории **Redist**:
rtDrivers.x86.v.2.15.01.148.exe - инсталляционный файл поддержки носителей ruToken;
RTE_3.66.msi - инсталляционный файл поддержки носителей eToken;
RTE_3.66.RUI.msi - русификатор для eToken.

					НКБГ. 501430.773И6	Лист
						21
Изм	Лист	№ документа	Подпись	Дата		

Установка драйверов носителей ruToken - запустить инсталляционный файл **rtDrives.x86.2.15.01.148.exe**. В процессе установки необходимо пройти через последовательность шагов, которые сопровождаются комментариями и являются стандартными для установки ПО в операционной системе WINDOWS.

Установка драйверов носителей eToken выполняется в следующей последовательности.

Запустить файл **RTE_3.66.msi**. В появившемся на экране окне (Рис. 4-3) нажать кнопку **Next**. В следующем окне (Рис. 4-4) в случае согласия с условиями лицензии нажать переключатель **I accept the license agreement** и затем нажать кнопку **Next**.



Рис. 4-3



Рис. 4-4

В появившемся окне (Рис. 4-5) нажатием кнопки **Next** запустить процесс инсталляции. После завершения установки драйверов на экран выводится окно (Рис. 4-6), в котором надо нажать кнопку **Finish**.

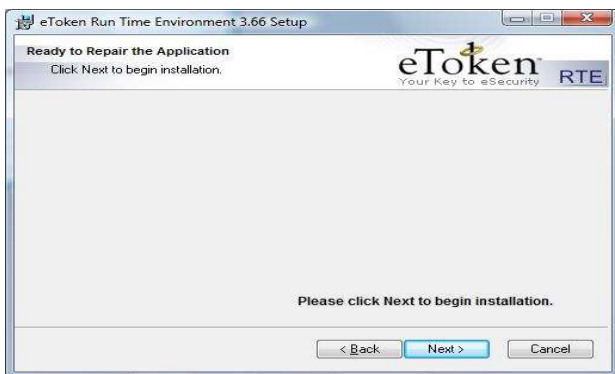


Рис. 4-5



Рис. 4-6

Далее для русификации установленного ПО драйверов носителей eToken надо запустить файл **RTE_3.66.RUI.msi**. В процессе установки необходимо следовать инструкциям, которые сопровождаются комментариями и являются стандартными для установки ПО в операционной системе WINDOWS.

						НКБГ. 501430.773И6	Лист
							22
Изм.	Лист	№ документа	Подпись	Дата			

По окончании установки драйверов следует подтвердить разрешение на перезагрузку системы.

4.5. Проверка контрольных сумм

Перед тем как начать работу с программой **DiSignCA**, пользователь должен проверить целостность полученного программного обеспечения. Для проверки используются программа **CheckWin** и файл **checksum.txt**, входящие в состав дистрибутивного пакета.

Файл **checksum.txt** содержит список файлов программного обеспечения Абонентского пункта ЭЦП **DiSignCA**, подлежащих обязательной проверке, вместе с эталонными значениями контрольных сумм. Содержимое файла **checksum.txt** дублируется в Формуляре на изделие **DiSignCA**. Пользователь должен, прежде всего, путем просмотра содержимого файла **checksum.txt** сверить значения контрольных сумм данного файла со значениями, содержащимися в Формуляре, и, только убедившись в их идентичности, приступить к дальнейшей проверке.

Запустить программу **CheckWin**. На этапе инсталляции программа запускается автоматически после завершения установки основного ПО.

Программа **CheckWin** вычислит контрольные суммы файлов, приведенных в списке, и сравнит их с эталонными значениями. Если суммы совпадут, то программа выдаст сообщение, что контрольные суммы проверены успешно.

Если будет обнаружено несовпадение, то программа укажет файл, где имеет место ошибка контрольной суммы. В таком случае программное обеспечение требует обязательной замены.

В процессе эксплуатации ПО **DiSignCA** следует периодически выполнять проверку контрольных сумм. Периодичность проверки целостности **DiSignCA** зависит от условий эксплуатации и определяется политикой безопасности эксплуатирующей организации.

					НКБГ. 501430.773И6	Лист
						23
Изм	Лист	№ документа	Подпись	Дата		

5.1. Начальная настройка и инициализация криптосистемы

Чтобы выполнить настройку криптосистемы, следует нажать кнопку **Настроить** в главном окне (Рис. 5-1). На экран будет выведено окно **Установки криптосистемы**, в котором установлен флажок **Отключить криптозащиту**. Флажок следует снять, после чего в окне станут доступными все кнопки, кроме двух: **Работа с хранилищем сертификатов** и **Удалить имитовставку хранилища** (Рис. 5-2).

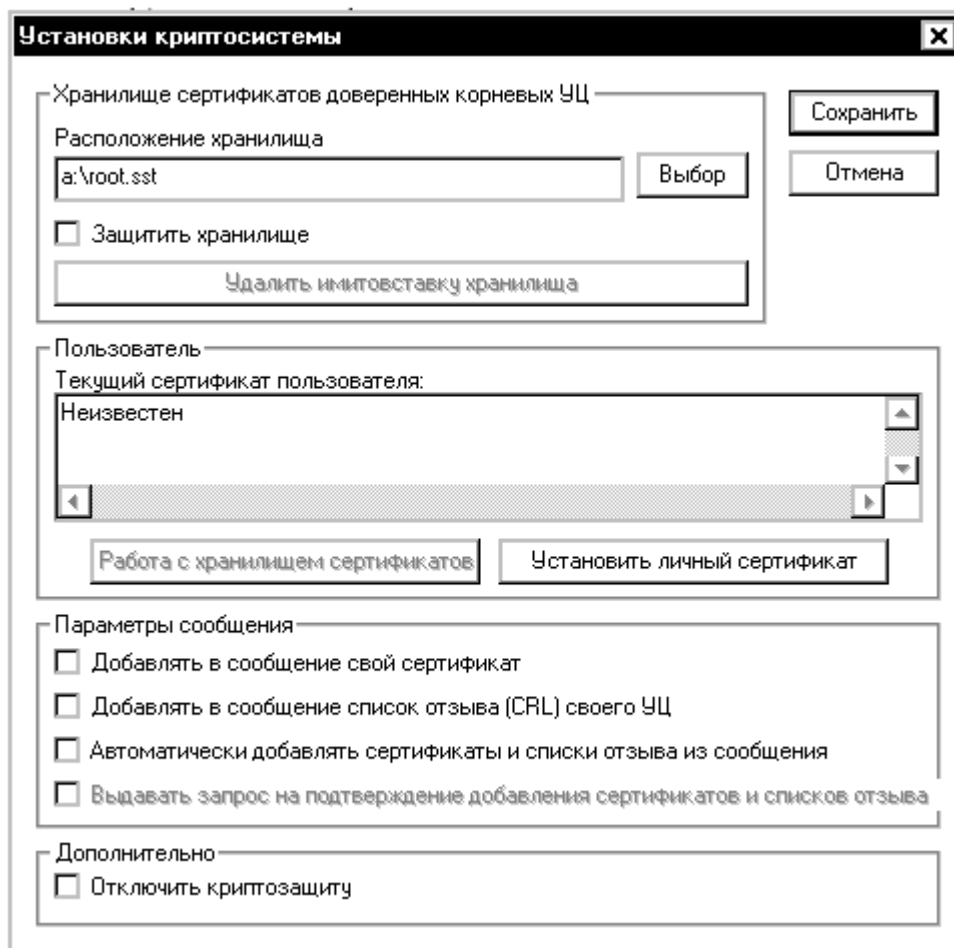


Рис. 5-2

При начальной настройке в окне заполнено только одно поле под заголовком **Расположение хранилища**. В это поле выводится имя файла (с указанием пути), в котором будет располагаться хранилище **Доверенные УЦ**. В нем будут храниться сертификаты всех корневых УЦ, замыкающих *цепочки доверия* (см. раздел 2.7, стр. 12). По умолчанию значение поля - **a:\root.sst**. Если предполагается поместить файл **root.sst** в другом месте, то следует нажать кнопку **Выбор** (справа от имени) и выбрать в стандартном диалоге WINDOWS нужную директорию. Имя файла изменить нельзя.

					НКБГ. 501430.773И6	Лист
						25
Изм	Лист	№ документа	Подпись	Дата		

Начальная настройка состоит из двух шагов:

- занесение личного сертификата ключа пользователя в хранилище **Сертификаты** и назначение его *текущим*;
- занесение в соответствующие хранилища всех сертификатов УЦ и списков отзыва сертификатов, необходимых для построения *цепочки доверия УЦ* для личного сертификата ключа пользователя.

5.1.1. Занесение личного сертификата в хранилище

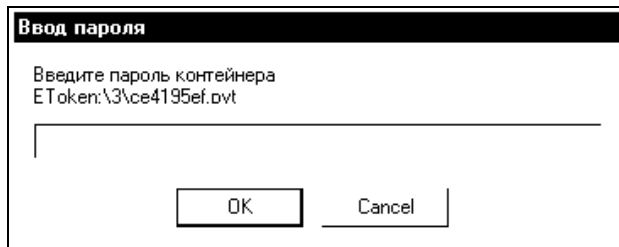
Занесение личного сертификата ключа пользователя в хранилище **Сертификаты** и назначение его *текущим* выполняется следующей последовательностью действий.

1. Пользователь должен вставить ключевой носитель в считывающее устройство и в окне **Установки криптосистемы** (Рис. 5-2) нажать кнопку **Установить личный сертификат** - на экран будет выведен список имен контейнеров (с указанием типа считывающего устройства) на этом ключевом носителе, а также и на других, если они вставлены в другие считывающие устройства. В этом списке следует выделить строчку с нужным контейнером (т.е. с тем контейнером, который содержит закрытый ключ пользователя) и нажать кнопку **Выбрать**.

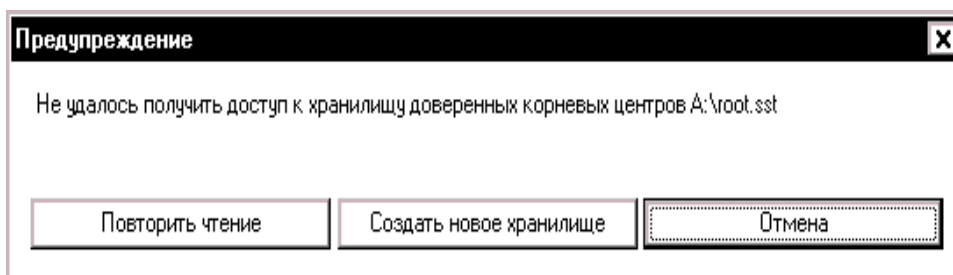


Если считывающее устройство не готово или формат носителя некорректен, то в списке не окажется нужного контейнера. В этом случае следует исправить ошибку и нажать кнопку **Повтор**.

2. Если контейнер закрытого ключа защищен паролем (для носителей eToken и ruToken он всегда защищен), то на экране появится запрос для ввода пароля. После корректного ввода пароля работа будет продолжена.

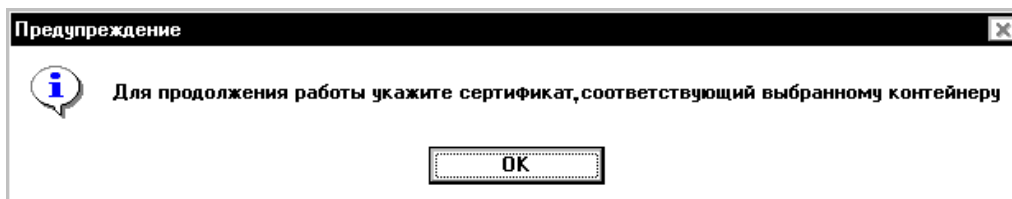


3. Программа **DiSignCA** проверит наличие файла с хранилищем **Доверенные УЦ** в указанном месте - поле под заголовком **Расположение хранилища** на Рис. 5-1. Если файла не окажется (при первой настройке хранилище отсутствует), то будет выдано предупреждение и предоставлена возможность хранилище создать.

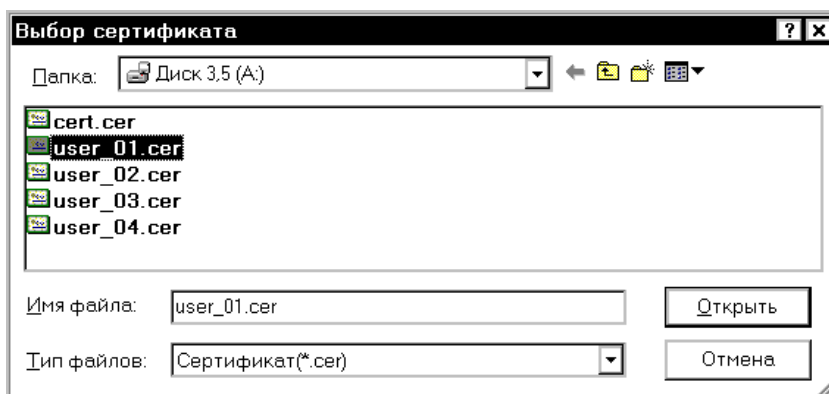


После нажатия кнопки **Создать новое хранилище** хранилище будет создано.

4. Программа **DiSignCA** приступит к созданию ссылки на сертификат ключа. Будет выдано сообщение.



После нажатия кнопки **OK** на экран будет выведено стандартное окно WINDOWS со списком файлов, имеющих имена с расширением **cer**.

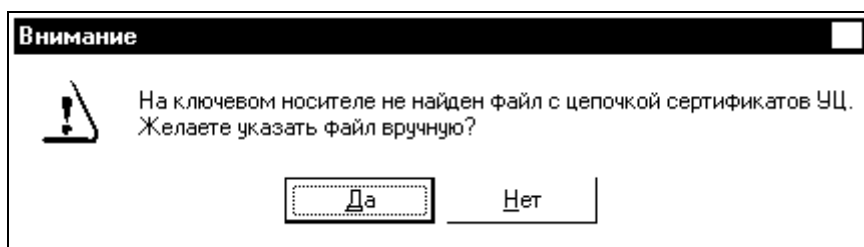


В этом списке следует выбрать файл, содержащий необходимый сертификат, и нажать кнопку **Открыть**.

Программа выполнит сравнение открытого ключа, соответствующего закрытому ключу на ключевом носителе, и открытого ключа в сертификате и при их совпадении

					НКБГ. 501430.773И6	Лист
Изм	Лист	№ документа	Подпись	Дата		27

в нем). Если файла не окажется на ключевом носителе, то программа **DiSignCA** предложит сначала указать его местоположение вручную (нажать кнопку **Да**):



Если будет нажата кнопка **Нет**, то нужную директорию можно будет выбрать в стандартном диалоге WINDOWS.

После того как файл будет найден, система занесет все необходимые сертификаты, кроме корневого, в хранилище **Сертификаты**. Затем выведет на экран информацию из корневого сертификата, которая позволит пользователю идентифицировать сертификат и предложит добавить его в хранилище (Рис. 5-3):

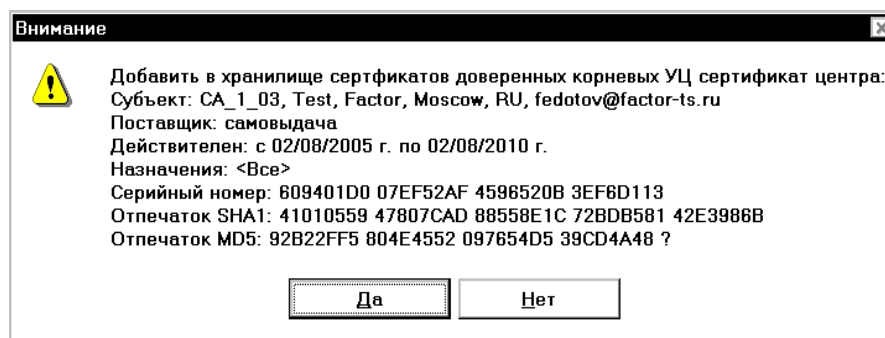


Рис. 5-3

По нажатию кнопки **Да** сертификат будет добавлен в оба хранилища **Сертификаты** и **Доверенные УЦ**.

2. Далее программа **DiSignCA** проанализирует наличие списка отозванных сертификатов в файле **cacert.p7b** или в файле **cert.crl**. При обнаружении СОС **DiSignCA** предложит добавить его в хранилище **Списки отзыва**. Если в этих файлах списка не окажется, **DiSignCA** предложит указать его местоположение вручную.

На этом начальная настройка заканчивается: личный сертификат пользователя назначен текущим, все необходимые сертификаты и списки отозванных сертификатов занесены в соответствующие хранилища.

Ключевой носитель должен оставаться в считывающем устройстве. В окне **Установки криптосистемы** (Рис. 5-2) следует нажать кнопку **Сохранить**. Все сделанные настройки будут записаны, будет автоматически выполнена инициализация криптосистемы и проверена *цепочка доверия* для текущего сертификата пользователя (если окажется, что цепочка

					НКБГ. 501430.773И6	Лист
						29
Изм	Лист	№ документа	Подпись	Дата		

некорректна, **DiSignCA** выдаст соответствующее предупреждение, но оставит за пользователем принятие решения об использовании текущего сертификата).

После этого на экран будет выдано соответствующее сообщение и **DiSignCA** перейдет в главное окно (Рис. 5-1).

5.2. Продолжение настройки криптосистемы

Для того чтобы пользователь Абонентского пункта ЭЦП мог обмениваться подписанными документами с другими абонентами, он должен занести в соответствующие хранилища сертификаты остальных участников обмена, необходимые сертификаты УЦ и списки отозванных сертификатов (СОС).

Кроме того, пользователь при необходимости может изменить настройки криптосистемы:

- заменить личный сертификат;
- добавить/удалить сертификаты в соответствующие хранилища;
- добавить/удалить списки отозванных сертификатов;
- а также задать выполнение некоторых дополнительных действий при формировании или при проверке ЭЦП.

Для этого он должен нажать кнопку **Настроить** в главном окне (Рис. 5-1) и получить окно **Установки криптосистемы** (Рис. 5-2), в котором отсутствует флажок **Отключить криптозащиту** и доступны все кнопки.

5.2.1. Установка личного сертификата пользователя

Кнопка **Установить личный сертификат** (Рис. 5-2) позволяет заменить текущий сертификат ключа пользователя. Пользователь должен нажать кнопку и далее выполнить те же действия, что и при начальной настройке (раздел 5.1, стр. 25).

Примечание. Если новый сертификат корневого УЦ совпадает с тем, который находится в хранилище **Доверенные УЦ**, то **DiSignCA** вместо запроса (Рис. 5-3) на добавление сертификата в хранилище предложит его заменить.

5.2.2. Защита хранилища доверенных УЦ

Флажок **Защитить хранилище** (Рис. 5-2). Если флажок установлен, то каждый раз при инициализации криптосистемы будет выполняться проверка имитовставки хранилища **Доверенные УЦ**. Данная проверка **ОБЯЗАТЕЛЬНА**, если хранилище **Доверенные УЦ** содержится на незащищенном носителе или жестком диске.

						НКБГ. 501430.773И6	Лист
							30
Изм.	Лист	№ документа	Подпись	Дата			

Флажок **Защитить хранилище** устанавливается автоматически только в том случае, если для хранилища **Доверенные УЦ** сформирована имитовставка (см. 5.4.3, стр. 38).

Если имитовставка не сформирована, то выдается сообщение об ошибке. Флажок **Защитить хранилище** можно установить вручную после того, как имитовставка будет сформирована.

Кнопка **Удалить имитовставку хранилища** (Рис. 5-2) служит для удаления имитовставки. После ее нажатия удаляется имитовставка, автоматически снимается флажок **Защитить хранилище**, и сама кнопка становится недоступной.

5.2.3. **Работа с хранилищами сертификатов**

Кнопка **Работа с хранилищем сертификатов** (Рис. 5-2) предназначена для просмотра, добавления и удаления сертификатов ключей и списков отозванных сертификатов из хранилищ. Подробно работа с хранилищами описана ниже в разделе 5.4, стр. 33.

5.2.4. **Установка параметров сообщения**

Флажки под заголовком **Параметры сообщения** задают выполнение соответствующих дополнительных действий при формировании и проверке ЭЦП документа.

Добавлять в сообщение свой сертификат - при формировании ЭЦП в посылаемый электронный документ вместе с ЭЦП будет автоматически добавляться сертификат ключа пользователя.

Добавлять в сообщение список отзыва (CRL) своего УЦ - при формировании ЭЦП в посылаемый электронный документ вместе с ЭЦП будет автоматически добавляться список отзыва сертификатов УЦ.

Автоматически добавлять сертификаты и списки отзыва из сообщения - из полученного подписанного криптографического сообщения автоматически извлекаются сертификаты ключей и списки отзыва и добавляются в хранилища сертификатов и списков отзыва принимающей стороны (если они присутствуют в сообщении).

Выдавать запрос на подтверждение добавления сертификатов и списков отзыва (установка флажка возможна только в том случае, если установлен флажок **Автоматически добавлять сертификаты и списки отзыва из сообщения**) - выдается сообщение о наличии сертификата ключа и списка отзыва в полученном подписанном электронном документе и предлагается добавить их в хранилище сертификатов принимающей стороны. Примеры сообщений приведены ниже на Рис. 5-4.

					НКБГ. 501430.773И6	Лист
						31
Изм	Лист	№ документа	Подпись	Дата		

выполнить, переведя курсор на объект, нажав правую кнопку мыши и выбрав необходимое действие во всплывающем (контекстном) меню.

5.4.1. Хранилище Сертификаты

Хранилище **Сертификаты** содержит личный сертификат ключа пользователя **DiSignCA**, сертификаты всех участников обмена и сертификаты всех доверенных УЦ, включая корневые.

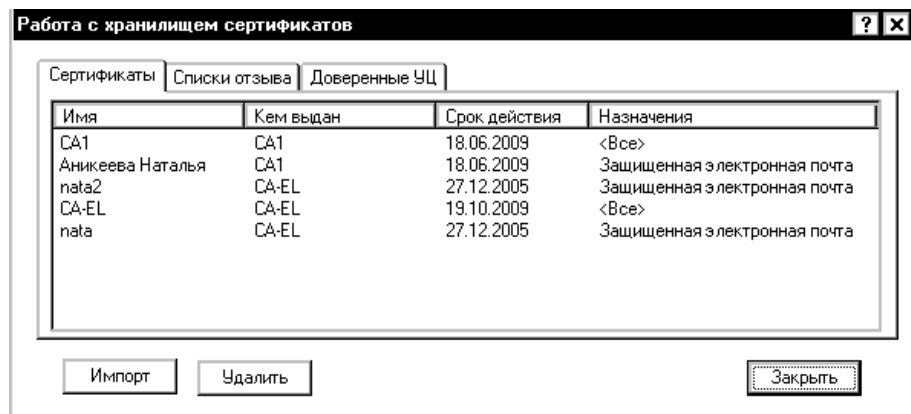


Рис. 5-5

В таблице (Рис. 5-5) каждый сертификат занимает одну строку. В первой графе таблицы выводится имя владельца сертификата, во второй - имя удостоверяющего центра, выдавшего сертификат, в третьей - срок действия сертификата и в четвертой – назначения сертификата.

Пользователь может добавить в хранилище новый сертификат, удалить имеющийся, а также получить более подробную информацию о сертификате.

5.4.1.1. Добавление сертификата в хранилище

Для *добавления* сертификата на экран выводится окно (Рис. 5-6), позволяющее выбрать файл с нужным сертификатом.



Рис. 5-6

Окно содержит список файлов с сертификатами пользователей, в поле **Тип файлов**: автоматически установлено **Сертификат (*.cer)** – имена файлов, содержащих сертификаты пользователей, хранятся, как правило, в файлах с расширением **cer**.

Если требуется добавить сертификат УЦ, то необходимо в списке **Тип файлов** выбрать значение **Хранилище сертификатов (*.p7b)** (имена файлов, содержащих сертификаты Удостоверяющих центров, хранятся, как правило, в файлах с расширением **p7b**), после чего список сертификатов УЦ появится в окне.

Примечание. В файлах с расширением **p7b** могут храниться не только сертификаты доверенных УЦ, но и все сертификаты пользователей, что упрощает добавление их в хранилище.

В списке следует перевести курсор на требуемый файл и нажать кнопку **Открыть** – выбранный сертификат будет добавлен в хранилище **Сертификаты**.

5.4.1.2. Удаление сертификата из хранилища

Для *удаления* сертификата из хранилища нужно выделить его в списке (Рис. 5-5) и нажать кнопку **Удалить**. Сертификат будет удален после подтверждения удаления, выданного пользователем в ответ на дополнительный запрос.

ТЕКУЩИЙ сертификат пользователя удалить нельзя, при попытке удаления программа **DiSignCA** выдает сообщение об ошибке.

5.4.1.3. Просмотр сертификата

Чтобы просмотреть сертификат, следует в списке (Рис. 5-5) перевести на него курсор и дважды щелкнуть левой кнопкой мыши либо в контекстном меню выбрать команду **Просмотреть сертификат**.

На экране появляется окно **Сертификат**, открытое на вкладке **Общие** (Рис. 5-7). На этой вкладке выводится результат анализа информации встроенными средствами WINDOWS. Криптосистема программы **DiSignCA** изолирована от криптографических сервисов WINDOWS и не предназначена для обеспечения совместимости с этими средствами, поэтому результат проверки целостности сертификата отрицательный, его следует проигнорировать. По этой же причине следует проигнорировать сообщение на вкладке **Путь сертификации** (Рис. 5-8).

					НКБГ. 501430.773И6	Лист
						35
Изм	Лист	№ документа	Подпись	Дата		

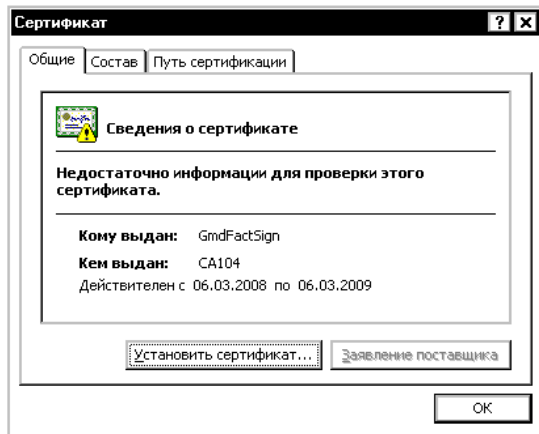


Рис. 5-7

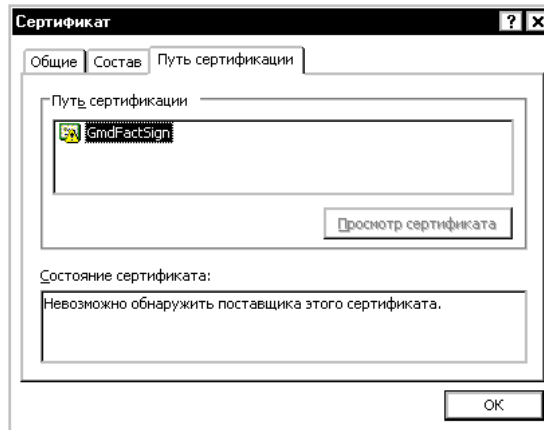


Рис. 5-8

Для просмотра фактической информации о сертификате надо открыть окно **Сертификат** на вкладке **Состав** (Рис. 5-9). На экран будет выведена подробная информация по всем полям структуры сертификата. При выделении одного из полей в нижней секции окна выводится полностью его значение.

При просмотре сертификата предоставляется возможность копирования его в файл в одном из предлагаемых далее в процессе экспорта форматов.

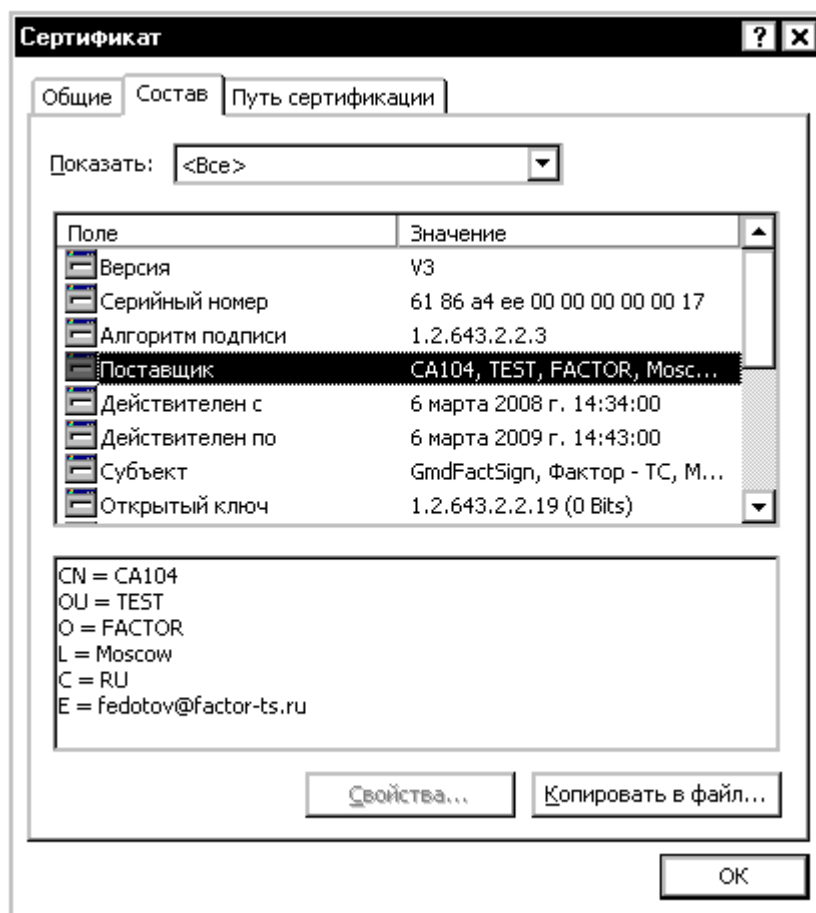


Рис. 5-9

5.4.2. Хранилище Списки отзыва

Хранилище **Списки отзыва** содержит ссылки на списки отозванных сертификатов (СОС) всех УЦ, необходимых для построения *цепочек доверия*.

В таблице (Рис. 5-10) каждый список занимает одну строку. В первой графе таблицы выводится имя удостоверяющего центра, выпустившего СОС, во второй – дата выпуска списка, в третьей - срок действия списка.

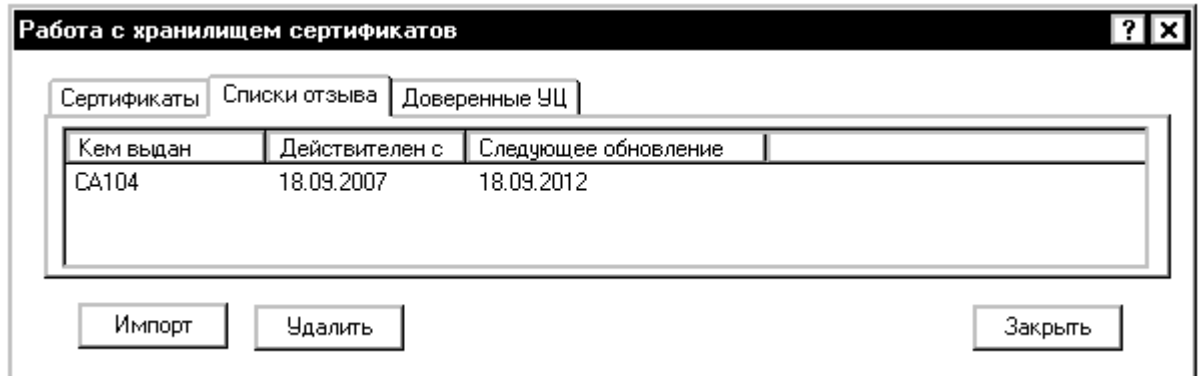
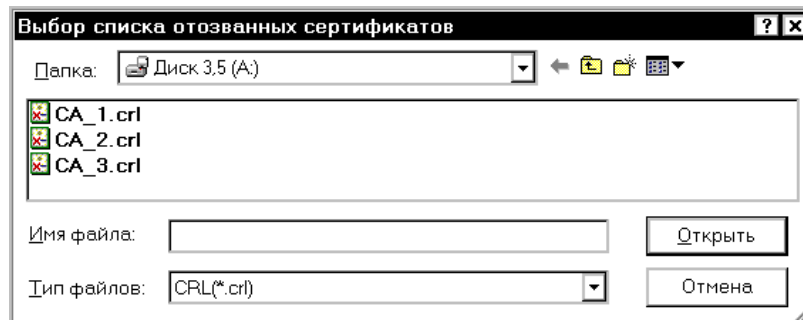


Рис. 5-10

Пользователь может добавить в хранилище новый список и удалить имеющийся, а также получить более подробную информацию о списке.

5.4.2.1. Добавление списка отзыва сертификатов

Для *добавления* списка на экран выводится окно **Выбор списка отозванных сертификатов**:



Окно содержит файлы со списками отзыва (имена файлов, содержащих списки отозванных сертификатов ключей, имеют обязательное расширение **crl**), в поле **Тип файлов**: автоматически установлено **CRL(*.crl)**.

Курсор следует перевести на требуемый файл и нажать кнопку **Открыть** – выбранный список будет добавлен в хранилище **Списки отзыва**.

Пользователь может добавить в хранилище новый сертификат, удалить имеющийся и получить более подробную информацию о сертификате. Эти действия выполняются так же, как и для хранилища **Сертификаты**.

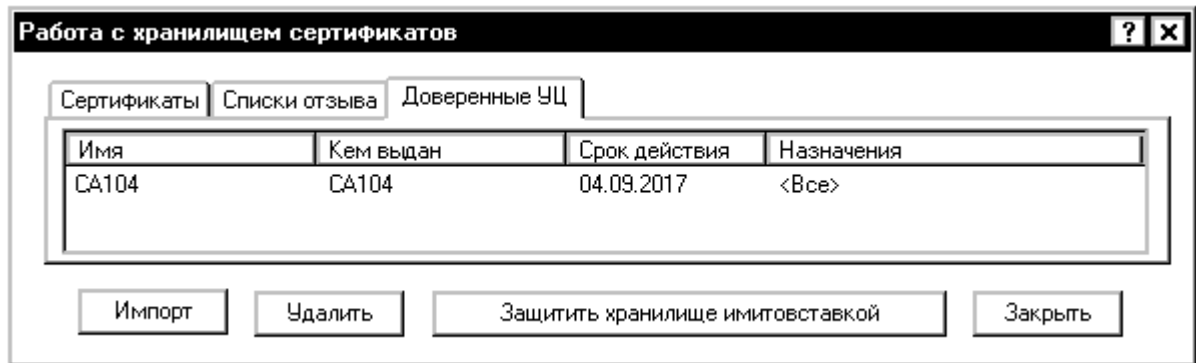


Рис. 5-12

Для хранилища **Доверенные УЦ** пользователь может сформировать имитовставку, нажав на кнопку **Защитить хранилище имитовставкой**. Имитовставка будет сформирована на текущем закрытом ключе пользователя.

Если имитовставка сформирована, то автоматически устанавливается режим защиты хранилища (см. раздел 5.2.2, стр. 30), при котором каждый раз при инициализации криптосистемы будет выполняться проверка имитовставки хранилища **Доверенные УЦ**. Данный режим является обязательным, если хранилище организовано на незащищенном носителе или жестком диске (см. раздел 3.4, стр. 16).

5.5. Рабочие папки

При работе программы **DiSignCA** используются пять рабочих папок, размещенных (по умолчанию) в системной (личной) папке текущего пользователя **Мои документы** (папка **Документы** в ОС WINDOWS Vista).

1. **На подпись** - папка для размещения файлов, подготовленных для формирования ЭЦП. В эту папку рекомендуется помещать файлы, которые необходимо защитить электронной цифровой подписью с помощью программы **DiSignCA**.
2. **Подписанные** – папка, в которую **DiSignCA** автоматически помещает «подписанные» файлы. При этом если ЭЦП помещена в отдельный файл, то основная часть имени этого файла совпадает с полным именем (основная часть и расширение) исходного файла, а расширение имеет значение **p7s**; если ЭЦП упакована вместе с исходным файлом в один файл (в формате PKCS#7), то упакованный файл получает имя, основная часть которого совпадает с полным именем (основная часть и расширение) исходного файла, а расширение имеет значение **p7m**.

3. **Входящие временные** – папка, которая предъявляется по умолчанию для проверки ЭЦП. В эту директорию помещаются полученные файлы: либо пара файлов, исходный и файл с ЭЦП, либо упакованный файл с расширением **p7m**.
4. **Входящие проверенные** - папка для размещения файлов, успешно прошедших проверку ЭЦП:
 - в случае, когда ЭЦП находится в отдельном файле, программа **DiSignCA** автоматически копирует в эту папку файлы документов, прошедших проверку ЭЦП,
 - в случае, когда ЭЦП размещена в одном файле с исходным документом, программа **DiSignCA** автоматически извлекает из него исходный файл и помещает в эту папку.
5. **Извлеченные** – папка, в которую по команде пользователя помещаются исходные файлы, извлеченные из упакованного. При этом ЭЦП не проверяется

Рабочие папки размещаются в директориях, указанных в файле **disign.ini** (о файле **disign.ini** см. раздел 5.7, стр. 40).

5.6. Протоколирование работы программы

При первом вызове программы **DiSignCA** в той же папке, в которой установлено ПО **DiSignCA**, создается протокольный файл (LOG-файл) **DiSignCA.log**, в который заносится информация обо всех действиях, производимых программой.

Ведение протокола выполняется следующим образом. Запись ведется в файл **DiSignCA.log** до тех пор, пока не будет превышен заданный размер файла. После этого файл **DiSignCA.log** переименовывается – получает имя **1o0**. Далее запись ведется снова в файл **DiSignCA.log**. При очередном заполнении LOG-файла имя файла **1o0** меняется на **1o1**, а имя файла **DiSignCA.log** - на **1o0**. И так до 10 раз, последнее имя - **1o9**, после чего начинается циклическое заполнение файлов и записанная ранее информация теряется. Если она нужна, то рекомендуется периодически сохранять содержимое файлов под другими именами.

Размещение и размер LOG-файла задаются в файле **disign.ini** (о файле **disign.ini** см. раздел 5.7).

5.7. Файл инициализации

Файл инициализации **disign.ini** содержит индивидуальные настройки пользователя и создается при первом запуске программы **DiSignCA** в системной (личной) папке текущего пользователя ОС WINDOWS (например, в WINDOWS XP эта директория имеет вид: **<Системный диск>\Documents and Settings**

						НКБГ. 501430.773И6	Лист
							40
Изм.	Лист	№ документа	Подпись	Дата			

Data\DiSignCA). При таком размещении обеспечивается независимость настроек программы для различных пользователей и защита от несанкционированного или случайного их изменения.

В файле устанавливается соответствие между рабочими папками и директориями файловой системы компьютера пользователя **DiSignCA**, а также задаются параметры протоколирования работы **DiSignCA**. Пользователь может менять местоположение и имена директорий. Для их изменения служат параметры в секции [DIRECTORY] конфигурационного файла **disign.ini**.

Фрагмент файла **disign.ini**, задающий размещение рабочих папок приведен ниже:

```
[DIRECTORY]
CheckSourceDir= Входящие временные
CheckOutputDir= Входящие проверенные
SignSourceDir= На подпись
SignOutputDir= Подписанные
ExtractP7MDir= Извлеченные
```

При таком значении параметров все папки пользователя устанавливаются в директорию: **<Системный диск>\Documents and Settings\<имя_пользователя>\Мои документы**. Например, местоположение подписанных писем пользователя **User**:

<Системный диск>\Documents and Settings\<User>\Мои документы\Подписанные.

В файле **disign.ini**, можно указать явно полный путь доступа к рабочим папкам, тогда папки будут размещены там, где указано. В этом случае необходимо убедиться, что у пользователя есть к ним доступ на запись.

Размещение и размер файла протокола (LOG-файла), который ведется во время работы программы **DiSignCA**, устанавливаются в секции [LOG] файла **disign.ini** значениями параметров **LogFile** и **LogLength**, соответственно, при этом указывается полный путь к файлу протокола, а размер указывается в байтах.

```
[LOG]
LogFile=
LogLength=1024000
```

					НКБГ. 501430.773И6	Лист
						41
Изм	Лист	№ документа	Подпись	Дата		

По умолчанию имя файла протокола не указано, и он находится в той же системной директории пользователя ОС WINDOWS, что и файл **disign.ini**.

При изменении содержимого файла **disign.ini** для вступления в действие новой конфигурации необходимо перезапустить **DiSignCA**.

При деинсталляции ПО **DiSignCA** файлы инициализации не удаляются, поэтому после повторной установки ПО **DiSignCA** пользователи могут работать с прежними настройками.

Для полного удаления ПО **DiSignCA** с компьютера следует после деинсталляции вручную удалить директории ПО **DiSignCA** в личной директории всех пользователей, работавших ранее с ПО **DiSignCA**.

					НКБГ. 501430.773И6	Лист
						42
Изм.	Лист	№ документа	Подпись	Дата		

6. Работа с программой

После того как будет выполнена настройка и инициализация криптосистемы, Абонентский пункт ЭЦП готов к выполнению своих основных функций – формированию и проверке ЭЦП.

В главном окне **DiSignCA** (Рис. 6-1) становятся доступными кнопки группы под заголовком **ЭЦП** и все кнопки группы под заголовком **Дополнительно**, кроме кнопки **Инициализировать криптосистему**. В верхнем поле окна выводится имя файла, который был подписан, проверен или извлечен последним. В окне также приведена информация о версии и разработчике программы.

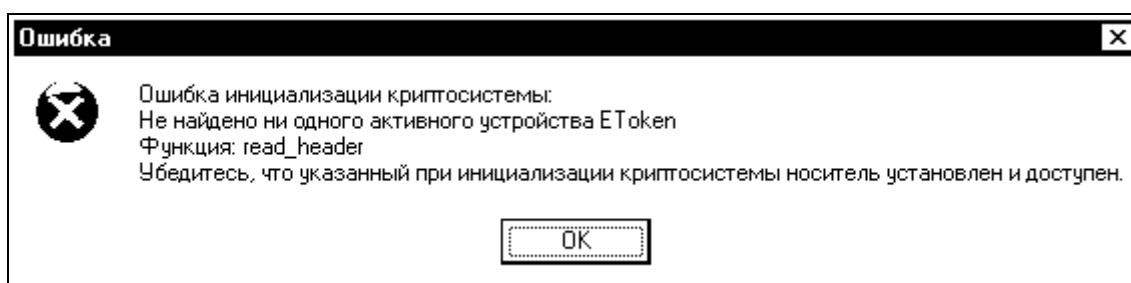


Рис. 6-1

6.1. Запуск программы

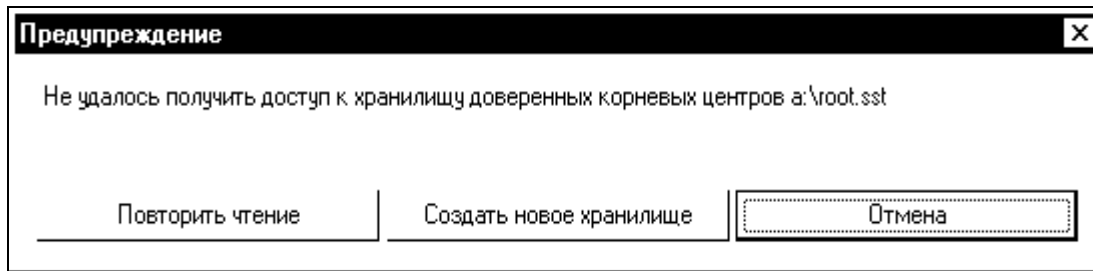
При повторном запуске программы выполняется инициализация криптосистемы в соответствии с настройками, выполненными в предыдущем сеансе работы, при этом выполняется считывание ключевой информации и проверка сертификата ключа пользователя посредством построения цепочки доверия УЦ.

При невозможности считывания ключевой информации будет выведено сообщение (в качестве примера приведено сообщение для ключевого носителя типа eToken):

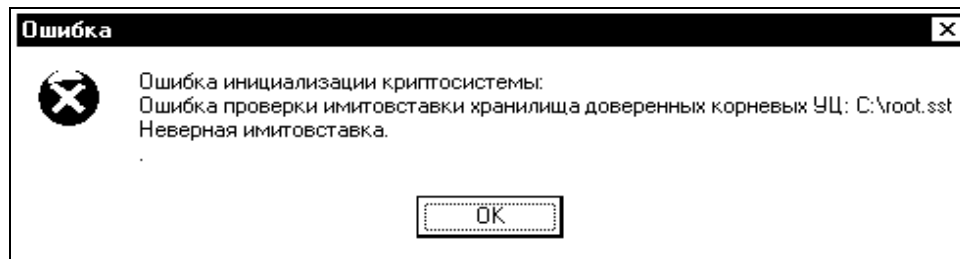


При отсутствии доступа к хранилищу корневых сертификатов (файл **root.sst**) будет выдано сообщение:

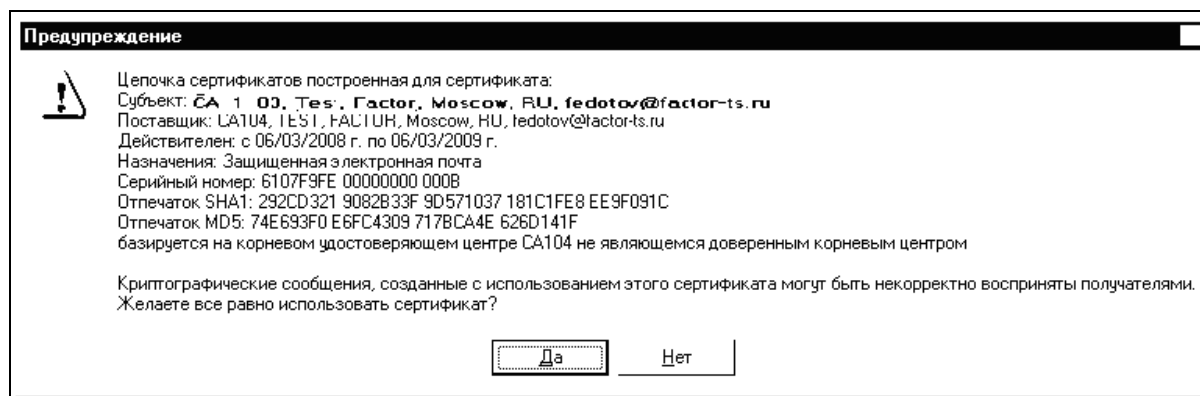
					НКБГ. 501430.773И6	Лист
Изм	Лист	№ документа	Подпись	Дата		43



Если была нарушена целостность хранилища корневых сертификатов, например, удален какой-либо сертификат из защищенного хранилища, но не был выполнен перерасчет имитовставки, то выдается сообщение:



Если файл найден, но он не соответствует существующим установкам, то выдается сообщение:



Программа будет запущена, при этом будет активизирована кнопка **Инициализировать криптосистему**. Следует установить необходимые носители и выполнить инициализацию криптосистемы либо выполнить настройку с другими носителями.

6.2. Формирование ЭЦП

Перед тем как приступить к формированию ЭЦП для одного или нескольких файлов, необходимо выбрать способ размещения результатов формирования ЭЦП файла. Этот выбор выполняется установкой флажка **Подпись отдельно** в главном окне **DiSignCA** (Рис. 6-1):

- если флажок не установлен, то исходный файл и файл с ЭЦП будут упакованы в один файл (расширение файла **p7m**);

- если флажок установлен, то исходный файл останется без изменений и будет создан файл с ЭЦП (расширение файла **p7s**).

После выбора способа размещения результатов следует нажать кнопку **Подписать**. На экран будет выведено стандартное окно WINDOWS, позволяющее указать файл (файлы), для которого требуется сформировать ЭЦП. Выбор файлов начинается с папки **На подпись**. Одновременно можно выбрать несколько файлов стандартным для ОС WINDOWS способом: щелкать мышью по именам файлов, удерживая клавишу **Shift** или **Ctrl**. Для файлов с ЭЦП (расширение файла **p7m**) можно повторно выполнить формирование ЭЦП. Можно также повторно подписать уже подписанный файл, при этом файл с ЭЦП (расширение файла **p7s**) должен находиться в той же директории, что и подписываемый файл.

После того как файлы будут выбраны, программа **DiSignCA** начнет формирование ЭЦП.

При формировании ЭЦП уже подписанного электронного документа выполняется проверка существующих ЭЦП. При положительном результате проверки выдается сообщение об этом и предлагается добавить новую ЭЦП. После подтверждения пользователем добавления операция формирования подписи продолжается. При отрицательном результате проверки операция формирования подписи прерывается и выдается сообщение об обнаруженной ошибке.

При формировании ЭЦП для уже подписанного электронного документа может быть предложено добавление в локальное хранилище обнаруженных в документе сертификатов и списков отзыва, если они были включены в документ ранее при формировании предыдущих ЭЦП.

Если формирование подписи прошло успешно, то в зависимости от заданного способа размещения файлов будут выполнены следующие действия.

- *Флажок **Подпись отдельно** установлен.*

Программа **DiSignCA** вычислит ЭЦП для каждого из выбранных файлов и разместит исходный файл и результат формирования ЭЦП в папке **Подписанные**

Имя файла, содержащего ЭЦП, имеет основную часть, совпадающую с полным именем (основная часть и расширение) исходного файла, и расширение **p7s**.

- *Флажок **Подпись отдельно** не установлен.*

					НКБГ. 501430.773И6	Лист
						45
Изм	Лист	№ документа	Подпись	Дата		

будет скопирован в папку **Входящие проверенные**. Оба файла (исходный и файл с ЭЦП) останутся на том месте, где они находились при вызове на проверку.

После успешной проверки на экран будет выведено окно **Результат проверки ЭЦП**, представленное на Рис. 6-2. Окно содержит информацию о проверенном файле и о сертификатах участников обмена, подписавших файл.

```
Результат проверки ЭЦП
+++
Результат проверки ЭЦП файла:
С:\Подписанные\Файл_1.DOC
Всего подписей: 1
Файл подписан сертификатом:
Субъект: fact1_2001, Тест, Factor, Moscow, RU, fact1_2001@factor-ts.ru
Поставщик: CA_1_03, Test, Factor, Moscow, RU, fedotov@factor-ts.ru
Действителен: с 11/07/2006 г. по 02/08/2010 г.
Назначения: Защищенная электронная почта
Серийный номер: 61295C1D 00000000 005E
Отпечаток SHA1: B280C766 A0DE17E7 3408C860 7C5DBA66 033DC51A
Отпечаток MD5: 1411ADFD CB1FAD73 594BE9CD A582CC47
Время генерации ЭЦП: 19/07/2006 - 15:27:45 (GMT)
Подпись верна

Файл сообщения успешно скопирован в: с:\Входящие проверенные\Файл_1.DOC
```

Рис. 6-2

В случае отрицательного результата операции будет выдано сообщение об ошибке. Программа **DiSignCA** не сможет выполнить проверку ЭЦП, например, в следующих случаях:

- в хранилище **Сертификаты** отсутствует сертификат пользователя (сертификаты пользователей), подписавшего исходный файл;
- в хранилище **Сертификаты** отсутствует сертификат хотя бы одного УЦ, необходимого для построения *цепочки доверия*;
- в хранилище **Доверенные УЦ** отсутствует сертификат корневого УЦ;
- в хранилище **Списки отзыва** отсутствует список отзыва сертификатов хотя бы одного УЦ, необходимого для построения *цепочки доверия*.

6.4. Извлечение исходного файла

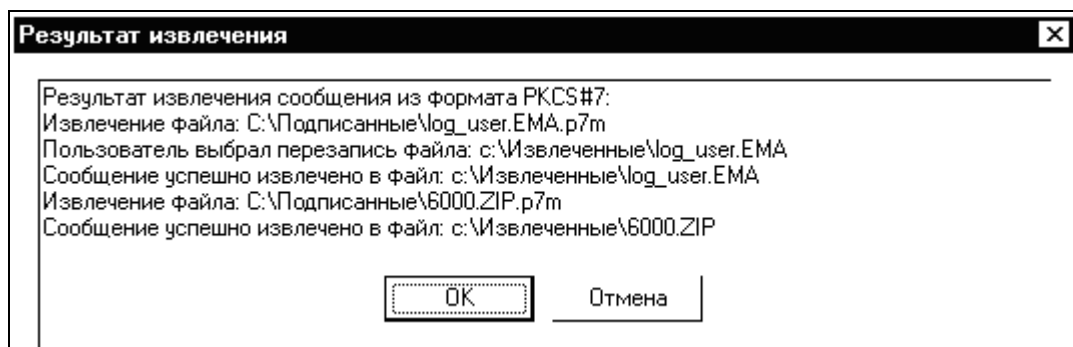
Если на проверку поступает файл, содержащий исходный файл и файл с ЭЦП, а проверку ЭЦП по тем или иным причинам выполнить не удастся или оказывается, что ЭЦП не верна, то исходный файл не извлекается из файла, поступившего на проверку (в формате PKCS#7), т.е. исходный файл не попадает в папку документов, прошедших проверку (в папку **Входящие проверенные**).

					НКБГ. 501430.773И6	Лист
						47
Изм	Лист	№ документа	Подпись	Дата		

Если пользователю необходимо ознакомиться с содержимым исходного файла, то **DiSignCA** позволяет его извлечь (без проверки ЭЦП). Для этого служит кнопка **Извлечь сообщение из PKCS#7** в главном окне **DiSignCA** (Рис. 6-1).

После нажатия кнопки на экран будет выведен стандартный файловый диалог WINDOWS, позволяющий выбрать тот файл (файлы), из которого требуется извлечь исходный файл. Выбор файла (файлов) начнется с папки **Входящие временные**. Выбирать файл для извлечения из него исходного файла можно из любой директории.

DiSignCA извлечет из выбранного файла (файлов) исходный файл (файлы) и выдаст окно с результатами извлечения файла (файлов):



При успешном извлечении исходный файл (файлы) будет помещен в папку **Извлеченные**.

7. Работа с макросами в Microsoft Word

В состав **DiSignCA** входит макрос для Microsoft Word, позволяющий пользователям, работающим с документами в программе Microsoft Word, пользоваться функциями программы **DiSignCA**, не выходя из Microsoft Word.

Замечание. Особенности работы с макросами в Microsoft Word 2007 рассмотрены в **Приложении 1** к настоящему документу.

Если при инсталляции **DiSignCA** в Microsoft Word был добавлен макрос ЭЦП – **disign.dot**, то среди панелей инструментов (надстроек) программы Microsoft Word появится дополнительная панель инструментов с двумя кнопками **Подписать документ** и **Проверить ЭЦП**:




Рис. 7-1

При использовании макроса возможен только один способ размещения подписанного файла и ЭЦП - в разных файлах.

Перед использованием макроса, необходимо настроить программу **DiSignCA** штатными средствами.

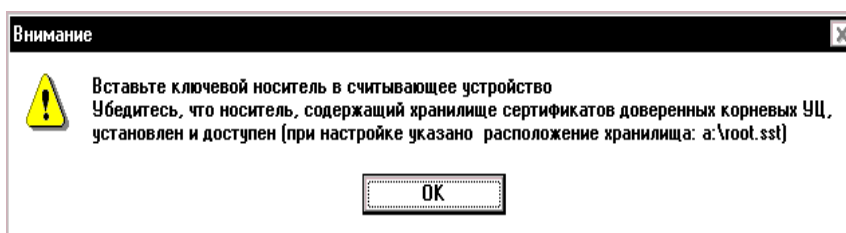
Примечание. Формирование ЭЦП выполняется только в том случае, если пользователь имеет права записи для данного документа (файл не открыт в режиме READ ONLY, и у пользователя имеются соответствующие права записи в директорию размещения файла документа).

7.1. Формирование ЭЦП при помощи макроса

Левая кнопка на панели **Подписать документ**  (Рис. 7-1) позволяет сформировать ЭЦП для документа в текущем окне Microsoft Word.

Напомним. Генерация ЭЦП невозможна для файлов, находящихся в папке подписанных документов (**Подписанные**).

В текущее окно Microsoft Word пользователь должен загрузить документ, для которого требуется сформировать ЭЦП, и на панели инструментов нажать кнопку **Подписать документ**. Будет выдано сообщение:



					НКБГ. 501430.773И6	Лист
Изм	Лист	№ документа	Подпись	Дата		49

8. Входные и выходные данные

В данном разделе приведена информация о составе, формате и размещении входных данных, используемых программой при ее настройке и функционировании, а также о составе, формате и размещении выходных данных, получаемых в результате выполнения ее функций.

8.1. Входные данные

Входными данными для программы **DiSignCA** являются:

1. Файлы, подлежащие обработке, то есть предназначенные для формирования ЭЦП или для проверки ЭЦП.
2. Закрытый ключ ЭЦП и необходимая для его использования информация, записанные на ключевой носитель.
3. Сертификаты ключей пользователя **DiSignCA** и других участников информационного обмена, записанные либо на ключевой носитель, либо на отдельный носитель информации.
4. Сертификаты и списки отозванных сертификатов всех доверенных УЦ.

8.1.1. Исходные файлы

Формирование ЭЦП выполняется для файлов, удовлетворяющих следующим условиям.

1. Файлы размещены в любой локальной или сетевой папке файловой системы WINDOWS компьютера пользователя **DiSignCA**, кроме папки **Подписанные**.
2. Файлы имеют любое, разрешенное в ОС WINDOWS имя и расширение (кроме расширения **p7m**).

Проверка ЭЦП выполняется для файлов, удовлетворяющих следующим условиям.

1. Файлы размещены в любой локальной или сетевой папке файловой системы WINDOWS компьютера пользователя **DiSignCA**, кроме папки **Подписанные**.
2. Исходный файл и файл с ЭЦП помещены в один файл, имя которого имеет расширение **p7m**; или исходный файл и файл с ЭЦП размещены в двух файлах: имя исходного файла может иметь любое расширение, кроме **p7s** и **p7m**; имя файла с ЭЦП имеет расширение **p7s**.

					НКБГ. 501430.773И6	Лист
						51
Изм	Лист	№ документа	Подпись	Дата		

8.1.2. **Формат информации на ключевом носителе**

Закрытый ключ ЭЦП и необходимая для его использования информация размещаются на ключевом носителе в двух файлах, заключенных в «контейнер».

Имена файлов в «контейнере»:

<идентификатор_ключа>.pvt – закрытый ключ ЭЦП;

<идентификатор_ключа>.hdr – дополнительная информация.

Основную часть имени файлов (<идентификатор_ключа>) задает программа **Модуль Генерации ключей**, указанные расширения имен являются обязательными.

8.1.3. **Открытые ключи и сертификаты ключей**

Сертификат ключа имеет следующую структуру: открытый ключ, электронная цифровая подпись удостоверяющего центра, выдавшего этот сертификат, и сопроводительная информация.

1. Сертификаты пользователей, как правило, находятся в файлах, имена которых имеют расширение **cer** или **p7b**. Файл с расширением **cer** может содержать только один сертификат.
2. Сертификаты удостоверяющих центров, как правило, находятся в файлах, имена которых имеют расширение **p7b** или **cer**. Файлы могут содержать как один, так и несколько сертификатов.

8.1.4. **Сертификаты и списки отозванных сертификатов доверенных УЦ**

1. Сертификаты удостоверяющих центров, как правило, находятся в файлах, имена которых имеют расширение **p7b**. Файл с расширением **p7b** может содержать как один, так и несколько сертификатов, а также списки отозванных сертификатов.
2. Имена файлов, содержащих списки отозванных сертификатов УЦ, имеют расширение **cr1** или **p7b**.

Эти файлы могут быть размещены на ключевом носителе или на отдельном носителе, а также могут быть получены вместе с подписанным электронным документом.

Сертификаты удостоверяющих центров и списки отозванных сертификатов должны своевременно обновляться и переноситься в соответствующие хранилища (Хранилище **Доверенные УЦ** и Хранилище **Списки отзыва**, соответственно).

					НКБГ. 501430.773И6	Лист
						52
Изм.	Лист	№ документа	Подпись	Дата		

8.2. Выходные данные

Выходными данными программы являются файлы, обработанные программой **DiSignCA**, то есть файл со сформированной ЭЦП для выбранного файла или обработанный файл, для которого проверена ЭЦП.

В результате формирования ЭЦП для выбранного пользователем файла при не установленном флажке **Подпись отдельно**, исходный файл и файл с ЭЦП будут упакованы в один файл с именем, совпадающим с именем исходного файла, и расширением файла **p7m**; если флажок установлен, то исходный файл останется без изменений и будет создан файл с ЭЦП с именем, совпадающим с именем исходного файла, и расширением файла **p7s**.

Выходные файлы помещаются в директории (рабочие папки), размещение которых в файловой системе компьютера определяется соответствующими параметрами в файле инициализации **design.ini** (см. раздел 5.7, стр. 40).

					НКБГ. 501430.773И6	Лист
						53
Изм	Лист	№ документа	Подпись	Дата		

Для этого надо выполнить следующее.

- вызвать команду **Макросы** (по умолчанию она вызывается нажатием клавиш <Alt+F8>),
- в появившемся окне **Макрос** в списке **Макросы из**: выбрать **Активные шаблоны**,
- в списке **Имя**: выбрать **DiSignCA**,
- нажать кнопку **Выполнить**.

В результате на ленте должна появиться вкладка **Надстройки**, которая будет содержать две кнопки макроса **DiSignCA: Подписать документ** и **Проверить ЭЦП**:

Эти же действия надо выполнить и при последующих запусках **DiSignCA**, если вкладка **Надстройки** отсутствует на ленте.

Замечание. Умалчиваемое значение клавиш вызова команды **Макросы** может быть изменено. Посмотреть новое значение можно на вкладке **Разработчик** (вкладка **Разработчик**, команда **ToolsMacro** в окне **Настройка клавиатуры**).

Работа с макросами в Microsoft Word 2007

При каждом запуске приложения Microsoft Word 2007 надо давать разрешение на запуск макроса так, как это описано выше.

Для работы с макросом надо на ленте выбрать вкладку **Надстройки**, на которой располагаются кнопки вызова макроса. Формирование ЭЦП при помощи макроса и проверка ЭЦП при помощи макроса выполняются так же, как описано в разделах 7.1, стр. 49 и 7.2, стр. 50.

					НКБГ. 501430.773И6	Лист
						55
Изм	Лист	№ документа	Подпись	Дата		

Приложение 2. Список терминов

Термин	Определение
Владелец сертификата ключа	Физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа и которое владеет соответствующим закрытым ключом.
Закрытый ключ	Уникальная последовательность символов, известная только его владельцу, используемая при шифровании информации и/или для создания электронной цифровой подписи (ЭЦП) в электронных документах.
Имитовставка	Последовательность данных, позволяющая установить отсутствие искажения в передаваемой или хранимой информации, полученная в результате преобразования исходной информации в соответствии с алгоритмом имитозащиты.
Имитозащита	Защита информации с целью подтверждения ее целостности в соответствии с алгоритмом имитозащиты.
Ключевая пара (несимметричная ключевая пара)	Пара, состоящая из закрытого ключа и соответствующего ему открытого ключа.
Ключевой носитель	Сменный носитель информации (дискета, flash-память и т.п.), содержащий ключевую информацию.
Криптографическая система (криптосистема)	Набор функций (модулей), реализующих криптографические преобразования (алгоритмы).
Открытый ключ	Уникальная последовательность символов: однозначно соответствующая закрытому ключу, доступная любому пользователю - участнику информационного обмена и предназначенная для подтверждения подлинности электронной цифровой подписи (ЭЦП) в электронных документах и/или для шифрования информации.
Сертификат ключа	Документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, который включает в себя открытый ключ и данные, идентифицирующие владельца сертификата ключа.
Удостоверяющий Центр (УЦ)	Организационный элемент информационной системы, выполняющий следующие функции: <ul style="list-style-type: none"> - изготовление сертификатов ключей; - создание ключей (ключевой пары); - приостановление и возобновление действия сертификатов ключей, а также аннулирование их; - ведение реестра сертификатов ключей; - проверку уникальности открытых ключей в реестре сертификатов ключей и архиве удостоверяющего центра;

Изм.	Лист	№ документа	Подпись	Дата
------	------	-------------	---------	------

	<ul style="list-style-type: none"> - выдачу сертификатов ключей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии; - по обращению владельцев сертификатов ключей подтверждение подлинности ЭЦП в электронном документе в отношении выданных им сертификатов ключей; - уведомление владельца сертификата ключа о фактах, которые стали известны удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа; - предоставляет участникам информационных систем иные услуги, связанные с использованием сертификатов ключей.
Электронная цифровая подпись (ЭЦП)	<p>Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате преобразования информации в соответствии с алгоритмом электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа, а также установить отсутствие искажения информации в электронном документе (предназначенный для подтверждения целостности электронного документа и подлинности его авторства).</p>

