SberSign 6.1

11485466.72.21.12.110 И3 02

Руководство пользователя

Содержание

Введение

Настоящий документ содержит руководство пользователя по работе с программным изделием SberSign 6.1. Руководство включает в себя справочную информацию по работе программного изделия SberSign 6.1.

1 Назначение и условия применения

1.1 Назначение системы

Программный продукт SberSign 6.1 предназначен для генерации и проверки электронной подписи (ЭП) файлов на базе алгоритмов, соответствующих стандартам ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012.

Программный продукт SberSign 6.1 разработан в двух исполнениях: SberSign 6.1 вариант исполнения 1 использует в качестве СКЗИ модуль криптографических библиотек «Бикрипт 5.0» вариант исполнения 1 модификация 2 (вариант исполнения 9 модификация 2)* и/или «Криптотокен ЭП», SberSign 6.1 вариант исполнения 2 использует в качестве СКЗИ модуль криптографических библиотек «Бикрипт 5.0» вариант исполнения 2 модификация 2 (вариант исполнения 10 модификация 2)* и/или «Криптотокен ЭП».

*Примечание: * программные модули и список функций СКЗИ «Бикрипт 5.0» в варианте исполнения 1 модификация 2 и варианте исполнения 9 модификация 2 идентичны, программные модули и список функций СКЗИ «Бикрипт 5.0» в варианте исполнения 2 модификация 2 и варианте исполнения 10 модификация 2 идентичны.*

В программном продукте SberSign 6.1 реализованы следующие основные функции:

- Генерация закрытого и открытого ключа ЭП в соответствии с алгоритмами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012. Создание запроса на выпуск сертификата.
- Формирование файла в формате rtf, содержащего открытый ключ и реквизиты пользователя.
- Поддержка однокомпонентного и двухкомпонентного ключей ЭП.
- Хранение основного и резервного закрытого ключа ЭП на ТМ-идентификаторе, устройстве VPN-Key, устройстве «JaCarta ГОСТ» («eToken ГОСТ») производства ЗАО «Алладин Р.Д.», а также флеш-

накопителе. Ключи на устройстве «JaCarta ГОСТ» являются неизвлекаемыми.

- Формирование и проверка ЭП файлов в соответствии со стандартами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.
- Формирование ЭП файла с добавлением сертификата открытого ключа ЭП.
- Проверка ЭП файла с использованием справочника открытых ключей ЭП или сертификатов открытых ключей ЭП.
- Контроль целостности справочника (сертификатов) открытых ключей ЭП и справочника открытых ключей администраторов.
- Проверка ЭП файла с использованием списка отозванных сертификатов.
- Работа в файлах сценариев автоматического выполнения команд (BAT, CMD).
- Ведение системного журнала.

1.2 Условия применения системы

SberSign 6.1 устанавливается на компьютер, удовлетворяющий следующим программным и аппаратным требованиям:

- Программный продукт SberSign 6.1 должен работать под управлением следующих 32-х и 64-х битных операционных систем: Windows 10, Windows 8.1, Windows 7, Windows 2000, Windows XP, Windows 2003 Server, Windows Vista, Windows 2008 Server.
- Процессор не ниже Intel Pentium IV.
- Жёсткий диск ёмкостью не менее 1 Гб.
- ОЗУ ёмкостью не менее 1 Гб.
- Считыватель электронных идентификаторов на USB порте и драйвер TMDRV.SYS для поддержки возможности хранения закрытого ключа на устройстве Touch Memory (TM).

2 Установка SberSign 6.1

Для того чтобы установить SberSign 6.1, необходимо запустить самораспаковывающийся архив SberSign_6.1_Setup.exe и в открывшемся окне (см. Рисунок 1) при необходимости выбрать путь установки, нажав кнопку **Сменить директорию**, и нажать кнопку **Установить.**

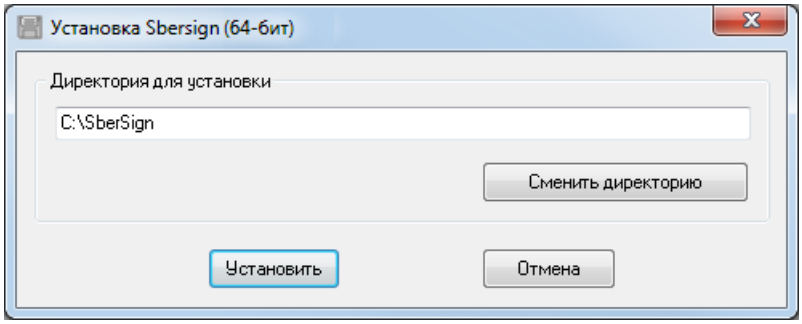

Рисунок 1 – Путь установки SberSign 6.1

После появления сообщения о завершении установки SberSign 6.1 (см. Рисунок 2) следует нажать кнопку **ОК**.

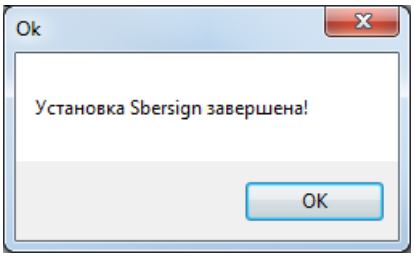

Рисунок 2 – Сообщение о завершении установки SberSign 6.1

3 Удаление SberSign 6.1

Для того чтобы удалить SberSign 6.1, следует в меню Windows **Все программы** открыть папку Sbersign и выбрать пункт **Деинсталляция** (см. Рисунок 5).

В открывшемся окне (см. Рисунок 3) программы удаления SberSign 6.1 следует нажать кнопку **Далее>>**. Для отмены удаления SberSign 6.1 следует нажать кнопку **Отмена**.

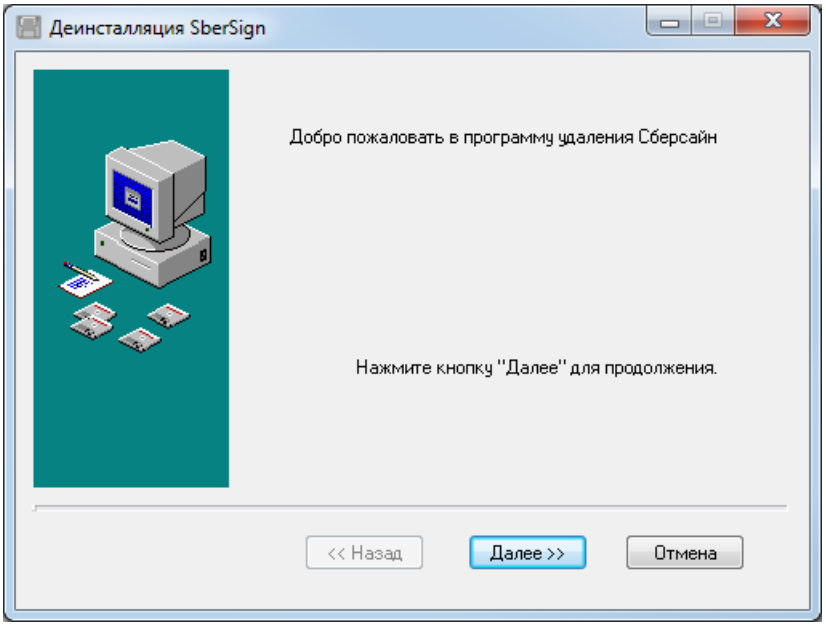

Рисунок 3 – Окно программы удаления SberSign 6.1

После появления сообщения о деинсталляции SberSign 6.1 (см. Рисунок 4) следует нажать кнопку **Готово**.

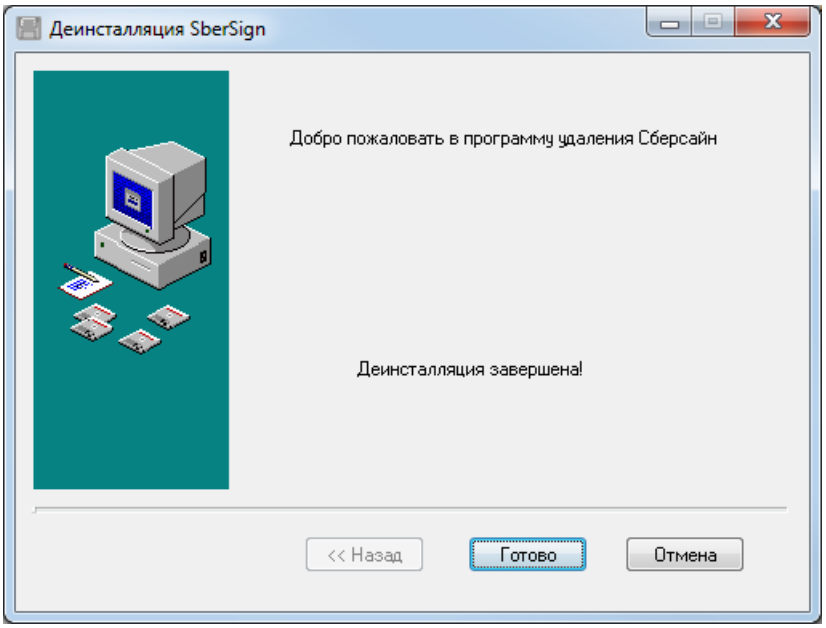

Рисунок 4 – Сообщение о деинсталляции SberSign 6.1

4 Описание операций

4.1 Начало работы с программным продуктом SberSign 6.1

Для начала работы с программным продуктом SberSign 6.1 следует в меню Windows **Все программы** открыть папку «Sbersign» (см. Рисунок 5) и выбрать нужный компонент программного продукта SberSign 6.1.

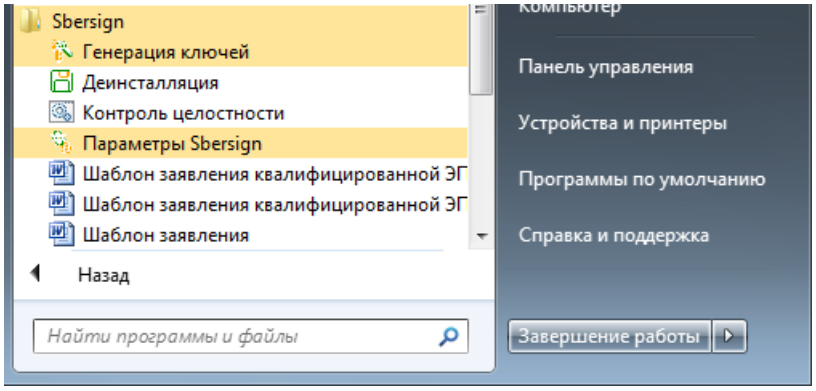

Рисунок 5 – Меню выбора компонентов программного изделия SberSign 6.1

Для работы с программным продуктом SberSign 6.1 необходимо произвести проверку SberSign 6.1 (см. раздел 4.2), настроить параметры SberSign 6.1 (см. раздел 4.3) и создать ключи электронной подписи (см. раздел 4.6).

4.2 Проверка целостности SberSign 6.1

Проверка целостности SberSign 6.1 производится автоматически после загрузки операционной системы.

Для того чтобы произвести дополнительную проверку целостности программного продукта SberSign 6.1, необходимо в меню выбора компонентов выбрать пункт **Контроль целостности** (см. Рисунок 5).

Если в процессе проверки обнаружена ошибка, появится соответствующее сообщение (см. Рисунок 6).

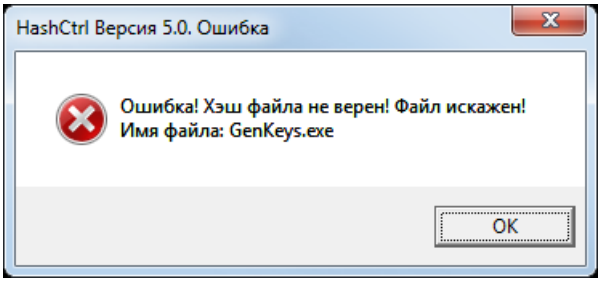

Рисунок 6 – Сообщение об ошибке проверки целостности SberSign 6.1

Внимание! Если обнаружена ошибка проверки целостности, SberSign 6.1 эксплуатировать нельзя. Необходимо заново установить программный продукт SberSign 6.1 (см. раздел 2) и повторно произвести проверку целостности.

4.3 Настройка параметров SberSign 6.1

Для того чтобы изменить значения параметров работы SberSign 6.1, необходимо в меню выбора компонентов (см. Рисунок 5) выбрать пункт **Параметры Sbersign**.

В результате будет отображено окно настройки параметров SberSign 6.1. Для варианта исполнения 1 это окно имеет следующий вид (см. Рисунок 7).

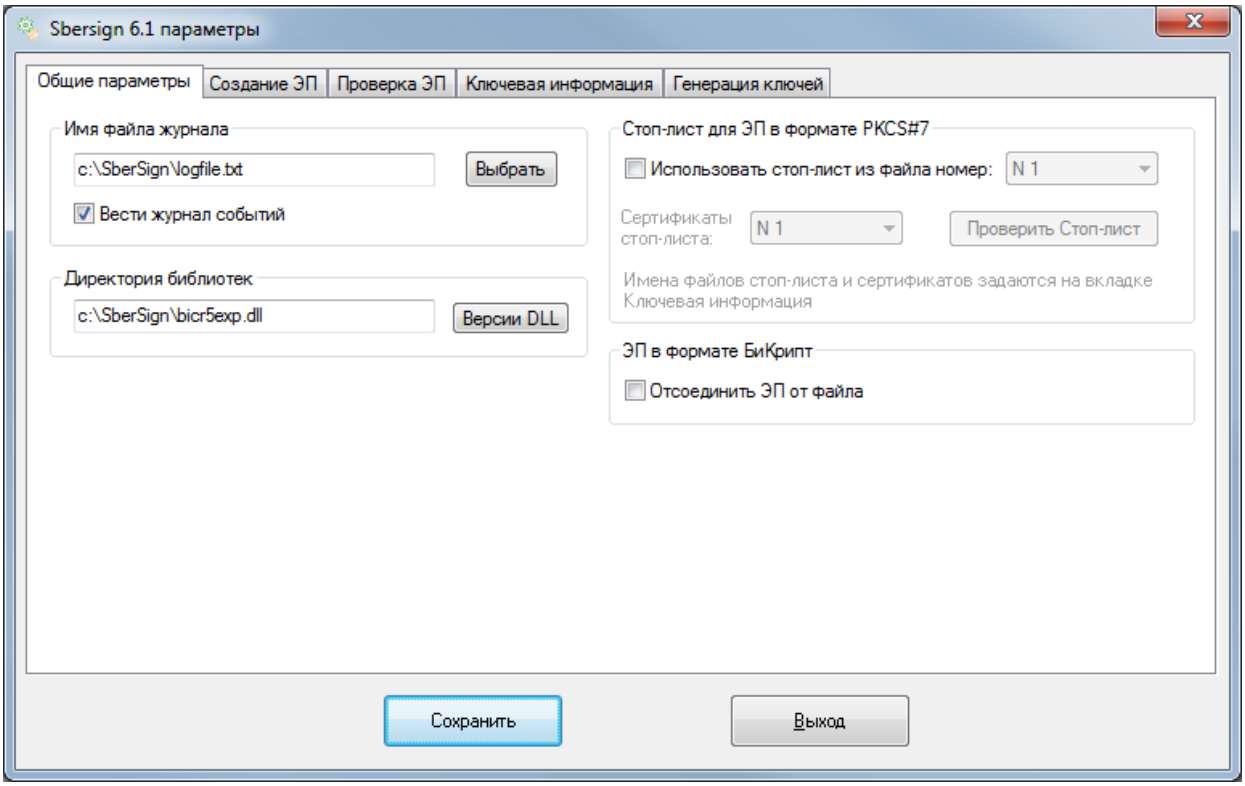

Рисунок 7 – Окно настройки параметров SberSign 6.1 (вариант исполнения 1)

Для варианта исполнения 2 окно настройки параметров SberSign 6.1 имеет следующий вид (см. Рисунок 8).

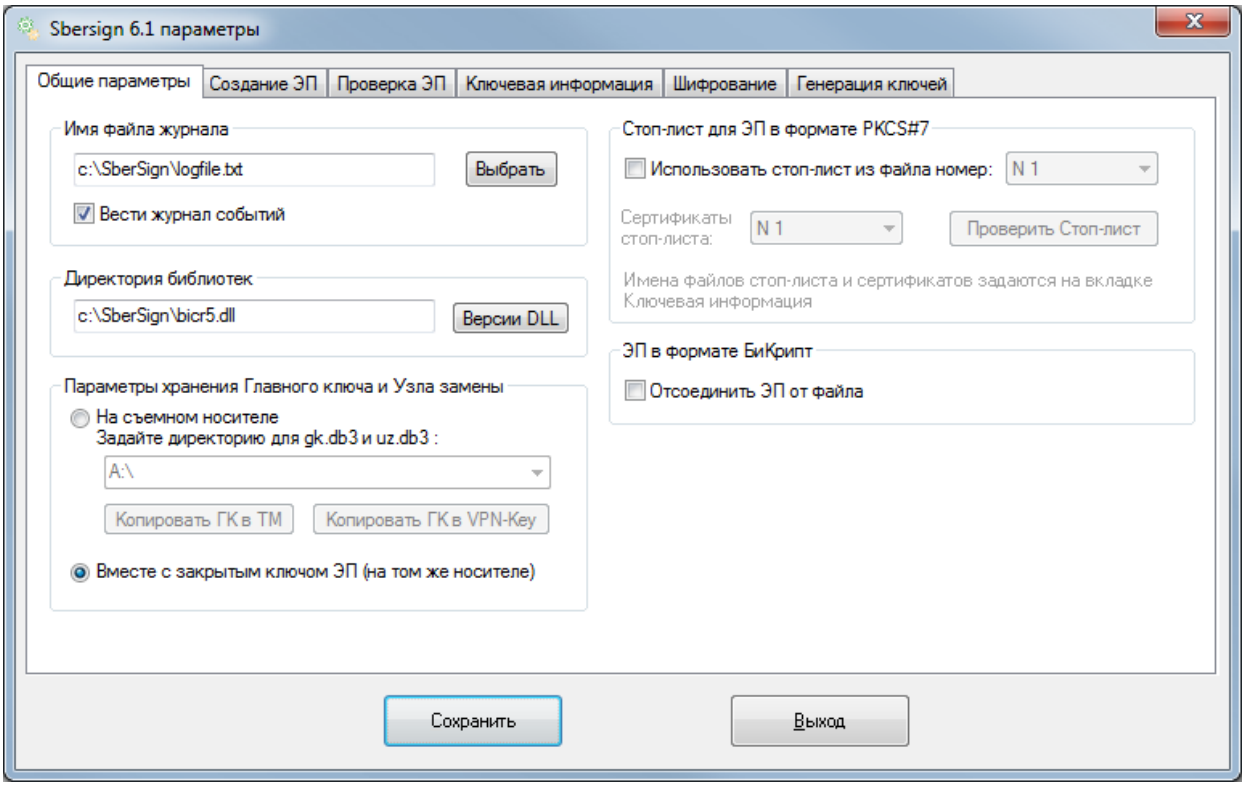

Рисунок 8 – Окно настройки параметров SberSign 6.1 (вариант исполнения 2)

Для того чтобы сохранить произведённые изменения параметров работы SberSign 6.1, необходимо нажать кнопку **Сохранить**.

Для продолжения работы в открывшемся окне с сообщением о сохранении значений параметров в реестре Windows следует нажать кнопку **ОК**.

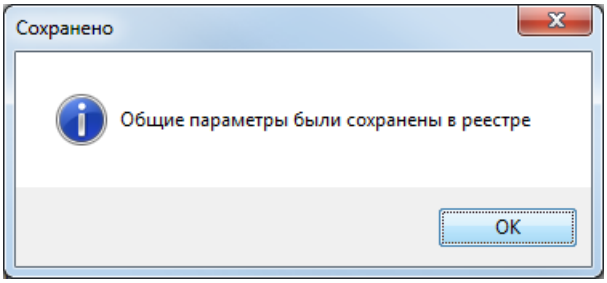

Рисунок 9 – Сообщение о сохранении значений параметров

4.3.1 Ведение журнала

В процессе работы SberSign 6.1 может фиксировать в текстовом журнале события, связанные с формированием и проверкой ЭП.

Для того чтобы включить режим ведения журнала, необходимо в окне настройки параметров SberSign 6.1 (см. Рисунок 7 для варианта исполнения 1 или Рисунок 8 для варианта исполнения 2) установить флажок «Вести журнал событий». Для того чтобы

выключить режим ведения журнала, необходимо снять флажок «Вести журнал событий».

Для того чтобы изменить расположение или имя файла журнала, следует нажать кнопку **Выбрать**, затем в открывшемся окне Windows Explorer выбрать каталог, указать нужное имя файла и нажать кнопку **Открыть**.

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить**.

4.3.2 Выбор места хранения главного ключа и узла замены

Выбор места хранения главного ключа и узла замены доступен только для варианта исполнения 2 SberSign 6.1. Предусмотрено два варианта поиска главного ключа и узла замены:

- на файловой системе по указанному расположению;
- на том же носителе, что и ключ ЭП.

Для того чтобы указать в качестве места хранения главного ключа и узла замены каталог файловой системы, следует в окне настройки параметров SberSign 6.1 (см. Рисунок 8) выбрать вариант «На съемном носителе» и, щёлкнув стрелку в правой части поля «Задайте директорию для gk.db3 и uz.db3», указать нужный каталог.

Для того чтобы указать в качестве места хранения главного ключа и узла замены носитель, на котором находится ключ ЭП, следует в окне настройки параметров SberSign 6.1 (см. Рисунок 8) выбрать вариант «Вместе с закрытым ключом ЭП (на том же носителе)».

4.3.3 Выбор директорий и файлов для БОК, стоп-листа и справочников сертификатов

Для того чтобы задать имена файлов для баз открытых ключей (БОК), стоп-листа и сертификатов, следует перейти на вкладку «Ключевая информация» (см. Рисунок 10).

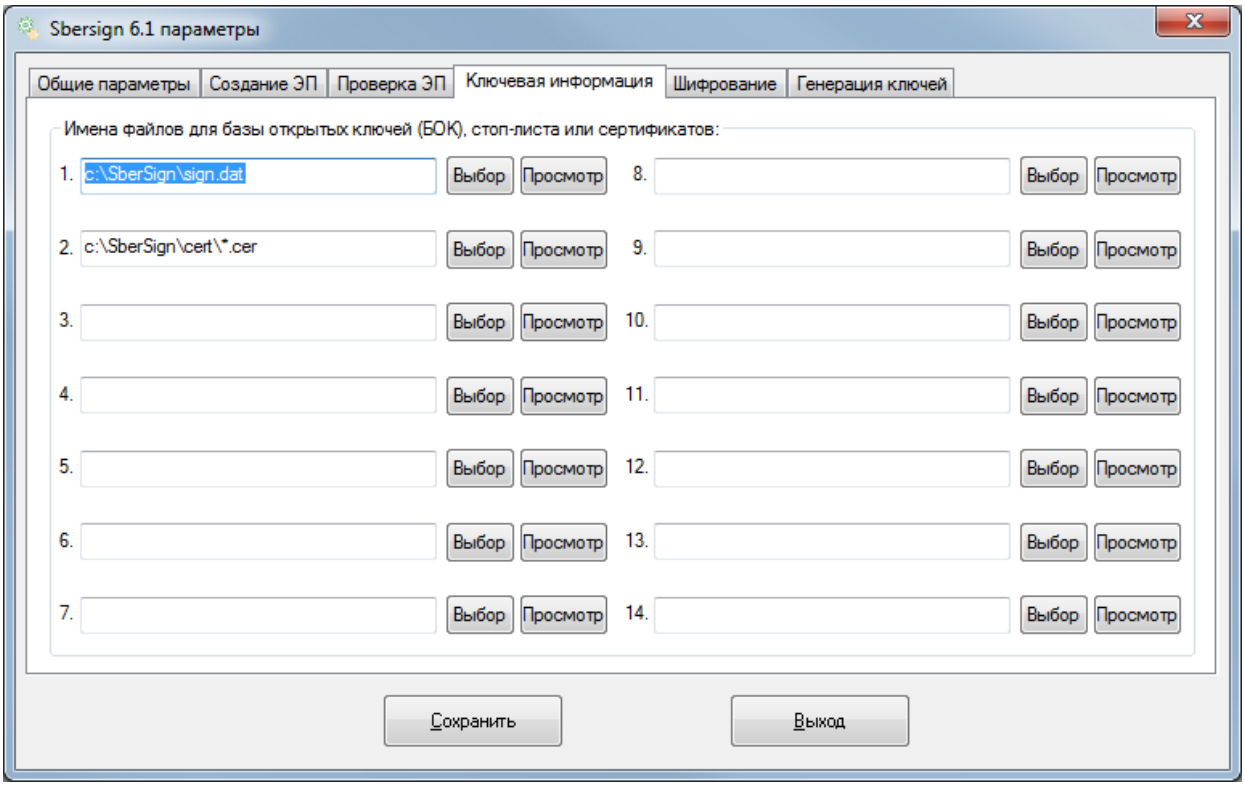

Рисунок 10 – Вкладка «Ключевая информация»

На этой вкладке можно указать до четырнадцати БОК, стоп-листов или справочников сертификатов. В первой строке должно быть указано расположение файла sign.dat, полученного из удостоверяющего центра.

Для того чтобы указать расположение нового файла БОК, стоп-листа или справочника сертификатов, необходимо нажать кнопку **Выбор** справа от незаполненной строки, затем в открывшемся окне Windows Explorer выбрать каталог, указать нужное имя файла и нажать кнопку **Открыть**.

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить**.

4.3.4 Выбор списка отозванных сертификатов для ЭП в формате PKCS#7

Для того чтобы сертификаты проверялись с помощью списка отозванных сертификатов (стоп-листа) из файла, необходимо указать этот файл в списке на вкладке «Ключевая информация» (см. раздел 4.3.3).

Для того чтобы указать файл стоп-листа, необходимо установить флажок «Использовать стоп-лист из файла номер:» и, щёлкнув стрелку в правой части поля,

выбрать из выпадающего списка номер соответствующего стоп-листа на вкладке «Ключевая информация».

Далее необходимо указать директорию, где находятся сертификаты, с помощью которых можно проверить электронную подпись под стоп-листом. Для этого следует щёлкнуть стрелку в правой части поля «Сертификаты стоп-листа», выбрать из выпадающего списка номер нужной директории сертификатов на вкладке «Ключевая информация».

Для того чтобы убедиться в том, что сертификаты из указанной директории соответствуют указанному стоп-листу и проверить подпись под стоп-листом, следует нажать кнопку **Проверить Стоп-лист**.

4.4 Просмотр БОК, стоп-листов, сертификатов и ключевых пар

В SberSign 6.1 предусмотрена возможность просмотра БОК, стоп-листов и сертификатов, перечисленных на вкладке «Ключевая информация» (см. Рисунок 10).

4.4.1 Просмотр информации об используемых криптобиблиотеках

Расположение используемых криптобиблиотек указано в поле «Директория библиотек» (см. Рисунок 7 для варианта исполнения 1 или Рисунок 8 для варианта исполнения 2).

Для того чтобы просмотреть информацию об используемых SberSign 6.1 криптобиблиотеках bicr_adm.dll и CmsSupport.dll, необходимо в окне настройки параметров SberSign 6.1 (см. Рисунок 7 для варианта исполнения 1 или Рисунок 8 для варианта исполнения 2) нажать кнопку **Версии DLL**. В открывшемся окне (см. Рисунок 11) с информацией о версиях используемых криптобиблиотек для продолжения работы следует нажать кнопку **ОК**.

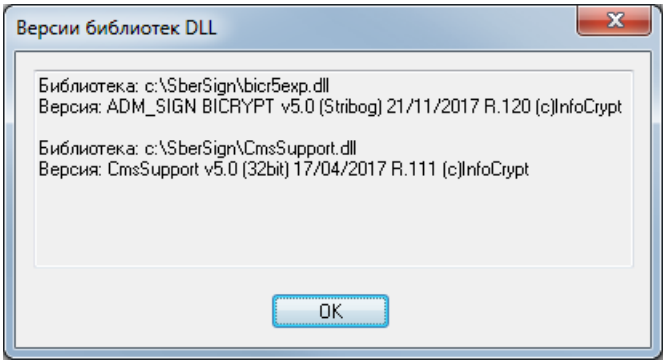

Рисунок 11 – Информация о версиях используемых криптобиблиотек

4.4.2 Просмотр БОК

Для того чтобы просмотреть БОК, следует перейти на вкладку «Ключевая информация» (см. Рисунок 10).

Для того чтобы просмотреть БОК, следует нажать кнопку **Просмотр** справа от строки, в которой указано имя файла этого справочника. В открывшемся окне будет отображён список открытых ключей в данном справочнике (см. Рисунок 12).

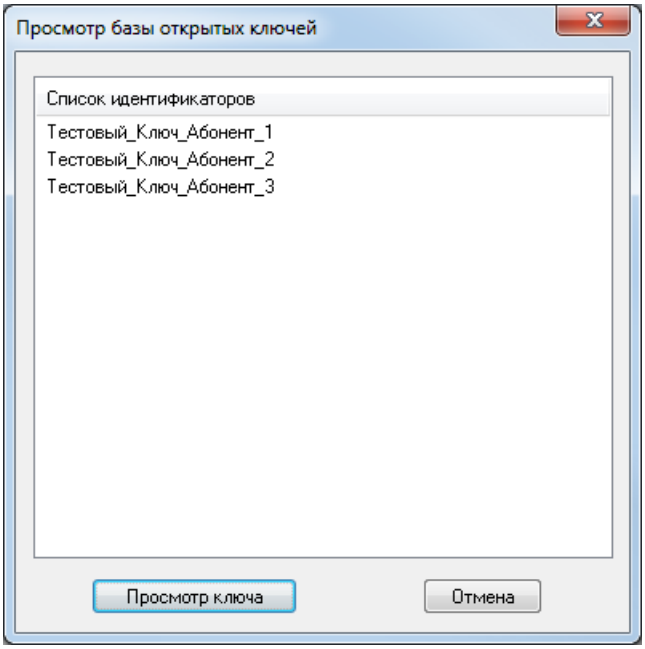

Рисунок 12 – Список открытых ключей

Для того чтобы просмотреть ключ, необходимо выбрать его в списке и нажать кнопку **Просмотр ключа**. В открывшемся окне (см. Рисунок 13) будет отображён выбранный ключ и соответствующий идентификатор абонента.

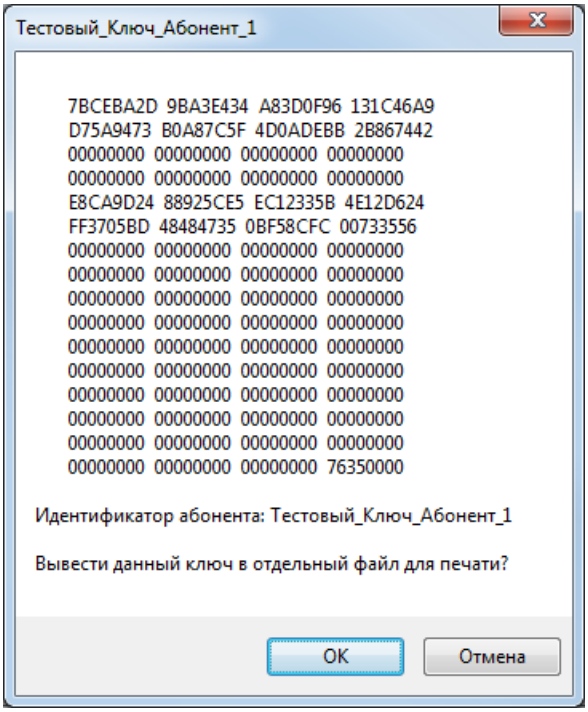

Рисунок 13 – Информация о ключе

Для того чтобы записать ключ в отдельный файл и распечатать его, следует нажать кнопку **ОК**. Для прекращения просмотра данного ключа следует нажать кнопку **Отмена**.

4.4.3 Просмотр стоп-листа

Для того чтобы просмотреть стоп-лист, следует перейти на вкладку «Ключевая информация» (см. Рисунок 10) и нажать кнопку **Просмотр** справа от строки, в которой указано имя файла этого стоп-листа. В открывшемся окне будут отображены общие сведения о стоп-листе (см. Рисунок 14).

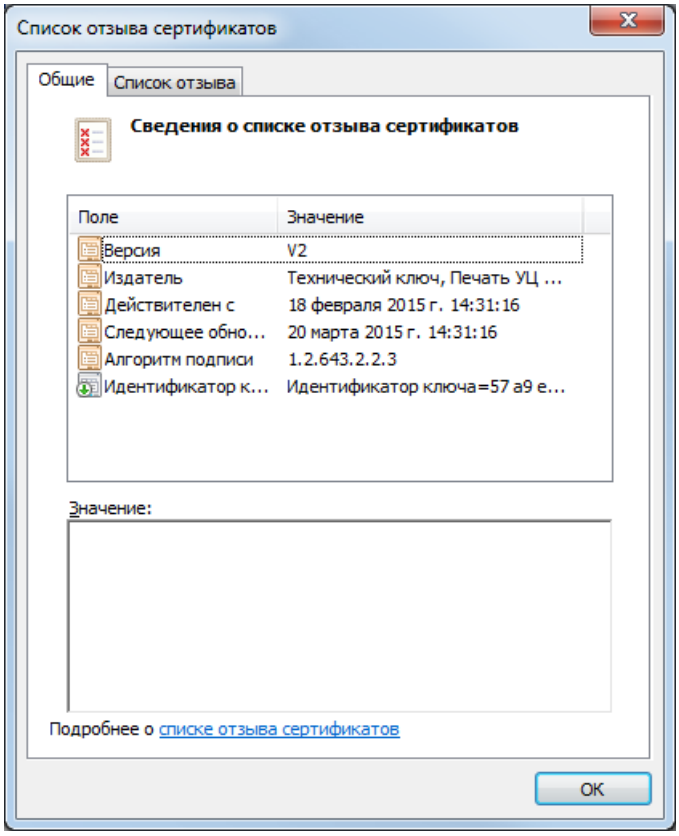

Рисунок 14 – Сведения о стоп-листе

Для того чтобы просмотреть список сертификатов, включённых в данный стоп-лист, следует перейти на вкладку «Список отзыва» (см. Рисунок 15).

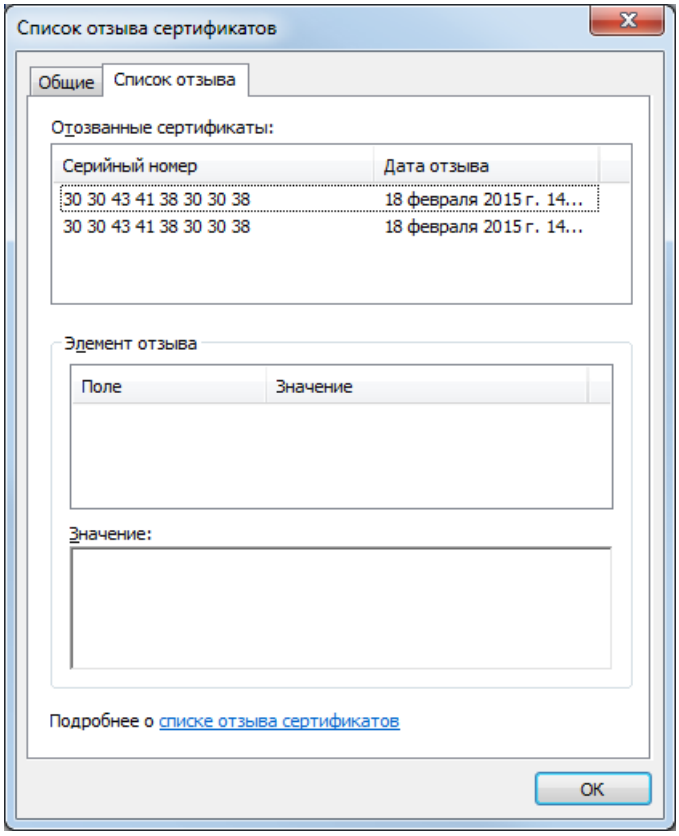

Рисунок 15 – Список сертификатов, включённых в стоп-лист

4.4.4 Просмотр сертификата

Для того чтобы просмотреть сертификат, следует перейти на вкладку «Ключевая информация» (см. Рисунок 10) и нажать кнопку **Просмотр** справа от строки, в которой указана папка с сертификатами.

В открывшемся окне Windows Explorer следует дважды щёлкнуть строку с нужным именем файла. В открывшемся окне будут отображены общие сведения о сертификате (см. Рисунок 16).

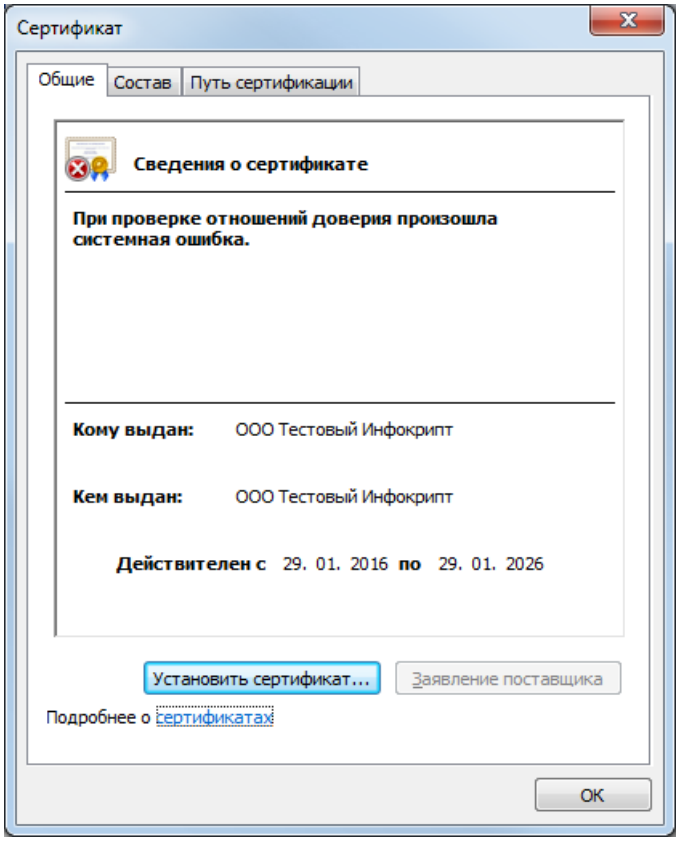

Рисунок 16 – Сведения о сертификате

4.4.5 Просмотр информации о ключевых парах

Для того чтобы просмотреть информации о ранее созданных ключевых парах, в меню выбора компонентов (см. Рисунок 5) необходимо выбрать пункт **Генерация ключей.**

В открывшемся окне приветствия мастера (см. Рисунок 21) следует нажать кнопку **Окно просмотра ранее сгенерированных ключей.** В открывшемся окне (см. Рисунок 17) отображается информация о последней созданной ключевой паре.

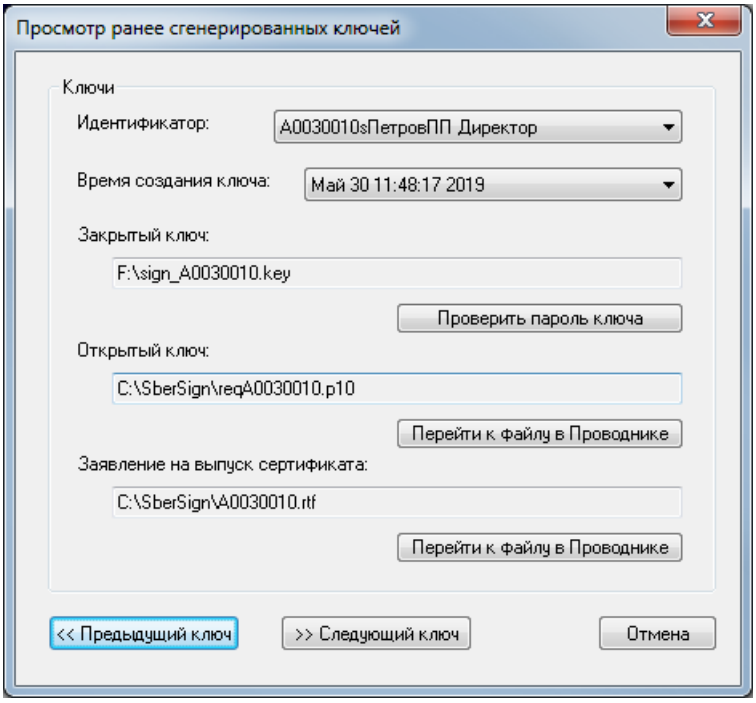

Рисунок 17 - Просмотр информации о ранее созданных ключевых парах

Для того чтобы перейти к информации о предыдущей ключевой паре, следует нажать кнопку <<**Предыдущий ключ**. Для того чтобы перейти к информации о следующей ключевой паре, следует нажать кнопку <<**Следующий ключ**.

Предусмотрен поиск ключевой пары по идентификатору и по времени создания.

Для того чтобы найти ключевую пару по идентификатору, следует щёлкнуть стрелку в правой части поля «Идентификатор» и в открывшемся выпадающем списке выбрать нужный идентификатор.

Для того чтобы найти ключевую пару по времени создания, следует щёлкнуть стрелку в правой части поля «Время создания ключа» и в открывшемся выпадающем списке выбрать нужное время создания.

Для того чтобы найти файл открытого ключа из данной ключевой пары, следует нажать кнопку **Перейти к файлу в Проводнике** под полем «Открытый ключ».

Для того чтобы найти файл заявления на изготовление сертификата для данной ключевой пары, следует нажать кнопку **Перейти к файлу в Проводнике** под полем «Заявление на выпуск сертификата».

Для того чтобы проверить, подходит ли пароль к данному закрытому ключу, следует нажать кнопку **Проверить пароль ключа**, в открывшемся окне (см. Рисунок 35) ввести проверяемый пароль и нажать кнопку **ОК**. Если введён пароль от другого закрытого ключа, в открывшемся окне с сообщением

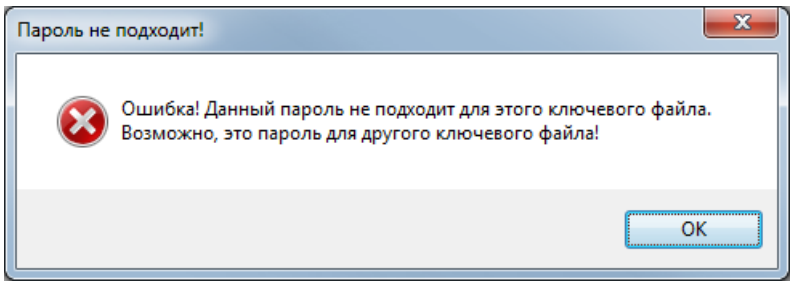

Рисунок 18 – Пароль не подходит к выбранной ключевой паре

Если пароль не подходит ни к одной ключевой паре, кнопка **ОК** будет недоступна. Для выхода следует нажать кнопку **Отмена**.

4.5 Копирование главного ключа и узла замены на устройства ТМ или VPN-Key

Копирование главного ключа и узла замены на устройства ТМ или VPN-Key доступно только для варианта исполнения 2 SberSign 6.1. Для того чтобы скопировать главный ключ и узел замены на устройство Touch Memory, необходимо указать место хранения главного ключа и узла замены в файловой системе (см. раздел 4.3.2). Затем следует приложить устройство Touch Memory к считывателю и нажать кнопку **Копировать ГК в ТМ**.

В открывшемся окне с сообщением о записи главного ключа и узла замены на устройство Touch Memory (см. Рисунок 19) следует нажать кнопку **ОК**.

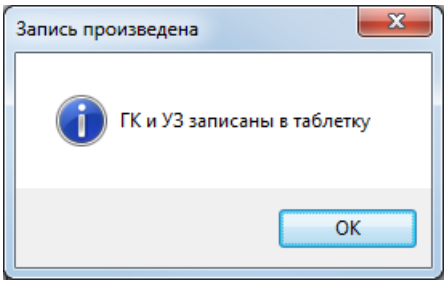

Рисунок 19 – Сообщение о записи главного ключа и узла замены на ТМ

Для того чтобы скопировать главный ключ и узел замены на устройство VPN-Key, необходимо указать место хранения главного ключа и узла замены в

файловой системе (см. раздел 4.3.2), вставить устройство VPN-Key в разъём USB и нажать кнопку **Копировать ГК в VPN-Key**.

4.6 Генерация ключей ЭП

4.6.1 Настройка параметров генерации ключей ЭП

Для того чтобы изменить значения параметров генерации ключей ЭП, необходимо в меню выбора компонентов (см. Рисунок 5) выбрать пункт **Параметры Sbersign** и в открывшемся окне настройки параметров SberSign 6.1 (см. Рисунок 7 для варианта исполнения 1 или Рисунок 8 для варианта исполнения 2) перейти на вкладку «Генерация ключей» (см. Рисунок 20).

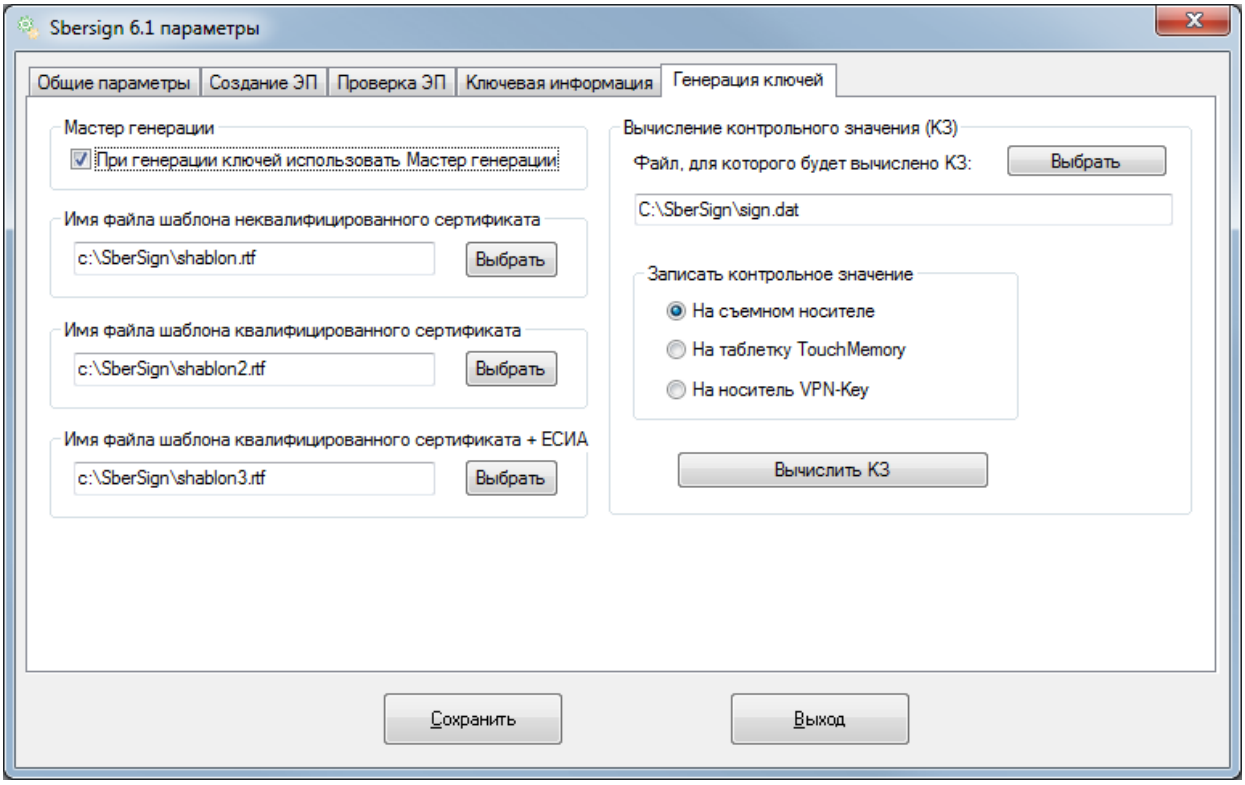

Рисунок 20 – Настройка параметров генерации ключей ЭП

В SberSign 6.1 предусмотрено создание ключей ЭП в двух режимах: режиме мастера создания ключей ЭП и режиме приложения создания ключей. По умолчанию программа работает в режиме мастера создания ключей ЭП. Режим приложения создания ключей оставлен для совместимости с предыдущими версиями ПО Sbersign. Для того чтобы указать приложение создания ключей в качестве режима генерации ключей, необходимо снять флажок «При генерации ключей использовать Мастер генерации».

В комплект ПО SberSign 6.1 включен шаблон для печати ключа проверки подписи. Шаблон реализован в виде стандартного файла в формате RTF. Возможна модификация любых полей шаблона, кроме полей, обозначенных значениями «1234 5678», а также полей «Контрольное значение», «Идентификатор» и «Номер таблетки».

Для того чтобы в процессе генерации ключей ЭП распечатывался ключ проверки подписи, необходимо установить имя файла шаблона, который будет использоваться при распечатке заявления на изготовление сертификата.

По умолчанию в качестве шаблона заявления на изготовление квалифицированного сертификата используется файл C:\SberSign\shablon2.rtf, а в качестве шаблона заявления на изготовление неквалифицированного сертификата используется файл C:\SberSign\shablon.rtf.

Для того чтобы выбрать другой файл шаблона заявления на изготовление квалифицированного сертификата, следует нажать кнопку **Выбрать** справа от поля «Имя файла шаблона квалифицированного сертификата», затем в открывшемся окне Windows Explorer выбрать каталог, указать нужное имя файла в формате RTF и нажать кнопку **Открыть**. Аналогично, для того чтобы выбрать другой файл шаблона заявления на изготовление неквалифицированного сертификата следует нажать кнопку **Выбрать** справа от поля «Имя файла шаблона неквалифицированного сертификата», затем в открывшемся окне Windows Explorer выбрать каталог, указать нужное имя файла в формате RTF и нажать кнопку **Открыть**.

Если на компьютере установлен пакет Microsoft Office, то в процессе генерации ключей ЭП распечатка открытого ключа будет отображена на экране с помощью текстового процессора Microsoft Word.

Аналогично для указания шаблона печати сертификатов следует нажать кнопку **Выбрать** справа от поля «Имя файла шаблона БОК», затем в открывшемся окне Windows Explorer выбрать каталог, указать нужное имя файла в формате RTF и нажать кнопку **Открыть**.

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить**.

4.6.2 Генерация ключевой пары с однокомпонентным закрытым ключом

В SberSign 6.1 предусмотрена возможность создания ключевой пары как с однокомпонентным закрытым ключом, так и с двухкомпонентным закрытым ключом.

Однокомпонентный ключ создаётся для личного использования, а двухкомпонентный – для использования в автоматизированных системах.

4.6.2.1 Генерация ключевой пары с однокомпонентным закрытым ключом с использованием мастера генерации ключей

Для того чтобы создать ключи ЭП с использованием мастера генерации ключей, необходимо указать при настройке параметров указать мастер генерации ключей в качестве режима генерации ключей (см. раздел 4.6.1). При необходимости печати открытых ключей следует также указать расположение шаблона печати открытых ключей (см. раздел 4.6.1).

Для того чтобы создать новую ключевую пару и запрос на сертификат ключа проверки электронной подписи, в меню выбора компонентов (см. Рисунок 5) необходимо выбрать пункт **Генерация ключей**.

В открывшемся окне приветствия мастера (см. Рисунок 21) следует нажать кнопку **Далее>** для продолжения процесса генерации ключей или кнопку **Отмена** для прекращения работы мастера.

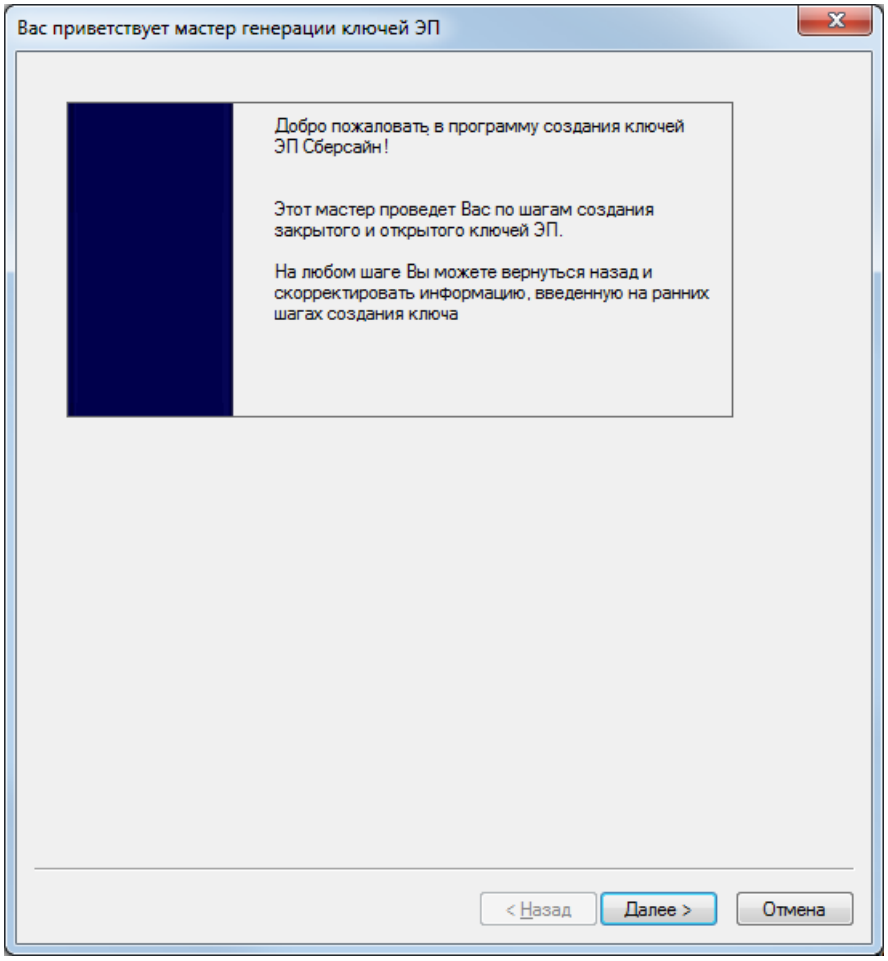

Рисунок 21 – Окно приветствия мастера генерации ключей

Работа мастера состоит из четырёх шагов. На первом шаге (см. Рисунок 22) следует выбрать тип создаваемого ключа ЭП – однокомпонентный.

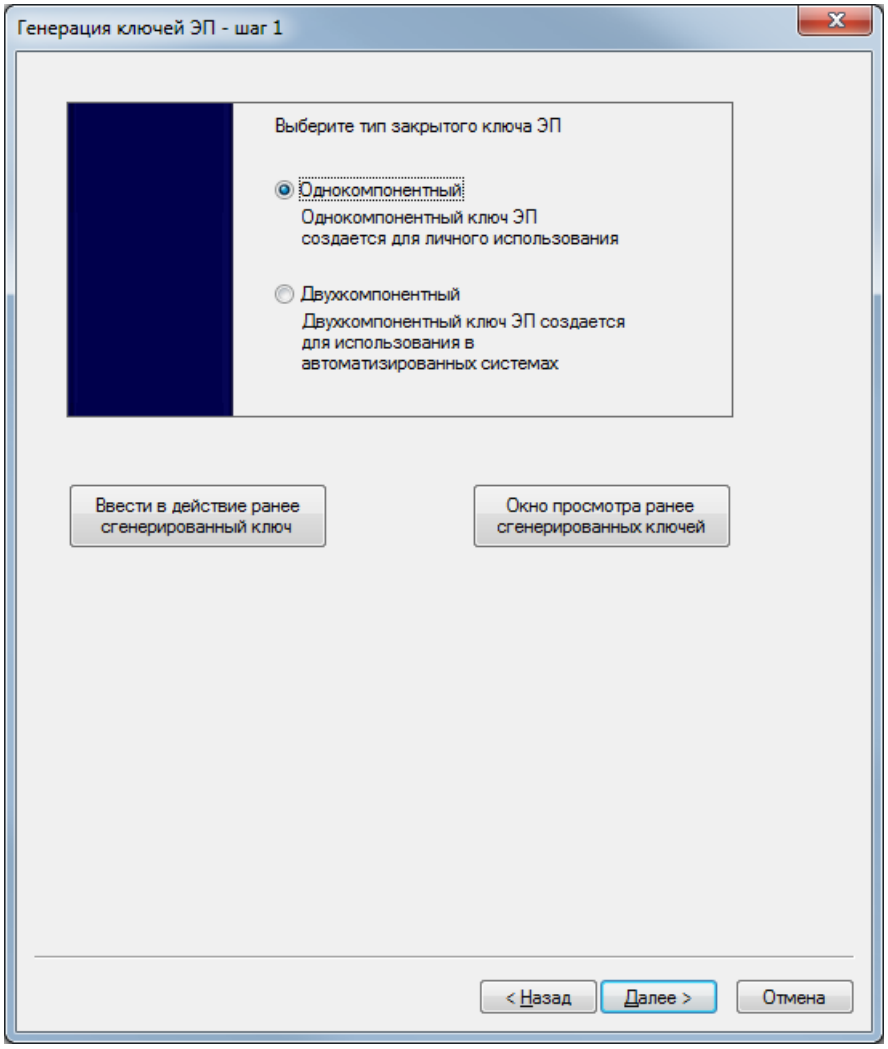

Рисунок 22 – Выбор типа создаваемого ключа ЭП

Для подтверждения выбора следует нажать кнопку **Далее>**, для возвращения к предыдущему шагу работы мастера – кнопку **<Назад**, для отказа от продолжения процесса генерации ключей – кнопку **Отмена**.

На втором шаге работы мастера следует заполнить данными владельца ключа поля: «Фамилия», «Имя», «Отчество», «Должность», «E-mail», «Наименование организации», «Код организации (КУЦ)», «ИНН», «ОГРН» (см. Рисунок 23).

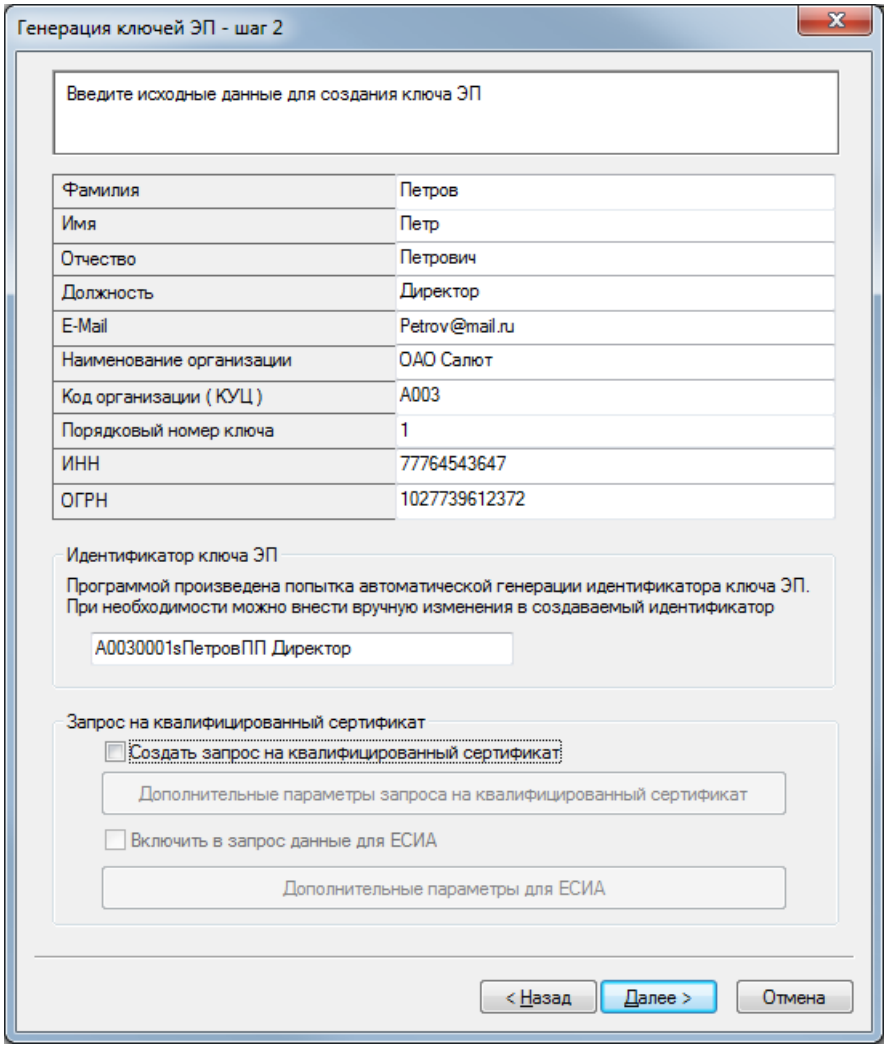

Рисунок 23 – Ввод данных владельца ключа

Поле «Порядковый номер ключа» заполняется автоматически. Также автоматически формируется идентификатор ключа ЭП. При необходимости этот идентификатор может быть изменён.

Идентификатор ключа ЭП не может состоять более чем из 32 символов (включая пробелы) и должен соответствовать формату: **YYYYNNNNsФИО должность организация**, где **YYYY** – уникальный четырехразрядный буквенно-цифровой код организации - клиента Сбербанка России, присваиваемый автоматизированной системой корневого Удостоверяющего центра ОАО «Сбербанк России»; **NNNN** – уникальный для каждого Участника системы ЭДО четырехразрядный порядковый номер ключа ЭП, который не должен использоваться повторно даже в случае перегенерации ключа; **s** – признак принадлежности ключа ЭП организации, являющейся клиентом Сбербанка.

При создании первого ключа ЭП с данным кодом организации, необходимо, чтобы номер ключа был равен 0001.

Идентификатор ключа ЭП создастся автоматически, но его можно отредактировать, чтобы сделать более информативным. Например, в автоматически сформированном идентификаторе не отражается название предприятия. Для него не хватает места, так как длина идентификатора не должна превышать 32 символов. Как вариант, можно сократить должность и убрать пробел после отчества, а затем добавить название предприятия (см. Рисунок 24).

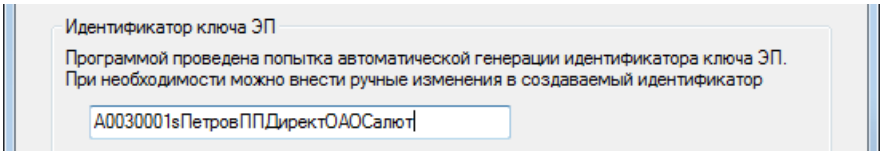

Рисунок 24 – Изменённый идентификатор

Если требуется создать запрос на квалифицированный сертификат, необходимо установить флажок «Создать запрос на квалифицированный сертификат», нажать кнопку «Дополнительные параметры запроса на квалифицированный сертификат» и в открывшемся окне (см. Рисунок 25) заполнить поля: «Страна», «Регион» и «Населённый пункт». Заполнение полей «Почтовый индекс», «Адрес», «СНИЛС», «Краткое наименование организации» и «Подразделение» не является обязательным. Для подтверждения введённых данных необходимо нажать кнопку **ОК**, для отказа от продолжения процесса создания запроса на квалифицированный сертификат – нажать кнопку **Отмена** и снять флажок «Создать запрос на квалифицированный сертификат».

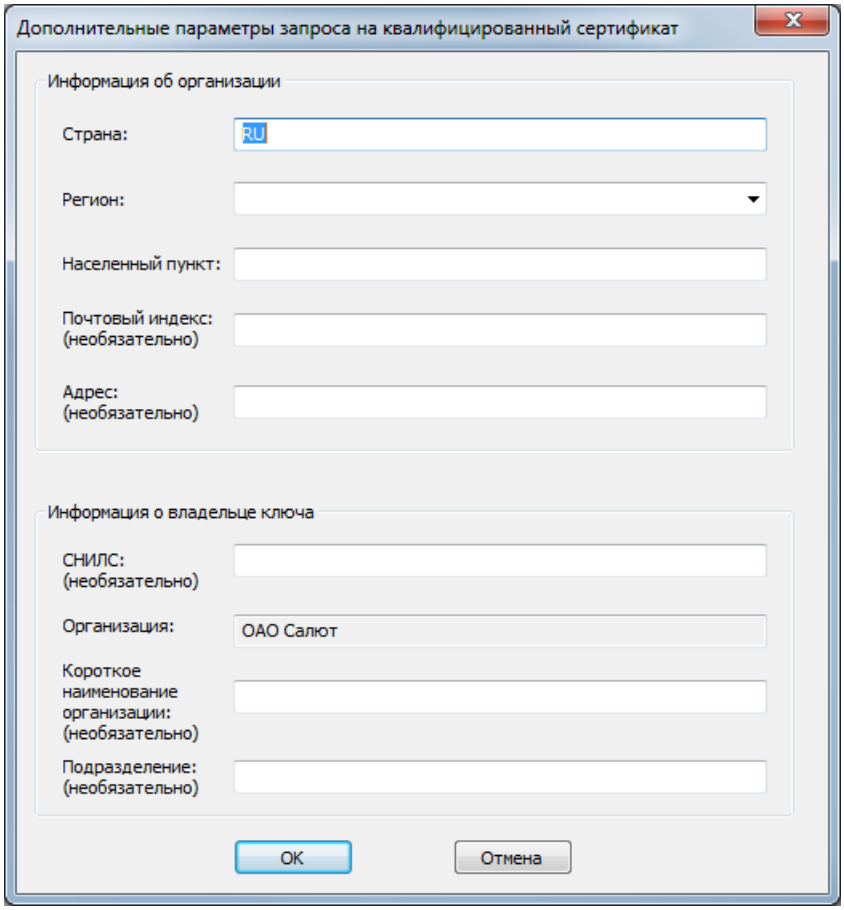

Рисунок 25 – Дополнительные параметры запроса на квалифицированный сертификат

Если требуется регистрация в единой системе идентификации и аутентификации (ЕСИА), необходимо установить флажок «Включить в запрос данные для ЕСИА», нажать кнопку «Дополнительные параметры для ЕСИА» и в открывшемся окне (см. Рисунок 26) ввести данные. Для подтверждения введённых данных необходимо нажать кнопку **OK**, для отказа от продолжения процесса создания запроса на квалифицированный сертификат – нажать кнопку **Отмена** и снять флажок «Включить в запрос данные для ЕСИА».

Для подтверждения введённых на втором шаге работы мастера данных (см. Рисунок 23) следует нажать кнопку **Далее>**, для возвращения к предыдущему шагу работы мастера – кнопку **<Назад**, для отказа от продолжения процесса генерации ключей – кнопку **Отмена**.

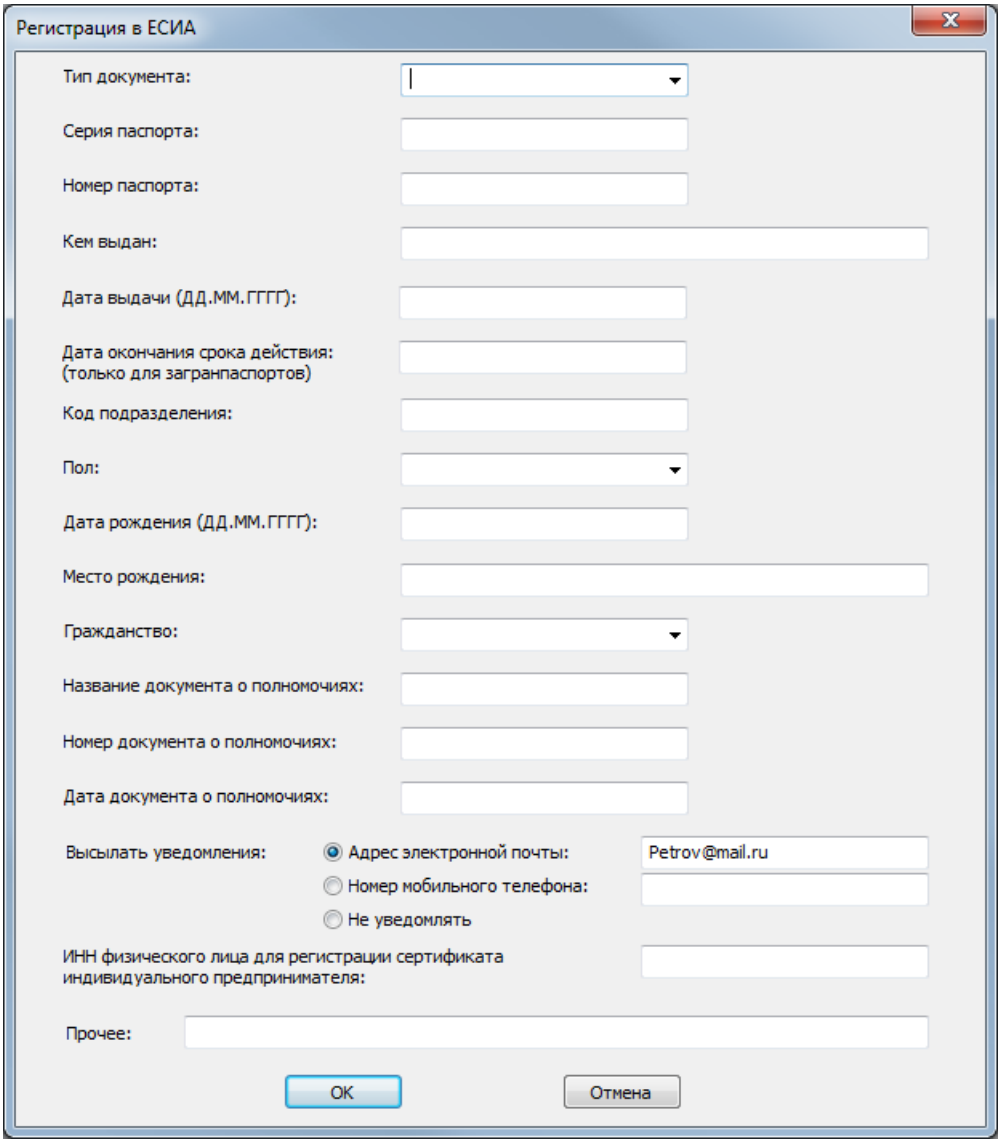

Рисунок 26 – Дополнительные параметры для регистрации в ЕСИА

На третьем шаге работы мастера (см. Рисунок 27) следует выбрать место, куда будет записан закрытый ключ ЭП.

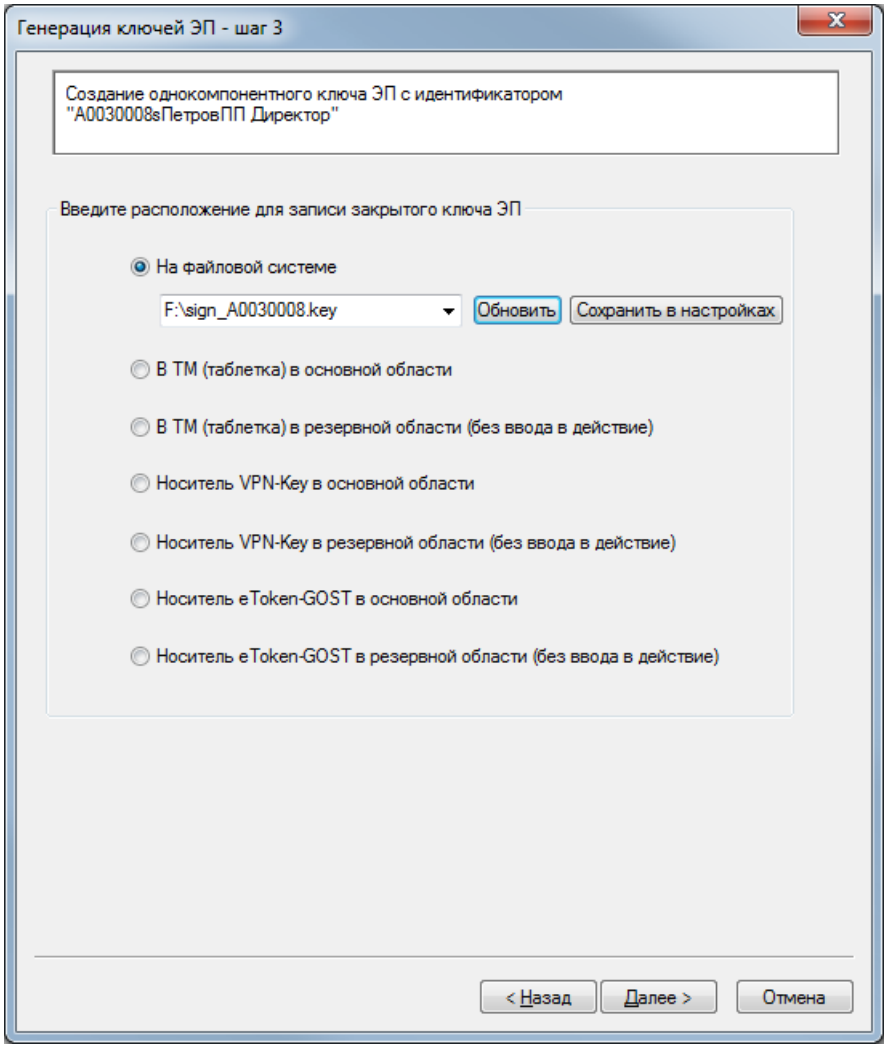

Рисунок 27 – Выбор места для записи закрытого ключа ЭП

Если в качестве места для записи закрытого ключа ЭП выбран вариант «На файловой системе», то необходимо указать конкретное место для записи ключа. Если съёмный носитель для записи закрытого ключа ЭП еще не подключен, следует подключить его и нажать кнопку **Обновить.** Для того чтобы в дальнейшем выбранное место предлагалось для записи закрытого ключа ЭП по умолчанию, следует нажать кнопку **Сохранить в настройках**, и в открывшемся окне с сообщением о сохранении пути к файлу закрытого ключа (см. Рисунок 28) нажать кнопку **OK.**

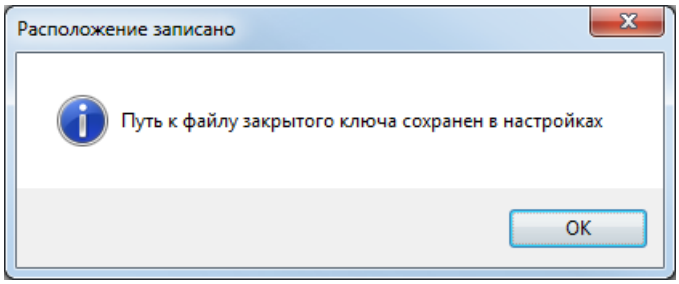

Рисунок 28 – Сообщение о сохранении пути к файлу закрытого ключа

Если в качестве места для записи закрытого ключа ЭП выбран один из вариантов «без ввода в действие», то впоследствии будет необходимо ввести ключ в действие (см. раздел 4.7).

Для подтверждения выбора места для записи закрытого ключа ЭП следует нажать кнопку **Далее>**, для возвращения к предыдущему шагу работы мастера – кнопку **<Назад**, для отказа от продолжения процесса генерации ключей – кнопку **Отмена**.

На четвёртом шаге работы мастера (см. Рисунок 29) следует выбрать место, куда будет записан открытый ключ ЭП и параметры генерации ключа.

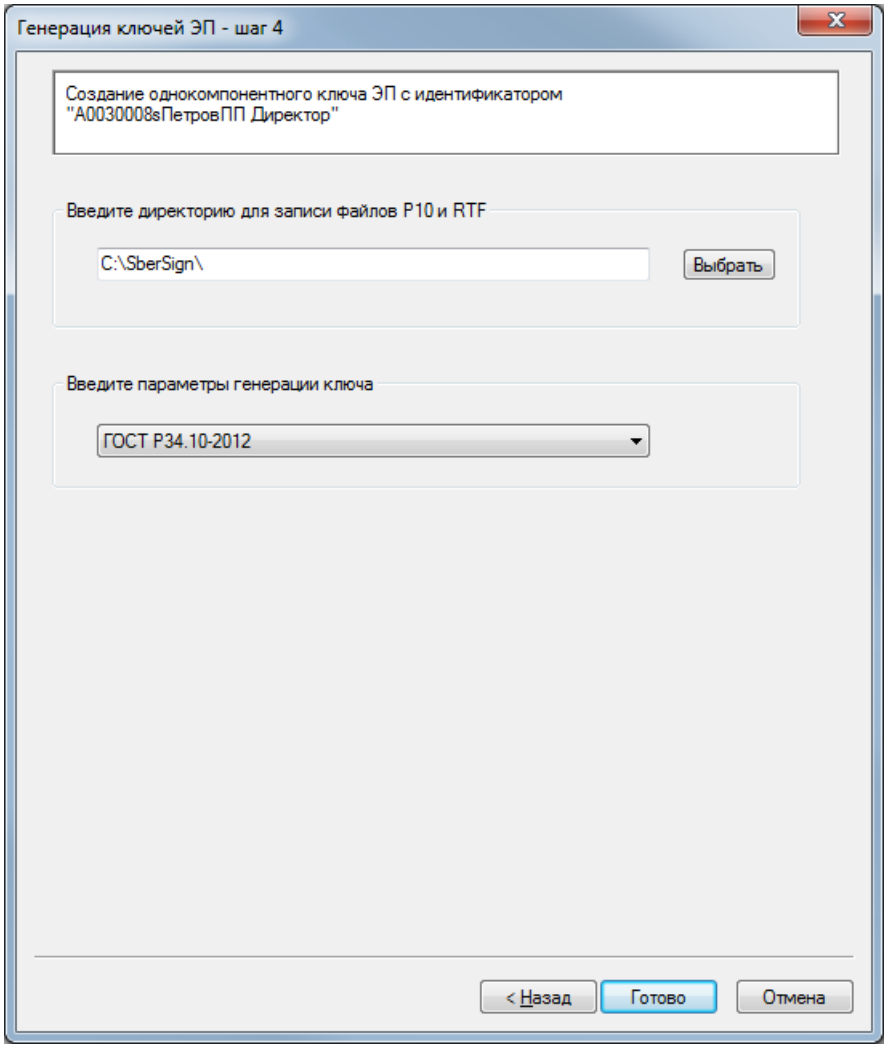

Рисунок 29 – Выбор места для записи открытого ключа ЭП

Для того чтобы выбрать параметры генерации ключа, необходимо щёлкнуть стрелку в правой части поля и выбрать нужные параметры из выпадающего списка.

Для подтверждения выбора места для записи открытого ключа ЭП следует нажать кнопку **Готово**. После этого в зависимости от сделанного выбора открытый ключ, сертификат открытого ключа или запрос на выдачу сертификата сохраняется в виде файла в указанной папке на жёстком диске или флэш-накопителе. Данный файл предназначен для передачи в удостоверяющий центр Сбербанка для его сертификации (установления принадлежности) и регистрации. Для возвращения к предыдущему шагу работы мастера следует нажать кнопку **<Назад**, для отказа от продолжения процесса генерации ключей – кнопку **Отмена**.

После появления соответствующего предложения (см. Рисунок 30) необходимо вставить флеш-накопитель с закрытым ключом ЭП в разъём USB и нажать кнопку **OK** для

создания ключей или кнопку **Отмена** для отказа от продолжения процесса генерации ключей.

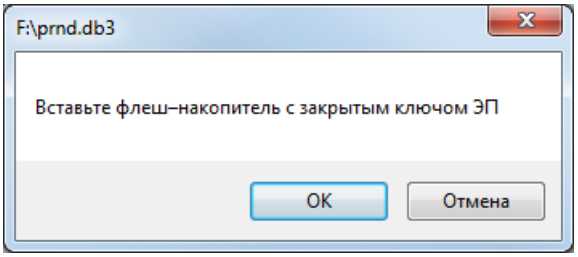

Рисунок 30 – Предложение вставить флеш-накопитель с закрытым ключом ЭП

При первом использовании данного носителя для генерации ключей может потребоваться сформировать ключ датчика случайных чисел (ДСЧ). При появлении соответствующего сообщения (см. Рисунок 31) необходимо нажать кнопку **OK** для продолжения создания ключей или кнопку **Отмена** для отказа от продолжения процесса генерации ключей.

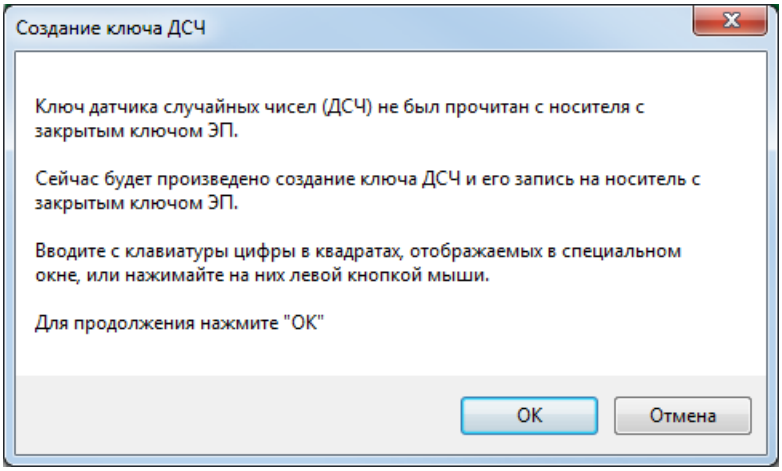

Рисунок 31 – Сообщение о необходимости создания ключа ДСЧ

После нажатия кнопки **OK** в открывшемся окне инициализации ДСЧ (см. Рисунок 32) необходимо последовательно щёлкать левой кнопкой мыши появляющиеся квадратики с цифрами (или нажимать клавиши с соответствующими цифрами) до тех пор, пока окно не закроется.

Рисунок 32 – Окно инициализации ДСЧ

Если в качестве места хранения однокомпонентного закрытого ключа ЭП указан съёмный носитель (см. раздел 4.6.2), по завершении процесса формирования закрытого ключа ЭП в открывшемся окне (см. Рисунок 33) будет предложен пароль для доступа к созданному ключу, состоящий из шести символов и включающий буквы английского алфавита и цифры.

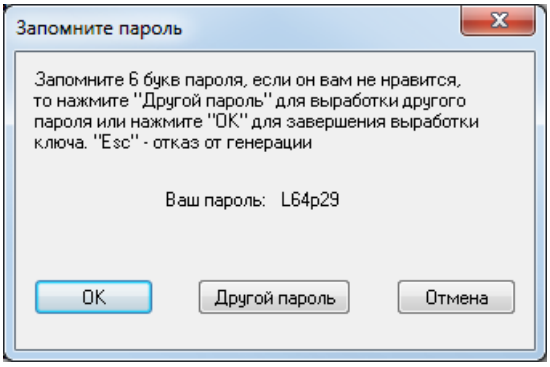

Рисунок 33 – Окно выбора пароля

Если пароль не устраивает, следует нажать кнопку **Другой пароль**. Можно нажимать кнопку **Другой пароль** несколько раз до тех пор, пока не появится приемлемая комбинация.

Выбранный пароль необходимо запомнить (сохранить в надёжном месте). Для подтверждения выбранного пароля следует нажать кнопку **OK**. После подтверждения пароля ключи ЭП записываются на указанный носитель. Для отказа от продолжения процесса генерации ключей следует нажать кнопку **Отмена**.

При появлении окна с сообщением об успешном создании ключей ЭП (см. Рисунок 34) необходимо запомнить пароль (сохранить в надёжном месте) и нажать кнопку **Да**.

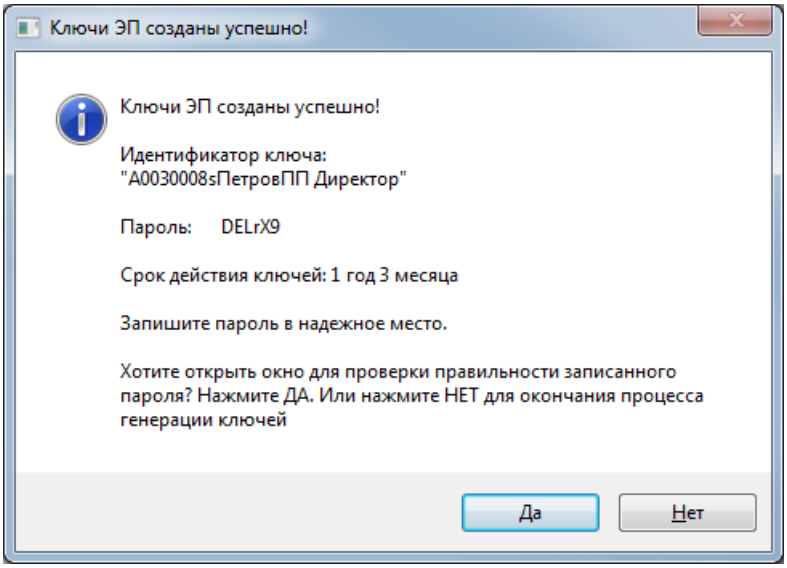

Рисунок 34 – Сообщение об успешном создании ключей ЭП

В открывшемся окне (см. Рисунок 35) необходимо ввести сохранённый пароль и нажать кнопку **ОК**.

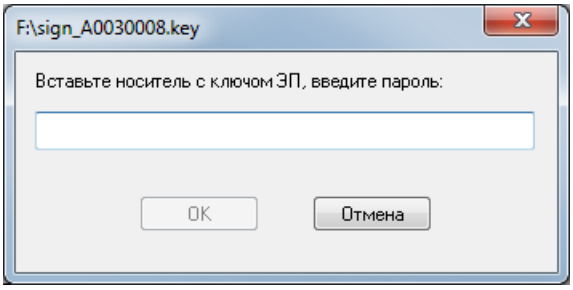

Рисунок 35 – Ввод пароля

Если пароль введён неверно, кнопка **ОК** будет недоступна. В этом случае следует нажать кнопку **Отмена**, в окне с сообщением об отказе от ввода пароля (см. Рисунок 36) нажать кнопку **ОК** и вернуться к окну с сообщением об успешном создании ключей ЭП (см. Рисунок 34).

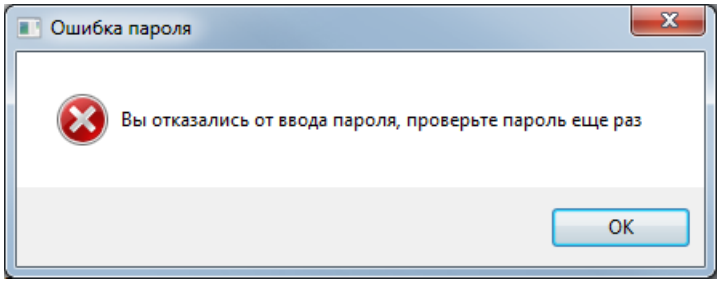

Рисунок 36 – Сообщение об отказе от ввода пароля

Если пароль введён верно, в открывшемся окне (см. Рисунок 37) следует нажать кнопку **ОК**.

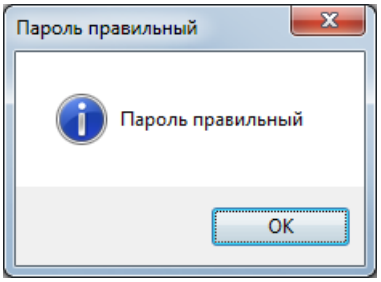

Рисунок 37 – Сообщение о правильном вводе пароля

В открывшемся окне MS Word с проектом заявления на изготовление сертификата ключа проверки ЭП следует проверить правильность данных, при необходимости внести исправления и сохранить заявление в файл. Этот файл должен быть распечатан в трёх экземплярах, заверен соответствующими подписями, оттиском печати и передан вместе с файлом открытого ключа в ПАО «Сбербанк России».

4.6.2.2 Генерация ключевой пары с однокомпонентным закрытым ключом с использованием приложения создания ключей

Для того чтобы создать ключи ЭП с использованием приложения создания ключей, необходимо при настройке параметров указать приложение создания ключей в качестве режима генерации ключей (см. раздел 4.6.1). При необходимости печати открытых ключей следует также указать расположение шаблона печати открытых ключей (см. раздел 4.6.1).

Для того чтобы создать новую ключевую пару и запрос на сертификат ключа проверки электронной подписи, в меню выбора компонентов (см. Рисунок 5) необходимо выбрать пункт **Генерация ключей**.

В открывшемся окне приложения создания ключей (см. Рисунок 38) следует перейти на вкладку «Генерация ключей ЭП».

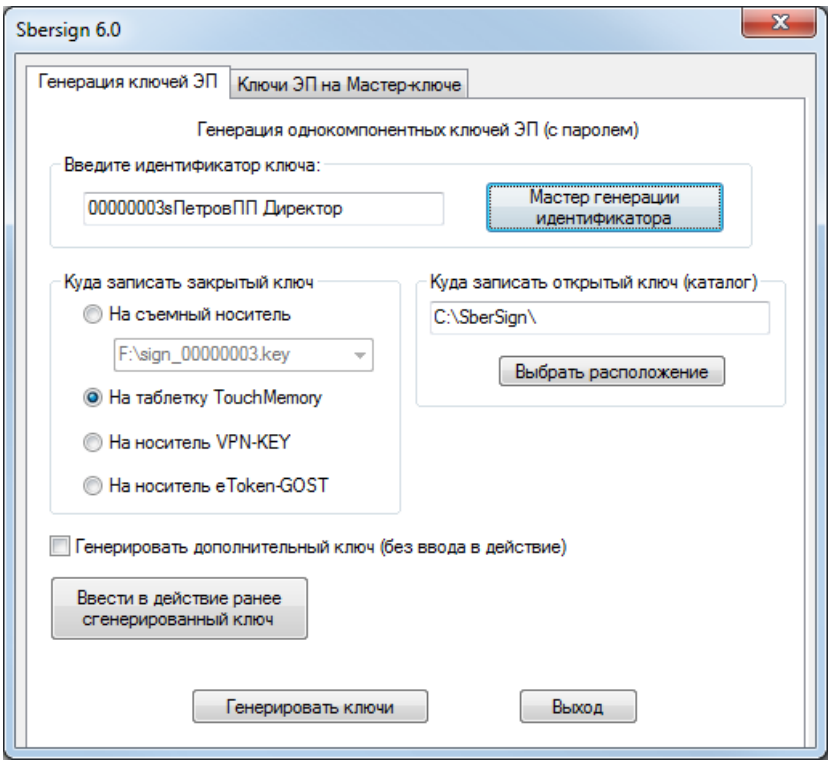

Рисунок 38 – Генерация однокомпонентных ключей с использованием приложения создания ключей

Для генерации ключевой пары необходимо ввести идентификатор ключа ЭП в поле «Введите идентификатор ключа».

Идентификатор ключа ЭП не может состоять более чем из 32 символов (включая пробелы) и должен соответствовать формату: **YYYYNNNNsФИО должность организация**, где **YYYY** – уникальный четырехразрядный буквенно-цифровой код организации - клиента Сбербанка России, присваиваемый автоматизированной системой корневого Удостоверяющего центра ОАО «Сбербанк России»; **NNNN** – уникальный для каждого Участника системы ЭДО четырехразрядный порядковый номер ключа ЭП, который не должен использоваться повторно даже в случае перегенерации ключа; **s** – признак принадлежности ключа ЭП организации, являющейся клиентом Сбербанка.

При создании первого ключа ЭП с данным кодом организации, необходимо, чтобы номер ключа был равен 0001.

Приложение создания ключей позволяет формировать идентификатор ключа ЭП автоматически. Для этого необходимо нажать кнопку «Мастер генерации идентификатора»

и в открывшемся окне (см. Рисунок 39) заполнить поля «Фамилия», «Имя», «Отчество», «Должность», «E-mail», «Наименование организации», «Код организации (КУЦ)», «ИНН», «ОГРН». Поле «Порядковый номер ключа» заполняется автоматически.

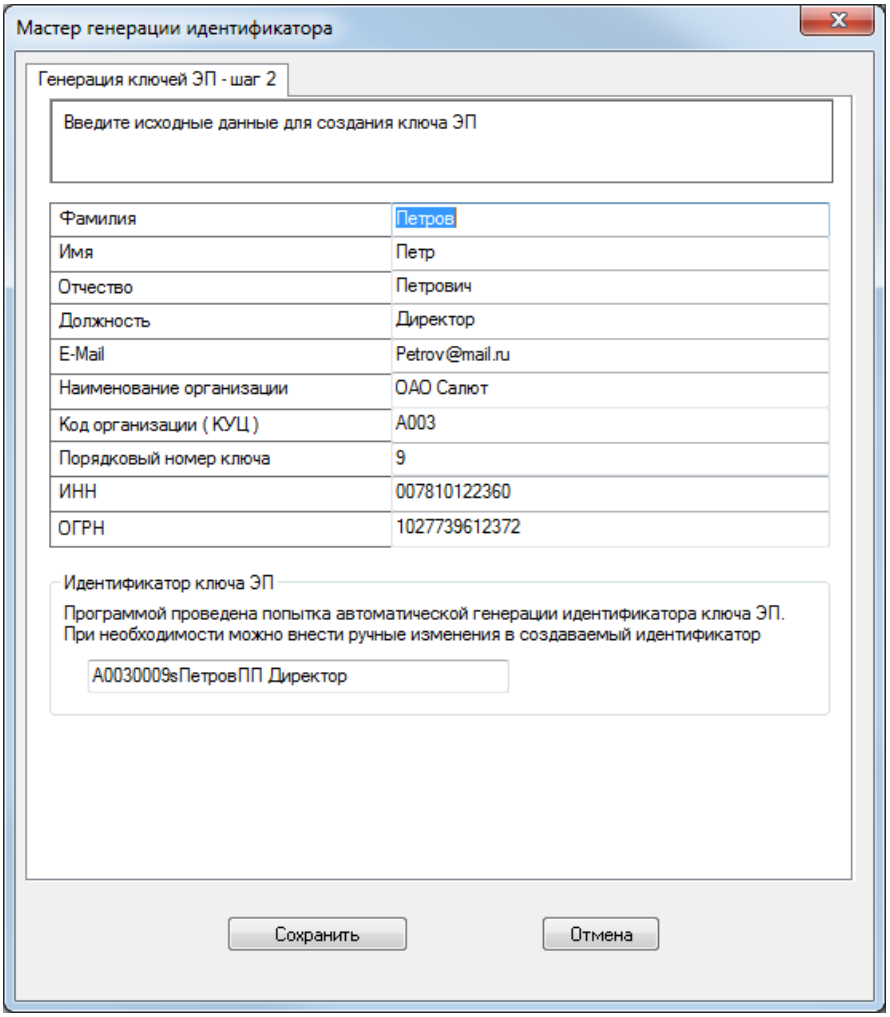

Рисунок 39 – Ввод данных для создания идентификатора ключа ЭП

Идентификатор ключа ЭП создастся автоматически, но его можно отредактировать, чтобы сделать более информативным. Например, в автоматически сформированном идентификаторе не отражается название предприятия. Для него не хватает места, так как длина идентификатора не должна превышать 32 символов. Как вариант, можно сократить должность и убрать пробел после отчества, а затем добавить название предприятия (см. Рисунок 24).

Для подтверждения выбора идентификатора ключа ЭП следует нажать кнопку **Сохранить**. В результате созданный идентификатор будет отображён в поле «Введите идентификатор ключа» (см. Рисунок 38). Для отказа от создания нового идентификатора ключа ЭП следует нажать кнопку **Отмена**.

Далее для генерации ключевой пары необходимо выполнить следующие действия:

- Выбрать место, куда будет записан закрытый ключ ЭП.
- Выбрать место, куда будет записан открытый ключ ЭП.
- В случае создания резервного ключа ЭП на носителе TouchMemory, VPN-KEY или eToken-GOST установить флажок «генерировать дополнительный ключ (без ввода в действие).
- Нажать кнопку **Генерировать ключи**.

По завершении процесса формирования ключей ЭП в открывшемся окне (см. Рисунок 33) будет предложен пароль для доступа к созданному закрытому ключу, состоящий из шести символов и включающий буквы английского алфавита и цифры.

Если пароль не устраивает, следует нажать кнопку **Другой пароль**. Можно нажимать кнопку **Другой пароль** несколько раз до тех пор, пока не появится приемлемая комбинация.

Выбранный пароль необходимо запомнить. Для подтверждения выбранного пароля следует нажать кнопку **OK**. После подтверждения пароля ключи ЭП записываются на указанный носитель. Для отказа от продолжения процесса генерации ключей следует нажать кнопку **Отмена**.

В открывшемся окне с сообщением об успешном создании ключей ЭП (см. Рисунок 34) следует нажать кнопку **OK.**

4.6.3 Генерация ключевой пары с двухкомпонентным закрытым ключом

В SberSign 6.1 предусмотрена возможность создания ключевой пары как с однокомпонентным закрытым ключом, так и с двухкомпонентным закрытым ключом. Однокомпонентный ключ создаётся для личного использования, а двухкомпонентный – для использования в автоматизированных системах.

Прежде чем создавать ключевую пару с двухкомпонентным закрытым ключом, необходимо в настройках SberSign 6.1 указать место хранения главного ключа и узла замены (см. раздел 4.3.2).

4.6.3.1 Генерация ключевой пары с двухкомпонентным закрытым ключом с использованием мастера генерации ключей

Для того чтобы создать ключи ЭП с использованием мастера генерации ключей, необходимо указать при настройке параметров указать мастер генерации ключей в качестве режима генерации ключей (см. раздел 4.6.1).

Для того чтобы создать новую ключевую пару и запрос на сертификат ключа проверки электронной подписи в меню выбора компонентов (см. Рисунок 5) необходимо выбрать пункт **Генерация ключей**.

В открывшемся окне приветствия мастера (см. Рисунок 21) следует нажать кнопку **Далее>** для продолжения процесса генерации ключей или кнопку **Отмена** для прекращения работы мастера.

Работа мастера состоит из четырёх шагов. На первом шаге (см. Рисунок 40) следует выбрать тип создаваемого ключа ЭП – двухкомпонентный.

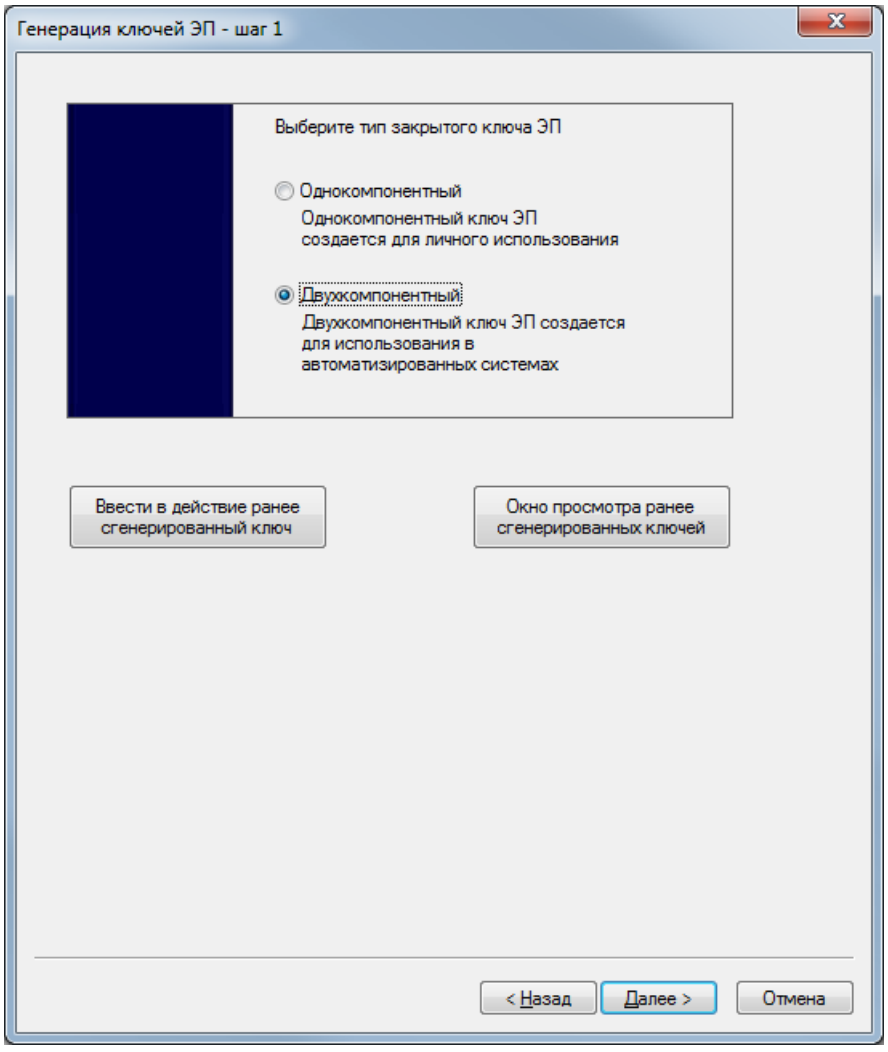

Рисунок 40 – Выбор типа создаваемого ключа ЭП

Для подтверждения выбора следует нажать кнопку **Далее>**, для возвращения к предыдущему шагу работы мастера – кнопку **<Назад**, для отказа от продолжения процесса генерации ключей – кнопку **Отмена**.

На втором шаге работы мастера следует заполнить данными владельца ключа поля: «Фамилия», «Имя», «Отчество», «Должность», «E-mail», «Наименование организации», «Код организации (КУЦ)», «ИНН», «ОГРН» (см. Рисунок 23).

Поле «Порядковый номер ключа» заполняется автоматически. Также автоматически формируется идентификатор ключа ЭП. При необходимости этот идентификатор может быть изменён.

Идентификатор ключа не может состоять более чем из 32 символов (включая пробелы) и должен соответствовать формату: **YYYYNNNNsФИО должность организация**, где **YYYY** – уникальный четырехразрядный буквенно-цифровой код организации - клиента Сбербанка России, присваиваемый автоматизированной системой корневого Удостоверяющего центра ОАО «Сбербанк России»; **NNNN** – уникальный для каждого Участника системы ЭДО четырехразрядный порядковый номер ключа ЭП, который не должен использоваться повторно даже в случае перегенерации ключа; **s** – признак принадлежности ключа ЭП организации, являющейся клиентом Сбербанка.

При создании первого ключа с данным кодом организации, необходимо, чтобы номер ключа был равен 0001.

Идентификатор ключа создастся автоматически, но его можно отредактировать, чтобы сделать более информативным. Например, в автоматически сформированном идентификаторе не отражается название предприятия. Для него не хватает места, так как длина идентификатора не должна превышать 32 символов. Как вариант, можно сократить должность и убрать пробел после отчества, а затем добавить название предприятия (см. Рисунок 24).

Если требуется создать запрос на квалифицированный сертификат, необходимо установить флажок «Создать запрос на квалифицированный сертификат», нажать кнопку «Дополнительные параметры запроса на квалифицированный сертификат» и в открывшемся окне (см. Рисунок 25) заполнить поля: «Страна», «Регион», «Населённый пункт» и «СНИЛС». Заполнение полей «Адрес» и «Подразделение» не является обязательным. Для подтверждения введённых данных необходимо нажать кнопку **OK**, для отказа от продолжения процесса создания запроса на квалифицированный сертификат – нажать кнопку **Отмена** и снять флажок «Создать запрос на квалифицированный сертификат».

Для подтверждения введённых на втором шаге работы мастера данных (см. Рисунок 23) следует нажать кнопку **Далее>**, для возвращения к предыдущему шагу работы мастера – кнопку **<Назад**, для отказа от продолжения процесса генерации ключей – кнопку **Отмена**.

На третьем шаге работы мастера (см. Рисунок 41) следует указать место хранения мастер-ключа или создать новый мастер-ключ.

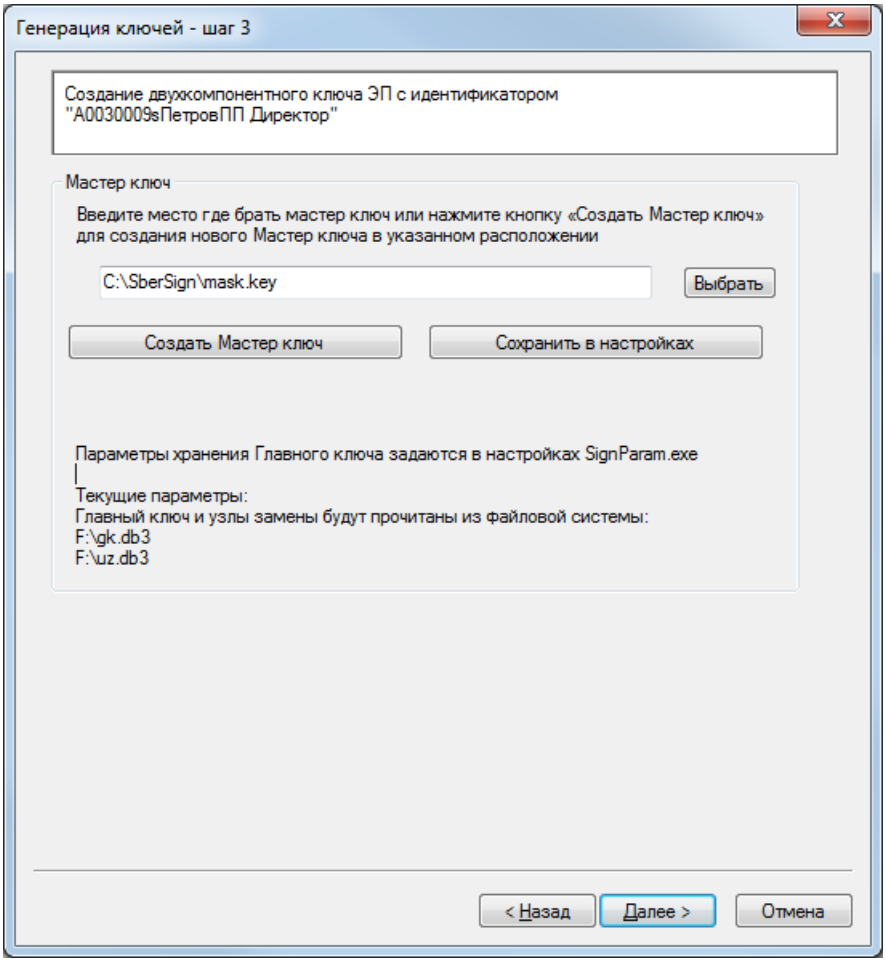

Рисунок 41 – Выбор места для записи закрытого ключа ЭП

Для того чтобы указать место хранения мастер-ключа, следует нажать кнопку **Выбрать,** затем в открывшемся окне Windows Explorer выбрать каталог, указать нужное имя файла и нажать кнопку **Открыть**.

Для того чтобы создать новый мастер-ключ, необходимо нажать кнопку **Создать Мастер ключ**. В открывшемся окне с сообщением о сохранении пути к файлу закрытого ключа (см. Рисунок 42) следует нажать кнопку **OK**.

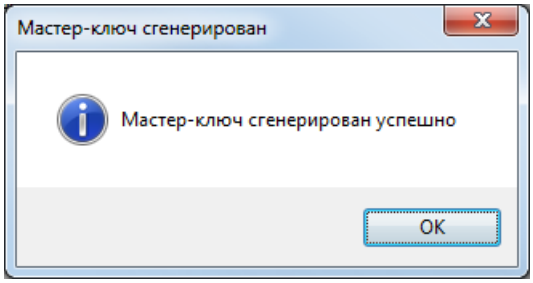

Рисунок 42 – Сообщение о создании мастер-ключа

Для того чтобы в дальнейшем выбранное место предлагалось для записи мастер-ключа по умолчанию, следует нажать кнопку **Сохранить в настройках**, и в открывшемся окне с сообщением о сохранении пути к файлу мастер-ключа (см. Рисунок 43) нажать кнопку **OK**.

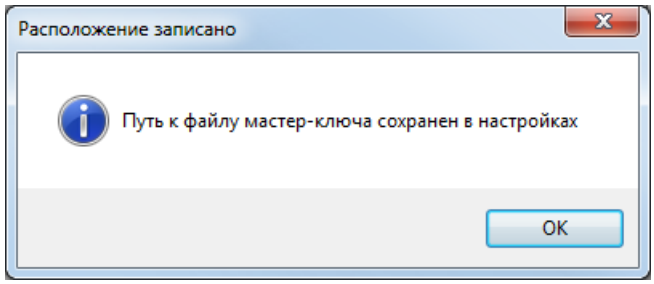

Рисунок 43 – Сообщение о сохранении пути к файлу мастер-ключа

На четвёртом шаге работы мастера (см. Рисунок 44) следует выбрать место, куда будет записана основная компонента двухкомпонентного закрытого ключа ЭП.

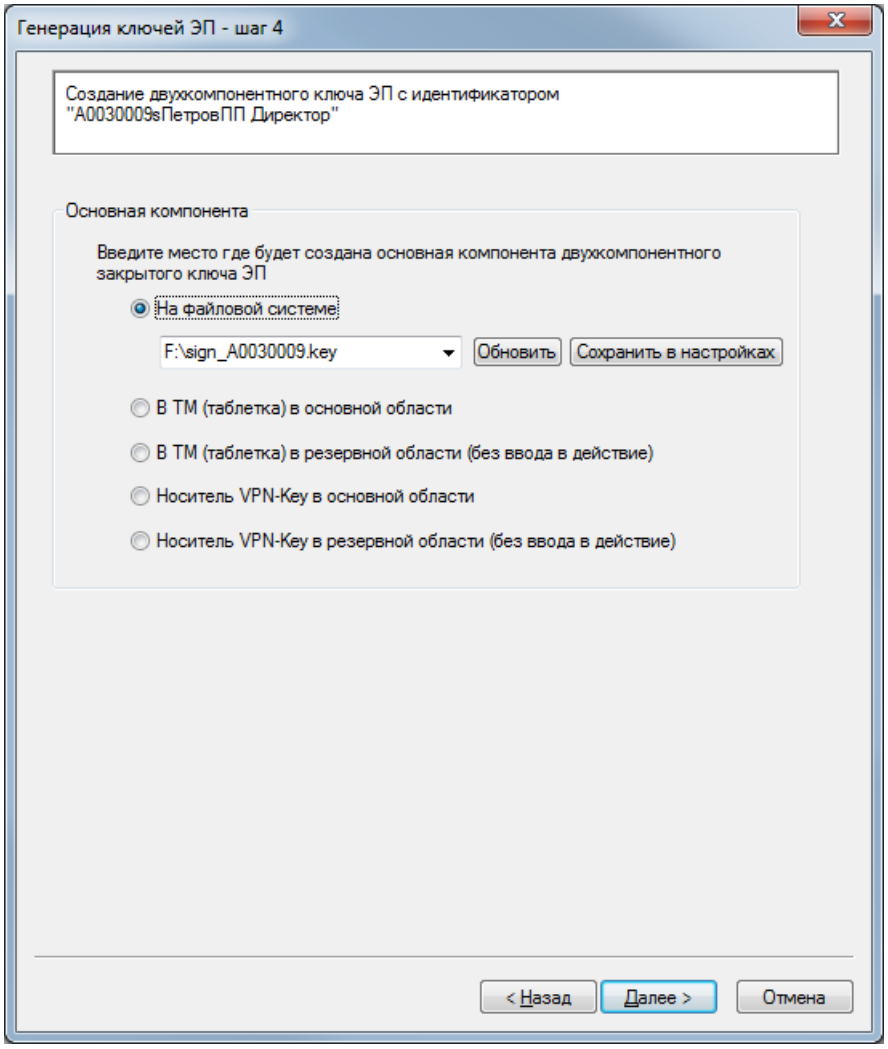

Рисунок 44 – Выбор места для записи основной компоненты двухкомпонентного закрытого ключа ЭП

Если в качестве места для записи основной компоненты двухкомпонентного закрытого ключа ЭП выбран вариант «На файловой системе», то необходимо указать конкретное место для записи основной компоненты. Для того чтобы в дальнейшем выбранное место предлагалось для записи основной компоненты двухкомпонентного закрытого ключа ЭП по умолчанию, следует нажать кнопку **Сохранить в настройках**, и в открывшемся окне с сообщением о сохранении пути к файлу основной компоненты (см. Рисунок 28) нажать кнопку **OK**.

На пятом шаге работы мастера (см. Рисунок 45) следует выбрать место, куда будет записан открытый ключ ЭП и параметры генерации ключа.

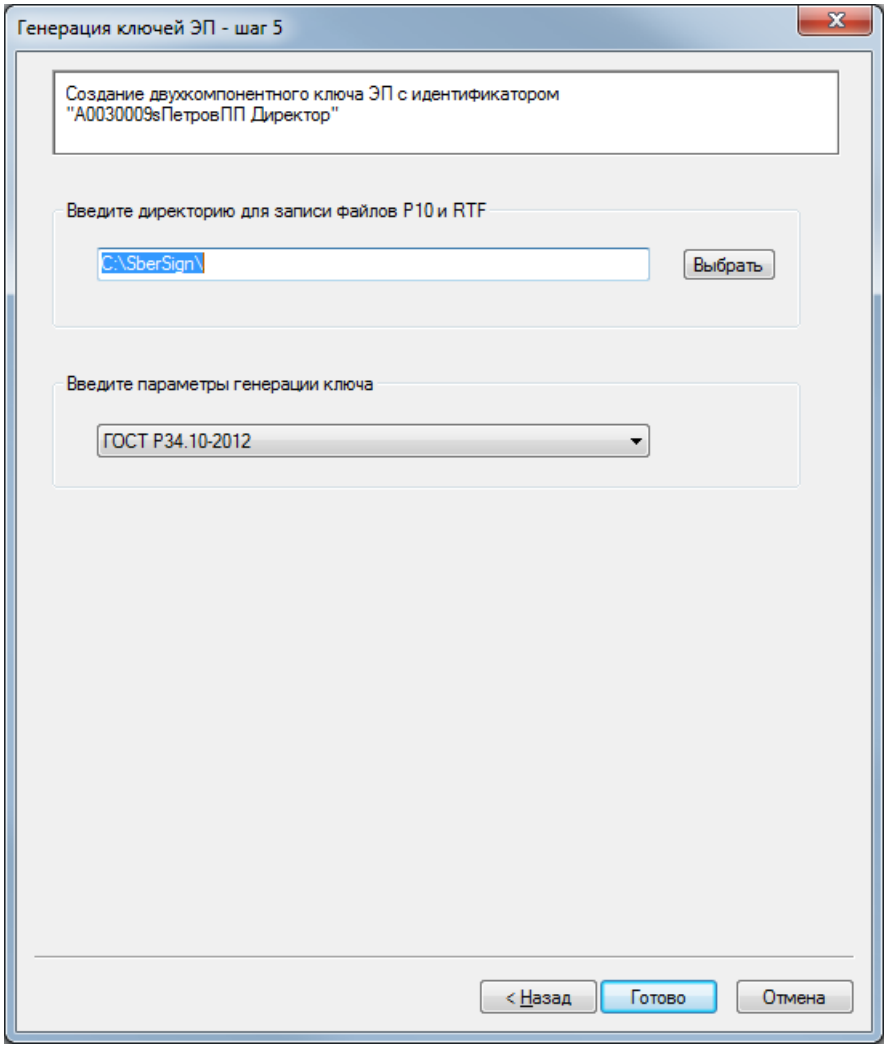

Рисунок 45 – Выбор места для записи открытого ключа ЭП

Для того чтобы выбрать параметры генерации ключа, необходимо щёлкнуть стрелку в правой части поля и выбрать нужные параметры из выпадающего списка.

Для подтверждения выбора места для записи открытого ключа ЭП следует нажать кнопку **Готово**. После этого в зависимости от сделанного выбора открытый ключ, сертификат открытого ключа или запрос на выдачу сертификата сохраняется в виде файла в указанной папке на жёстком диске или флэш-накопителе. Данный файл предназначен для передачи в удостоверяющий центр Сбербанка для его сертификации (установления принадлежности) и регистрации. Для возвращения к предыдущему шагу работы мастера следует нажать кнопку **<Назад**, для отказа от продолжения процесса генерации ключей – кнопку **Отмена**.

В открывшемся окне с сообщением об успешном создании ключей ЭП (см. Рисунок 34) следует нажать кнопку **OK**.

В открывшемся окне MS Word с проектом заявления на изготовление сертификата ключа проверки ЭП следует проверить правильность данных, при необходимости внести исправления и сохранить заявление в файл. Этот файл должен быть распечатан в трёх экземплярах, заверен соответствующими подписями, оттиском печати и передан вместе с файлом открытого ключа в ПАО «Сбербанк России».

4.6.3.2 Генерация ключевой пары с двухкомпонентным закрытым ключом с использованием приложения создания ключей

Для того чтобы создать ключи ЭП с использованием приложения создания ключей, необходимо при настройке параметров указать приложение создания ключей в качестве режима генерации ключей (см. раздел 4.6.1). Если мастер ключ зашифрован на главном ключе, необходимо указать расположение главного ключа (см. раздел 4.3.2).

При необходимости печати открытых ключей следует также указать расположение шаблона печати открытых ключей (см. раздел 4.6.1).

Для того чтобы создать новую ключевую пару и запрос на сертификат ключа проверки электронной подписи в меню выбора компонентов (см. Рисунок 5) необходимо выбрать пункт **Генерация ключей**.

В открывшемся окне приложения создания ключей следует перейти на вкладку «Ключи ЭП на Мастер-ключе» (см. Рисунок 46).

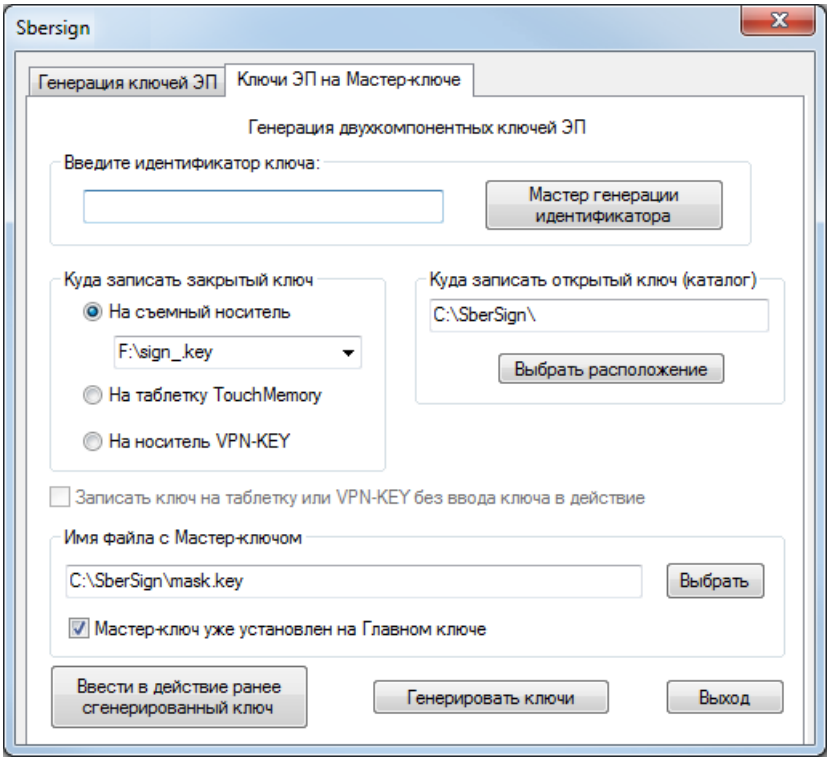

Рисунок 46 – Генерация двухкомпонентных ключей с использованием приложения создания ключей

Для генерации ключевой пары необходимо ввести идентификатор ключа ЭП в поле «Введите идентификатор ключа».

Идентификатор ключа ЭП не может состоять более чем из 32 символов (включая пробелы) и должен соответствовать формату: **YYYYNNNNsФИО должность организация**, где **YYYY** – уникальный четырехразрядный буквенно-цифровой код организации - клиента Сбербанка России, присваиваемый автоматизированной системой корневого Удостоверяющего центра ОАО «Сбербанк России»; **NNNN** – уникальный для каждого Участника системы ЭДО четырехразрядный порядковый номер ключа ЭП, который не должен использоваться повторно даже в случае перегенерации ключа; **s** – признак принадлежности ключа ЭП организации, являющейся клиентом Сбербанка.

При создании первого ключа ЭП с данным кодом организации, необходимо, чтобы номер ключа был равен 0001.

Приложение создания ключей позволяет формировать идентификатор ключа ЭП автоматически. Для этого необходимо нажать кнопку «Мастер генерации идентификатора» и в открывшемся окне (см. Рисунок 39) заполнить поля «Фамилия», «Имя», «Отчество»,

«Должность», «E-mail», «Наименование организации», «Код организации (КУЦ)», «ИНН», «ОГРН». Поле «Порядковый номер ключа» заполняется автоматически.

Идентификатор ключа ЭП создастся автоматически, но его можно отредактировать, чтобы сделать более информативным. Например, в автоматически сформированном идентификаторе не отражается название предприятия. Для него не хватает места, так как длина идентификатора не должна превышать 32 символов. Как вариант, можно сократить должность и убрать пробел после отчества, а затем добавить название предприятия (см. Рисунок 24).

Для подтверждения выбора идентификатора ключа ЭП следует нажать кнопку **Сохранить**. В результате созданный идентификатор будет отображён в поле «Введите идентификатор ключа» (см. Рисунок 38). Для отказа от создания нового идентификатора ключа ЭП следует нажать кнопку **Отмена.**

Далее для генерации ключевой пары необходимо выполнить следующие действия:

- Выбрать место, куда будет записан закрытый ключ ЭП.
- Выбрать место, куда будет записан открытый ключ ЭП.
- В случае создания резервного ключа ЭП на носителе TouchMemory или VPN-KEY установить флажок «Записать ключ на таблетку или VPN-KEY без ввода ключа в действие».
- В поле «Имя файла с Мастер-ключом» указать путь к мастер-ключу. По умолчанию флажок «Мастер ключ уже установлен на Главном ключе» установлен. Не следует снимать его без необходимости.
- Нажать кнопку **Генерировать ключи**.

В открывшемся окне с сообщением об успешном создании ключей ЭП (см. Рисунок 34) следует нажать кнопку **OK.**

4.7 Ввод в действие ключа ЭП

Если при генерации ключей ЭП в качестве места для записи закрытого ключа ЭП был выбран один из вариантов «без ввода в действие», то для использования этого ключа ЭП его необходимо ввести в действие.

Если в качестве режима генерации ключей указан мастер генерации ключей (см. раздел 4.6.1), Для того чтобы ввести в действие ранее созданный ключ ЭП, следует в меню выбора компонентов (см. Рисунок 5) выбрать пункт **Генерация ключей.**

Если в качестве режима генерации ключей указан мастер генерации ключей (см. раздел 4.6.1), следует нажать кнопку **Ввести в действие ранее сгенерированный ключ** в окне выбора типа создаваемого ключа ЭП (см. Рисунок 22).

Если в качестве режима генерации ключей указано приложение создания ключей (см. раздел 4.6.1), следует нажать кнопку **Ввести в действие ранее сгенерированный ключ** в окне приложения создания ключей (см. Рисунок 38).

В открывшемся окне выбора носителя ключа для ввода в действие (см. Рисунок 47) следует выбрать нужный тип носителя и нажать кнопку **ОК**. Для отказа от ввода ключа в действие следует нажать кнопку **Отмена**.

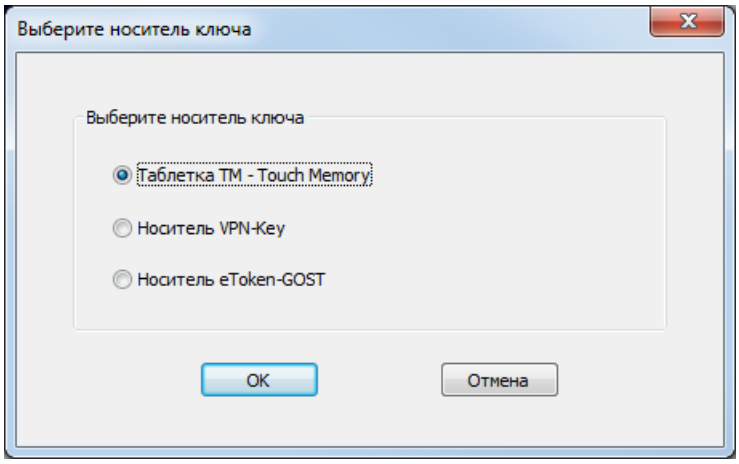

Рисунок 47 – Выбор носителя ключа для ввода в действие

После появления соответствующего предложения (см. Рисунок 48) необходимо предъявить устройство, на котором находится вводимый в действие ключ или нажать кнопку **Отмена** для отказа от ввода ключа в действие.

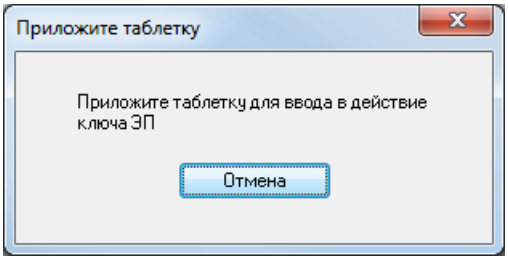

Рисунок 48 – Предложение предъявить устройство для ввода ключа в действие

При наличии на предъявленном носителе основного ключа появится окно с предупреждением о том, что данный ключ будет заменён на вводимый в действие (см. Рисунок 49).

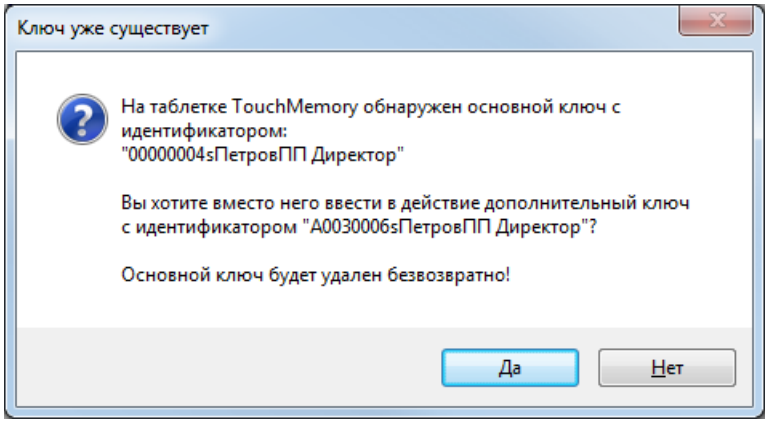

Рисунок 49 – Предупреждение о замене основного ключа

Для отказа от удаления имеющегося основного ключа необходимо нажать кнопку **Нет**, для подтверждения удаления основного ключа и ввода в действие нового ключа необходимо нажать кнопку **Да** и в открывшемся окне с сообщением об успешном вводе ключа в действие (см. Рисунок 50) нажать кнопку **ОК**.

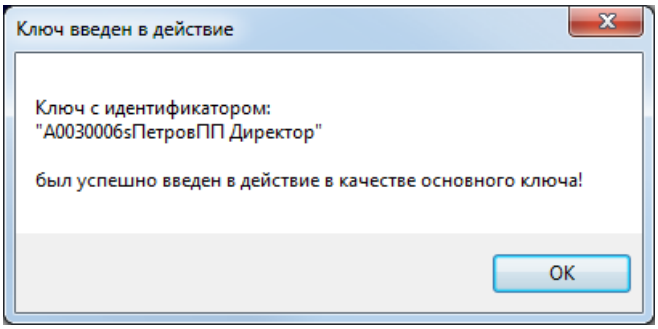

Рисунок 50 – Сообщение об успешном вводе ключа в действие

4.8 Создание ЭП

4.8.1 Настройка параметров создания ЭП

Для того чтобы изменить значения параметров создания ЭП, необходимо в меню выбора компонентов (см. Рисунок 5) выбрать пункт **Параметры Sbersign** и в открывшемся окне настройки параметров SberSign 6.1 (см. Рисунок 7 для варианта исполнения 1 или Рисунок 8 для варианта исполнения 2) перейти на вкладку «Создание ЭП» (см. Рисунок 51).

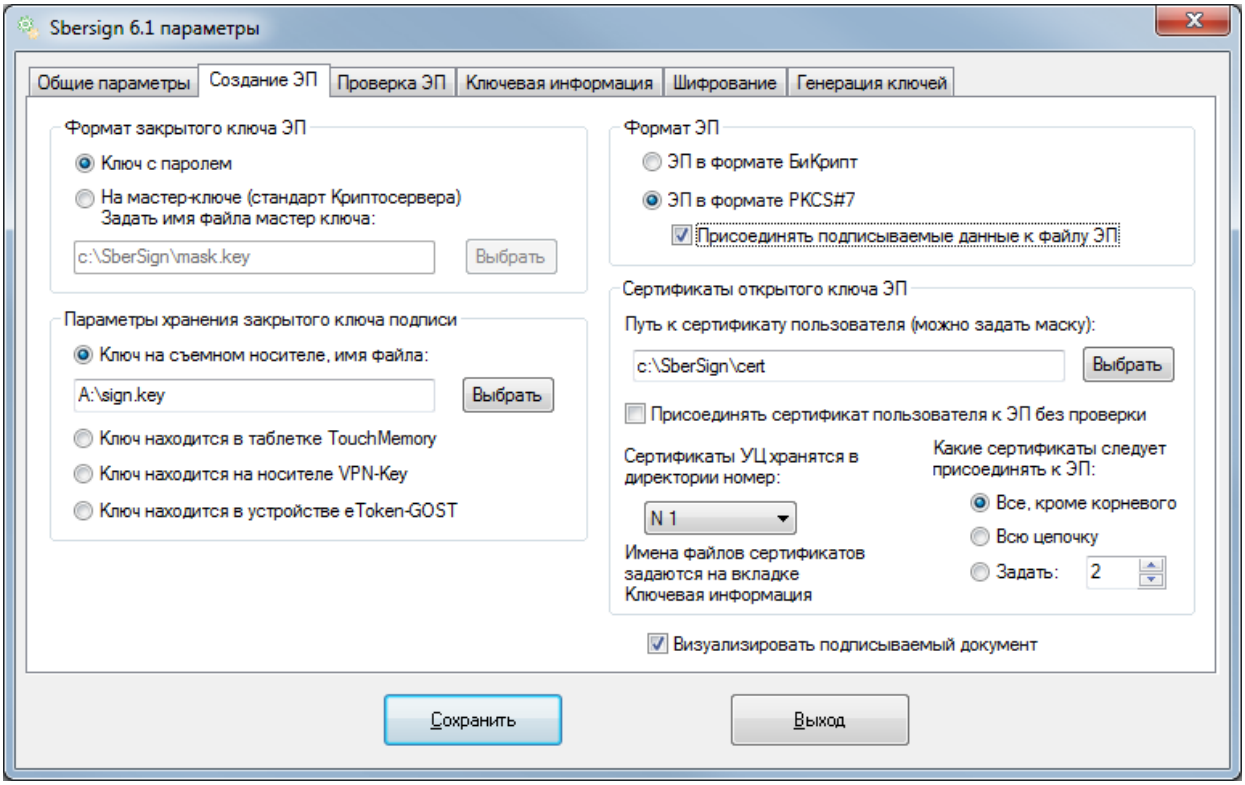

Рисунок 51 – Настройка параметров создания ЭП

4.8.1.1 Выбор типа ключа ЭП

Для того чтобы выбрать в качестве используемого ключа ЭП однокомпонентный ключ, следует в окне настройки параметров создания ЭП (см. Рисунок 51) в секции «Формат закрытого ключа ЭП» выбрать вариант «Ключ с паролем».

Для того чтобы выбрать в качестве используемого ключа ЭП двухкомпонентный ключ, следует в окне настройки параметров создания ЭП (см. Рисунок 51) выполнить следующие действия:

- В секции «Формат закрытого ключа ЭП» выбрать вариант «На мастер-ключе (стандарт Криптосервера)».
- Нажать кнопку **Выбрать** справа от поля «Задать имя файла мастер ключа».
- В открывшемся окне Windows Explorer выбрать каталог, указать файл мастер-ключа и нажать кнопку **Открыть.**
- Нажать кнопку **Сохранить**.

4.8.1.2 Выбор формата ЭП

В SberSign 6.1 предусмотрено два формата электронной подписи: Бикрипт и PKCS#7.

Для того чтобы электронная подпись создавалась в формате Бикрипт, необходимо в окне настройки параметров создания ЭП (см. Рисунок 51) в секции «Формат ЭП» выбрать вариант «ЭП в формате БиКрипт».

По умолчанию электронная подпись в формате Бикрипт записывается в подписываемый файл. Для того чтобы электронная подпись в формате Бикрипт записывалась в отдельный файл (и проверялась из отдельного файла), необходимо в окне настройки параметров SberSign 6.1 (см. Рисунок 7 для варианта исполнения 1 или Рисунок 8 для варианта исполнения 2) установить флажок «Отсоединить ЭП от файла».

Для того чтобы электронная подпись создавалась в формате PKCS#7, необходимо в окне настройки параметров создания ЭП (см. Рисунок 51) в секции «Формат ЭП» выбрать вариант «ЭП в формате PKCS#7».

По умолчанию электронная подпись в формате PKCS#7 записывается в отдельный файл. Для того чтобы электронная подпись в формате PKCS#7 добавлялась в подписываемый файл (и проверялась из подписанного файла), необходимо в окне настройки параметров создания ЭП (см. Рисунок 51) установить флажок «Присоединить подписываемые данные к файлу ЭП». При этом необходимо учитывать, что при таких настройках размер подписываемого файла не должен превышать 300 Мбайт.

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить**.

4.8.1.3 Выбор присоединяемой к ЭП цепочки сертификатов

В SberSign 6.1 предусмотрена возможность присоединения сертификата открытого ключа ЭП к подписи файла в формате PKCS#7. В данном режиме реализована поддержка сертификатов открытых ключей ЭП в формате X.509.

Для того чтобы присоединять сертификат к подписи файла, необходимо секции «Сертификаты открытого ключа ЭП» в поле «Путь к сертификату пользователя (можно задать маску)» указать расположение файла сертификата. Для этого следует нажать кнопку **Выбрать** и в открывшемся окне Windows Explorer выбрать каталог, указать нужное имя файла и нажать кнопку **Открыть**.

Для того чтобы присоединять к подписи файла цепочку сертификатов, необходимо указать расположение файлов сертификатов, входящих в цепочку. Для этого следует щёлкнуть стрелку в правой части поля «Сертификаты УЦ хранятся в директории номер» и выбрать из выпадающего списка номер нужной директории сертификатов на вкладке «Ключевая информация» (см. раздел 4.3.3).

По умолчанию к подписи файла в формате PKCS#7 присоединяется вся цепочка сертификатов кроме корневого.

Для того чтобы присоединять к подписи файла всю цепочку сертификатов, включая корневой сертификат, необходимо в секции «Сертификаты открытого ключа ЭП» выбрать вариант «Всю цепочку».

Для того чтобы присоединять к подписи файла цепочку сертификатов определённой длины, необходимо в секции «Сертификаты открытого ключа ЭП» выбрать вариант «Задать» и в поле справа указать длину цепочки сертификатов.

Для того чтобы не присоединять сертификаты к подписи файла, необходимо в секции «Сертификаты открытого ключа ЭП» выбрать вариант «Задать» и в поле справа задать значение 0.

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить**.

4.8.1.4 Выбор ключа ЭП

В SberSign 6.1 предусмотрена возможность выбора места хранения закрытого ключа ЭП. Выбор производится в секции «Параметры хранения закрытого ключа подписи» окна настройки параметров создания ЭП (см. Рисунок 51).

Для того чтобы указать в качестве места хранения закрытого ключа ЭП каталог файловой системы, необходимо выбрать вариант «Ключ на съемном носителе, имя файла», нажать кнопку **Выбрать** и в открывшемся окне Windows Explorer выбрать каталог, указать файл, содержащий закрытый ключ ЭП, и нажать кнопку **Открыть**.

Для того чтобы указать в качестве места хранения закрытого ключа ЭП устройство Touch Memory, необходимо выбрать вариант «Ключ находится в таблетке TouchMemory».

Для того чтобы указать в качестве места хранения закрытого ключа ЭП устройство VPN-Key, необходимо выбрать вариант «Ключ находится на носителе VPN-Key».

Для того чтобы указать в качестве места хранения закрытого ключа ЭП устройство eToken-GOST, необходимо выбрать вариант «Ключ находится в устройстве eToken-GOST».

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить**.

4.8.1.5 Визуализация подписываемого документа

В SberSign 6.1 предусмотрена возможность визуализации подписываемого документа.

Для того чтобы подписываемый документ отображался при формировании ЭП, необходимо в окне настройки параметров создания ЭП (см. Рисунок 51) установить флажок «Визуализировать подписываемый документ».

4.8.2 Формирование ЭП файлов

Процедура подписания файла (или группы файлов) встроена в Windows Explorer.

При использовании варианта исполнения 1 SberSign 6.1 для подписания одного файла необходимо в Windows Explorer щёлкнуть его правой кнопкой мыши и в контекстном меню файла выбрать пункт **Подписать ЭП** (см. Рисунок 52).

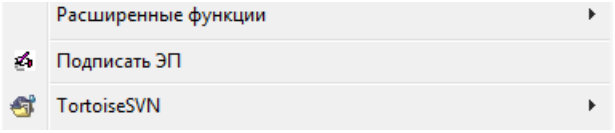

Рисунок 52 – Подписание файла для варианта исполнения 1 SberSign 6.1

При использовании варианта исполнения 1 SberSign 6.1 для подписания нескольких файлов следует выделить эти файлы и воспользоваться пунктом **Подписать ЭП** в контекстном меню.

При использовании варианта исполнения 2 SberSign 6.1 для подписания одного файла необходимо в Windows Explorer щёлкнуть его правой кнопкой мыши и в контекстном меню файла выбрать пункт **SberSign 6.1** подпункт **Подписать ЭП** (см. Рисунок 53).

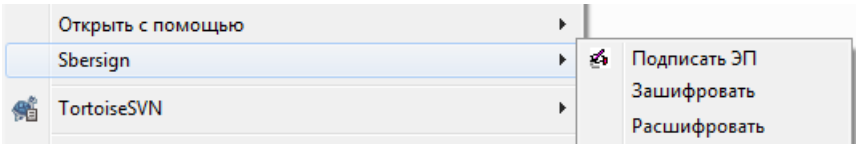

Рисунок 53 – Подписание файла для варианта исполнения 2 SberSign 6.1

При использовании варианта исполнения 2 SberSign 6.1 для подписания нескольких файлов следует выделить эти файлы и воспользоваться пунктом **SberSign 6.1** в контекстном меню.

Если при настройке параметров создания ЭП установлен флажок «Визуализировать подписываемый документ» (см. раздел 4.8.1.5), то будет запущено ассоциированное с форматом подписываемого файла приложение (например, Microsoft Word для формата .doc), в котором будет отображён подписываемый документ.

Если для формата подписываемого файла нет ассоциированного приложения, формирования ЭП в режиме визуализации невозможно, на экране появится соответствующее сообщение (см. Рисунок 54).

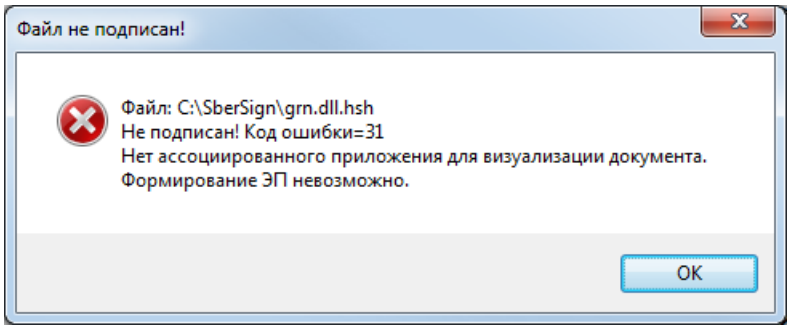

Рисунок 54 – Сообщение о невозможности формирования ЭП

Если для формата подписываемого файла имеется ассоциированное приложение, в открывшемся окне (см. Рисунок 55) следует нажать кнопку **Да** для просмотра документа или кнопку **Нет** для отказа от подписания данного документа.

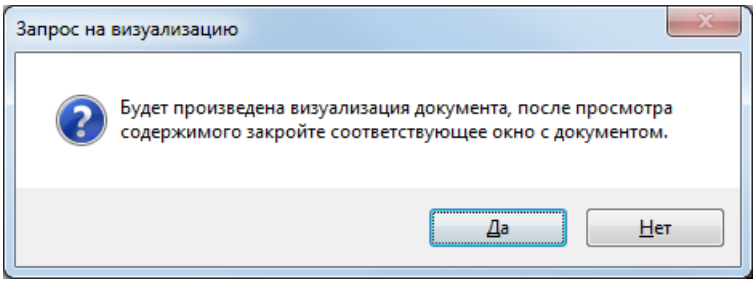

Рисунок 55 – Подтверждение визуализации документа

После ознакомления с документом следует закрыть окно с документом и в открывшемся окне (см. Рисунок 56) нажать кнопку **Да** для формирования ЭП или кнопку **Нет** для отказа от подписания данного документа.

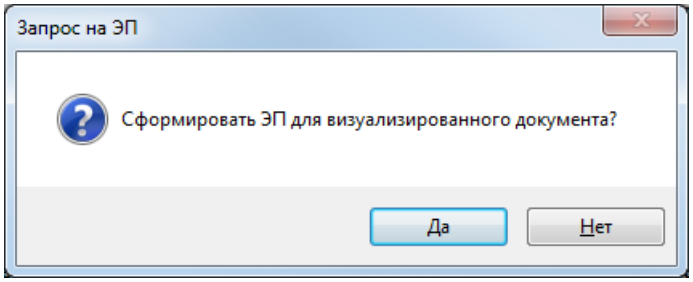

Рисунок 56 – Подтверждение формирования ЭП

Если для подписи используется однокомпонентный закрытый ключ ЭП на съёмном носителе, необходимо в открывшемся окне (см. Рисунок 57) ввести пароль закрытого ключа, назначенный в процессе генерации ключей (см. раздел 4.6).

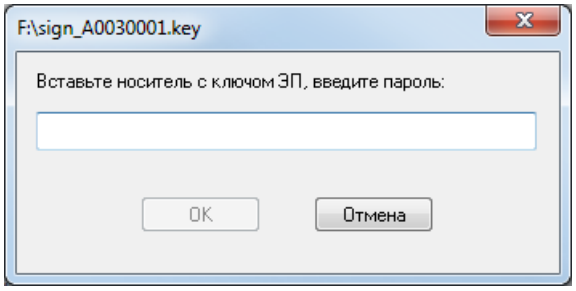

Рисунок 57 – Окно ввода пароля однокомпонентного закрытого ключа ЭП

Если для подписи используется однокомпонентный закрытый ключ ЭП на устройстве Touch Memory, после появления соответствующего предложения (см. Рисунок 58) необходимо предъявить устройство, на котором находится данный ключ или нажать кнопку **Отмена** для отказа от продолжения процесса подписи.

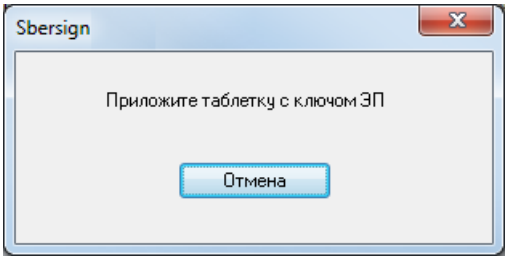

Рисунок 58 – Предложение предъявить устройство Touch Memory

Затем в открывшемся окне с сообщением об успешном завершении процесса подписи файла (см. Рисунок 59) необходимо нажать кнопку **ОК**.

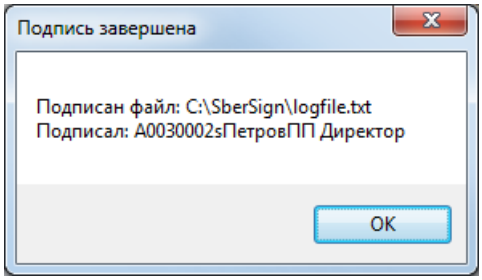

Рисунок 59 – Сообщение об успешном завершении процесса подписи файла

4.9 Проверка ЭП

4.9.1 Настройка параметров проверки ЭП

Для того чтобы изменить значения параметров проверки ЭП, необходимо в меню выбора компонентов (см. Рисунок 5) выбрать пункт **Параметры Sbersign** и в открывшемся окне настройки параметров SberSign 6.1 (см. Рисунок 7 для варианта исполнения 1 или Рисунок 8 для варианта исполнения 2) перейти на вкладку «Проверка ЭП» (см. Рисунок 60).

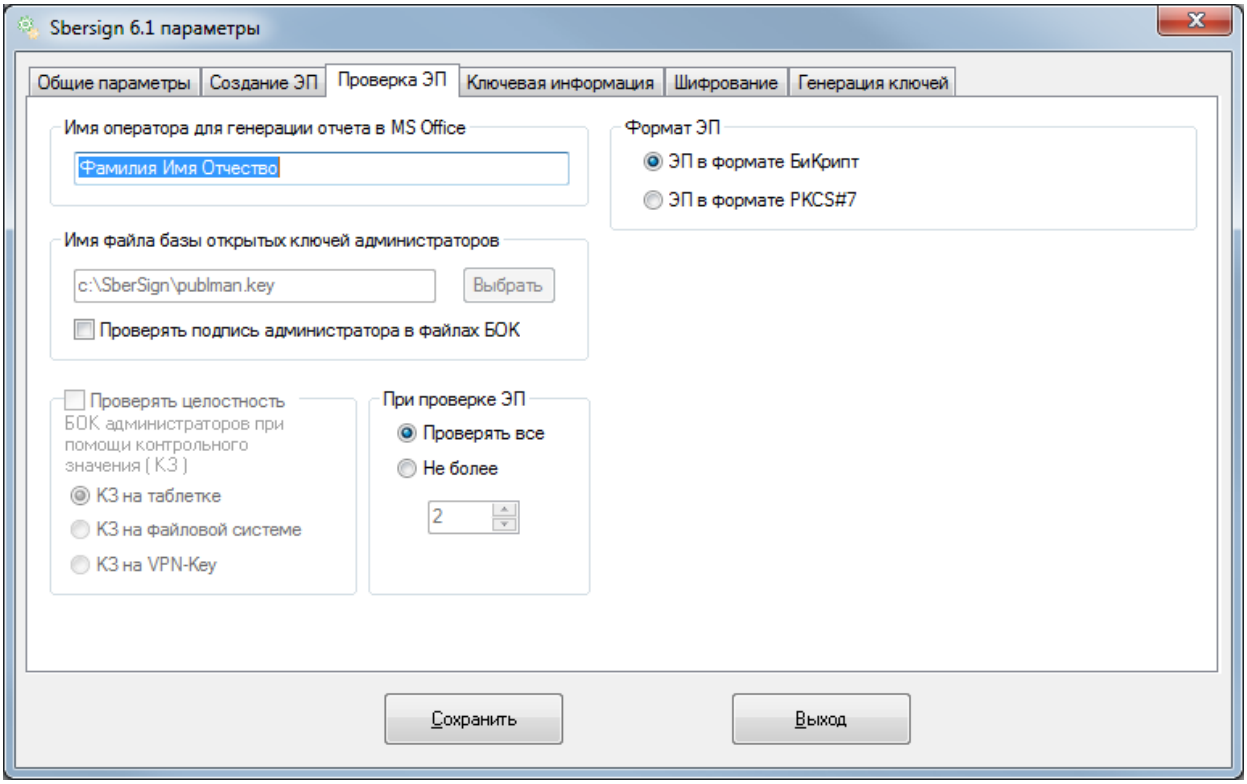

Рисунок 60 – Настройка параметров проверки ЭП

4.9.1.1 Выбор формата ЭП

В SberSign 6.1 предусмотрено два формата электронной подписи: Бикрипт и PKCS#7.

Если предполагается проверять электронную подпись в формате Бикрипт, необходимо в окне настройки параметров проверки ЭП (см. Рисунок 60) в секции «Формат ЭП» выбрать вариант «ЭП в формате БиКрипт».

Если предполагается проверять электронную подпись в формате PKCS#7, необходимо в окне настройки параметров проверки ЭП (см. Рисунок 60) в секции «Формат ЭП» выбрать вариант «ЭП в формате PKCS#7».

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить**.

4.9.1.2 Выбор количества проверяемых подписей

Файл может быть подписан несколькими подписями. По умолчанию проверяются все подписи.

Если проверять все подписи не требуется, можно ограничить число проверяемых подписей. Для этого необходимо в окне настройки параметров проверки

ЭП (см. Рисунок 60) в секции «При проверке ЭП» выбрать вариант «Не более» и в поле ниже указать число проверяемых подписей.

Для того чтобы проверять все подписи, необходимо в секции «При проверке ЭП» выбрать вариант «Проверять все».

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить**.

4.9.1.3 Настройка имени оператора для отчёта о проверке ЭП

Для того чтобы задать имя оператора, которое будет указываться в отчёте о проверке ЭП (см. раздел 4.9.2), необходимо ввести его в окне настройки параметров проверки ЭП (см. Рисунок 60) в секции «Имя оператора для генерации отчета в MS Office» и нажать кнопку **Сохранить**.

4.9.1.4 Проверка целостности файлов БОК

В SberSign 6.1 предусмотрена возможность проверять целостность БОК в режиме проверки электронной подписи в формате Бикрипт (см. раздел 4.9.1.1).

Для того чтобы при проверке ЭП в формате Бикрипт проверять целостность БОК, необходимо в окне настройки параметров проверки ЭП (см. Рисунок 60) в секции «Имя файла базы открытых ключей администраторов» выполнить следующие действия:

- Установить флажок «Проверять подпись администратора в файлах БОК».
- Нажать кнопку **Выбрать**.
- В открывшемся окне Windows Explorer выбрать каталог, указать файл БОК администраторов и нажать кнопку **Открыть**.

Предусмотрена также возможность проверять целостность базы открытых ключей администраторов.

Для того чтобы при проверке целостности БОК проверять целостность БОК администраторов, необходимо выполнить следующие действия:

- Вычислить контрольное значение (см. раздел 4.9.1.5) для БОК администраторов, указанной в секции «Имя файла базы открытых ключей администраторов».

- В окне настройки параметров проверки ЭП (см. Рисунок 60) установить флажок «Проверять целостность БОК администраторов при помощи контрольного значения (КЗ)».
- Выбрать носитель, на котором записано контрольное значение файла БОК администраторов.

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить**.

4.9.1.5 Контроль целостности базы администраторов криптоключей

В SberSign 6.1 предусмотрена возможность проверять целостность БОК администраторов с помощью контрольного значения (КЗ). Режим проверки по базе открытых ключей администраторов не функционирует при проверке ЭП в формате PKCS#7.

Для того чтобы вычислить контрольное значение, необходимо выполнить следующие действия:

- В меню выбора компонентов (см. Рисунок 5) выбрать пункт **Параметры Sbersign** и в открывшемся окне настройки параметров SberSign 6.1 (см. Рисунок 7 для варианта исполнения 1 или Рисунок 8 для варианта исполнения 2) перейти на вкладку «Генерация ключей» (см. Рисунок 20).
- На этой вкладке выбрать носитель, на который следует записать контрольное значение.
- Нажать кнопку **Выбрать** справа от поля «Файл, для которого будет вычислено КЗ».
- В открывшемся окне Windows Explorer выбрать каталог, указать файл БОК администраторов, для которого будет вычислено КЗ, и нажать кнопку **Открыть**.
- Нажать кнопку **Вычислить КЗ**.

4.9.2 Проверка подписи для документов в Windows Explorer

Процедура проверки ЭП файла встроена в Windows Explorer. Для проверки ЭП файла необходимо в Windows Explorer щёлкнуть его правой кнопкой мыши и в контекстном меню файла выбрать пункт **Свойства** и перейти на вкладку «Электронная подпись» (см. Рисунок 61). Эта вкладка доступна, если у файла имеется хотя бы одна ЭП.

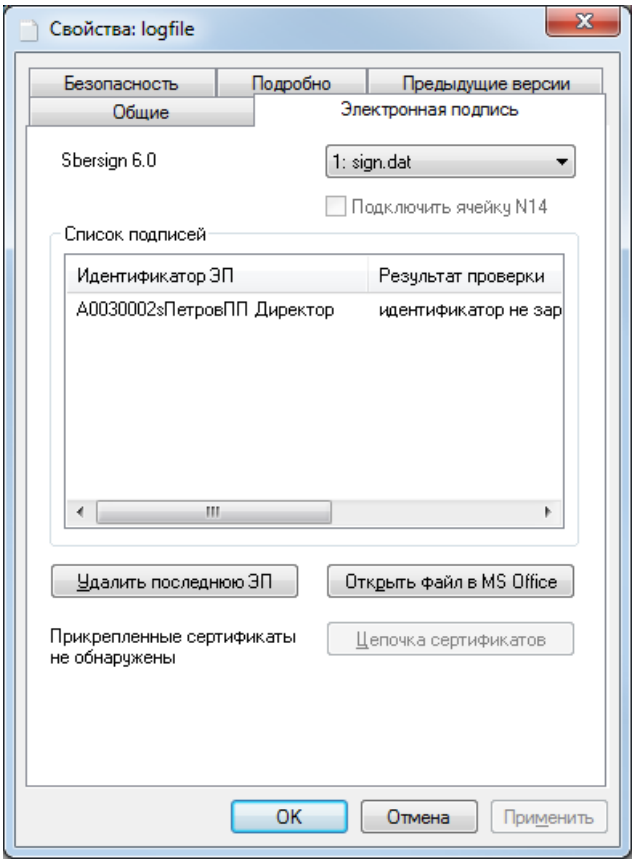

Рисунок 61 – Вкладка «Электронная подпись»

На данной вкладке отображаются сообщения о результатах проверки всех обнаруженных ЭП для данного файла.

Электронная подпись в формате Бикрипт по умолчанию проверяется с помощью БОК sign.dat, расположение которой указано в ячейке №1 на вкладке «Ключевая информация» (см. раздел 4.3.3). Для того чтобы выбрать другую БОК для проверки подписи, необходимо щёлкнуть стрелку в правой части поля и выбрать нужную БОК из выпадающего списка. При этом необходимо, чтобы новая БОК была указана в одной из строк на вкладке «Ключевая информация» (см. раздел 4.3.3). Подпись будет перепроверена сразу же после выбора новой БОК.

Электронная подпись в формате PKCS#7 по умолчанию проверяется с помощью сертификатов, расположение которых указано в ячейке №2 на вкладке «Ключевая информация» (см. раздел 4.3.3). Дополнительное место хранения сертификатов для проверки ЭП может быть указано в строке №14. Для того чтобы проверять подпись с

помощью этих дополнительных сертификатов, необходимо установить флажок «Подключить ячейку №14».

Дополнительно предусмотрен режим контроля целостности используемой базы (сертификатов) открытых ключей ЭП (см. раздел 4.9.1.5). В случае включения данного режима при проверке ЭП файла с использованием базы (сертификатов) открытых ключей сначала производится проверка ЭП под базой, и в случае положительного результата проверки проверяется подпись под файлом. При этом на экран выводятся результаты проверки ЭП файла. Если целостность базы (сертификатов) открытых ключей нарушена, на экран выводится соответствующее сообщение об ошибке.

4.9.3 Проверка подписи для документов в Microsoft Office

Для документов, созданных с использованием приложений Word и Excel из пакета Microsoft Office, предусмотрена возможность вывода результатов проверки ЭП непосредственно в текст документа для получения распечатки с результатами проверки ЭП.

Для того чтобы внести результаты проверки ЭП в текст документа, для файлов с расширениями *.TXT, *.DOC, *.DOCX *.RTF, *.XLS, *.XLSX следует на вкладке «Электронная подпись» (см. Рисунок 61) нажать кнопку **Открыть файл в MS Office**.

При наличии установленного пакета Microsoft Office проверяемый документ с добавлением результатов проверки ЭП будет открыт с помощью соответствующего офисного приложения.

Пример:

```
Проверка ЭП
Файл:       00CA0006.rtf
Дата/время проверки:    07.08.2016 17:12:09
Библиотека подписи: ADM BICRYPT v5.0 (Stribog) 21/11/2017 R.120 (c)InfoCrypt

проверяются файлы:
C:\temp\00CA0006.rtf: подпись
A5FA0011sИвановАВ_РукМолоко33  истинная

Оператор:                              /Петров А.Б./
```

Поле «Оператор» заполняется значением, указанным в поле «Имя оператора для генерации отчета в MS Office» на вкладке «Проверка ЭП» (см. раздел 4.9.1.3).

4.10 Удаление ЭП

При подписании файла код ЭП добавляется непосредственно в конец файла, при этом внутренняя структура файла может быть нарушена. Для восстановления

первоначального вида файла без подписи в SberSign 6.1 предусмотрена возможность удаления ЭП.

Для удаления ЭП из файла необходимо в Windows Explorer щёлкнуть его правой кнопкой мыши и в контекстном меню файла выбрать пункт **Свойства** и перейти на вкладку (см. Рисунок 61) и нажать кнопку **Удалить последнюю ЭП**. Вкладка «Электронная подпись» доступна, если у файла имеется хотя бы одна ЭП.

При использовании SberSign 6.1 совместно с ПО, которое чувствительно к изменению структуры данных, при добавлении подписи в конец файла рекомендуется использовать формат подписи PKCS#7.

4.10.1 Удаление ЭП с использованием командной строки

С использованием утилиты командной строки возможно удаление всех или указанного количества ЭП под файлами.

Для удаления ЭП в командной строке необходимо дать команду:

```
sbersign /e <имя_файла>
```

Для удаления ЭП для нескольких файлов следует указать маску файлов (например, для удаления ЭП у всех файлов в текущем каталоге следует дать команду sbersign /e *.*).

Для удаления определенного количества ЭП необходимо дать команду:

```
sbersign /e=n <имя_файла>
```

где n – количество удаляемых ЭП.

```
SBERSIGN V6.1 Copyright (C)2004,2018 InfoCrypt LTD., Moscow
удаляются подписи:
<имя_файла>
удалены n подписей
```

При использовании параметра /e в переменную ERRORLEVEL возвращается количество удалённых ЭП.