

Общество с ограниченной ответственностью «Русь-Телеком»

Утверждено

ГТКМ.00001-03 90 03-ЛУ

Утверждаю

Директор ООО «Русь-Телеком»

_____ В.Н. Затолокин

31.08.2012

М.П.

КРИПТО-ЭКСПРЕСС

Версия 1.1

Руководство пользователя

Листов 63

Инь. N подл.	Подп. и дата
Инь. N дубл.	
Взам. инв. N	
Подп. и дата	
Инь. N подл.	

Аннотация

Документ содержит подробные инструкции по использованию программного продукта «Крипто-Экспресс» версии 1.1 для Windows XP/Windows Vista/Windows Server 2003/Windows Server 2008/Windows 7/ Windows Server 2008 R2 (дата публикации: 31 августа 2012), включая настройку, выполнение сервисных функций, а также действия при возникновении внештатных ситуаций.

Документ предназначен для пользователей, которым требуется выполнение шифрования и расшифрования данных, заверение данных электронной цифровой подписью и проверка корректности ЭЦП.

Сведения о поставщике

Общество с ограниченной ответственностью "Русь-Телеком"

214019, Смоленская область, г. Смоленск, проезд Маршала Конева, д. 29

Тел: (4812)65-32-42

Факс: (4812)65-78-96

Электронная почта: info@rus-telecom.ru

Интернет-сайт: <http://rus-telecom.ru>

Содержание

1.	Термины, условные обозначения и сокращения	4
2.	Стандарты и нормативные акты	4
3.	Общие сведения	5
4.	Работа с программой	5
4.1.	Главное окно	5
4.2.	Шифрование файлов	6
4.3.	Расшифрование файлов	12
4.4.	Подписывание файлов	18
4.5.	Проверка подписей	25
4.6.	Добавление подписей к файлу	31
4.7.	Визирование подписей	38
4.8.	Удаление подписей	47
5.	Сервисные функции	53
5.1.	О программе	54
5.2.	Лицензии	54
5.3.	Обновление программы	55
5.4.	Параметры	57
6.	Руководство по устранению неполадок	63

1. Термины, условные обозначения и сокращения

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

Корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

Информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

2. Стандарты и нормативные акты

- Федеральный закон Российской Федерации от 25 марта 2011 г. N 169-ФЗ «Об электронной подписи».
- ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
- ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.
- ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование. (Разделы 1,2, п.3.1, 3.2, п.п. 3.3.1, 3.3.3, 3.3.5, Раздел 4).
- ГОСТ Р ИСО 9127-94. Системы обработки информации. Документация пользователя и информация на упаковке для потребительских программных пакетов. (п.п. 6.1, 6.3-6.5, 6.8).

3. Общие сведения

Программа «Крипто-Экспресс» версии 1.1 для Windows XP/Windows Vista/Windows Server 2003/Windows Server 2008/Windows 7/ Windows Server 2008 R2 (дата публикации: 31 августа 2012) предназначена для организаций и частных пользователей, перед которыми стоят задачи защиты и обеспечения юридической значимости различных видов электронного документооборота.

4. Работа с программой

Начать работу с программой можно одним из двух способов: запустив Крипто-Экспресс с помощью стандартного меню «Пуск» или с помощью расширения проводника Windows.

Для запуска программы через стандартное меню выберите в меню Пуск пункт «Все программы→Русь-Телеком→Крипто-Экспресс». Откроется главное окно программы.

Для начала работы с помощью расширения проводника Windows выделите обрабатываемый файл или несколько файлов и нажмите правую кнопку мыши. В контекстном меню выберите «Крипто-Экспресс» и одно из действий для обработки файла (Рисунок 1).

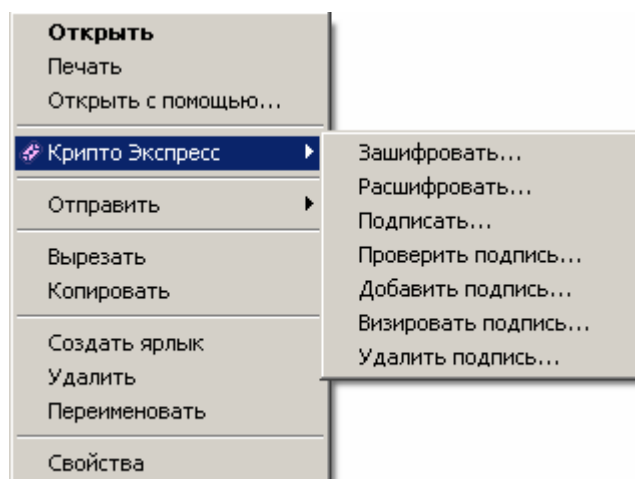


Рисунок 1. Запуск программы из контекстного меню

Откроется окно мастера обработки файлов.

4.1. Главное окно

Главное окно программы показывает (Рисунок 2).

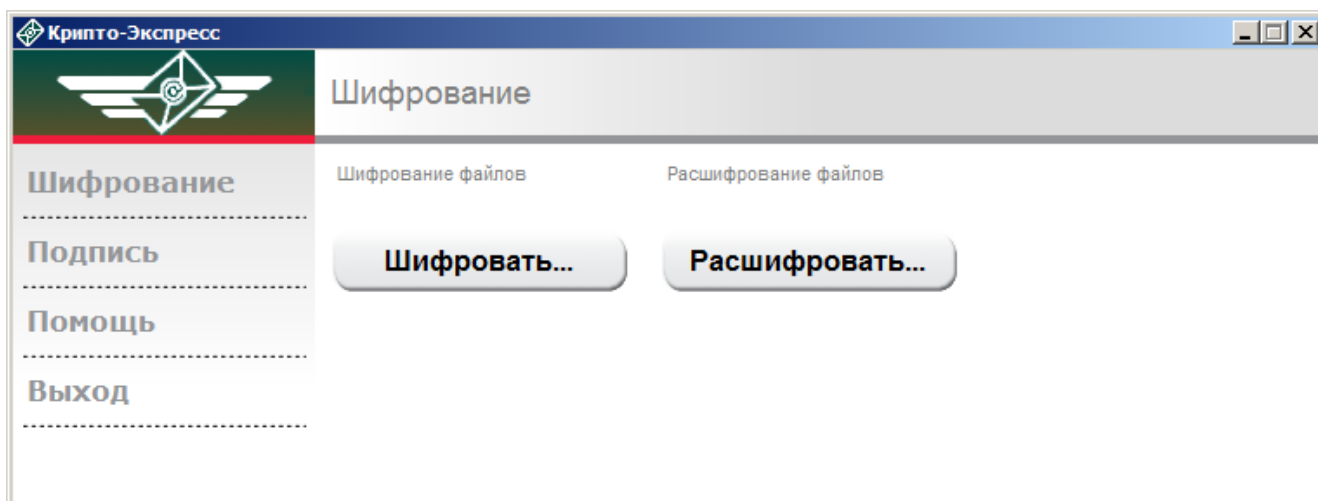


Рисунок 2. Главное окно

В левой части окна расположено меню, содержащее типы действий, которые можно произвести с файлами документов, и команды для управления программой.

Справа отображаются кнопки действий, содержание этой области зависит от выбранного пункта меню.

4.2. Шифрование файлов

Чтобы зашифровать файлы, необходимо предварительно выполнить следующие действия:

- выбрать файлы для шифрования;
- выбрать один или несколько сертификатов получателей зашифрованных данных.

Для того, чтобы зашифровать файл, выберите в меню главного окна программы (Рисунок 2) пункт «Шифрование» и нажмите кнопку «Зашифровать», либо через меню проводника Windows (Рисунок 1) нажмите правую кнопку мыши и выберите «Крипто-Экспресс → Зашифровать...», предварительно выделив файл или несколько файлов, которые нужно обработать.

Откроется окно приветствия Мастера шифрования данных (Рисунок 3).

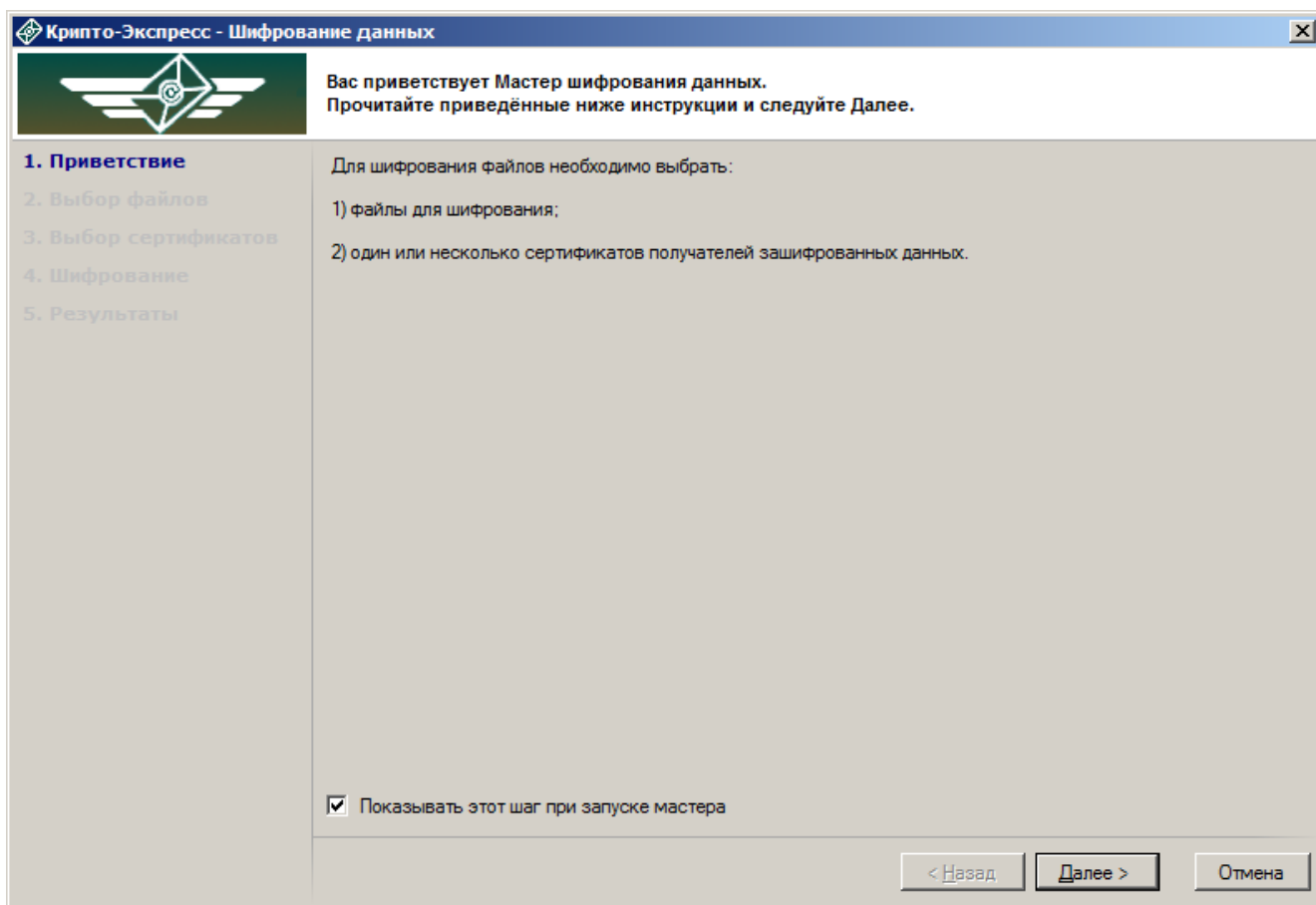


Рисунок 3. Приветствие Мастера шифрования данных

Чтобы больше не выводить приветствие, уберите галочку внизу формы.

Нажмите «Далее», чтобы перейти к шагу выбора файлов (Рисунок 4).

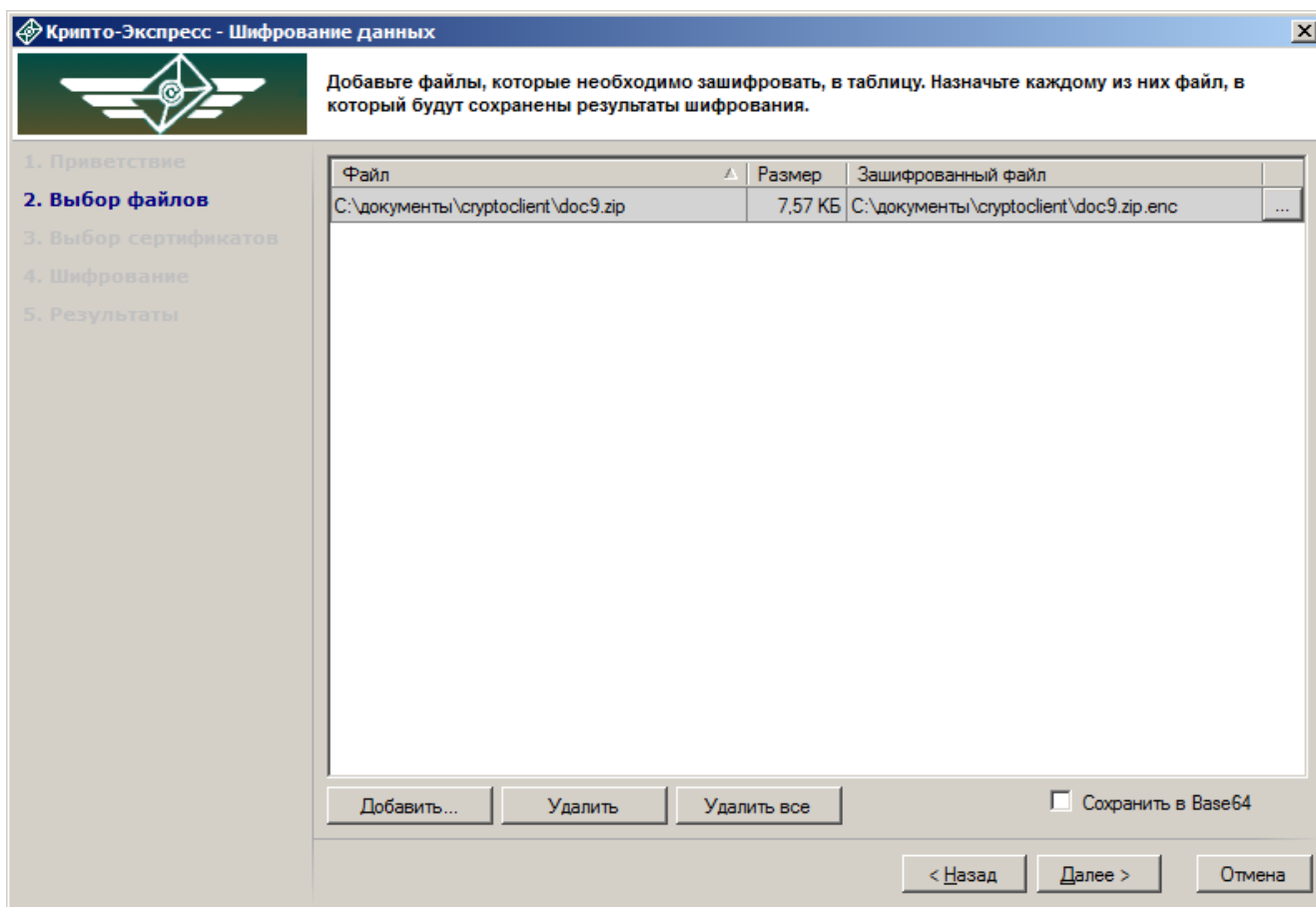


Рисунок 4. Выбор файлов для шифрования

На этом шаге нужно добавить файлы, которые будут зашифрованы. Если файлы уже были выбраны, они отобразятся в таблице окна. Если файлы ещё не были выбраны или необходимо добавить ещё несколько файлов для шифрования, воспользуйтесь кнопкой «Добавить» под таблицей, которая откроет стандартное окно выбора файлов.

Чтобы удалить ненужные файлы из обработки или полностью очистить таблицу, выделите строки с файлами и нажмите «Удалить» или «Удалить все» соответственно.

В таблице выбора файлов выводятся следующие сведения:

- имя шифруемого файла и его расположение на жестком диске;
- размер файла;
- имя файла для сохранения результатов шифрования и место на жестком диске, куда он будет сохранён.

Имя шифруемого файла и путь для сохранения можно изменить, нажав на кнопку в правой части строки и сделав необходимые изменения через стандартный диалог сохранения.

Если зашифрованный файл с таким именем уже существует в папке, куда сохраняется результат шифрования (в поле «Зашифрованный файл» выведено предупреждение об этом), рекомендуется выбрать другую папку или изменить имя зашифрованного файла.

По умолчанию зашифрованные файлы сохраняются в кодировке DER, но при необходимости (например, если планируется передача файлов по сети), можно сохранить их в кодировке Base64, поставив отметку «Сохранить в Base64» в правой нижней части окна.

Для перехода к шагу выбора сертификатов нажмите кнопку «Далее».

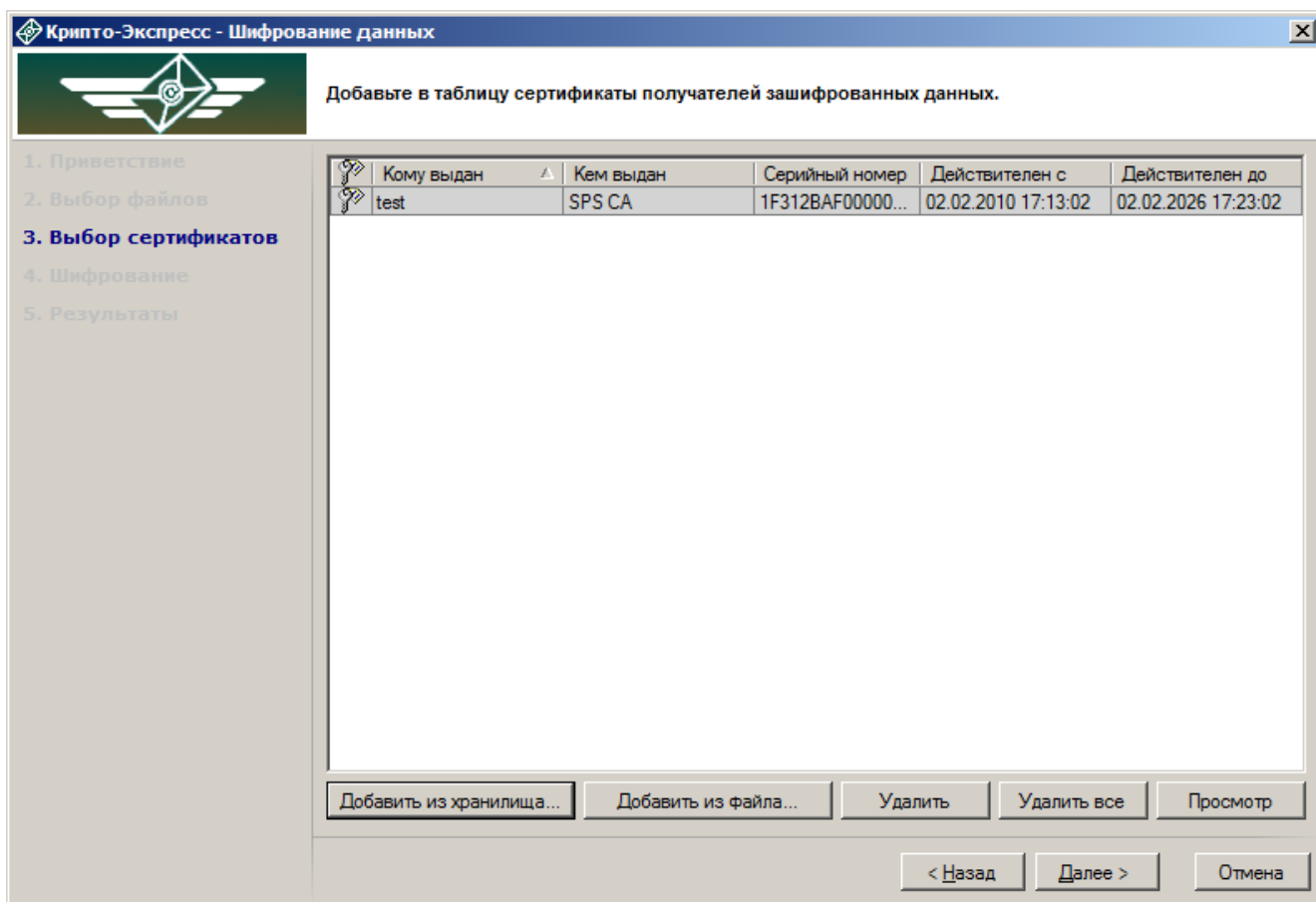


Рисунок 5. Выбор сертификатов

На этом шаге необходимо выбрать сертификаты получателей зашифрованных данных. Их можно добавить в таблицу из хранилища сертификатов или из файла.

Для того чтобы добавить сертификат из хранилища, нажмите кнопку «Добавить из хранилища». Откроется форма выбора сертификатов (Рисунок 6).

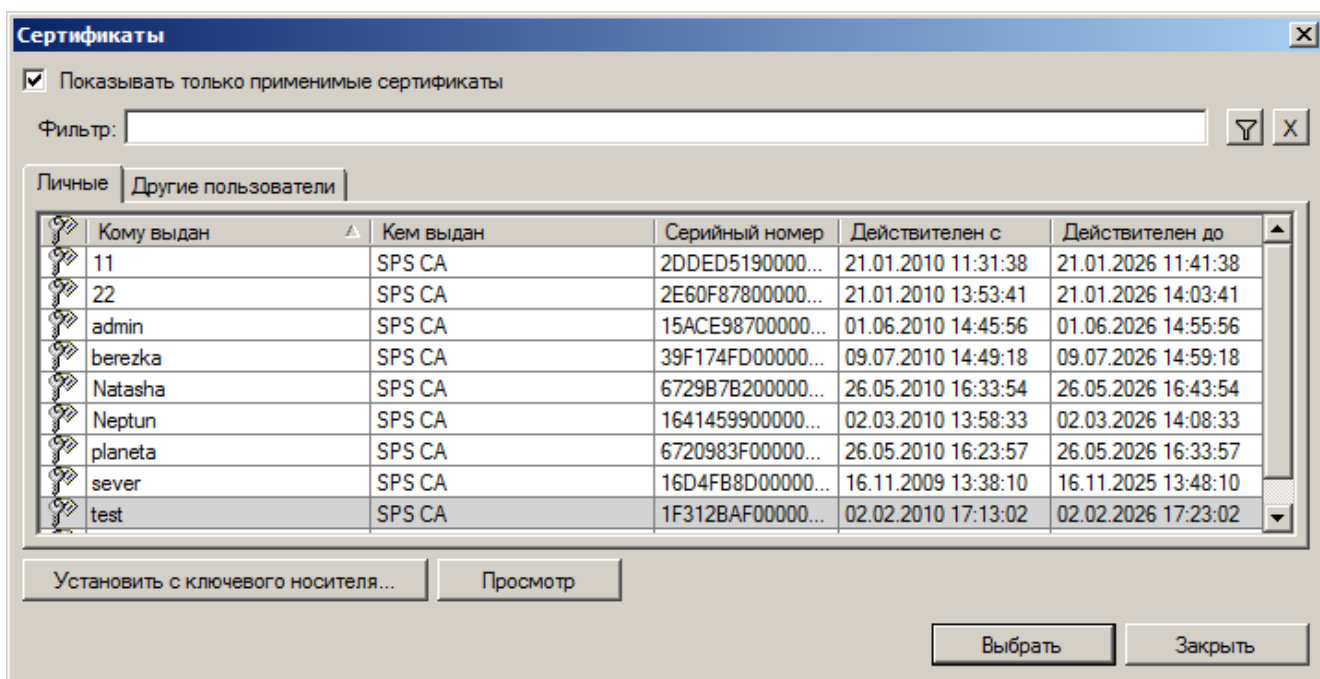


Рисунок 6. Выбор сертификата получателя из хранилища «Личные»

В этой форме можно выбрать сертификат из хранилища «Личные» или хранилища «Другие пользователи». Отметка «Показывать только применимые сертификаты» отфильтровывает валидные сертификаты, срок действия которых в данный момент уже наступил и не истёк. При необходимости снимите эту отметку, в списке появятся все сертификаты, которыми можно зашифровать файл.

Чтобы установить сертификат с ключевого носителя в хранилище «Личные», убедитесь, что ключевой носитель подключен и нажмите соответствующую кнопку под списком сертификатов. Откроется форма «Сертификаты на ключевых носителях», в которой можно выбрать необходимый сертификат.

Для просмотра сертификата выберите его в списке и нажмите кнопку «Просмотр».

В хранилище «Другие пользователи» сертификат можно добавить из файла (Рисунок 7). Для этого нажмите кнопку «Установить из файла» и выберите путь к файлу сертификата из стандартного окна выбора.

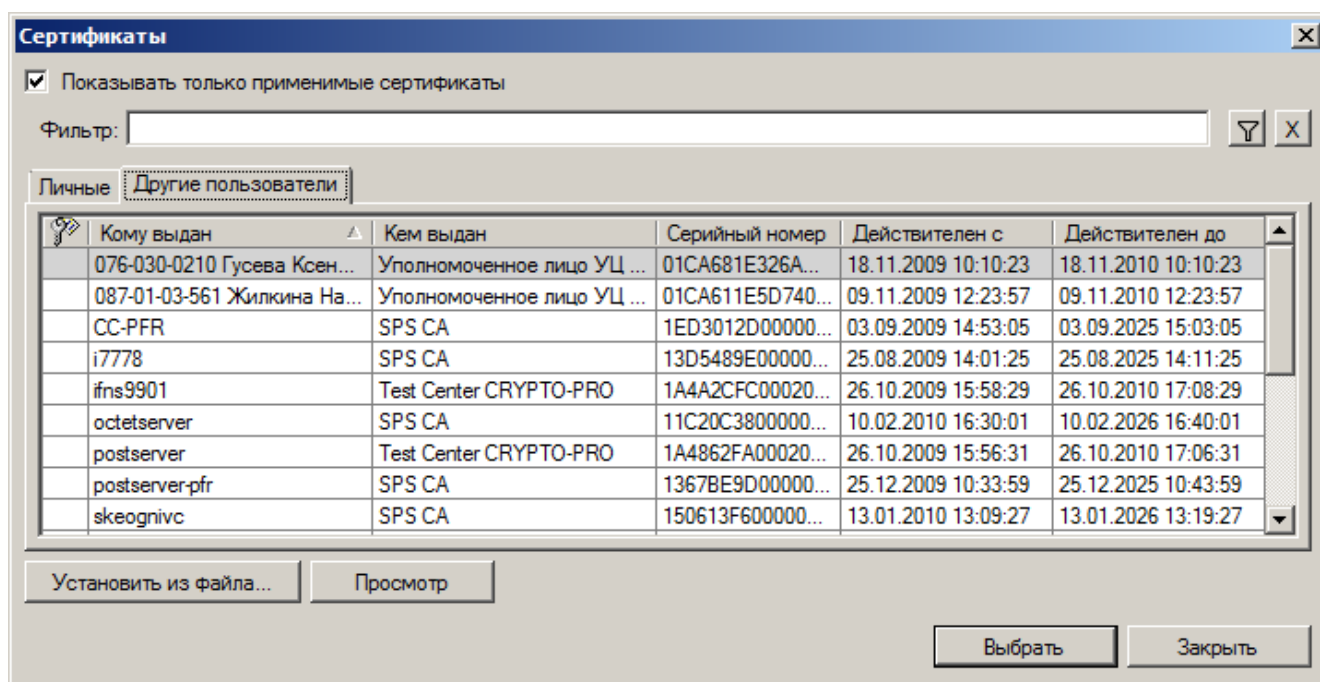


Рисунок 7. Выбор сертификата получателя из хранилища «Другие пользователи»

Выделите сертификат получателя и нажмите кнопку «Выбрать». Если нажать кнопку «Заккрыть», выбор будет отменён.

Также сертификат получателя можно выбрать непосредственно из файла, нажав на окне выбора сертификатов (Рисунок 5) кнопку «Добавить из файла».

Когда в таблице будет выбран сертификат или несколько сертификатов, становятся доступны следующие действия:

- для удаления сертификата из списка выделите строку с сертификатом и нажмите кнопку «Удалить»;
- для того, чтобы очистить список сертификатов, нажмите кнопку «Удалить все»;
- чтобы открыть форму просмотра сертификата, выделите строку с сертификатом и нажмите кнопку «Просмотр».

Убедитесь, что выбраны правильные сертификаты и перейдите к шагу «Шифрование», нажав кнопку «Далее».

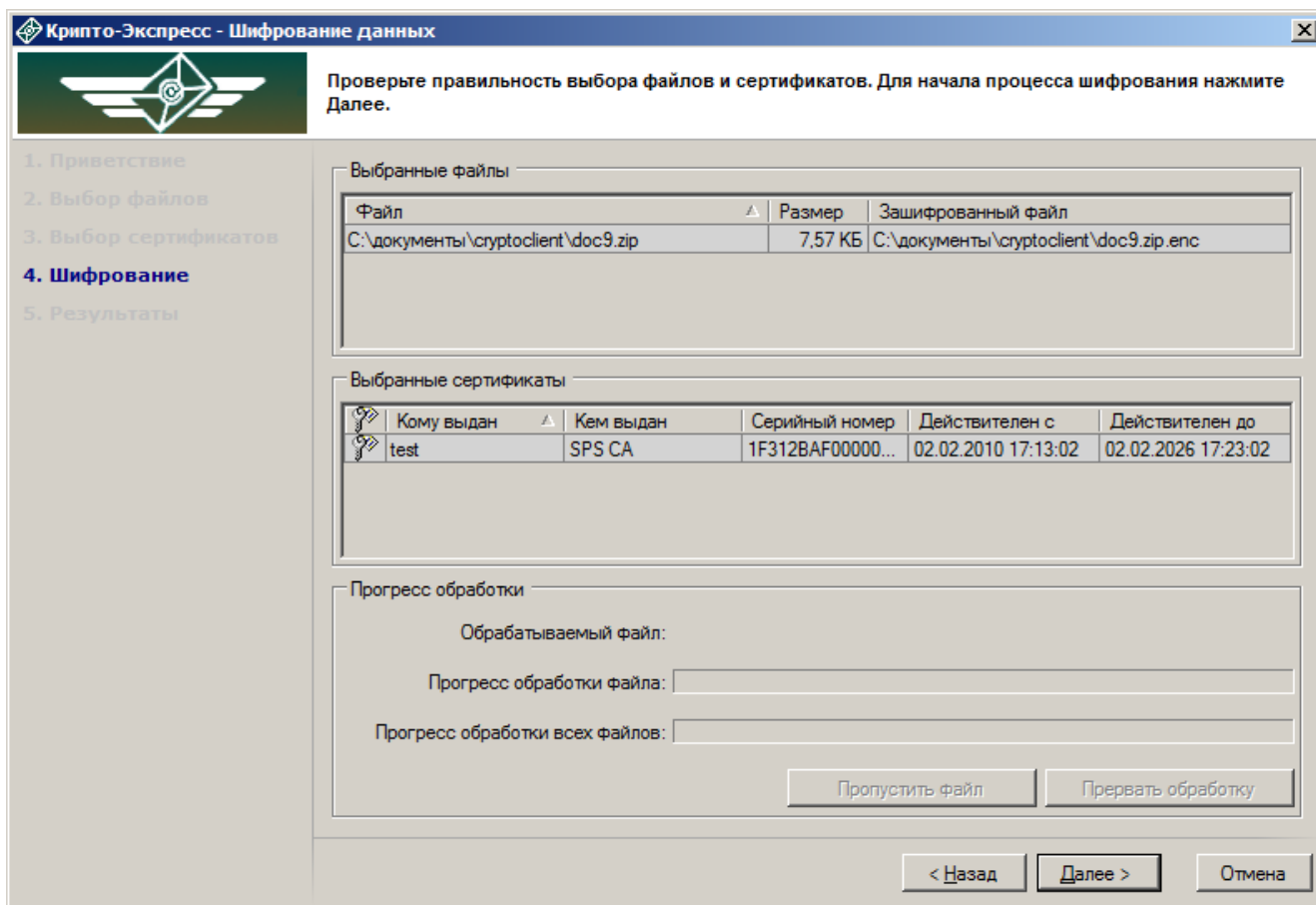


Рисунок 8. Шифрование данных

На этом шаге выводятся список «Выбранные файлы» и список «Выбранные сертификаты». Для того, чтобы начать шифрование, нажмите кнопку «Далее».

Ход обработки отображается в блоке «Прогресс обработки». Если возникли проблемы при шифровании определённого файла, нажмите «Пропустить файл», тогда будет продолжена обработка остальных файлов, или «Прервать обработку». Шифрование больших файлов может производиться продолжительное время.

После того, как файлы обработаются, на экран будет выведено окно со следующим шагом – «Результаты» (Рисунок 9).

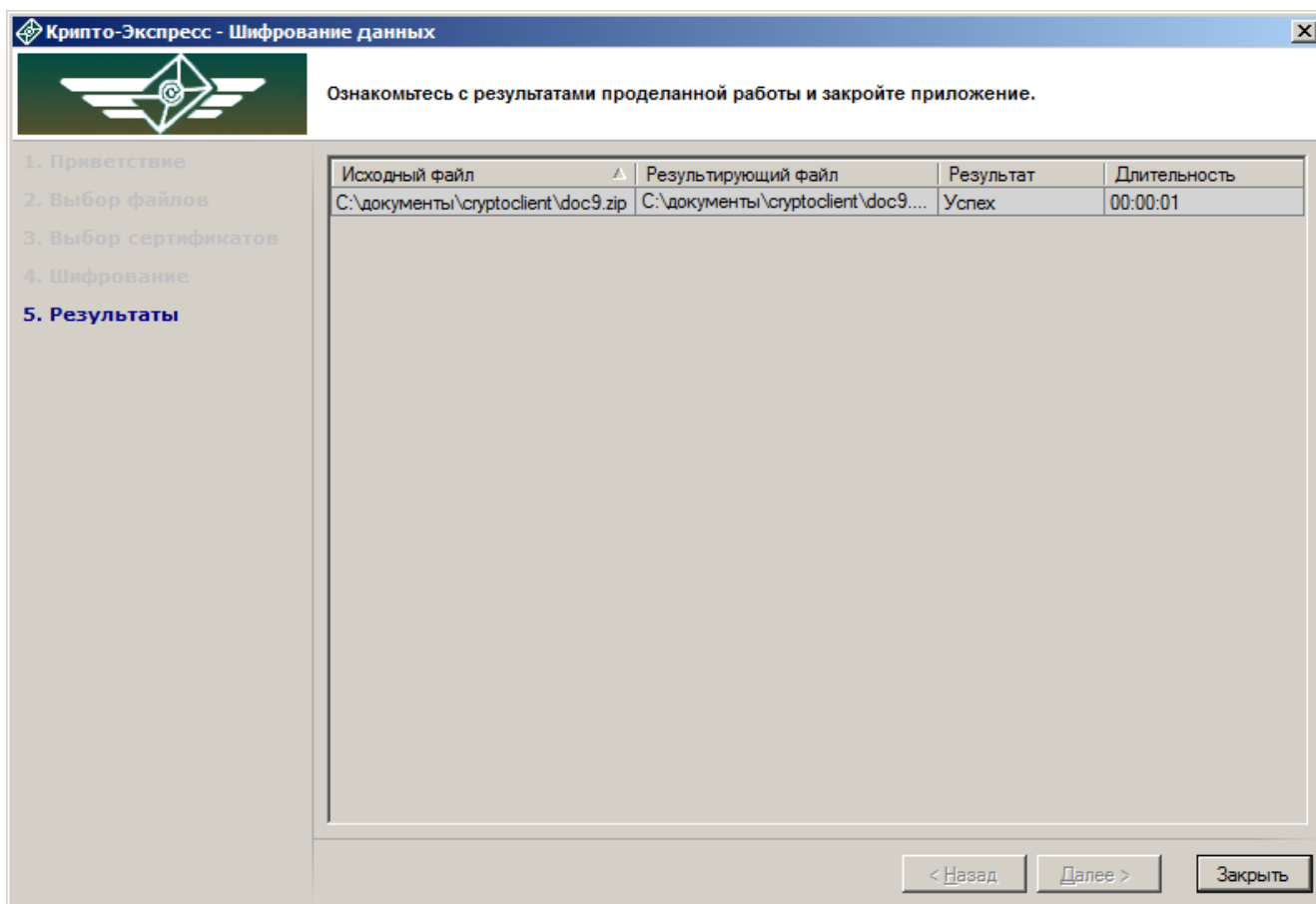


Рисунок 9. Результаты шифрования

Результаты шифрования показываются в виде таблицы. Если возникли проблемы с шифрованием одного или нескольких файлов, это будет отражено в графе «Результат».

Для того, чтобы закончить работу Мастера, нажмите кнопку «Закрыть».

4.3. Расшифрование файлов

Чтобы расшифровать файлы, необходимо предварительно выполнить следующие действия:

- выбрать зашифрованные файлы, которые требуется расшифровать;
- каждому из зашифрованных файлов назначить личный сертификат, с помощью которого файл можно расшифровать.

Для того, чтобы расшифровать файл, выберите в меню главного окна программы (Рисунок 2) пункт «Шифрование» и нажмите кнопку «Расшифровать», либо через меню проводника Windows (Рисунок 1) нажмите правую кнопку мыши и выберите «Крипто-Экспресс → Расшифровать...», предварительно выделив файл или несколько файлов, которые нужно обработать.

Откроется окно приветствия Мастера расшифрования данных (Рисунок 10).

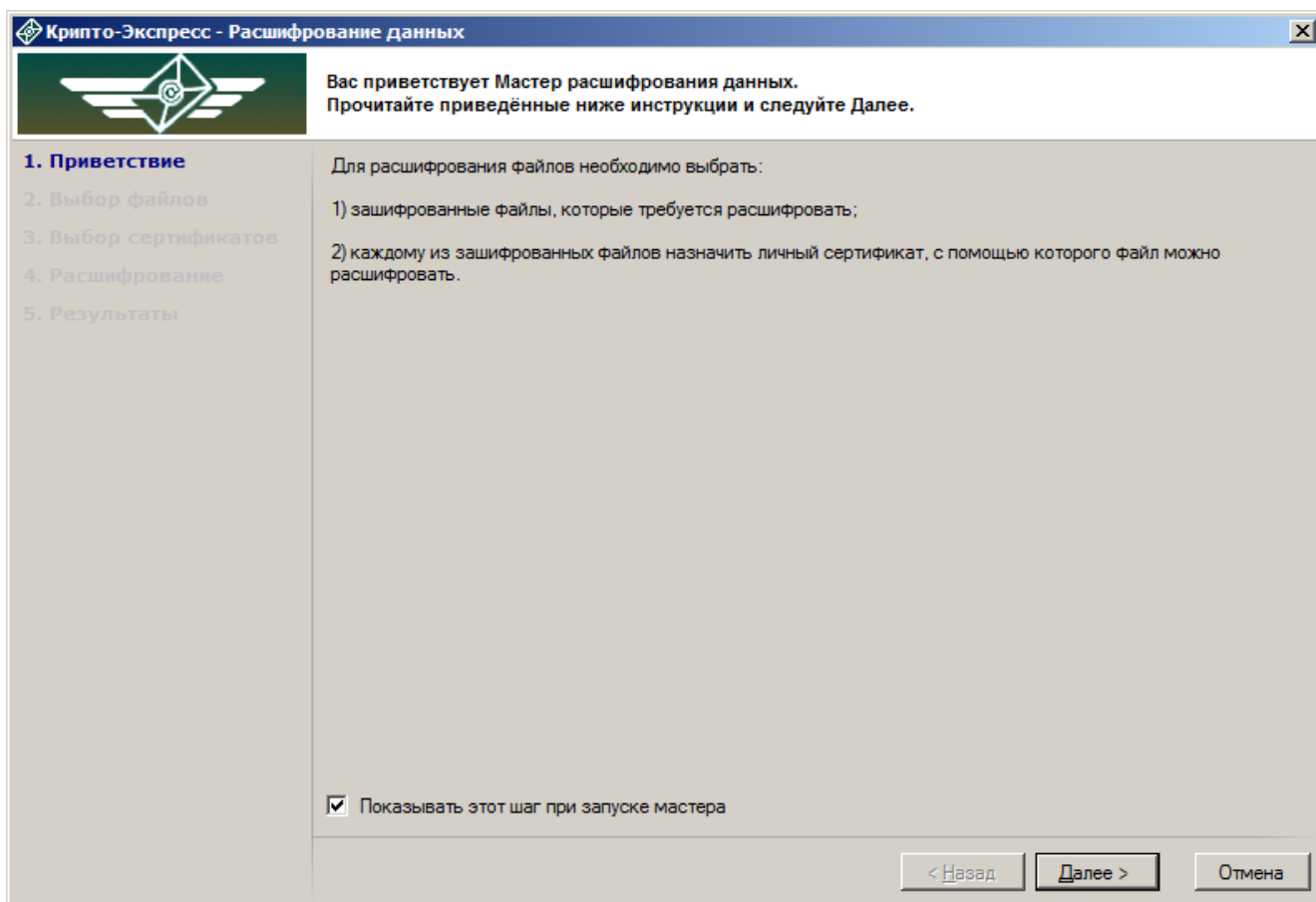


Рисунок 10. Приветствие Мастера расшифрования данных

Чтобы больше не выводить приветствие, уберите галочку внизу формы.

Нажмите «Далее», чтобы перейти к шагу выбора файлов (Рисунок 11).

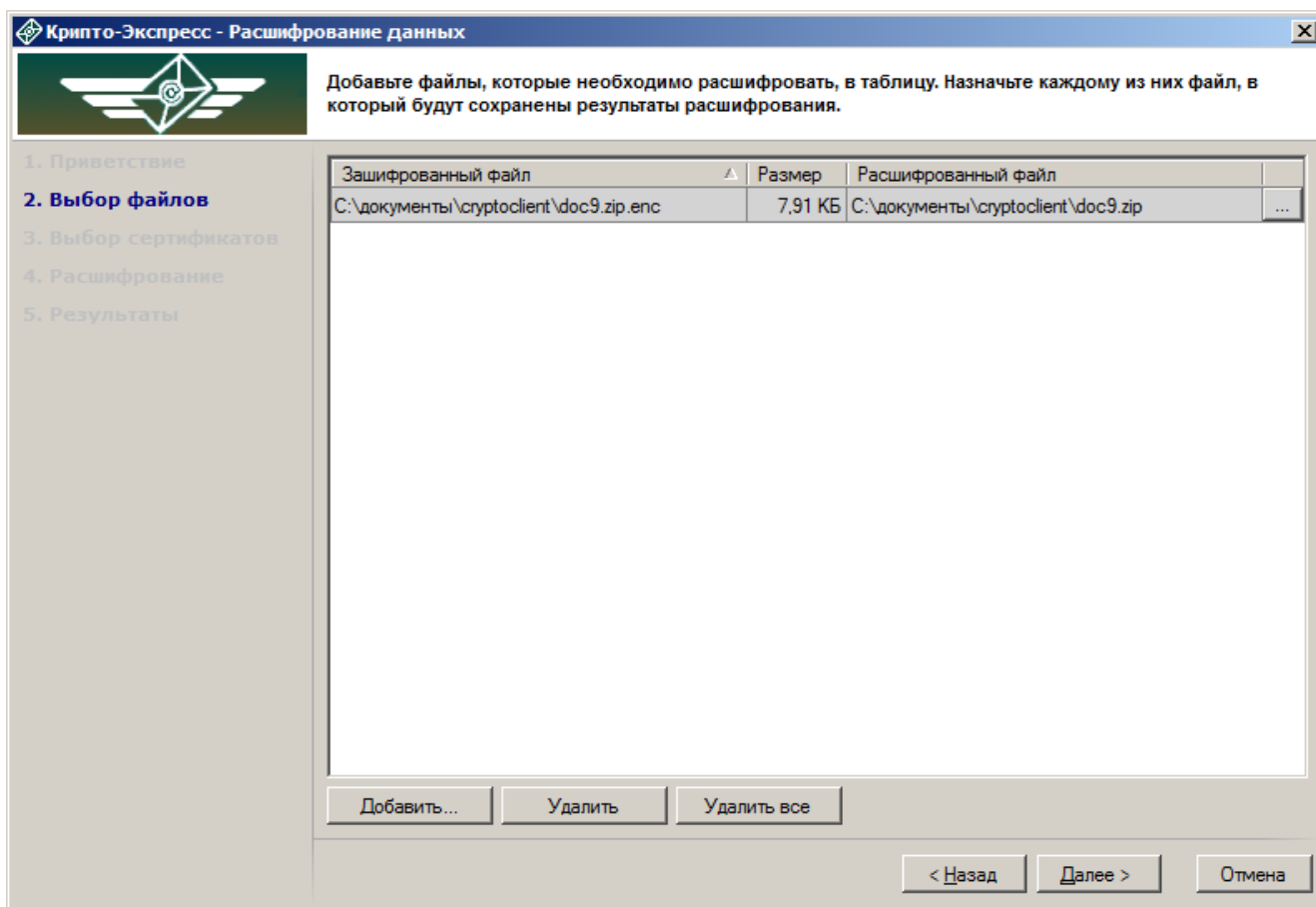


Рисунок 11. Выбор файлов для расшифрования

На этом шаге нужно добавить файлы, которые будут расшифрованы. Если файлы уже были выбраны, они отобразятся в таблице окна. Если файлы ещё не были выбраны или необходимо добавить ещё несколько файлов для расшифрования, воспользуйтесь кнопкой «Добавить» под таблицей, которая откроет стандартное окно выбора файлов.

Чтобы удалить ненужные файлы из обработки или полностью очистить таблицу, выделите строки с файлами и нажмите «Удалить» или «Удалить все» соответственно.

В таблице выбора файлов выводятся следующие сведения:

- имя файла для расшифрования и его расположение на жестком диске;
- размер файла;
- имя файла для сохранения результатов расшифрования и место на жестком диске, куда он будет сохранён.

Имя расшифрованного файла и путь для сохранения можно изменить, нажав на кнопку в правой части строки и сделав необходимые изменения через стандартный диалог сохранения.

Если файл с таким именем уже существует в папке, куда сохраняется результат расшифрования (в поле «Расшифрованный файл» выведено предупреждение об этом), рекомендуется выбрать другую папку или изменить имя расшифрованного файла.

Для перехода к шагу выбора сертификатов нажмите кнопку «Далее» (Рисунок 12).

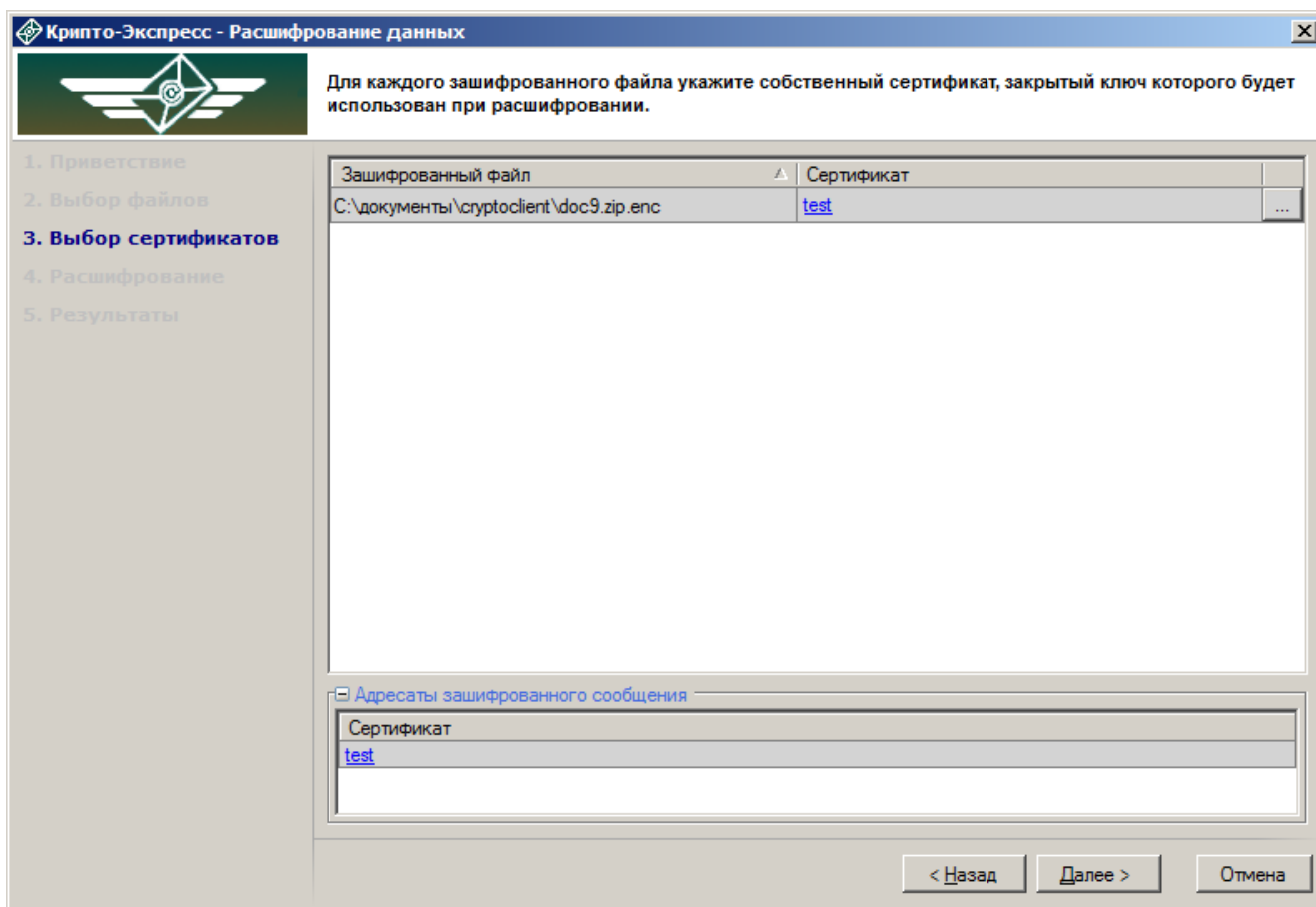


Рисунок 12. Выбор сертификатов для расшифрования

На этом шаге для каждого зашифрованного файла указывается собственный сертификат, закрытый ключ которого будет использован при расшифровании. Выбор сертификата производится с помощью кнопки в правой части строки, в которой указывается файл для обработки. Нажмите на кнопку выбора, чтобы открыть окно «Сертификаты», которое покажет список всех доступных сертификатов, обладающих закрытым ключом (Рисунок 13).

Список «Адресаты зашифрованного сообщения» показывает все сертификаты, для которых было зашифровано сообщение.

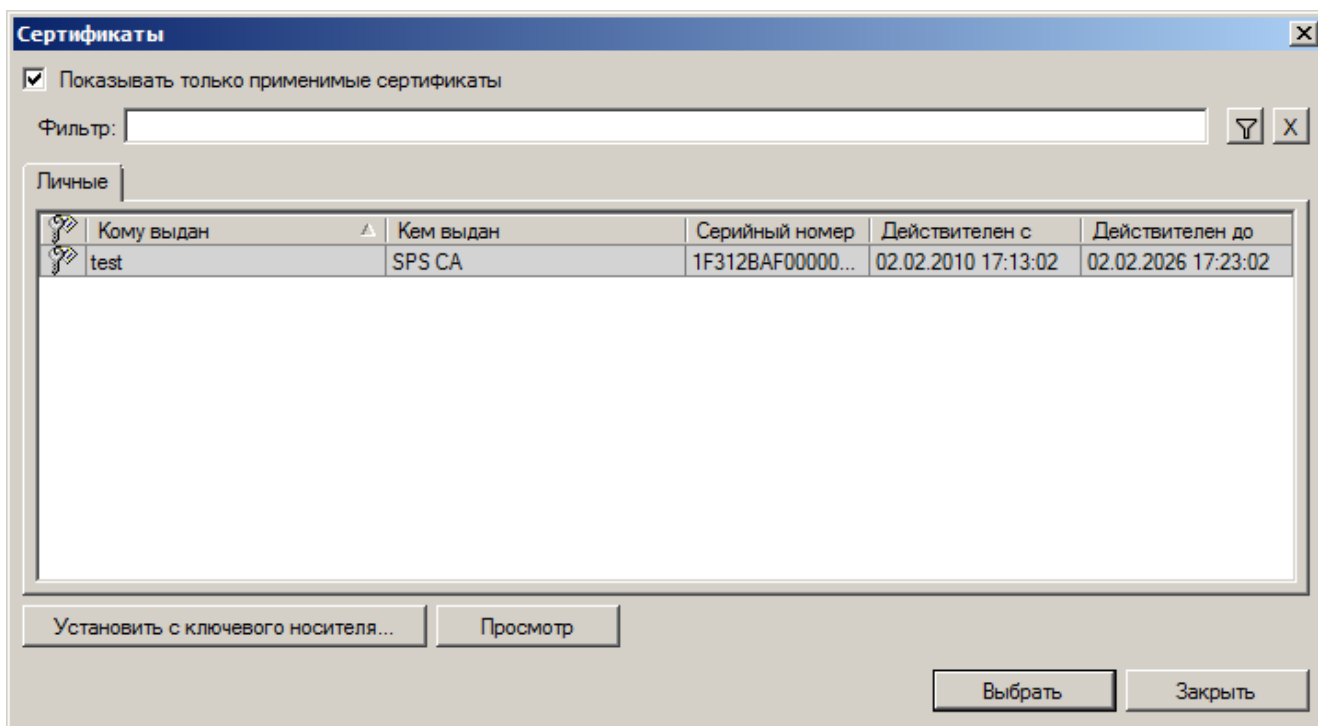


Рисунок 13. Выбор сертификата для расшифрования из хранилища «Личные»

При необходимости можно установить сертификат для расшифрования с ключевого носителя. Чтобы установить сертификат с ключевого носителя в хранилище «Личные», убедитесь, что ключевой носитель подключен и нажмите соответствующую кнопку под списком сертификатов. Откроется форма «Сертификаты на ключевых носителях», в которой можно выбрать необходимый сертификат.

Для просмотра сертификата выберите его в списке и нажмите кнопку «Просмотр».

Выделив строку с нужным сертификатом, нажмите кнопку «Выбрать».

Убедитесь, что выбраны правильные сертификаты и перейдите к шагу «Расшифрование», нажав кнопку «Далее».

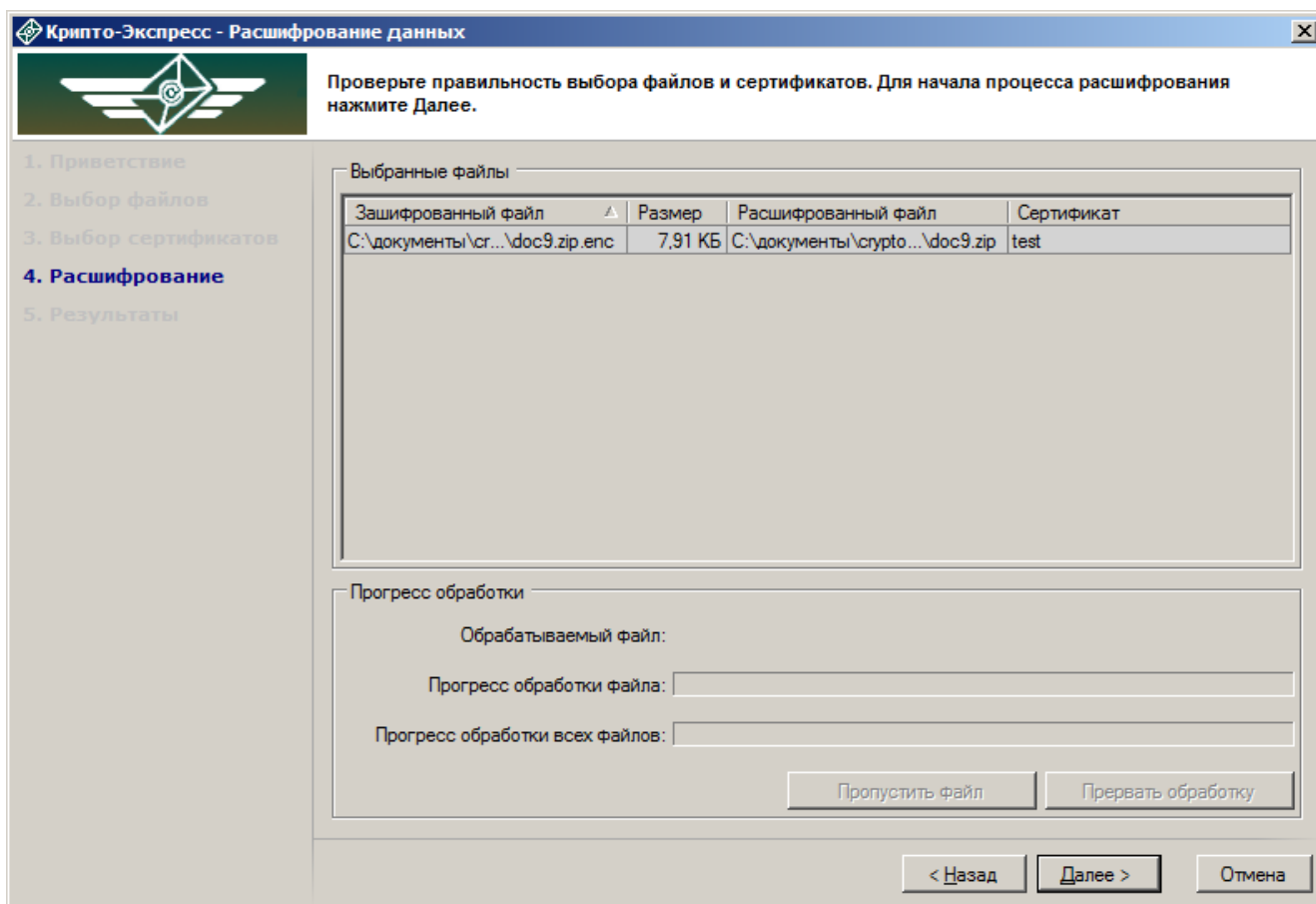


Рисунок 14. Расшифрование данных

В окне программы отображен список файлов, которые будут расшифрованы, имена и расположение файлов, в который будут сохранены данные, а также сертификаты получателя с закрытым ключом, с помощью которых файлы будут обработаны.

Нажмите кнопку «Далее», чтобы начать расшифрование файлов.

Ход обработки отображается в блоке «Прогресс обработки». Если возникли проблемы при расшифровании определённого файла, нажмите «Пропустить файл», тогда будет продолжена обработка остальных файлов, или «Прервать обработку». Расшифрование больших файлов может производиться продолжительное время.

После того, как файлы обработаются, на экран будет выведено окно со следующим шагом – «Результаты» (Рисунок 15).

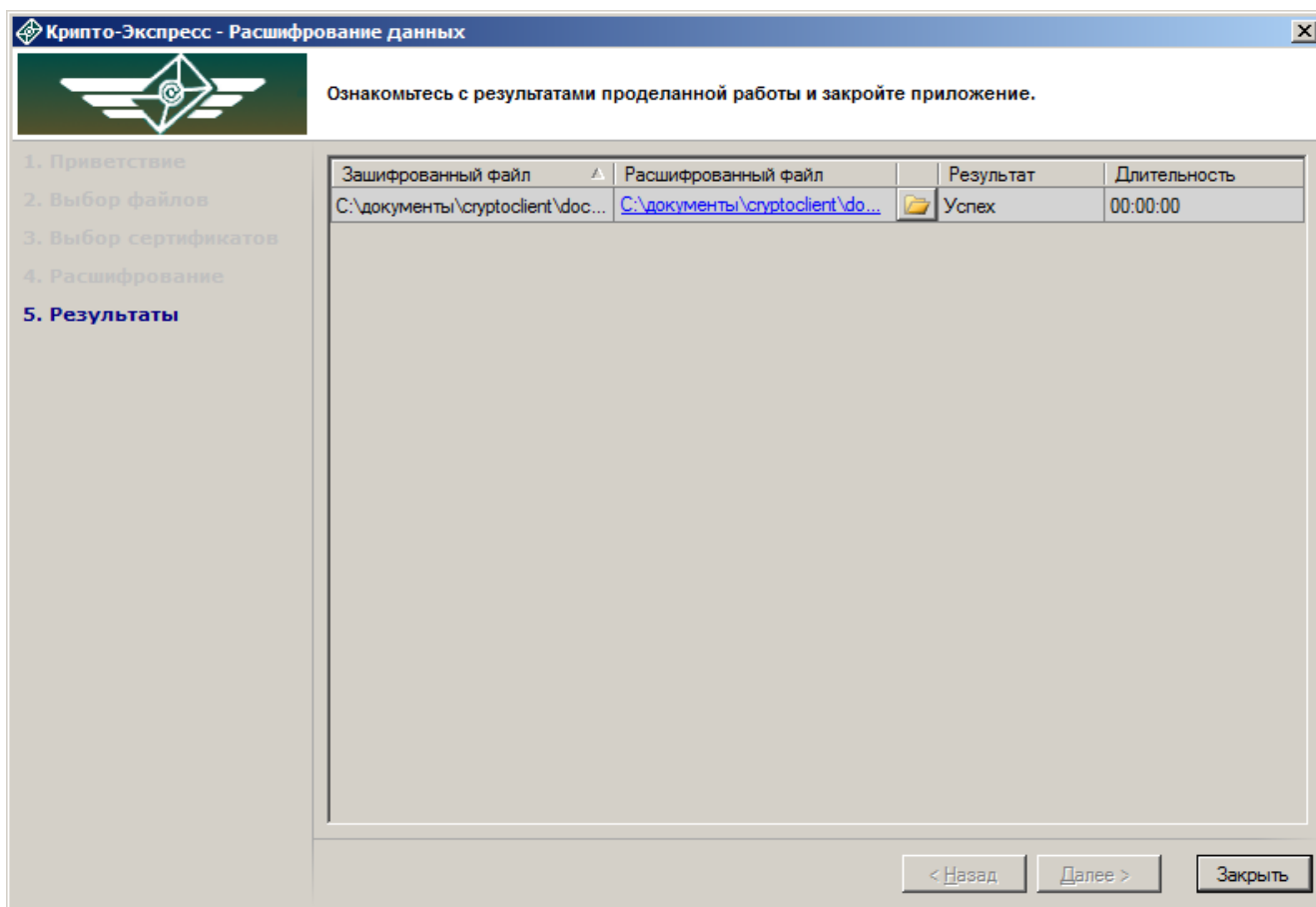


Рисунок 15. Результаты расшифрования

Результаты расшифрования показываются в виде таблицы. Если возникли проблемы с шифрованием одного или нескольких файлов, это будет отражено в графе «Результат».

Можно открыть расшифрованный документ, нажав на ссылку в поле «Расшифрованный файл» или открыть папку, в которую документ был сохранён, нажав значок с изображением папки.

Для того, чтобы закончить работу Мастера, нажмите кнопку «Заккрыть».

4.4. Подписание файлов

Обработка подписей может быть произведена как с помощью контекстного меню проводника Windows (Рисунок 1), так и через меню главного окна программы (Рисунок 16).

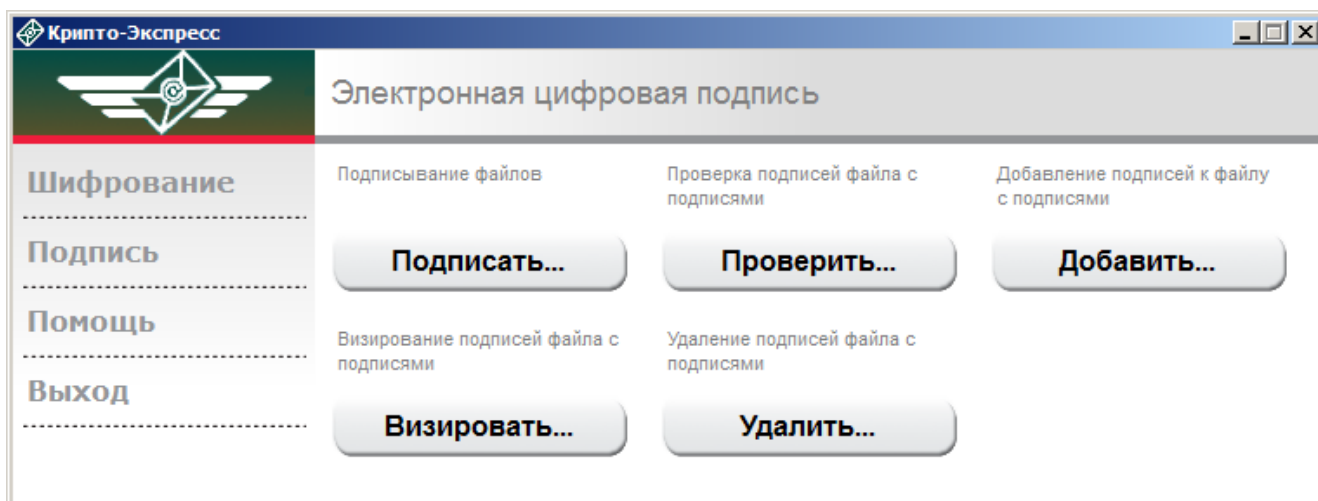


Рисунок 16. Работа с подписями

Чтобы подписать файлы, необходимо предварительно выполнить следующие действия:

- выбрать файлы для подписи;
- выбрать личные сертификаты, которыми будет подписан каждый файл.

Для того, чтобы подписать файл, выберите в меню главного окна программы (Рисунок 16) пункт «Подпись» и нажмите кнопку «Подписать», либо через меню проводника Windows (Рисунок 1) нажмите правую кнопку мыши и выберите «Крипто-Экспресс → Подписать...», предварительно выделив файл или несколько файлов, которые нужно обработать.

Откроется окно приветствия Мастера создания электронной цифровой подписи (Рисунок 17).

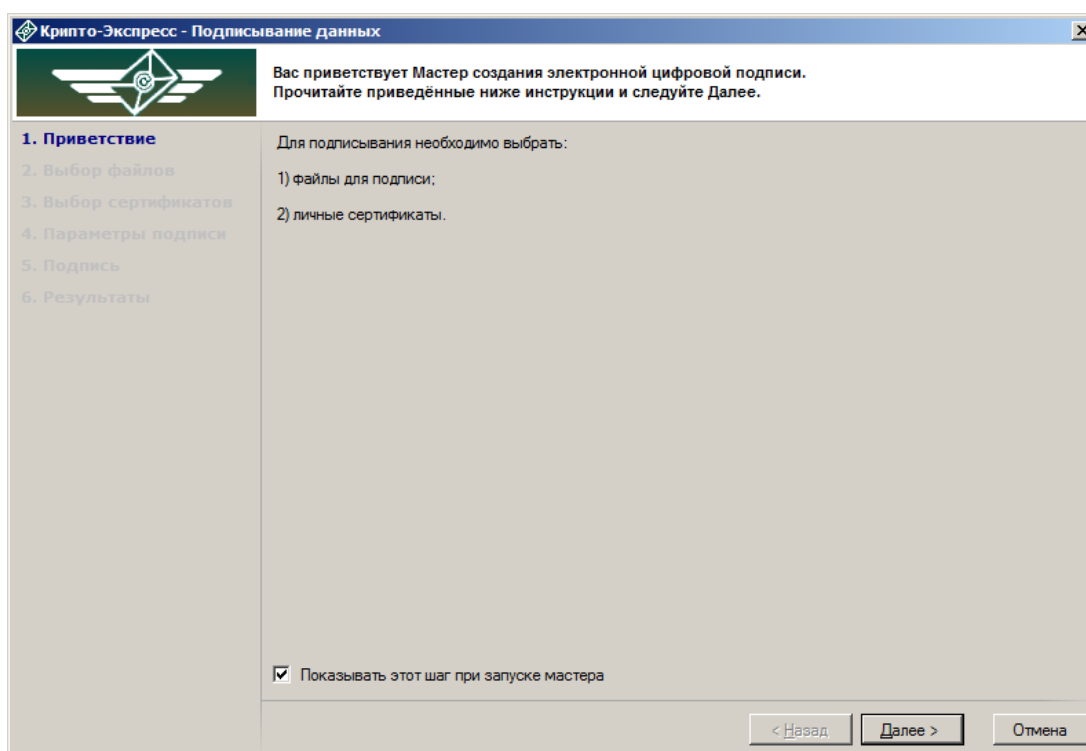


Рисунок 17. Приветствие Мастера создания электронной цифровой подписи

Чтобы больше не выводить приветствие, уберите галочку в нижней части формы.

Нажмите «Далее», чтобы перейти к шагу выбора файлов (Рисунок 18).

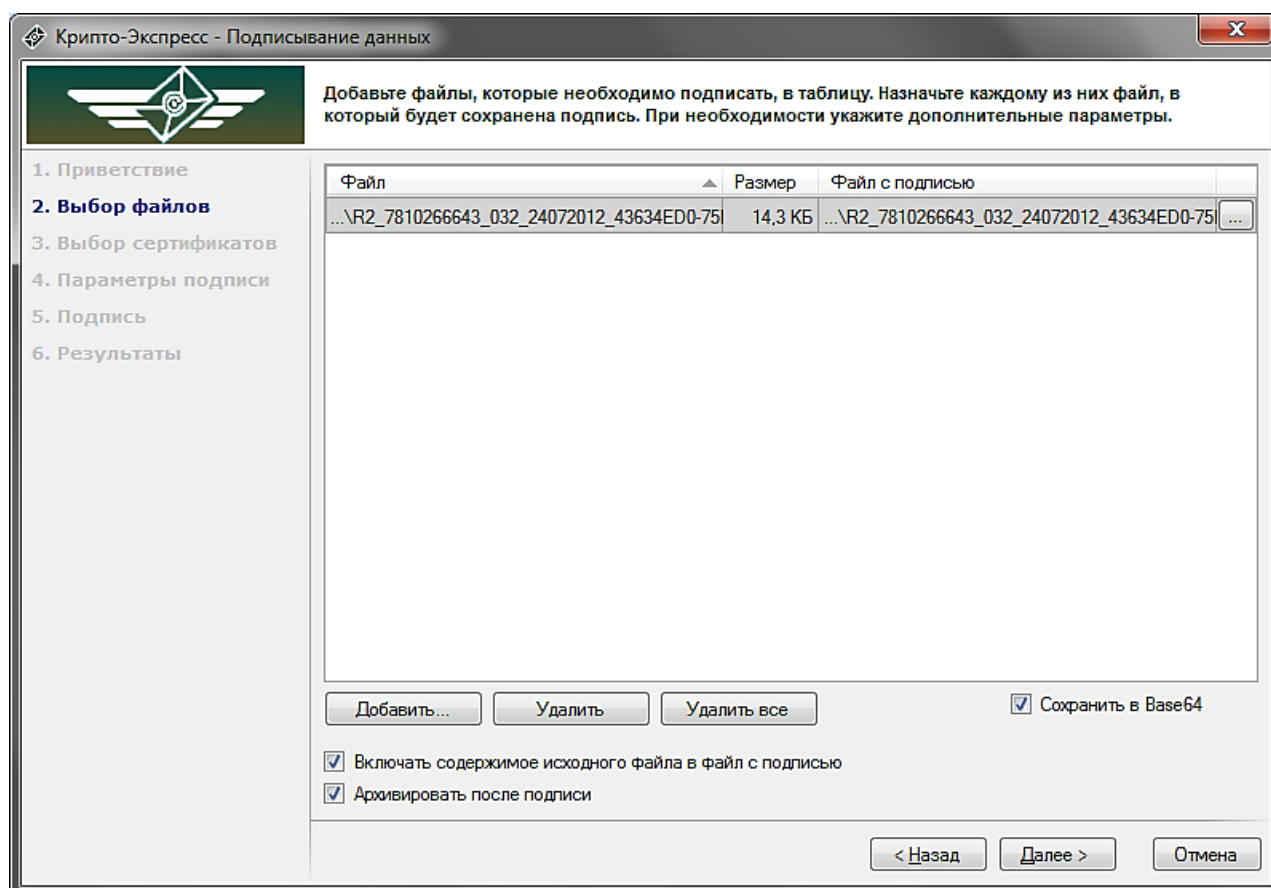


Рисунок 18. Выбор файлов для подписи

На этом шаге нужно добавить файлы, которые будут подписаны. Если файлы уже были выбраны, они отобразятся в таблице окна. Если файлы ещё не были выбраны или необходимо добавить ещё несколько файлов для подписывания, воспользуйтесь кнопкой «Добавить» под таблицей, которая откроет стандартное окно выбора файлов.

Чтобы удалить ненужные файлы из обработки или полностью очистить таблицу, выделите строки с файлами и нажмите «Удалить» или «Удалить все» соответственно.

В таблице выбора файлов выводятся следующие сведения:

- имя подписываемого файла и его расположение на жестком диске;
- размер файла;
- имя файла с подписью и место на жестком диске, куда он будет сохранён.

Имя файла с подписью и путь для сохранения можно изменить, нажав на кнопку в правой части строки и сделав необходимые изменения через стандартный диалог сохранения.

Если подписанный файл с таким именем уже существует в папке, куда сохраняется результат обработки (в поле «Файл с подписью» выведено предупреждение об этом), рекомендуется выбрать другую папку или изменить имя файла с подписью.

Если при подписании файла поставить отметку «Включать содержимое исходного файла в файл с подписью», то результатом обработки будет файл, не содержащий исходного документа.

По умолчанию файлы с подписью сохраняются в кодировке DER, но при необходимости (например, если планируется передача файлов по сети), можно сохранить их в кодировке Base64, поставив отметку «Сохранить в Base64» в правой нижней части окна.

Если поставить отметку «Архивировать после подписи» подписанный файл будет заархивирован и сохранен в формате .zip

Для перехода к шагу выбора сертификатов нажмите кнопку «Далее».

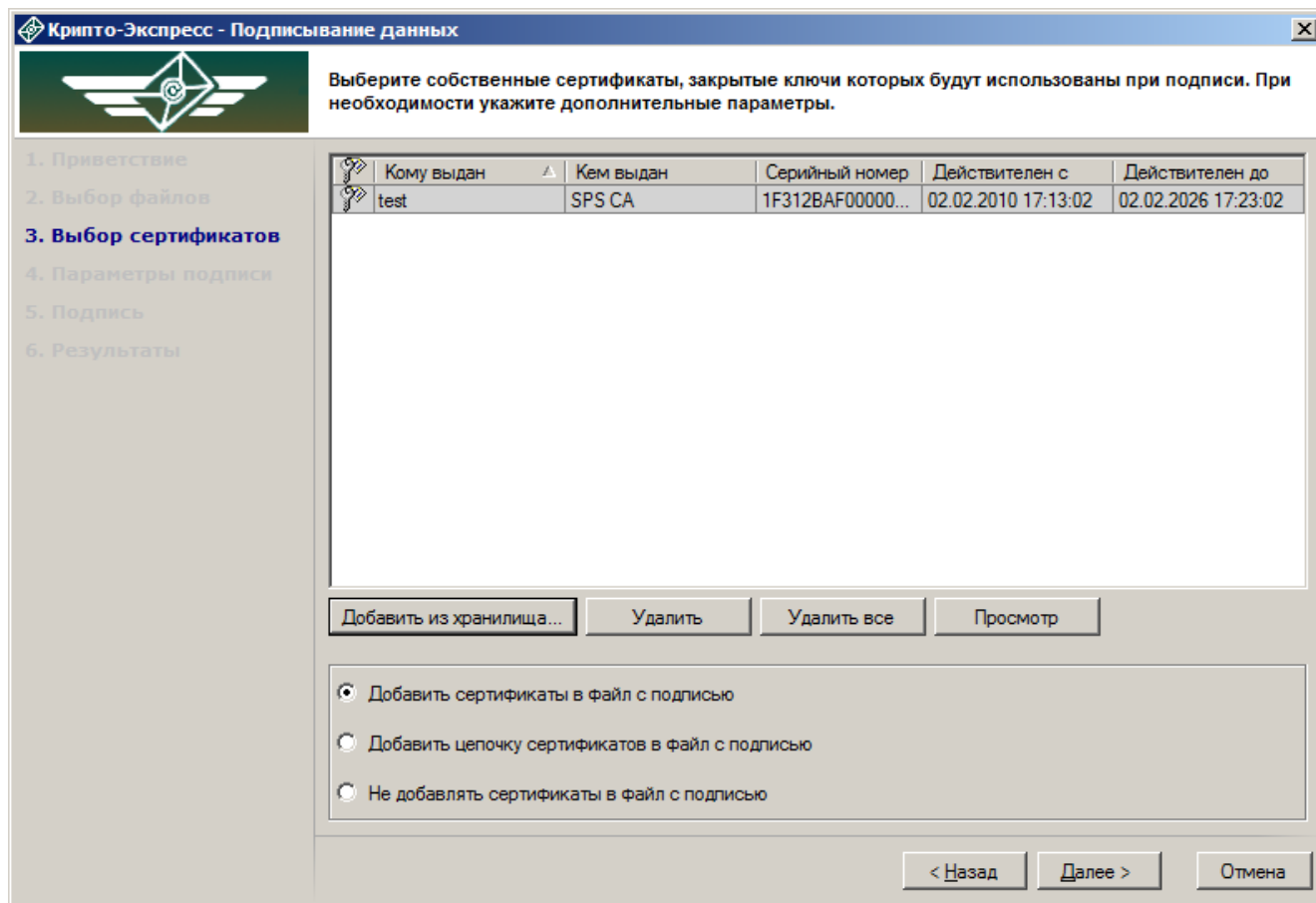


Рисунок 19. Выбор сертификатов для подписи

На этом шаге необходимо выбрать собственные сертификаты, закрытые ключи которых будут использованы при подписи. Их можно добавить в таблицу из хранилища сертификатов.

Для того чтобы добавить сертификат из хранилища, нажмите кнопку «Добавить из хранилища». Откроется форма выбора сертификатов (Рисунок 20).

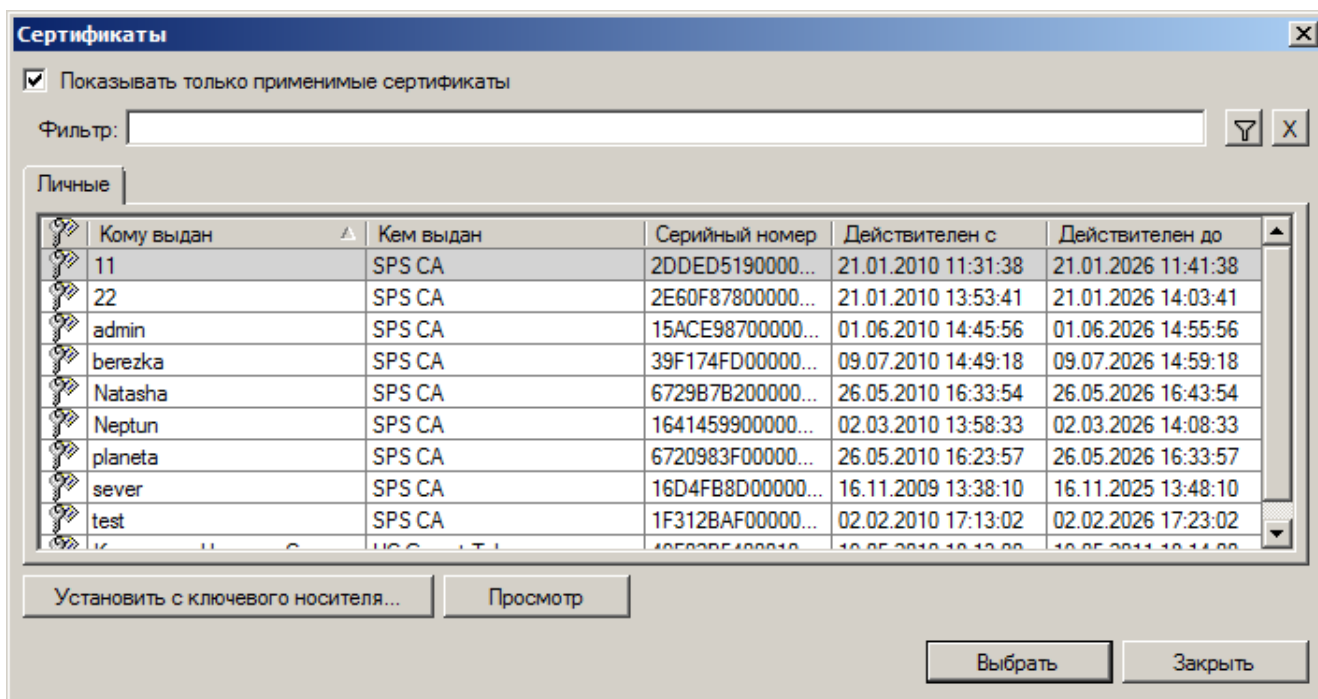


Рисунок 20. Выбор сертификата для подписи из хранилища «Личные»

При необходимости можно установить сертификат с ключевого носителя. Чтобы установить сертификат с ключевого носителя в хранилище «Личные», убедитесь, что ключевой носитель подключен и нажмите соответствующую кнопку под списком сертификатов. Откроется форма «Сертификаты на ключевых носителях», в которой можно выбрать необходимый сертификат.

Для просмотра сертификата выберите его в списке и нажмите кнопку «Просмотр».

Выделив строку с нужным сертификатом, нажмите кнопку «Выбрать».

При необходимости в форме выбора (Рисунок 19) можно указать одно из следующих действий:

- Добавить сертификаты в файл с подписью;
- Добавить цепочку сертификатов в файл с подписью;
- Не добавлять сертификаты в файл с подписью.

По умолчанию выбрано «Добавить сертификаты в файл с подписью».

Убедитесь, что выбраны правильные сертификаты и перейдите к следующему шагу, нажав кнопку «Далее».

Шаг «Параметры подписи» (Рисунок 21) даёт пользователю возможность указать дополнительные параметры подписи: добавить штампы времени на подписываемые данные и на подпись, а также включить в файл с подписью доказательства подлинности (например, цепочку сертификатов до доверенного УЦ).

Крипто-Экспресс - Подписывание данных

Укажите параметры, которые необходимо добавить к подписи.

1. Приветствие
2. Выбор файлов
3. Выбор сертификатов
4. Параметры подписи
5. Подпись
6. Результаты

☐ Включить в подпись доказательства подлинности

Адрес службы штампов времени:

☐ Включить штамп времени на подписываемые данные

Адрес

☐ Включить штамп времени на подпись

Адрес

Рисунок 21. Дополнительные атрибуты к подписи

Этот шаг можно пропустить, нажав кнопку «Далее», чтобы продолжить обработку и перейти к шагу подписи данных (Рисунок 22).

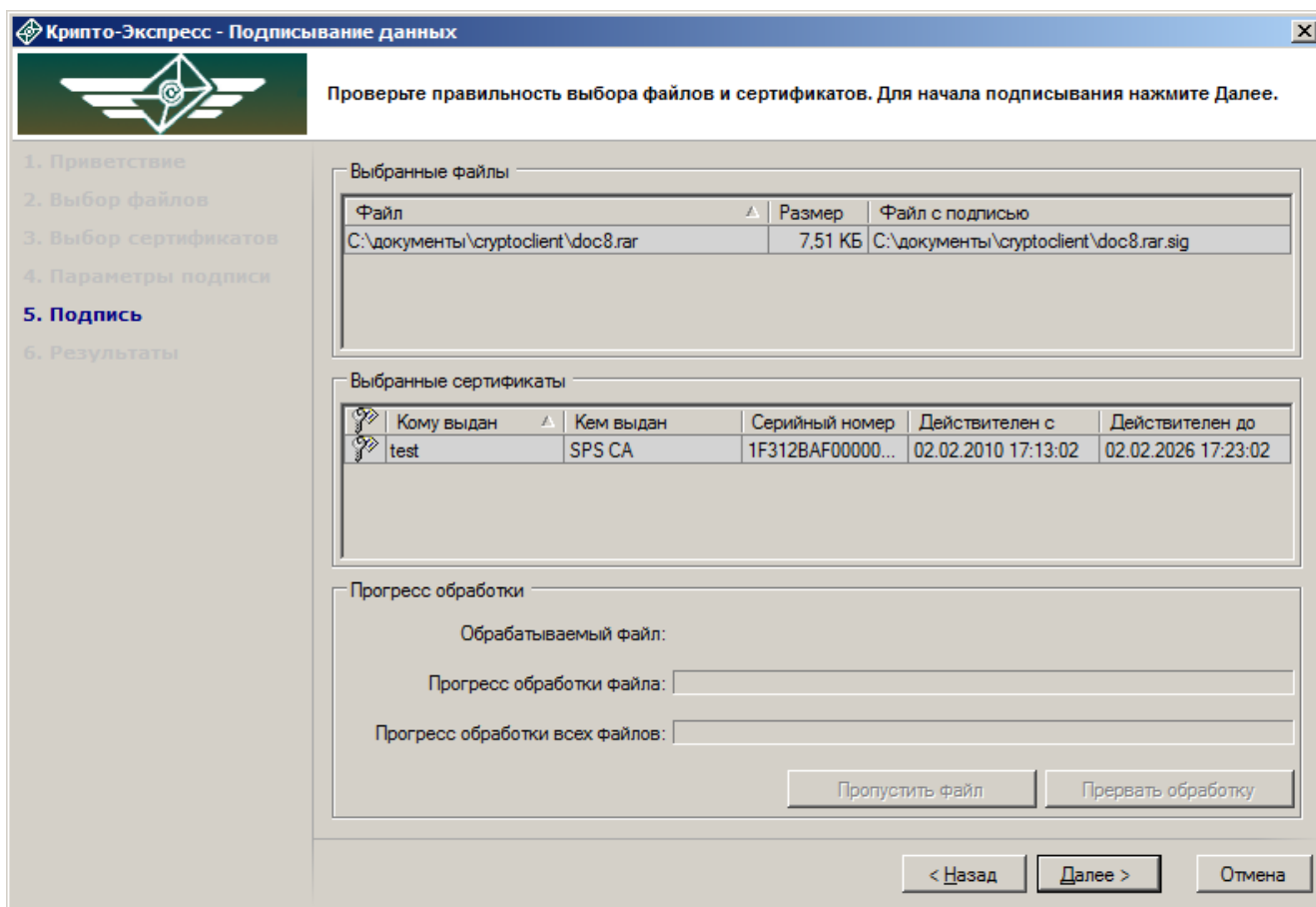


Рисунок 22. Подписывание данных

На этом шаге выводятся список «Выбранные файлы» и список «Выбранные сертификаты». Для того, чтобы начать подписывание, нажмите кнопку «Далее».

Ход обработки отображается в блоке «Прогресс обработки». Если возникли проблемы при подписывании определённого файла, нажмите «Пропустить файл», тогда будет продолжена обработка остальных файлов, или «Прервать обработку». Обработка больших файлов может производиться продолжительное время.

После того, как файлы обработаются, на экран будет выведено окно со следующим шагом – «Результаты» (Рисунок 23).

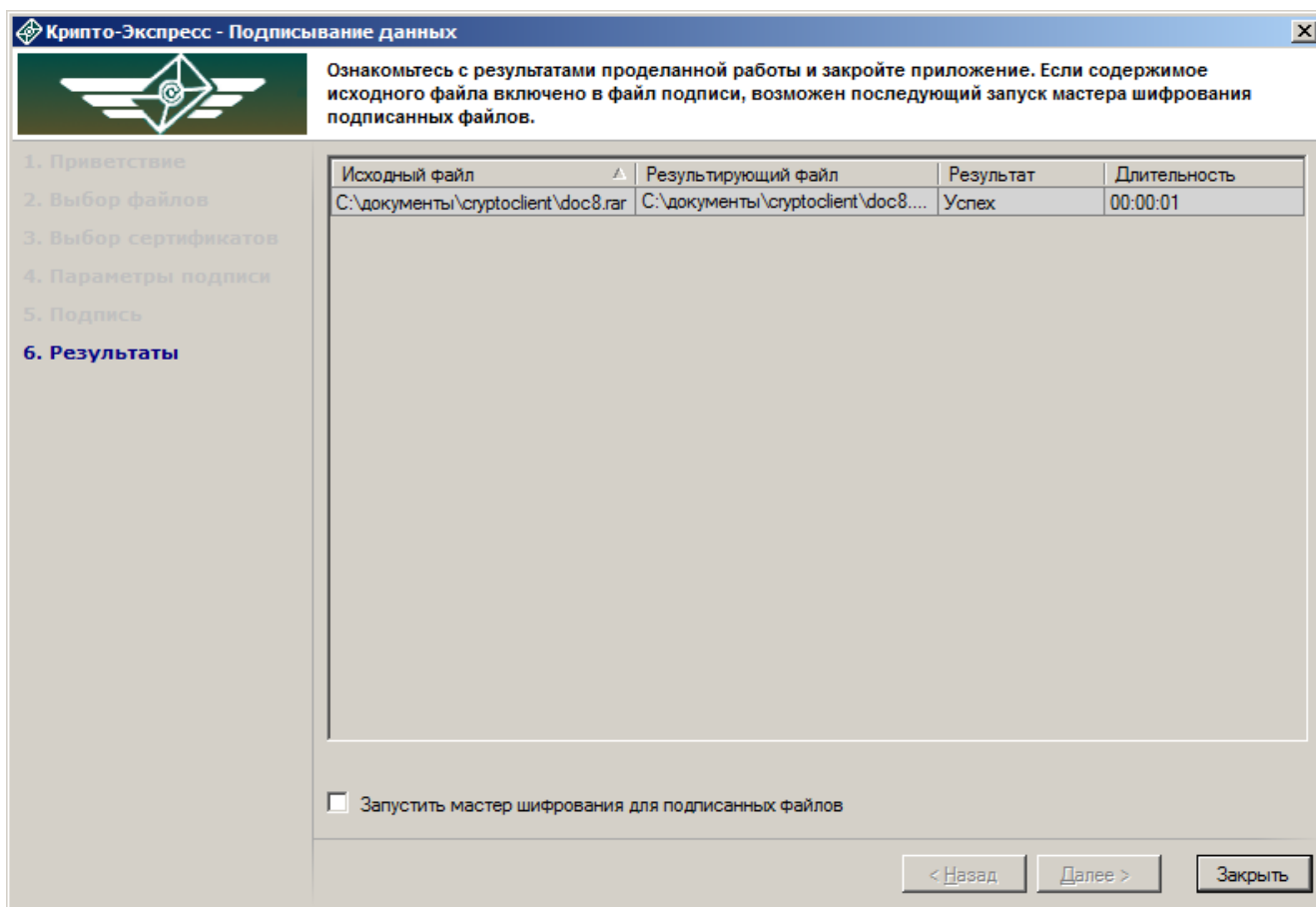


Рисунок 23. Результаты подписывания

Результаты обработки показываются в виде таблицы. Если возникли проблемы с подписанием одного или нескольких файлов, это будет отражено в графе «Результат».

После подписания файла его можно зашифровать в адрес получателя, запустив Мастер шифрования. Для этого поставьте отметку «Запустить мастер шифрования для подписанных файлов».

Для того чтобы закончить работу Мастера создания электронной цифровой подписи нажмите кнопку «Закреть».

4.5. Проверка подписей

Для проверки подписей используется Мастер проверки электронной цифровой подписи.

Чтобы проверить подписи в файлах с подписями, необходимо предварительно выполнить следующие действия:

- выбрать файлы с подписями;
- выбрать сертификаты.

Для того, чтобы проверить подпись файла, выберите в меню главного окна программы (Рисунок 16) пункт «Подпись» и нажмите кнопку «Проверить», либо через меню проводника Windows (Рисунок 1) нажмите правую кнопку мыши и выберите «Крипто-Экспресс → Проверить подпись...», предварительно выделив файл или несколько файлов, которые нужно обработать.

Откроется окно приветствия Мастера проверки электронной цифровой подписи (Рисунок 24).

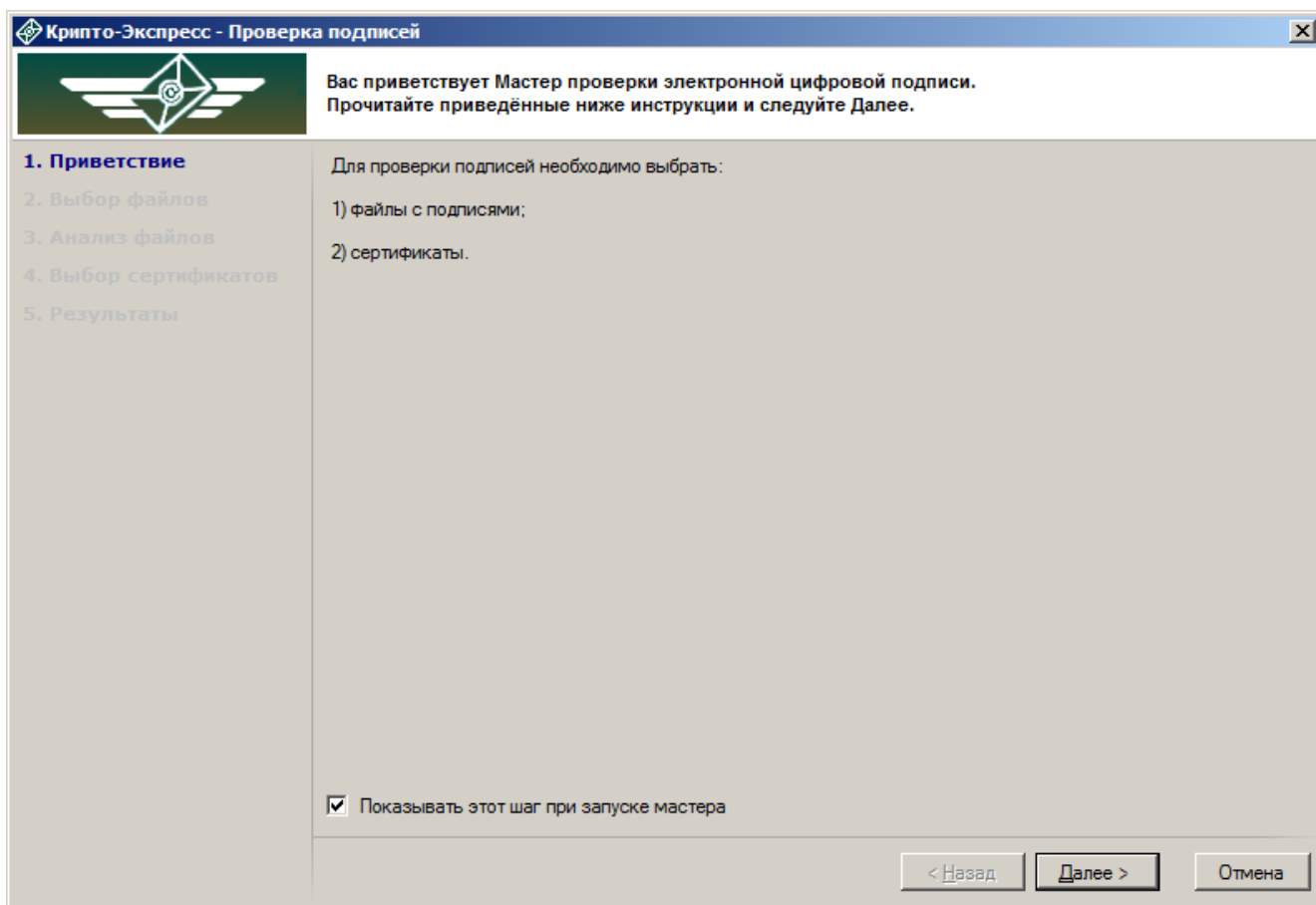


Рисунок 24. Приветствие Мастера проверки электронной цифровой подписи

Чтобы больше не выводить приветствие, уберите галочку в нижней части формы.

Нажмите «Далее», чтобы перейти к шагу выбора файлов (Рисунок 25Рисунок 25).

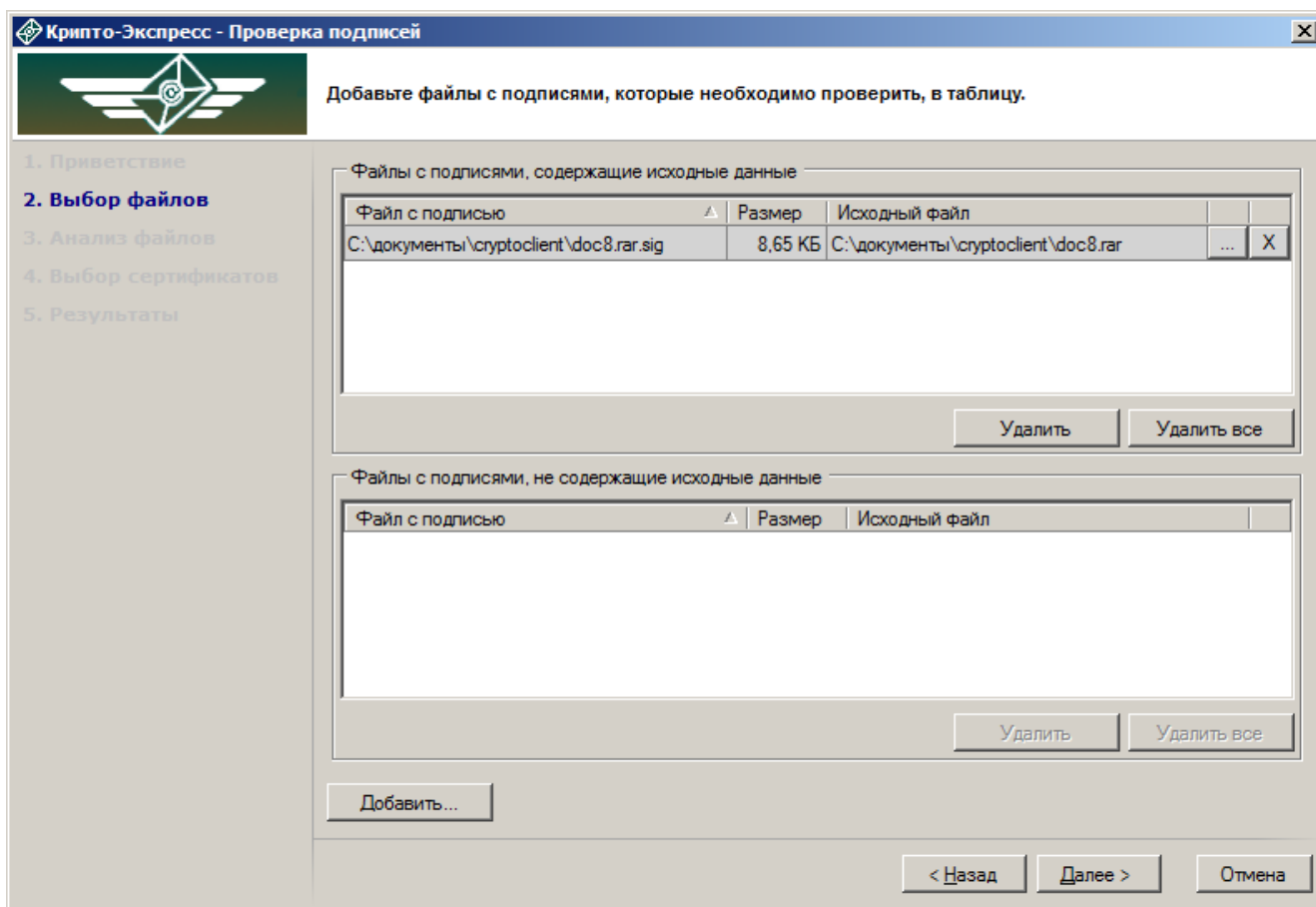


Рисунок 25. Выбор файлов для проверки подписей

Добавьте файлы, которые необходимо проверить, в таблицу. Если выбранные файлы с подписями содержат исходные данные, то они будут помещены в список «Файлы с подписями, содержащие исходные данные». Если файл с подписью содержит только подпись, без исходных данных, то он будет добавлен в таблицу «Файлы с подписями, не содержащие исходные данные» и потребуются указать в соответствующем поле исходный файл.

После того, как файлы будут выбраны, перейдите к анализу файлов, нажав кнопку «Далее». На шаге анализа файлов нужно правильность выбора файлов с подписями, которые показаны в списке выбранных файлов (Рисунок 26).

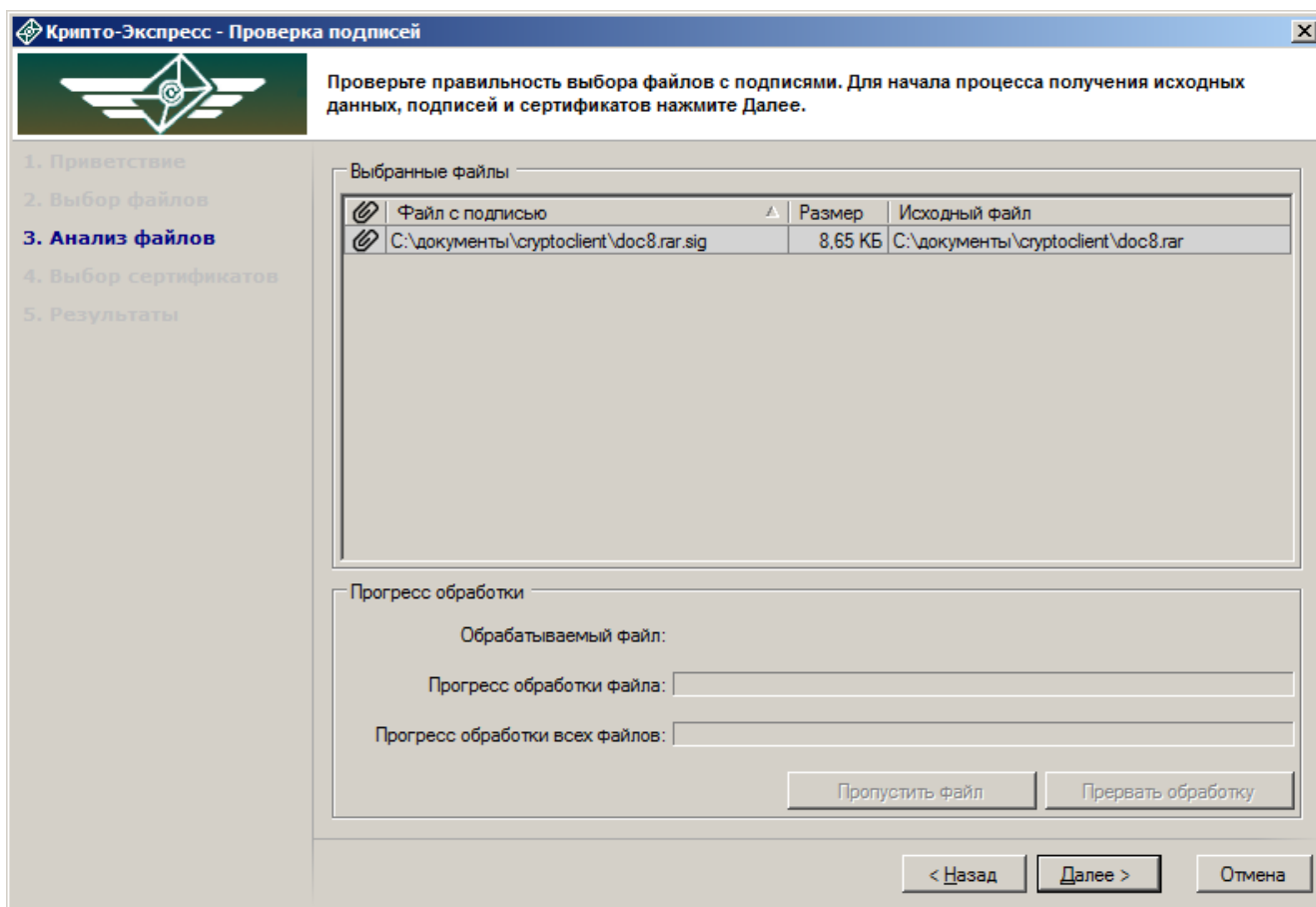


Рисунок 26. Анализ файлов с подписями

Список выбранных файлов содержит данные по именам и расположению файлов с подписью, размеру файлов, а также информацию о заданных именах файлов, в которых будут сохранены исходные документы.

Нажмите кнопку «Далее», чтобы начать анализ файлов.

Ход обработки отображается в блоке «Прогресс обработки». Если возникли проблемы при анализе определённого файла, нажмите «Пропустить файл», тогда будет продолжена обработка остальных файлов, или «Прервать обработку». Анализ подписей больших файлов может производиться продолжительное время.

После того, как файлы обработаются, программа перейдёт к шагу выбора сертификатов (Рисунок 27).

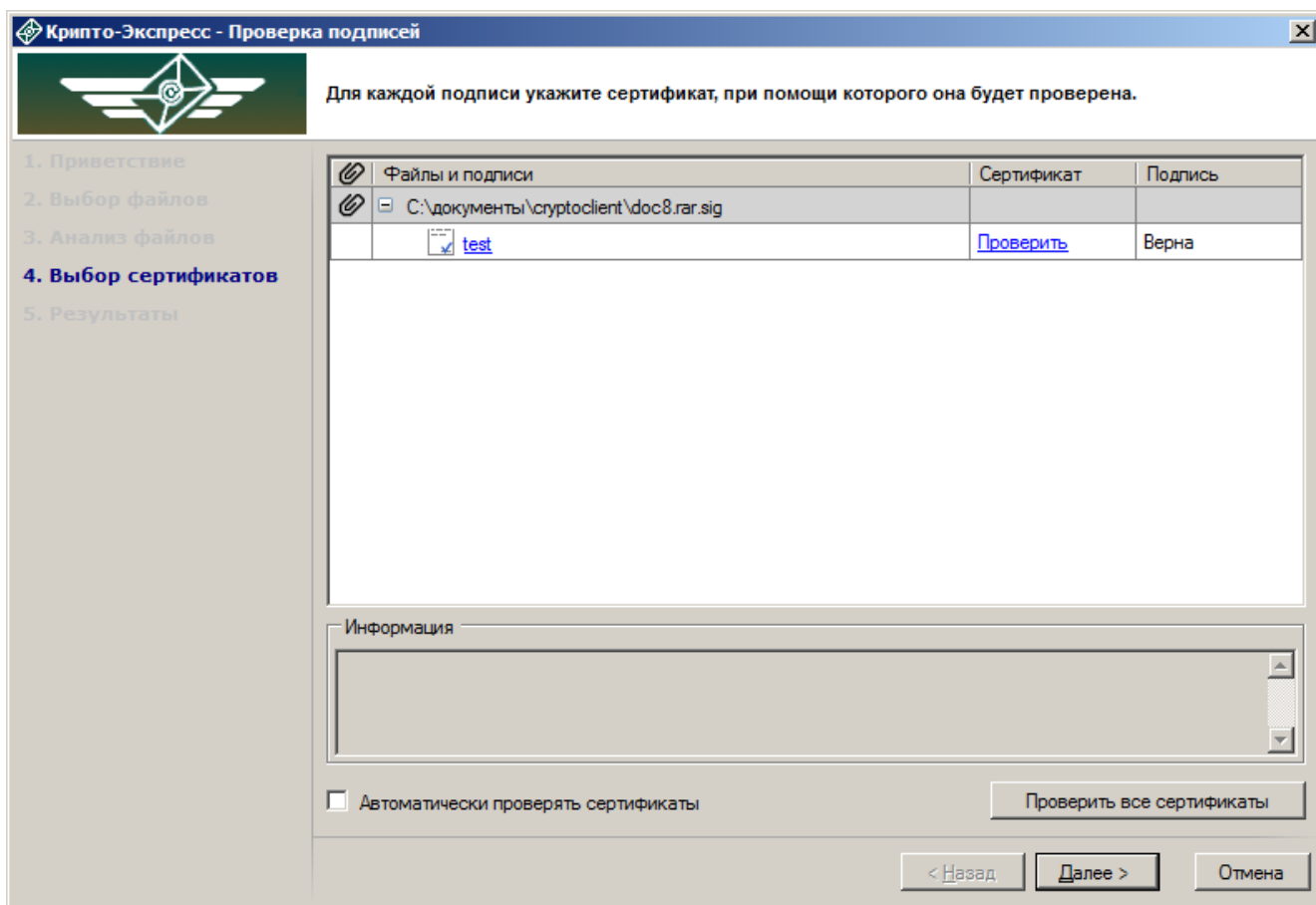


Рисунок 27. Выбор сертификатов для проверки подписей

На этом шаге для каждой подписи нужно проверить сертификаты подписи. Для этого нажмите ссылку «Проверить» в строке интересующей подписи или кнопку «Проверить все сертификаты». Для автоматической проверки сертификатов на этом шаге поставьте галку «Автоматически проверять сертификаты».

Если при создании файла с подписью была указана настройка «Не добавлять сертификаты в файл с подписью» (см. Подписание файлов), а на компьютере пользователя нет требуемого сертификата для проверки, то в таблице выбора сертификатов будет отображена информация о сертификате, который должен быть установлен для проверки подписи. В этом случае информация о подписи будет выглядеть следующим образом:

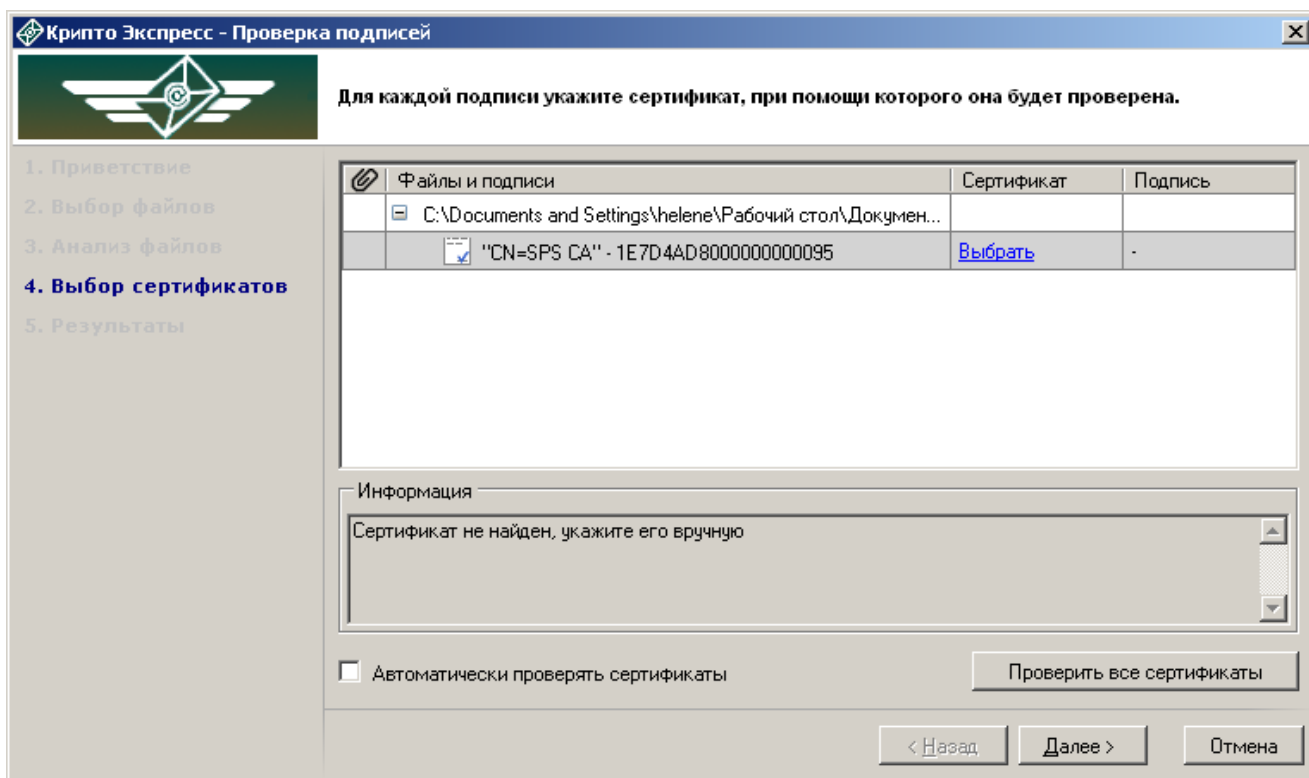


Рисунок 28. Не найден сертификат для проверки подписи

Выберите вручную необходимый сертификат. Для этого нажмите ссылку «Выбрать» в строке с информацией о подписи, откроется окно выбора сертификатов. Если сертификат отсутствует в хранилище, загрузите его с ключевого носителя в хранилище «Личные» или их файла в хранилище «Другие пользователи». Процедура загрузки сертификатов аналогична описанной в пункте Шифрование файлов.

В таблице «Файлы и подписи» отображаются файлы, подписи и результат проверки подписей, а также сведения о валидности сертификата, с помощью которого был подписан файл.

В поле «Информация» показывается описание возможной проблемы.

Для автоматической проверки сертификатов поставьте отметку в нижней части формы: «Автоматически проверять сертификаты», или же запустите проверку сертификатов вручную, нажав кнопку «Проверить все сертификаты».

Для того, чтобы перейти к заключительному шагу проверки (Рисунок 29Рисунок 29), нажмите кнопку «Далее».

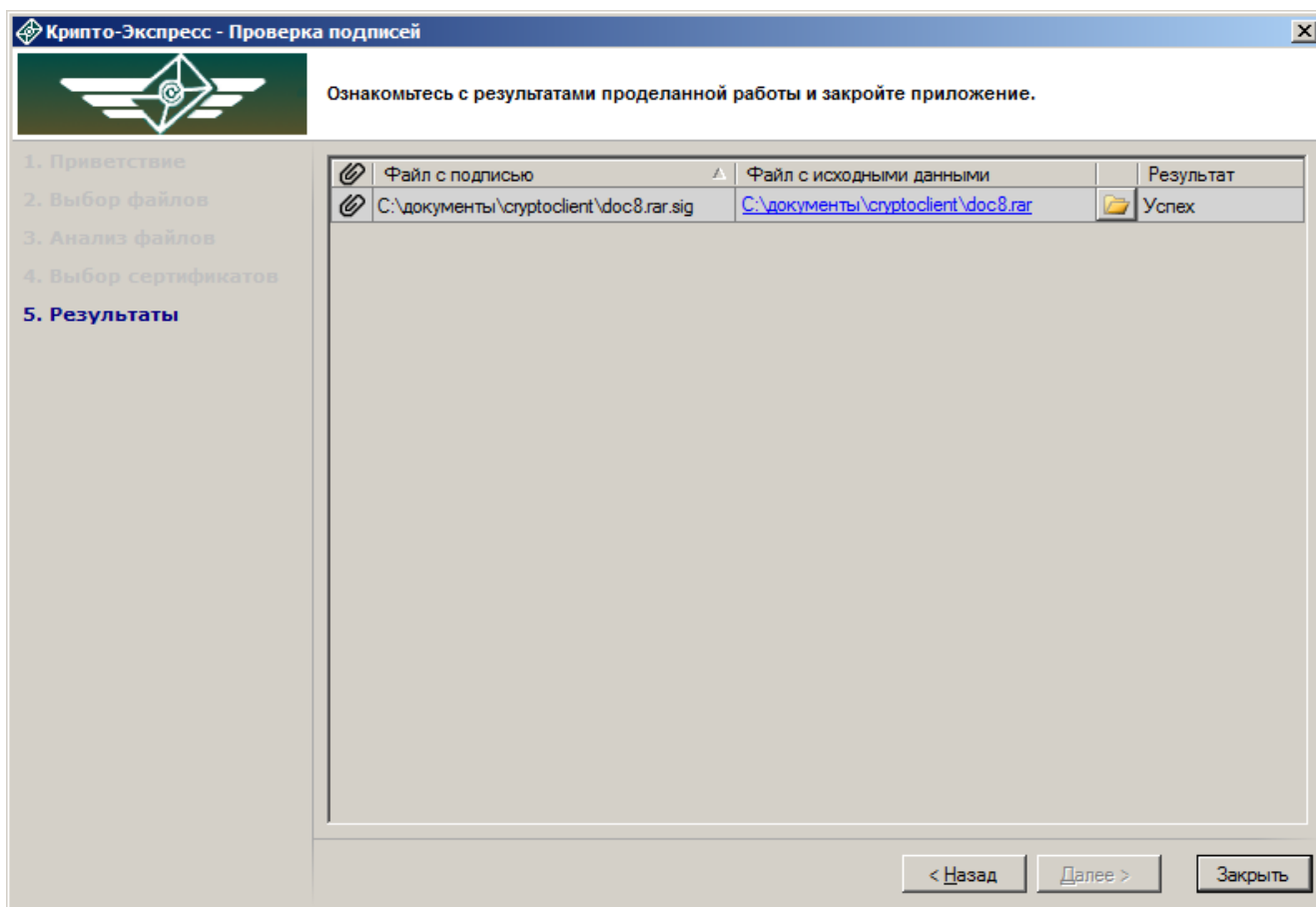


Рисунок 29. Результаты проверки подписей

Результаты проверки подписей показываются в виде общей таблицы. Если возникли проблемы с шифрованием одного или нескольких файлов, это будет отражено в графе «Результат».

Можно открыть исходный документ, нажав на ссылку в поле «Файл с исходными данными» или открыть папку, в которую документ был сохранён, нажав значок с изображением папки.

Для того, чтобы закончить работу Мастера, нажмите кнопку «Заккрыть».

4.6. Добавление подписей к файлу

Если необходимо добавить подпись к файлу, ранее подписанному с помощью другого сертификата, воспользуйтесь Мастером добавления электронной цифровой подписи к файлу с подписью.

Чтобы добавить подписи к файлам уже содержащим подписи, необходимо предварительно выполнить следующие действия:

- выбрать файлы с подписями;
- выбрать сертификаты добавляемых подписей.

Для того, чтобы добавить подпись к файлу с подписями, выберите в меню главного окна программы (Рисунок 16) пункт «Подпись» и нажмите кнопку «Добавить», либо через меню проводника Windows (Рисунок 1) нажмите правую кнопку мыши и выберите «Крипто-Экспресс → Добавить подпись...», предварительно выделив файл или несколько файлов, которые нужно обработать.

Откроется окно приветствия Мастера добавления электронной цифровой подписи к файлу с подписью (Рисунок 30).

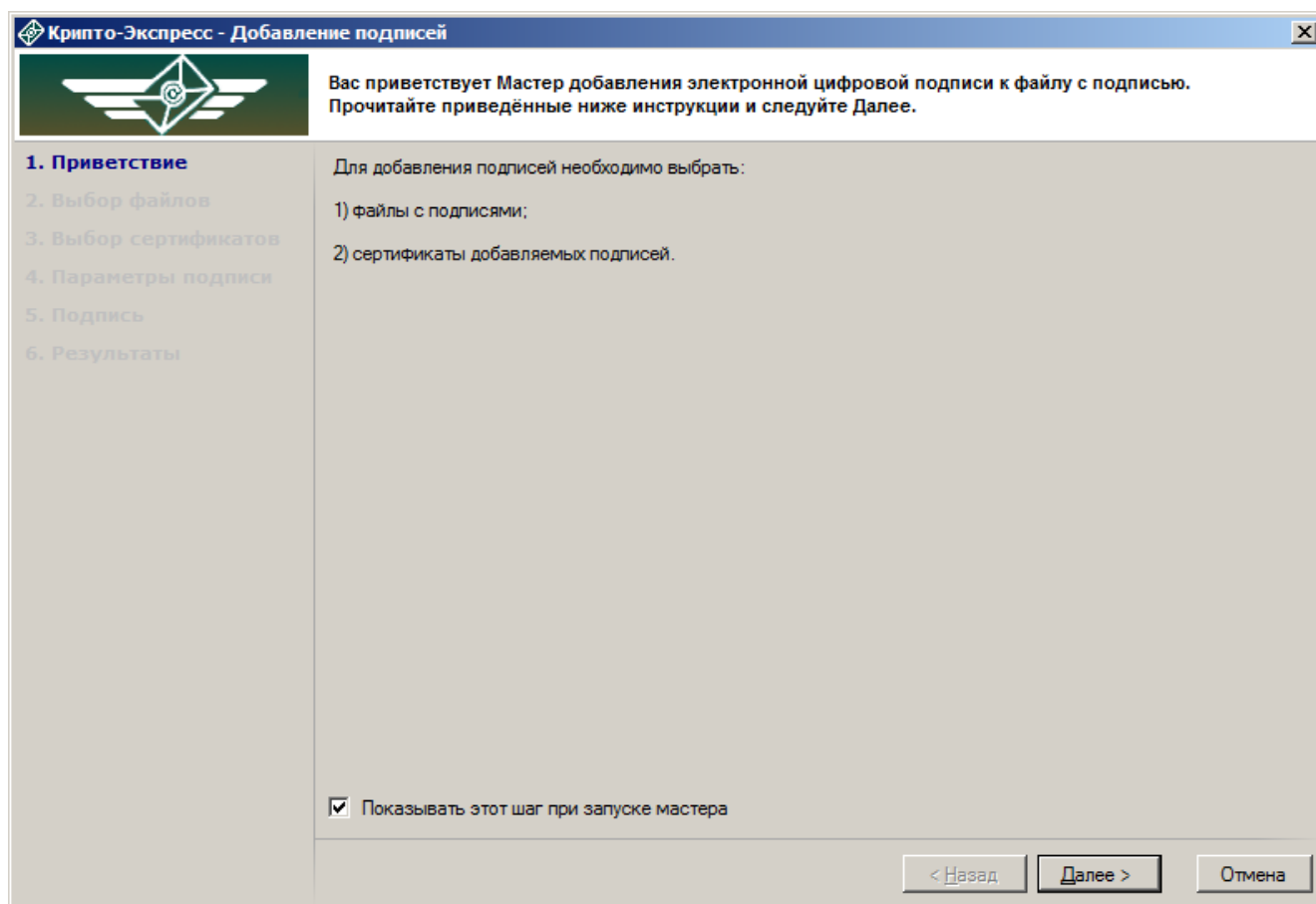


Рисунок 30. Приветствие Мастера добавления электронной цифровой подписи к файлу с подписью

Чтобы больше не выводить приветствие, уберите галочку в нижней части формы.

Нажмите «Далее», чтобы перейти к шагу выбора файлов (Рисунок 31).

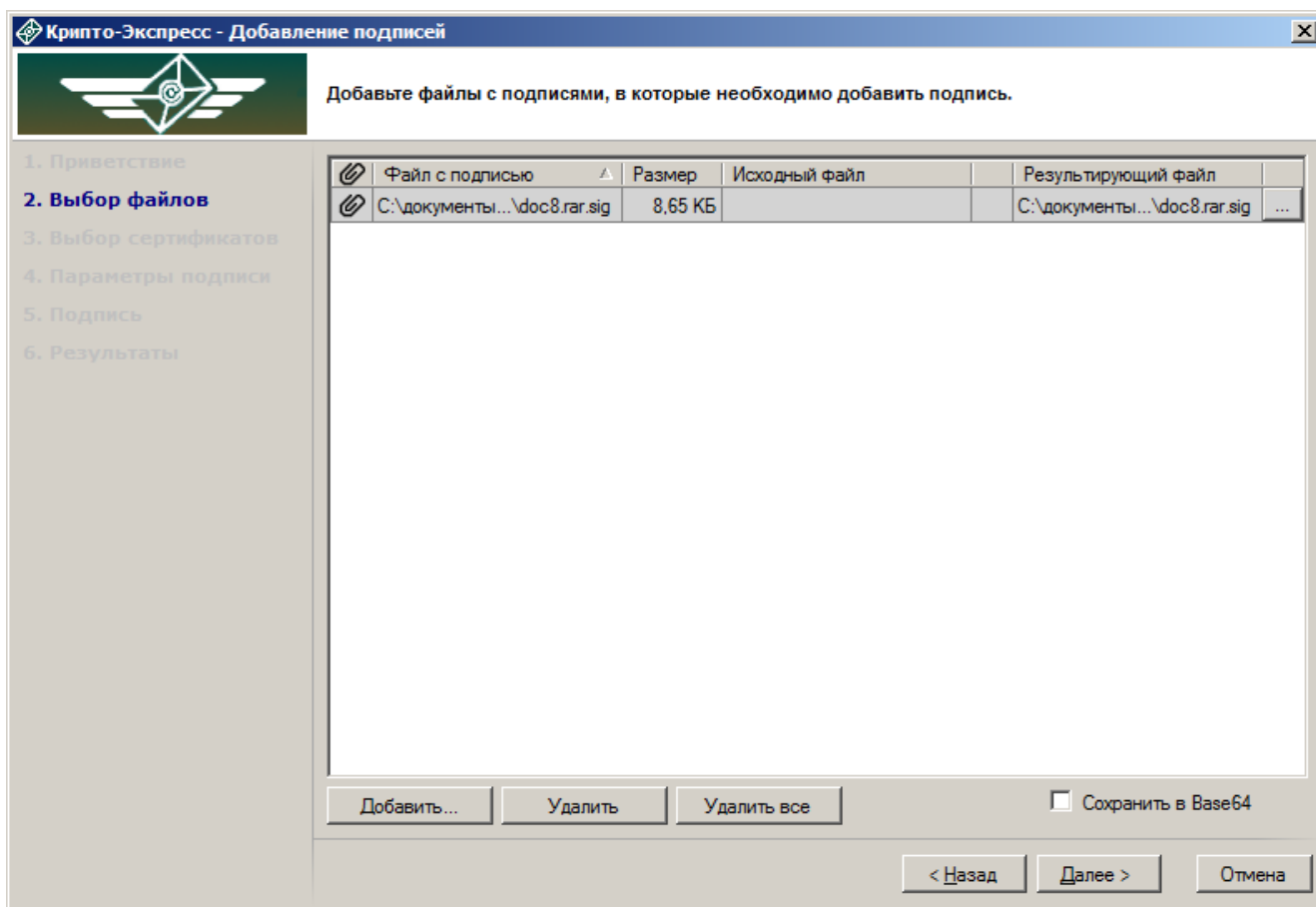


Рисунок 31. Выбор файлов для добавления подписей

На этом шаге нужно добавить файлы с подписями, в которые необходимо добавить подпись. Если файлы уже были выбраны, они отобразятся в таблице окна. Если файлы ещё не были выбраны или необходимо добавить ещё несколько файлов для подписывания, воспользуйтесь кнопкой «Добавить» под таблицей, которая откроет стандартное окно выбора файлов.

В случае, если файл подписи не содержит исходного файла, необходимо указать исходный файл в соответствующем поле.

Чтобы удалить ненужные файлы из обработки или полностью очистить таблицу, выделите строки с файлами и нажмите «Удалить» или «Удалить все» соответственно.

В таблице выбора файлов выводятся следующие сведения:

- имя подписываемого файла и его расположение на жестком диске;
- размер файла;
- исходный файл;
- имя файла с подписью, к которому будет добавлена подпись (результирующий файл) и место на жестком диске, куда он будет сохранён.

Имя результирующего файла и путь для сохранения можно изменить, нажав на кнопку в правой части строки и сделав необходимые изменения через стандартный диалог сохранения.

Если файл с таким именем уже существует в папке, куда сохраняется результат обработки (в поле «Результирующий файл» выведено предупреждение об этом), рекомендуется выбрать другую папку или изменить имя результирующего файла.

Если не стоит галочка «Сохранить в Base64», файлы с подписью сохраняются в кодировке DER.

Для перехода к шагу выбора сертификатов нажмите кнопку «Далее».

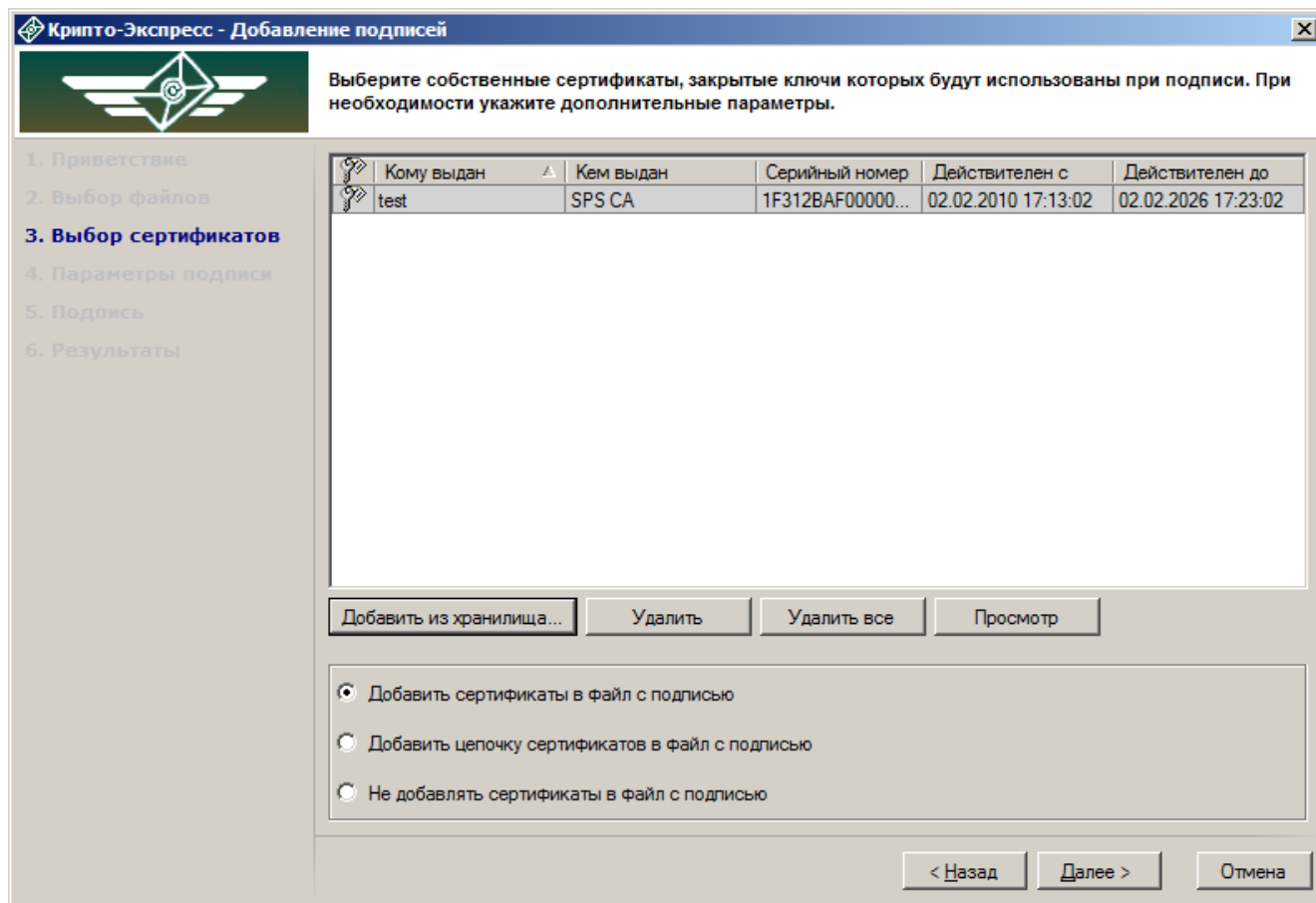


Рисунок 32. Выбор сертификатов для подписи

На этом шаге необходимо выбрать собственные сертификаты, закрытые ключи которых будут использованы при подписи. Их можно добавить в таблицу из хранилища сертификатов.

Для того чтобы добавить сертификат из хранилища, нажмите кнопку «Добавить из хранилища». Откроется форма выбора сертификатов (Рисунок 33).

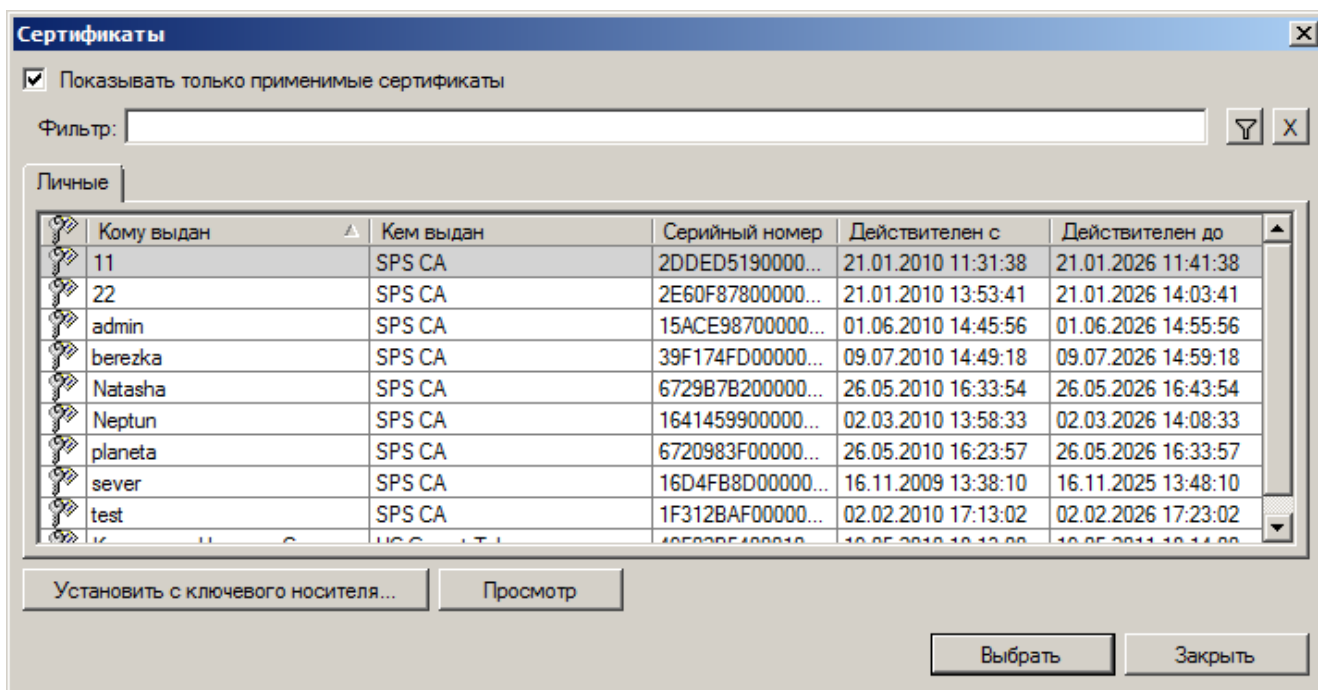


Рисунок 33. Выбор сертификата для подписи файла с подписью из хранилища «Личные»

При необходимости можно установить сертификат с ключевого носителя. Чтобы установить сертификат с ключевого носителя в хранилище «Личные», убедитесь, что ключевой носитель подключен и нажмите соответствующую кнопку под списком сертификатов. Откроется форма «Сертификаты на ключевых носителях», в которой можно выбрать необходимый сертификат.

Для просмотра сертификата выберите его в списке и нажмите кнопку «Просмотр».

Выделив строку с нужным сертификатом, нажмите кнопку «Выбрать».

При необходимости в форме выбора (Рисунок 32) можно указать одно из следующих действий:

- Добавить сертификаты в файл с подписью;
- Добавить цепочку сертификатов в файл с подписью;
- Не добавлять сертификаты в файл с подписью.

По умолчанию выбрано «Добавить сертификаты в файл с подписью».

Нажмите кнопку «Далее». Шаг «Параметры подписи» (Рисунок 34) даёт пользователю возможность указать дополнительные параметры подписи: добавить штампы времени на подписываемые данные и на подпись, а также включить в файл с подписью доказательства подлинности (например, цепочку сертификатов до доверенного УЦ).

Крипто-Экспресс - Добавление подписей

Укажите параметры, которые необходимо добавить к подписи.

1. Приветствие
2. Выбор файлов
3. Выбор сертификатов
4. Параметры подписи
5. Подпись
6. Результаты

☐ Включить в подпись доказательства подлинности

Адрес службы штампов времени:

☐ Включить штамп времени на подписываемые данные

Адрес

☐ Включить штамп времени на подпись

Адрес

Рисунок 34. Дополнительные атрибуты подписи при добавлении подписей

Этот шаг можно пропустить, нажав кнопку «Далее», чтобы продолжить обработку и перейти к шагу добавления подписи (Рисунок 35).

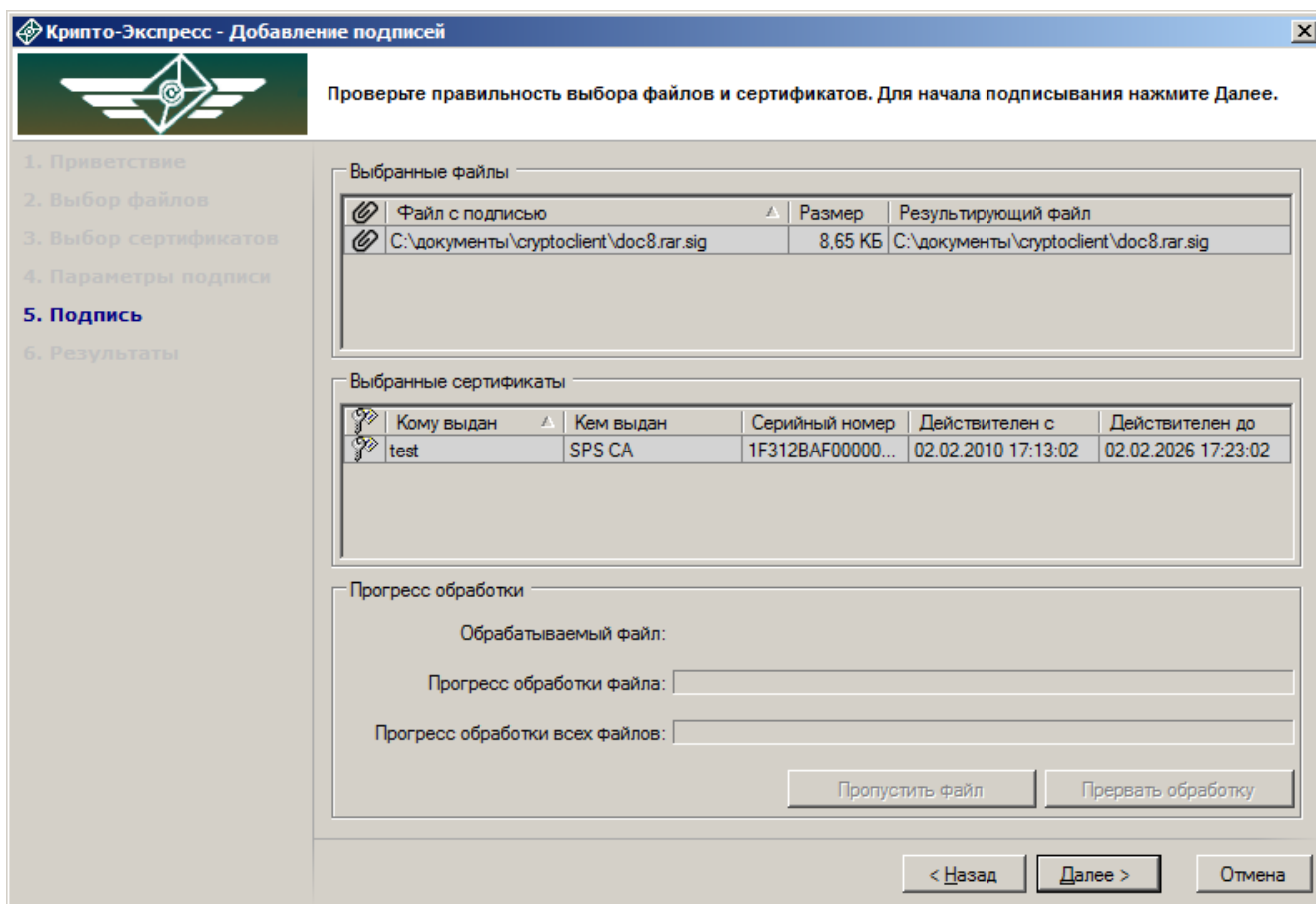


Рисунок 35. Добавление подписи

На этом шаге выводятся список «Выбранные файлы» и список «Выбранные сертификаты». Для того, чтобы начать подписывание, нажмите кнопку «Далее».

Ход обработки отображается в блоке «Прогресс обработки». Если возникли проблемы при подписывании определённого файла с подписью, нажмите «Пропустить файл», тогда будет продолжена обработка остальных файлов, или «Прервать обработку». Обработка больших файлов может производиться продолжительное время.

После того, как файлы обработаются, на экран будет выведено окно со следующим шагом – «Результаты» (Рисунок 36).

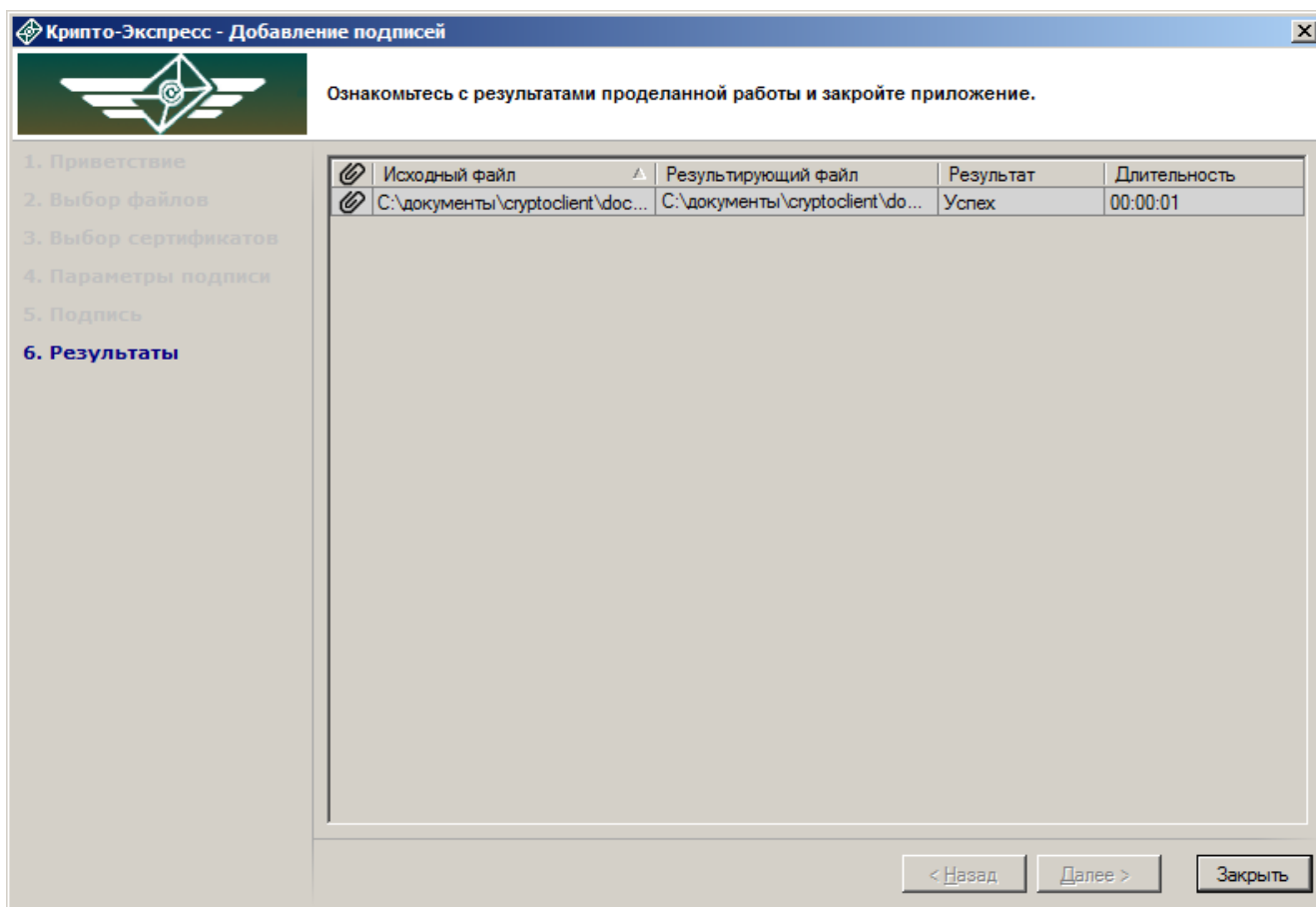


Рисунок 36. Результаты добавления подписи

Результаты обработки показываются в виде таблицы. Если возникли проблемы с подписанием одного или нескольких файлов, это будет отражено в графе «Результат».

Для того чтобы закончить работу Мастера нажмите кнопку «Заккрыть».

4.7. Визирование подписей

В программе предусмотрена функция визирования (заверения) подписей файлов с подписями.

Чтобы завизировать подпись, необходимо предварительно выполнить следующие действия:

- выбрать файлы с подписями;
- выбрать подписи, которые необходимо завизировать;
- выбрать личные сертификаты, с помощью которых будут завизированы подписи.

Для того, чтобы завизировать подписи, выберите в меню главного окна программы (Рисунок 16) пункт «Подпись» и нажмите кнопку «Визировать», либо через меню проводника Windows (Рисунок 1) нажмите правую кнопку мыши и выберите «Крипто-Экспресс → Визировать подпись...», предварительно выделив файл или несколько файлов, которые нужно обработать.

Откроется окно приветствия Мастера визирования электронных цифровых подписей (Рисунок 37).

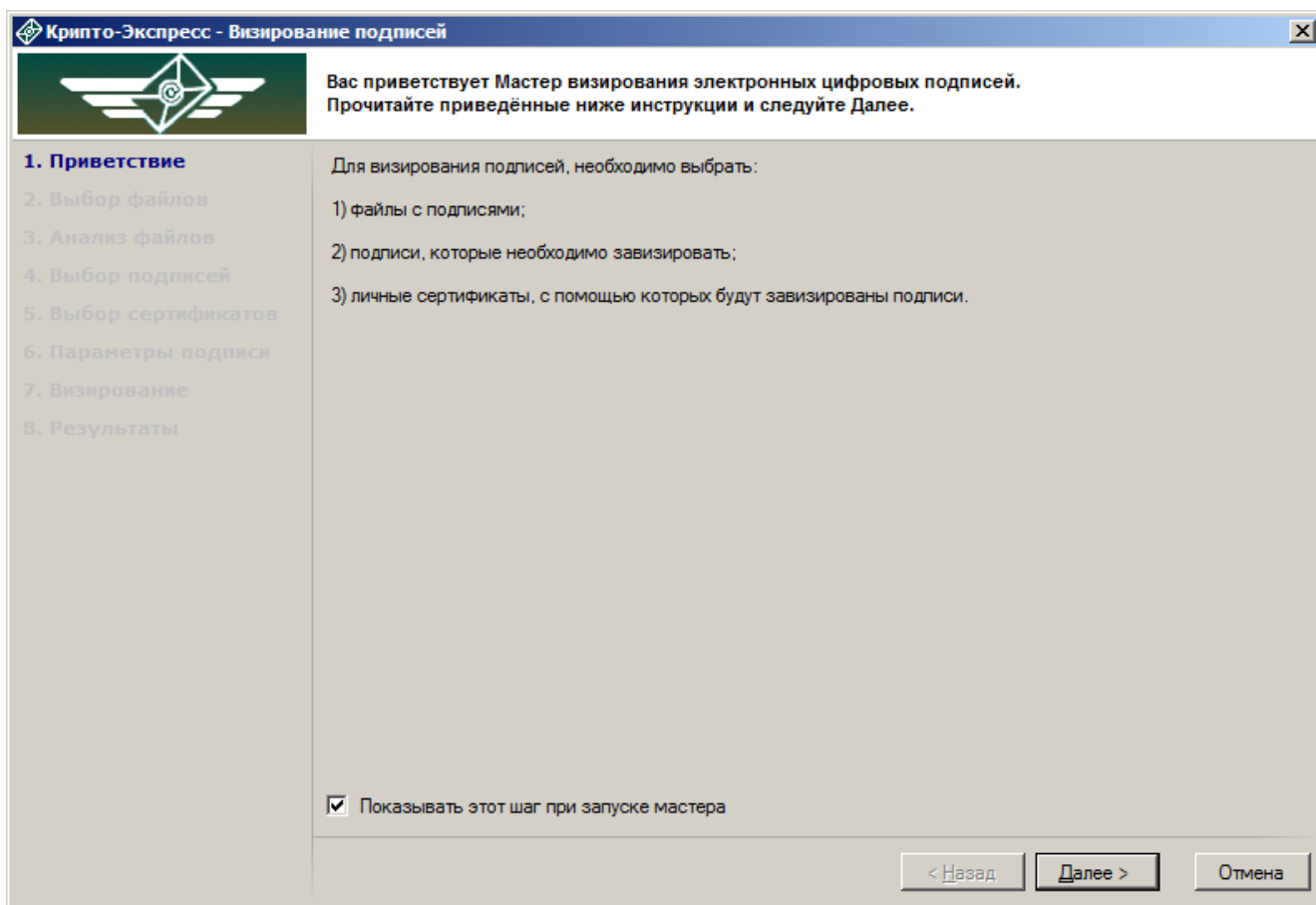


Рисунок 37. Приветствие мастер визирования электронных цифровых подписей

Чтобы больше не выводить приветствие, уберите галочку в нижней части формы.

Нажмите «Далее», чтобы перейти к шагу выбора файлов (Рисунок 38).

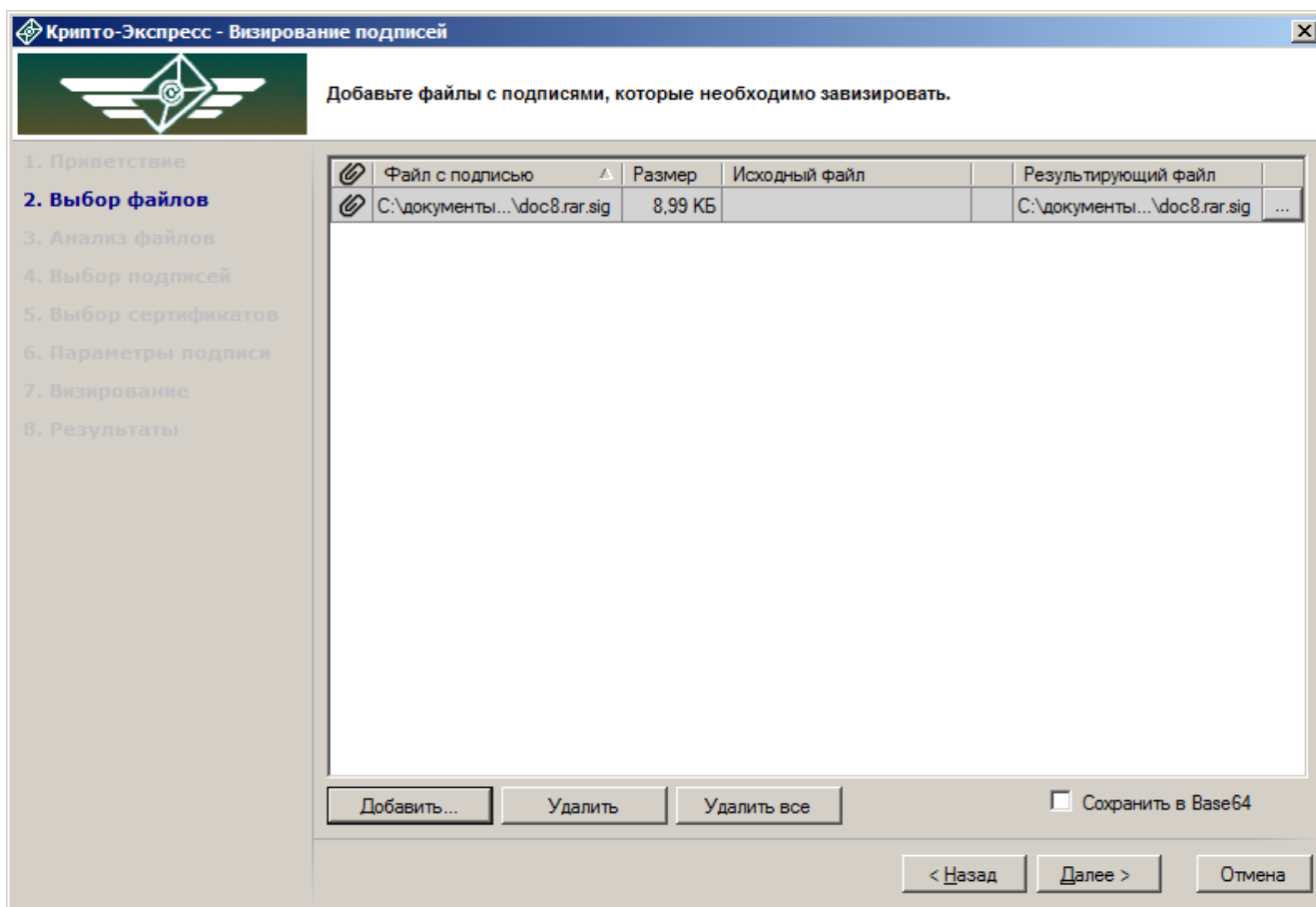


Рисунок 38. Выбор файлов с подписями, которые необходимо завизировать

На этом шаге нужно добавить файлы с подписями, которые необходимо завизировать. Если файлы уже были выбраны, они отобразятся в таблице окна. Если файлы ещё не были выбраны или необходимо добавить ещё несколько файлов для визирования, воспользуйтесь кнопкой «Добавить» под таблицей, которая откроет стандартное окно выбора файлов.

В случае, если файл с подписями не содержит исходного файла, требуется указать исходный файл в соответствующем поле.

Чтобы удалить ненужные файлы из обработки или полностью очистить таблицу, выделите строки с файлами и нажмите «Удалить» или «Удалить все» соответственно.

В таблице выбора файлов выводятся следующие сведения:

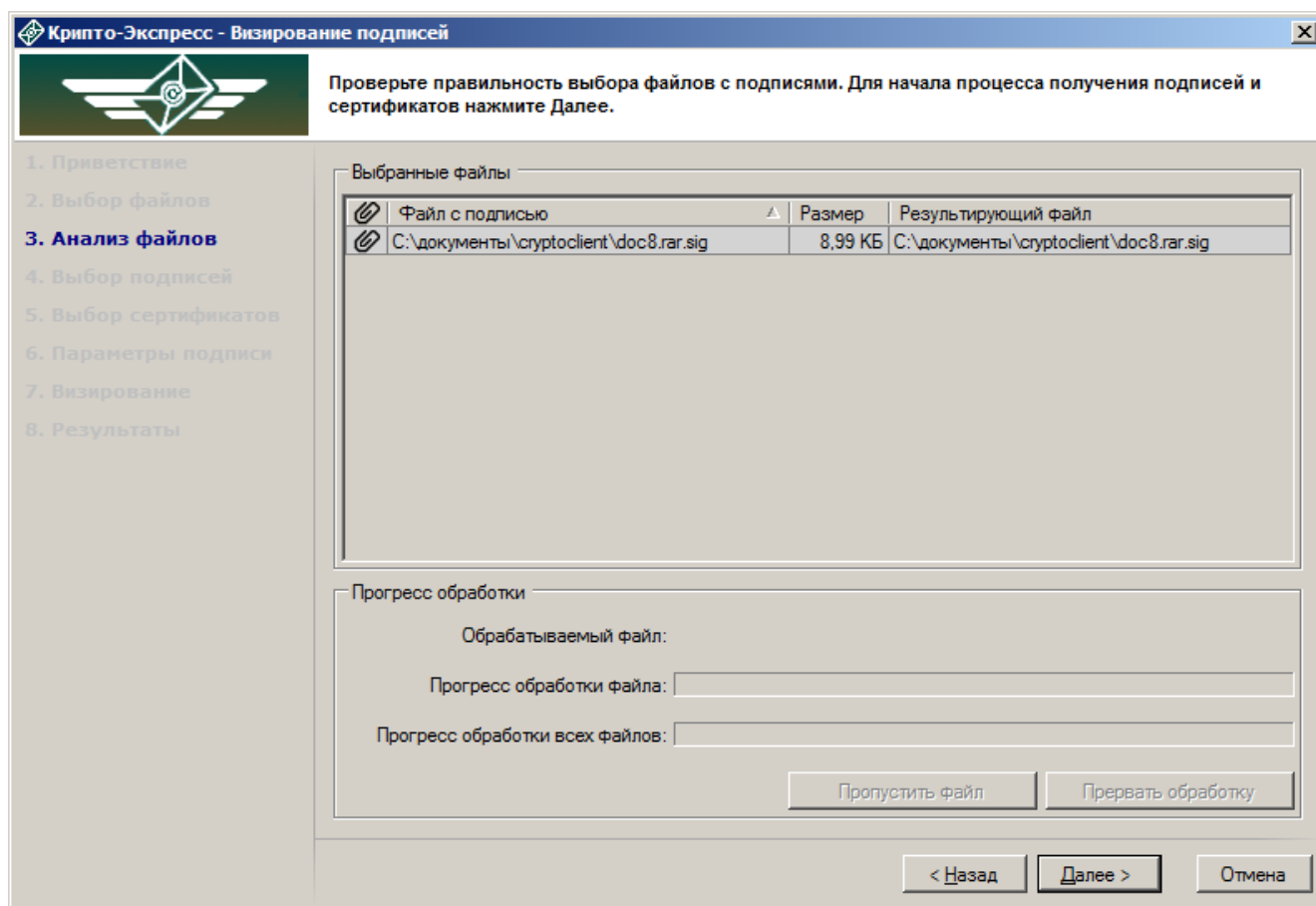
- имя файла с подписью и его расположение на жестком диске;
- размер файла;
- исходный файл;
- имя файла, подпись которого требует визирования (результирующий файл) и место на жестком диске, куда он будет сохранён.

Имя результирующего файла и путь для сохранения можно изменить, нажав на кнопку в правой части строки и сделав необходимые изменения через стандартный диалог сохранения.

Если файл с таким именем уже существует в папке, куда сохраняется результат обработки (в поле «Результирующий файл» выведено предупреждение об этом), рекомендуется выбрать другую папку или изменить имя результирующего файла.

Если не стоит галочка «Сохранить в Base64», файлы с подписью сохраняются в кодировке DER.

Для перехода к анализу файлов нажмите кнопку «Далее».



Список выбранных файлов содержит данные по именам и расположению файлов с подписью, размеру файлов, а также информацию о заданных именах файлов, в которых будут сохранены исходные документы.

Нажмите кнопку «Далее», чтобы начать обработку файлов.

Ход обработки отображается в блоке «Прогресс обработки». Если возникли проблемы при обработке определённого файла, нажмите «Пропустить файл», тогда будет продолжена обработка остальных файлов, или «Прервать обработку». Обработка больших файлов может производиться продолжительное время.

После того, как файлы обработаются, программа перейдёт к шагу выбора сертификатов (Рисунок 39Рисунок 39).

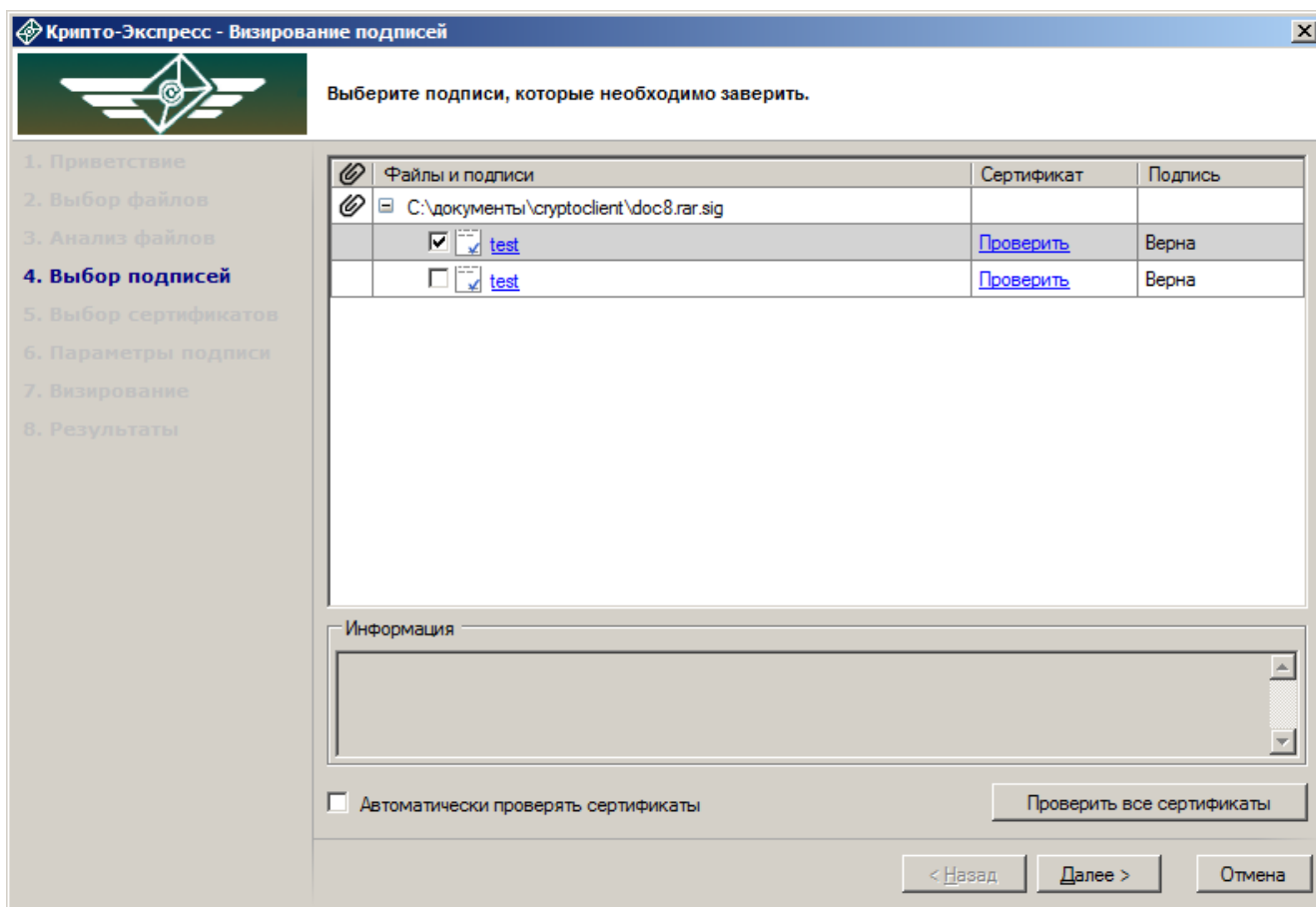


Рисунок 39. Выбор подписей, которые необходимо заверить

Выберите в таблице те подписи к файлам, которые необходимо заверить, отметив их галками. Для проверки валидности сертификатов можно нажать ссылку «Проверить» в строке сертификата, после чего в поле отобразится результат проверки, либо нажмите кнопку «Проверить все сертификаты». После того, как нужные сертификаты проверены и отмечены, нажмите кнопку «Далее» и перейдите к шагу выбора сертификатов, при помощи которых будут завизированы подписи (Рисунок 40).

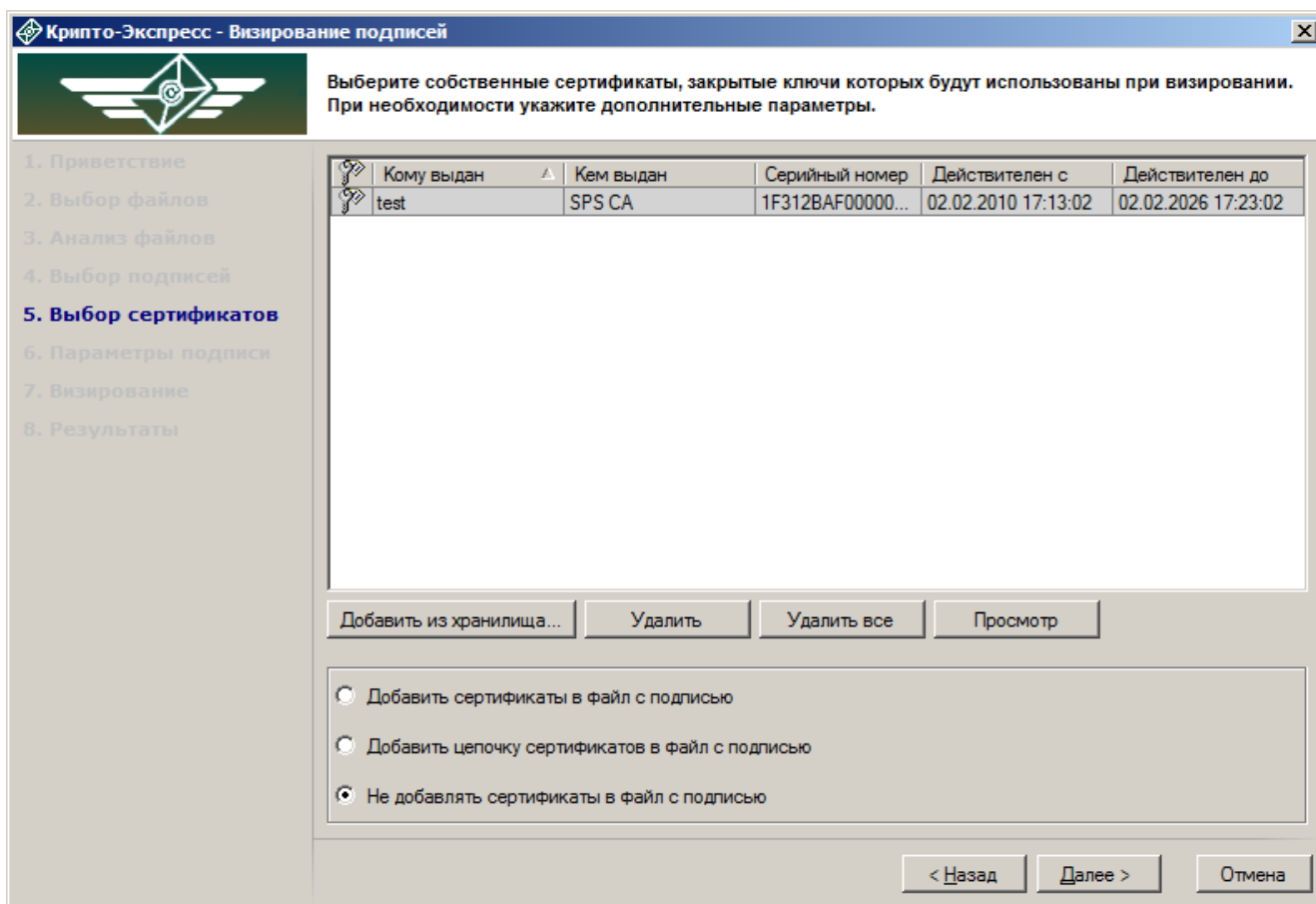


Рисунок 40. Выбор сертификатов для заверения подписей

На этом шаге необходимо выбрать собственные сертификаты, закрытые ключи которых будут использованы при заверении. Их можно добавить в таблицу из хранилища сертификатов.

Для того чтобы добавить сертификат из хранилища, нажмите кнопку «Добавить из хранилища». Откроется форма выбора сертификатов (Рисунок 41).

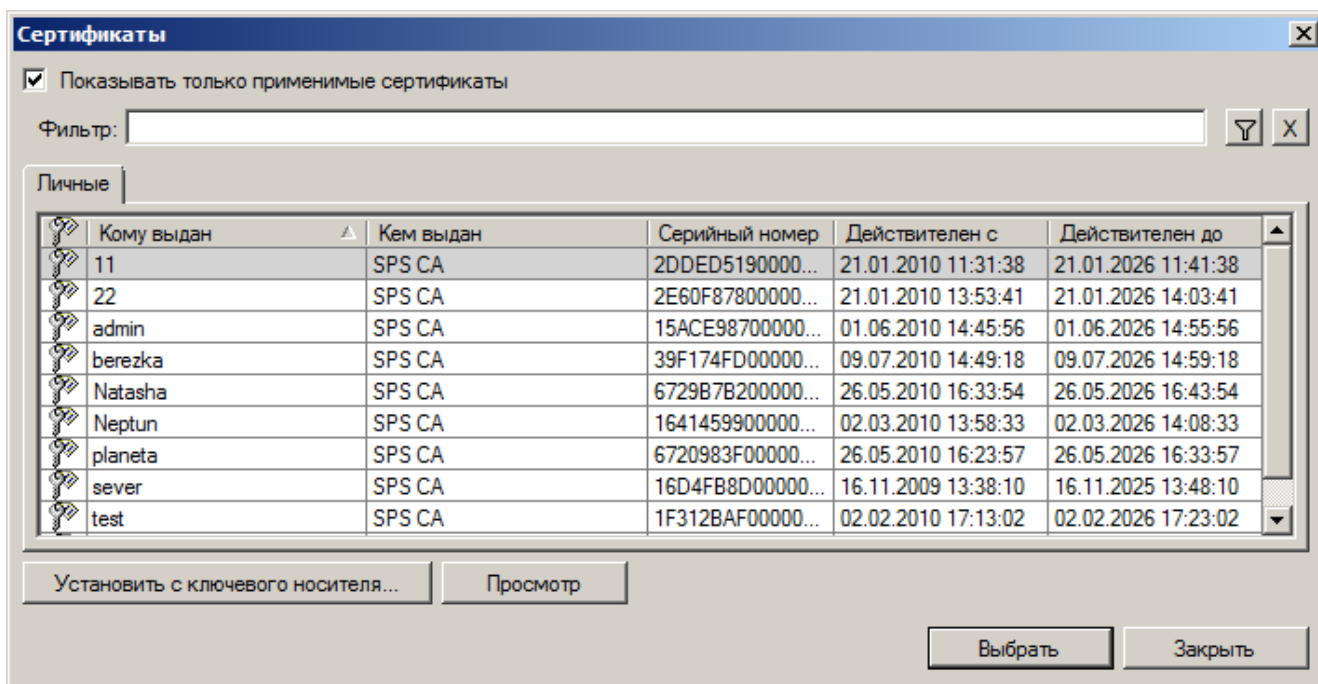


Рисунок 41. Выбор сертификата для заверения подписей файла с подписями из хранилища «Личные»

При необходимости можно установить сертификат с ключевого носителя. Чтобы установить сертификат с ключевого носителя в хранилище «Личные», убедитесь, что ключевой носитель подключен и нажмите соответствующую кнопку под списком сертификатов. Откроется форма «Сертификаты на ключевых носителях», в которой можно выбрать необходимый сертификат.

Для просмотра сертификата выберите его в списке и нажмите кнопку «Просмотр».

Выделив строку с нужным сертификатом, нажмите кнопку «Выбрать».

При необходимости в форме выбора (Рисунок 40Рисунок 32) можно указать одно из следующих действий:

- Добавить сертификаты в файл с подписью;
- Добавить цепочку сертификатов в файл с подписью;
- Не добавлять сертификаты в файл с подписью.

По умолчанию выбрано «Добавить сертификаты в файл с подписью».

Нажмите кнопку «Далее». Шаг «Параметры подписи» (Рисунок 42) даёт пользователю возможность указать дополнительные параметры подписи: добавить штампы времени на подписываемые данные и на подпись, а также включить в файл с подписью доказательства подлинности (например, цепочку сертификатов до доверенного УЦ).

Крипто-Экспресс - Визирование подписей

Укажите параметры, которые необходимо добавить к визирующей подписи.

1. Приветствие
2. Выбор файлов
3. Анализ файлов
4. Выбор подписей
5. Выбор сертификатов
6. Параметры подписи
7. Визирование
8. Результаты

☐ Включить в подпись доказательства подлинности

Адрес службы штампов времени:

☐ Включить штамп времени на подписываемые данные

Адрес

☐ Включить штамп времени на подпись

Адрес

Рисунок 42. Дополнительные атрибуты подписи при визировании файла с подписями

Этот шаг можно пропустить, нажав кнопку «Далее», чтобы продолжить обработку и перейти к шагу визирования (Рисунок 43Рисунок 43).

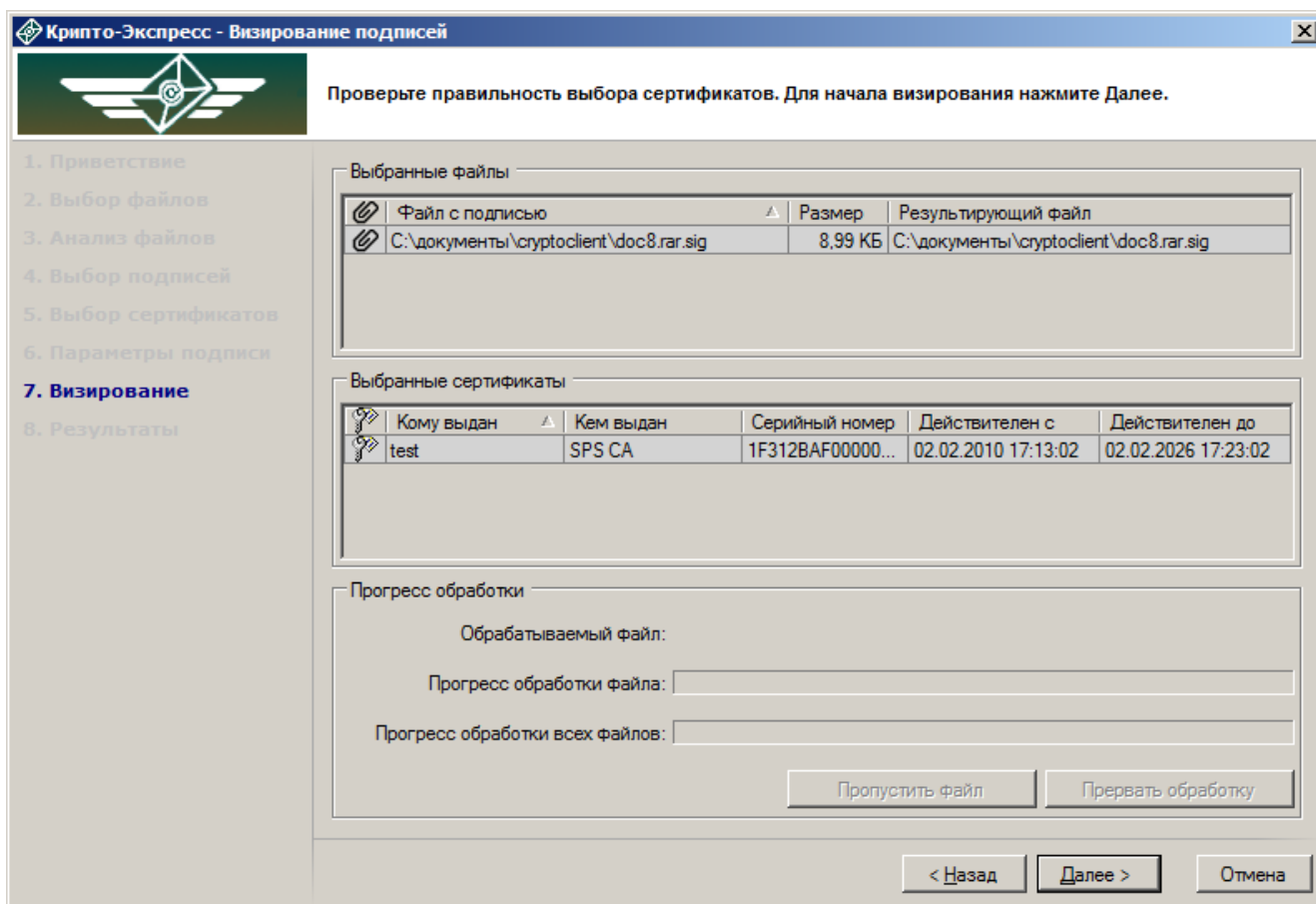


Рисунок 43. Визирование подписей

На этом шаге выводятся список «Выбранные файлы» и список «Выбранные сертификаты». Для того, чтобы начать обработку, нажмите кнопку «Далее».

Ход обработки отображается в блоке «Прогресс обработки». Если возникли проблемы при обработке определённого файла с подписью, нажмите «Пропустить файл», тогда будет продолжена обработка остальных файлов, или «Прервать обработку». Обработка больших файлов может производиться продолжительное время.

После того, как файлы обработаются, на экран будет выведено окно со следующим шагом – «Результаты» (Рисунок 44Рисунок 36).

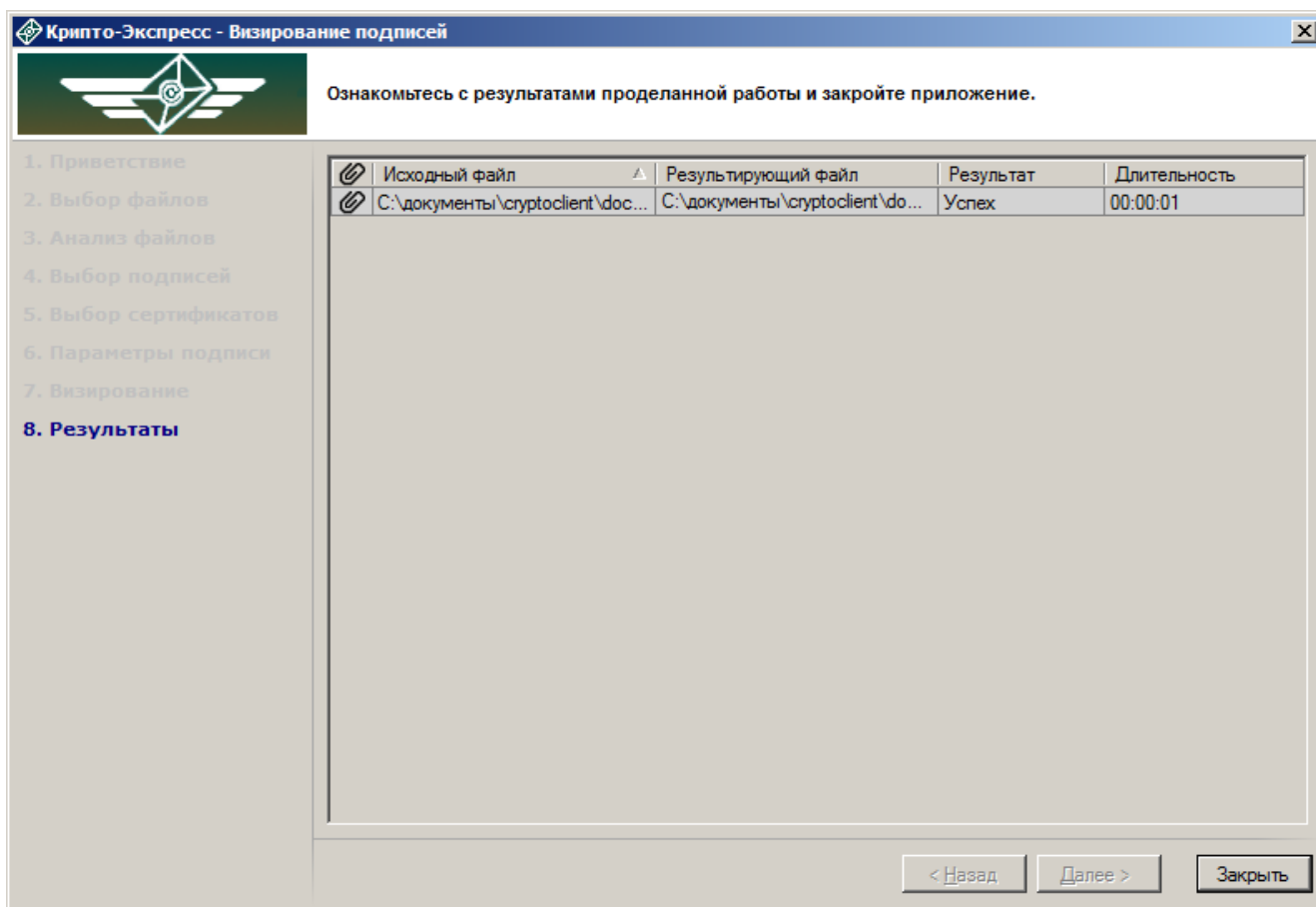


Рисунок 44. Результаты заверения подписей файлов с подписями

Результаты обработки показываются в виде таблицы. Если возникли проблемы с подписанием одного или нескольких файлов, это будет отражено в графе «Результат».

Для того чтобы закончить работу Мастера нажмите кнопку «Заккрыть».

4.8. Удаление подписей

Функция удаления подписи из файла реализована с помощью Мастера удаления электронных цифровых подписей.

Для удаления подписей, необходимо предварительно выполнить следующие действия:

- выбрать файлы с подписями;
- выбрать подписи, которые необходимо удалить;

Для того, чтобы удалить подписи из файлов, выберите в меню главного окна программы (Рисунок 16) пункт «Подпись» и нажмите кнопку «Удалить», либо через меню проводника Windows (Рисунок 1) нажмите правую кнопку мыши и выберите «Крипто-Экспресс → Удалить подпись...», предварительно выделив файл или несколько файлов, которые нужно обработать.

Откроется окно приветствия Мастера удаления электронных цифровых подписей (Рисунок 45Рисунок 45).

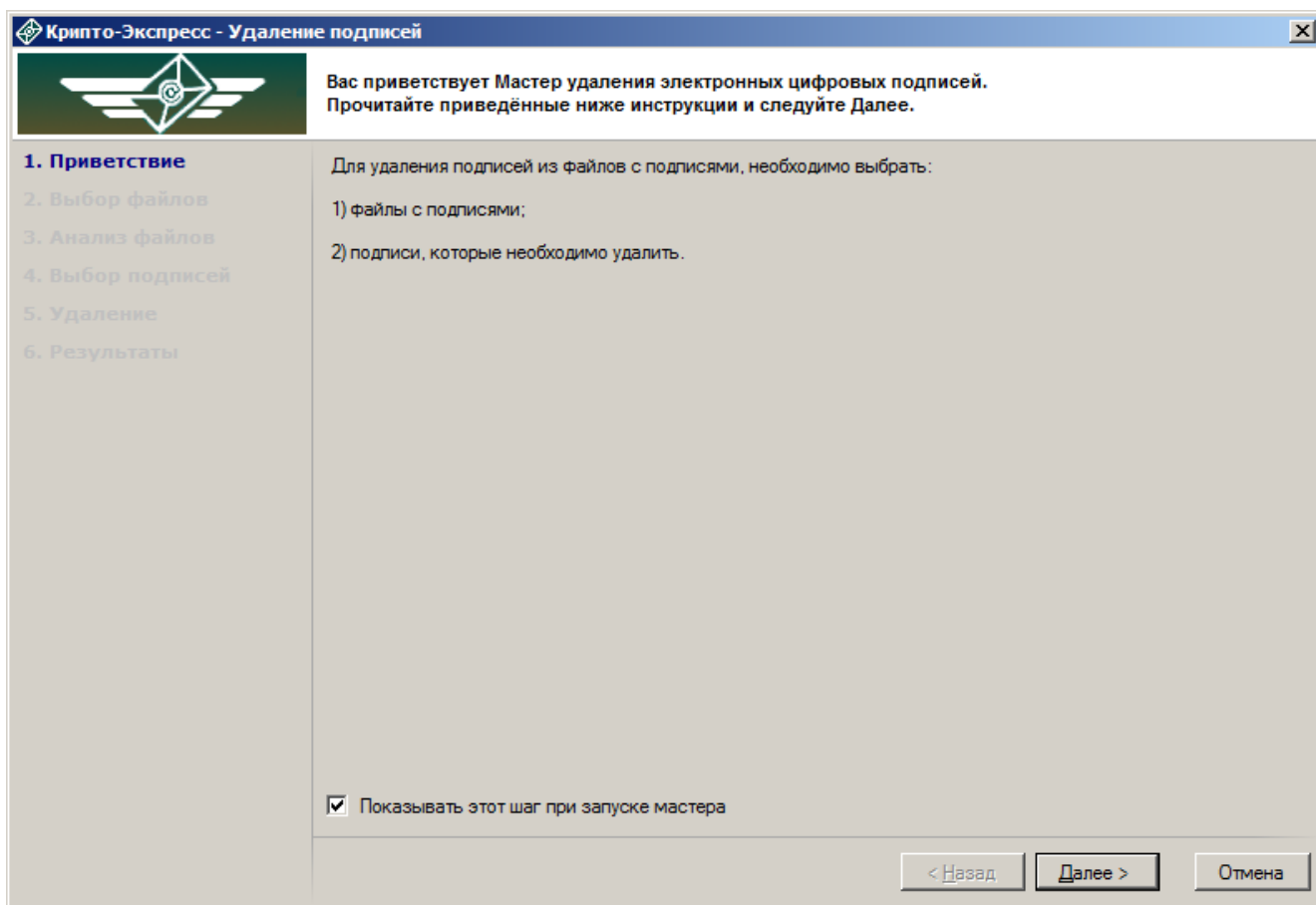


Рисунок 45. Приветствие Мастера удаления электронных цифровых подписей

Чтобы больше не выводить приветствие, уберите галочку в нижней части формы.

Нажмите «Далее», чтобы перейти к шагу выбора файлов (Рисунок 46Рисунок 38).

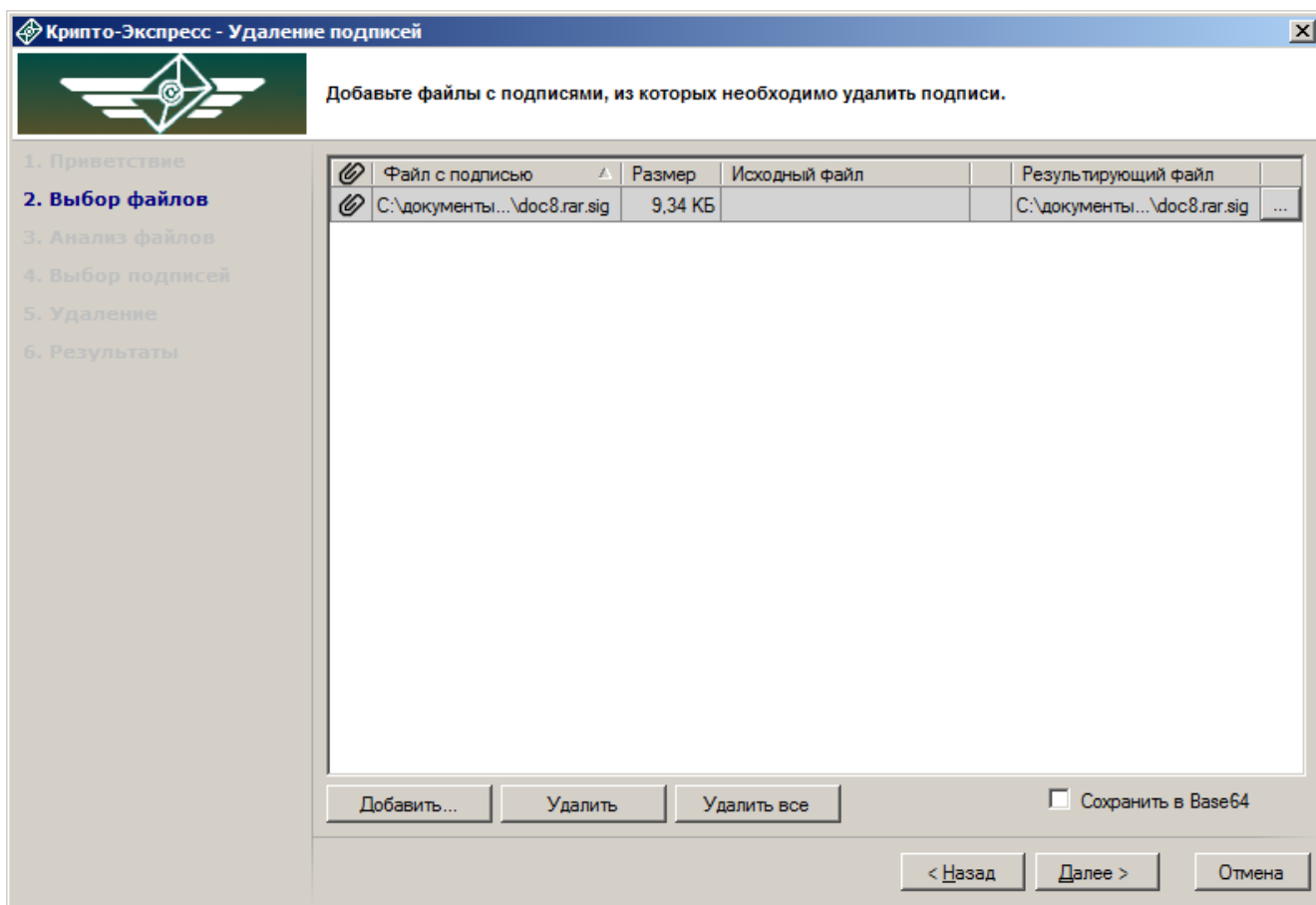


Рисунок 46. Выбор файлов, из которых необходимо удалить подписи

На этом шаге нужно добавить в таблицу файлы с подписями, из которых необходимо удалить подписи. Если файлы уже были выбраны, они отобразятся в таблице окна. Если файлы ещё не были выбраны или необходимо добавить ещё несколько файлов для визирования, воспользуйтесь кнопкой «Добавить» под таблицей, которая откроет стандартное окно выбора файлов.

В случае, если файл с подписями не содержит исходного файла, требуется указать исходный файл в соответствующем поле.

Чтобы удалить ненужные файлы из обработки или полностью очистить таблицу, выделите строки с файлами и нажмите «Удалить» или «Удалить все» соответственно.

В таблице выбора файлов выводятся следующие сведения:

- имя файла с подписью и его расположение на жестком диске;
- размер файла;
- исходный файл;
- имя результирующего файла и место на жестком диске, куда он будет сохранён.

Имя результирующего файла и путь для сохранения можно изменить, нажав на кнопку в правой части строки и сделав необходимые изменения через стандартный диалог сохранения.

Если файл с таким именем уже существует в папке, куда сохраняется результат обработки (в поле «Результирующий файл» выведено предупреждение об этом), рекомендуется выбрать другую папку или изменить имя результирующего файла.

Для перехода к анализу файлов нажмите кнопку «Далее».

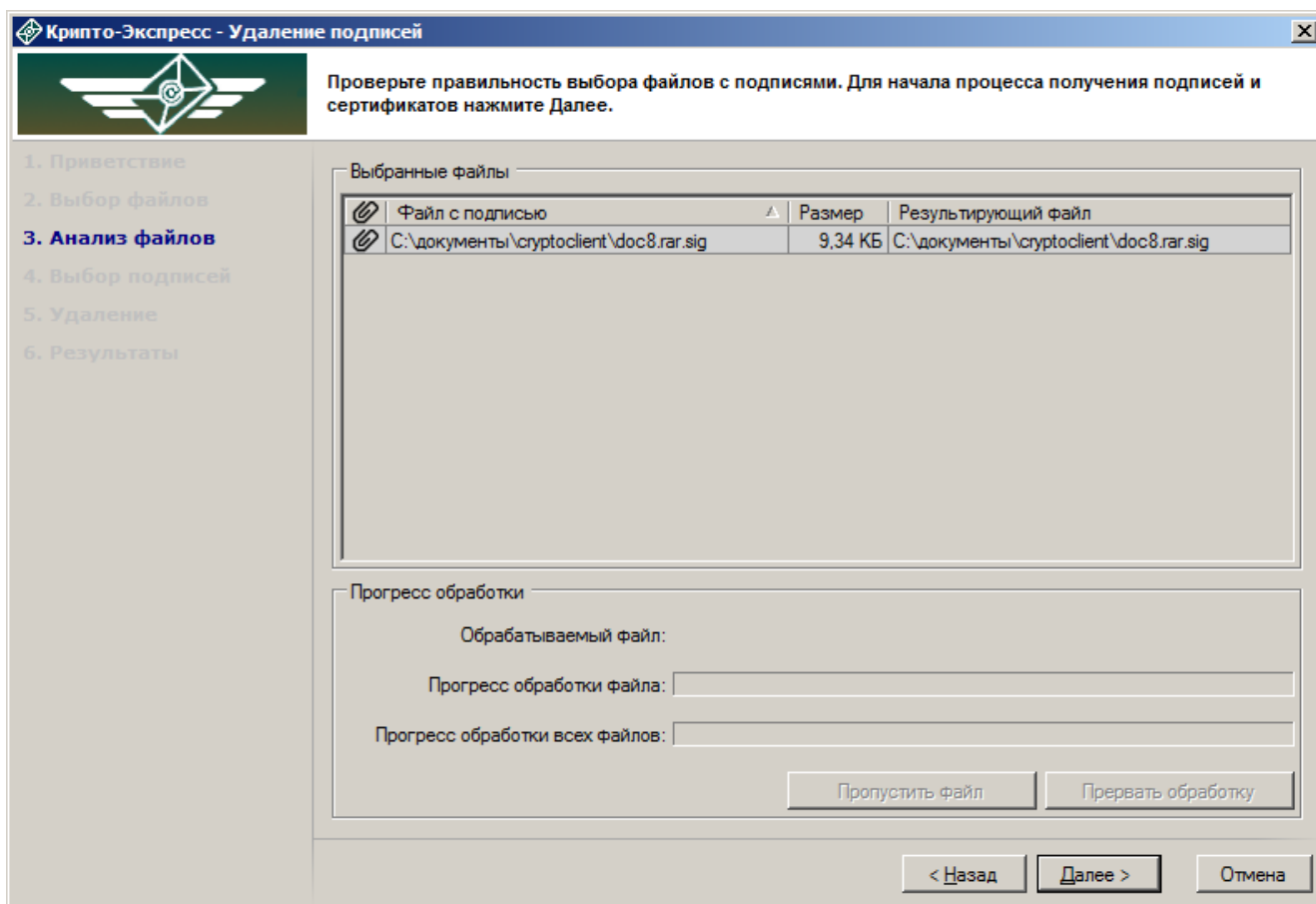


Рисунок 47. Анализ файлов с подписями

Список выбранных файлов содержит данные по именам и расположению файлов с подписью, размеру файлов, а также информацию о заданных именах результирующих файлов.

Нажмите кнопку «Далее», чтобы начать обработку файлов, получение подписей и сертификатов.

Ход обработки отображается в блоке «Прогресс обработки». Если возникли проблемы при обработке определённого файла, нажмите «Пропустить файл», тогда будет продолжена обработка остальных файлов, или «Прервать обработку». Обработка больших файлов может производиться продолжительное время.

После того, как файлы обработаются, программа перейдёт к шагу выбора подписей для удаления (Рисунок 48Рисунок 48).

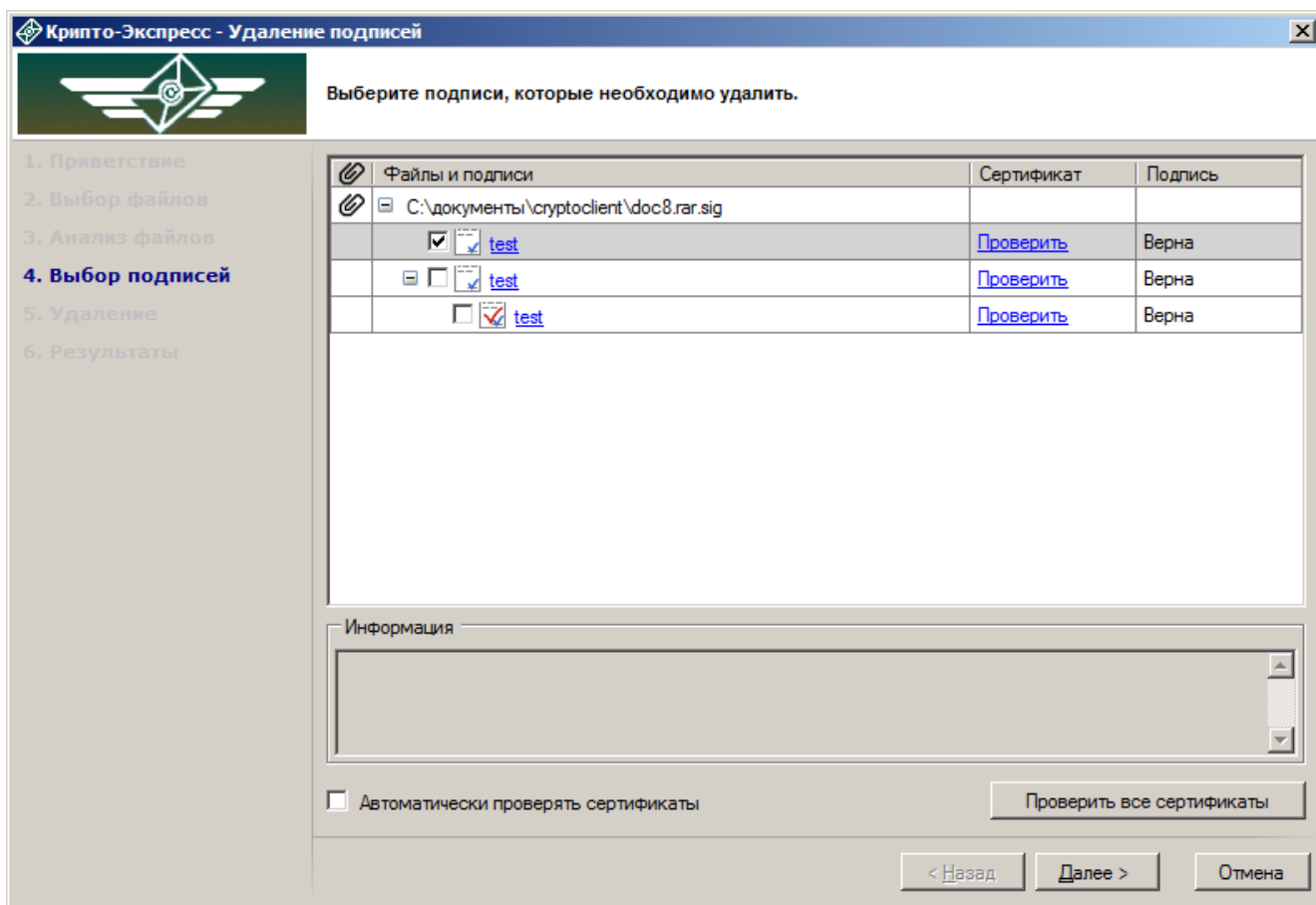


Рисунок 48. Выбор подписей для удаления

Выберите в таблице те подписи к файлам, которые необходимо удалить, отметив их галками. Если необходима проверка валидности сертификатов можно нажать ссылку «Проверить» в строке сертификата, после чего в поле отобразится результат проверки, либо нажмите кнопку «Проверить все сертификаты». После того, как нужные сертификаты проверены и отмечены подписи, которые нужно удалить, нажмите кнопку «Далее» и перейдите к шагу удаления подписей (Рисунок 49).

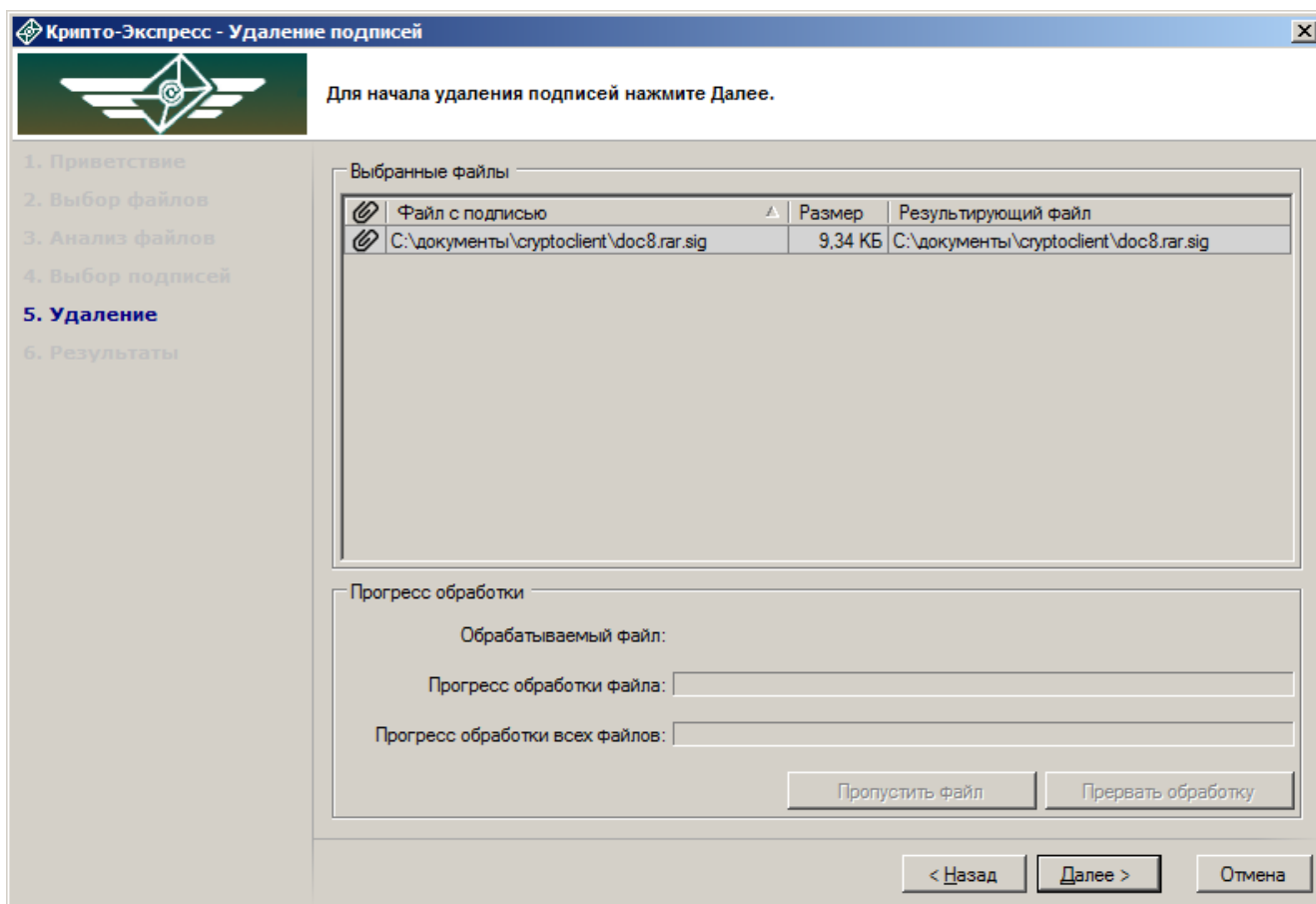


Рисунок 49. Удаление подписей

В окне программы отображен список файлов, которые будут обработаны, имена и расположение файлов, в который будут сохранены данные.

Нажмите кнопку «Далее», чтобы начать удаление подписей.

Ход обработки отображается в блоке «Прогресс обработки». Если возникли проблемы при обработке определённого файла, нажмите «Пропустить файл», тогда будет продолжена обработка остальных файлов, или «Прервать обработку». Обработка больших файлов может производиться продолжительное время.

После того, как файлы обработаются, на экран будет выведено окно с результатами (Рисунок 50Рисунок 50).

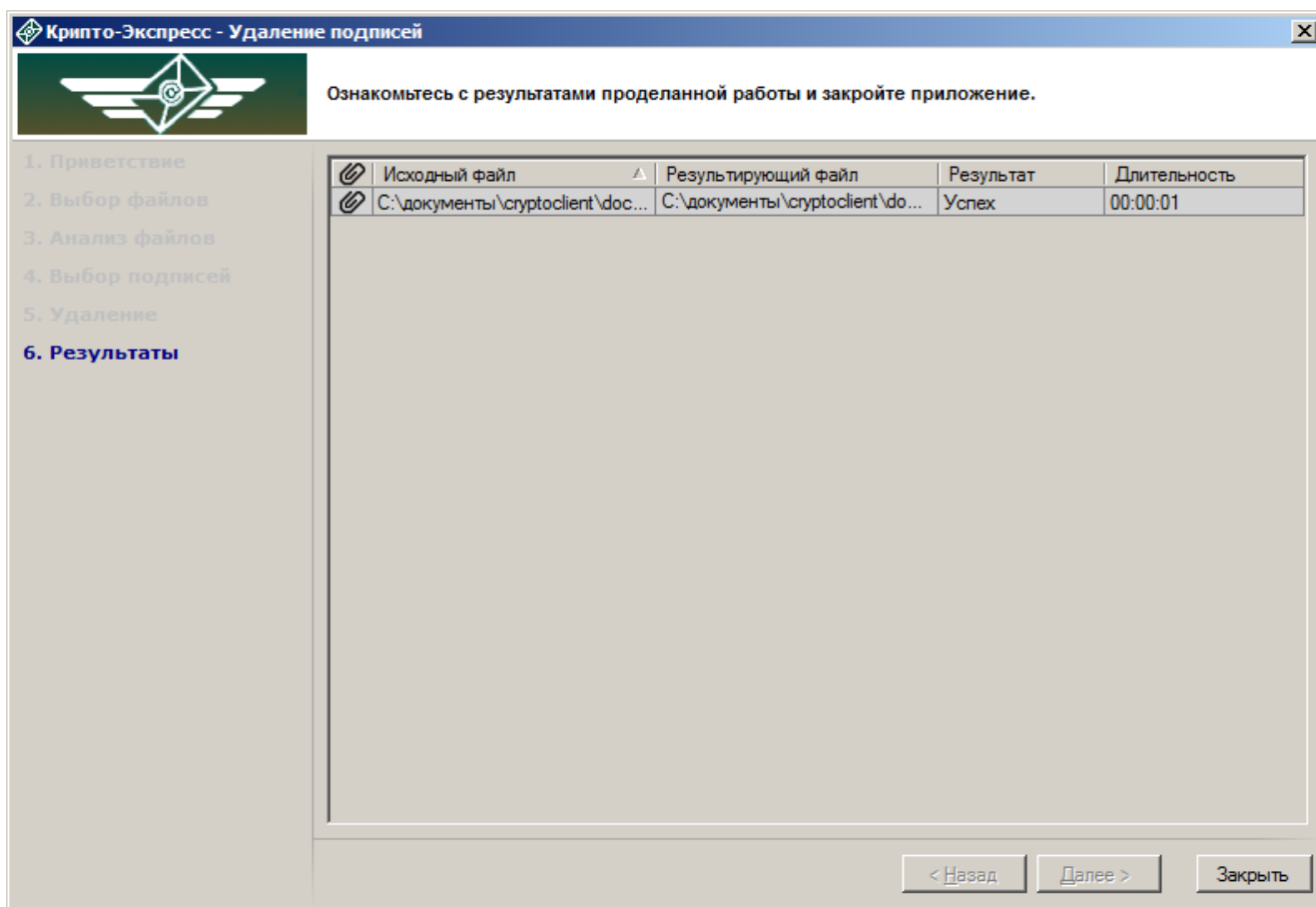


Рисунок 50. Результаты удаления подписей

Результаты обработки показываются в виде таблицы. Если возникли проблемы с подписанием одного или нескольких файлов, это будет отражено в графе «Результат».

Для того чтобы закончить работу Мастера нажмите кнопку «Заккрыть».

5. Сервисные функции

Воспользоваться сервисными функциями можно, нажав в главном окне программы кнопку «Помощь» (Рисунок 51Рисунок 51).

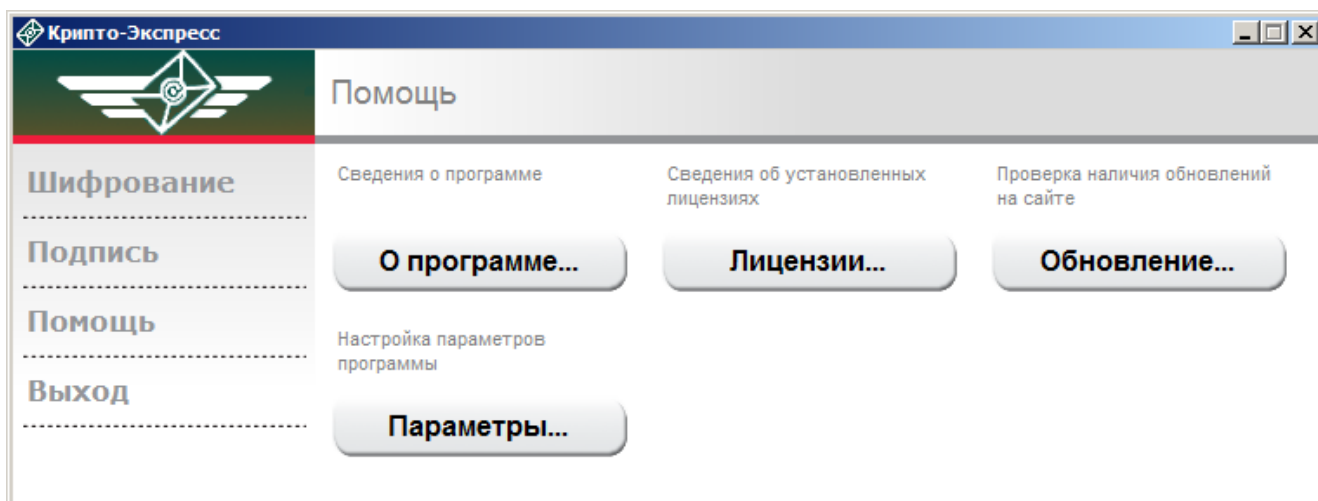


Рисунок 51. Сервисные функции

Из этого пункта меню доступны сведения о версии программы и лицензии, а также функция обновления.

5.1. О программе

Получить сведения о версии программы можно с помощью пункта меню «О программе» (Рисунок 52).

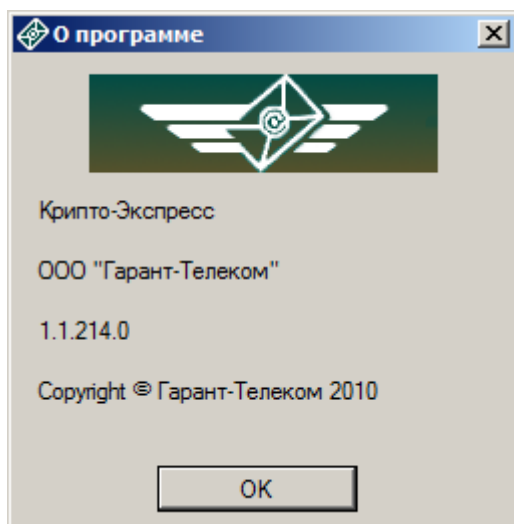


Рисунок 52. Сведения о программе

5.2. Лицензии

Получить сведения о лицензии, а также ввести серийный номер продукта можно с помощью пункта меню «Лицензии» (Рисунок 53Рисунок 53).

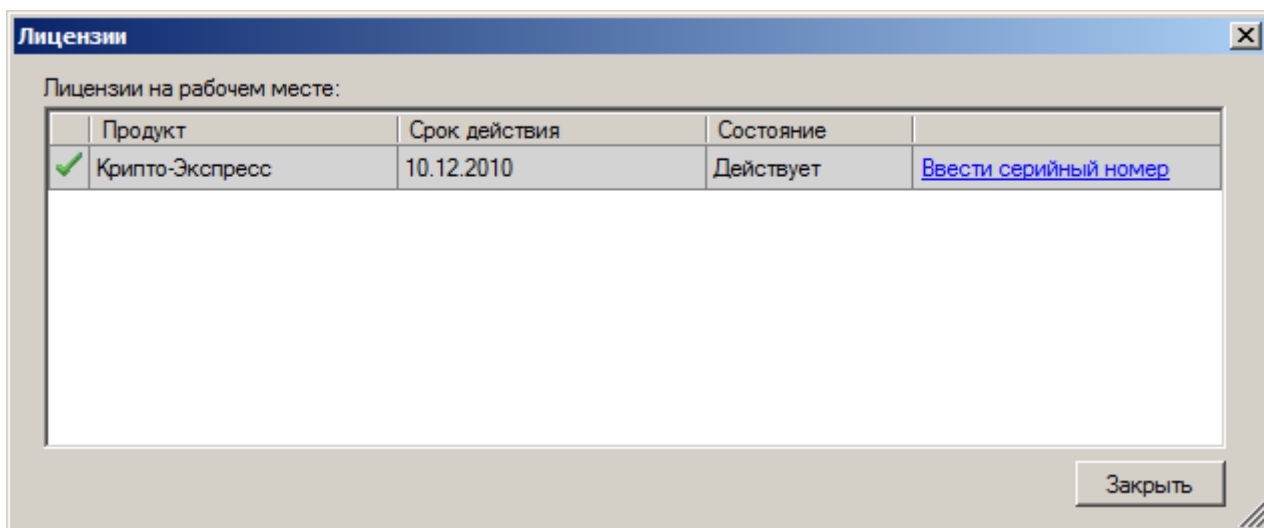


Рисунок 53. Сведения о лицензиях

Чтобы ввести новый серийный номер, нажмите ссылку «Ввести серийный номер» в блоке «Лицензии на рабочем месте».

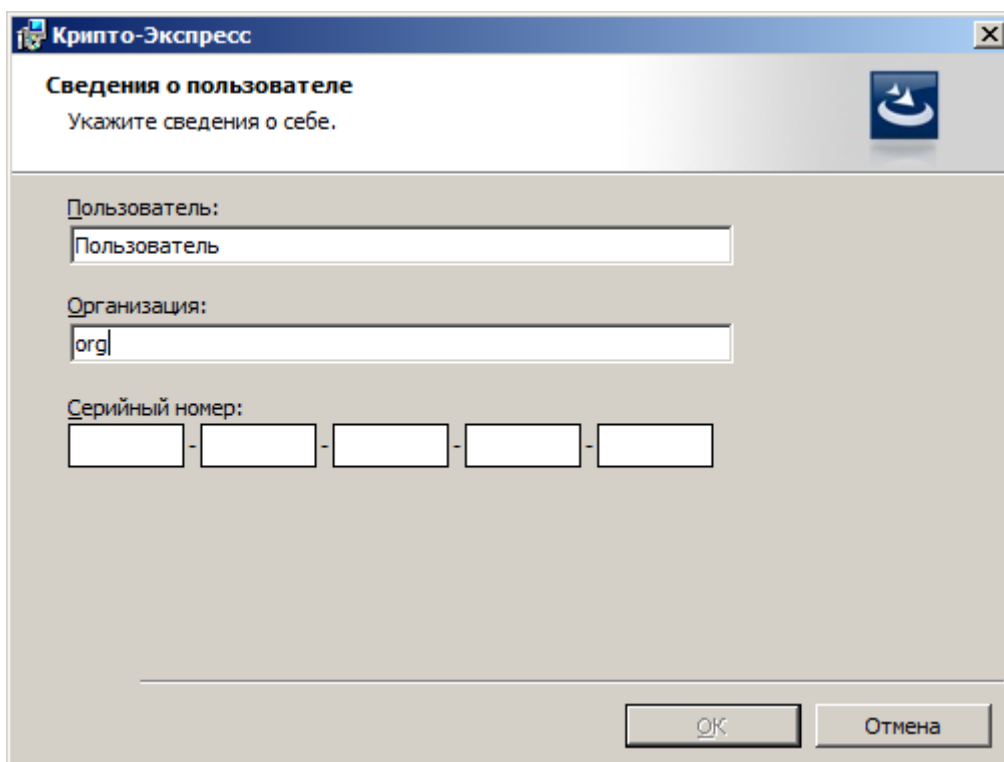


Рисунок 54. Ввод серийного номера

Введите серийный номер и нажмите «OK» для его сохранения.

5.3. Обновление программы

Программа может автоматически получать и устанавливать обновления с Сервера обновлений через Интернет.

Чтобы проверить наличие новой версии программы на сайте разработчика, выберите пункт меню «Помощь → Обновление».

Диалог обновления программы выведет на экран сведения о дате последней проверки обновлений (Рисунок 55Рисунок 55)

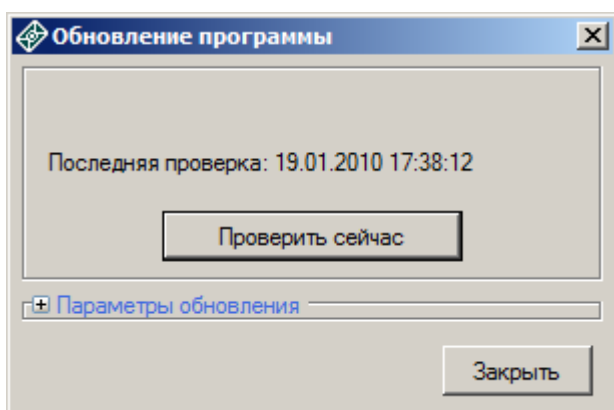


Рисунок 55. Диалог обновления программы

Можно изменять параметры обновления через настройки, тогда программа будет автоматически посылать запрос на проверку обновления (Рисунок 56Рисунок 56).

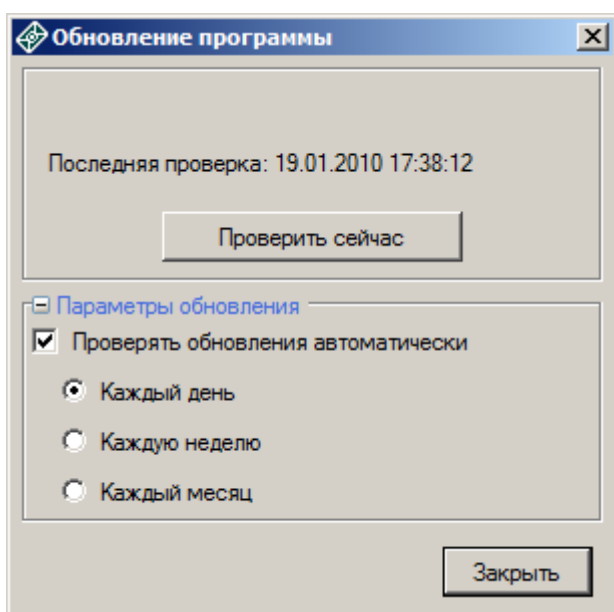


Рисунок 56. Параметры обновления

Если требуется автоматическая проверка обновлений, поставьте отметку «Проверять обновления автоматически» и отметьте частоту проверки.

Нажмите кнопку «Проверить сейчас». Если используется последняя версия программы, будет выведено сообщение о том, что обновления отсутствуют (Рисунок 57Рисунок 57).

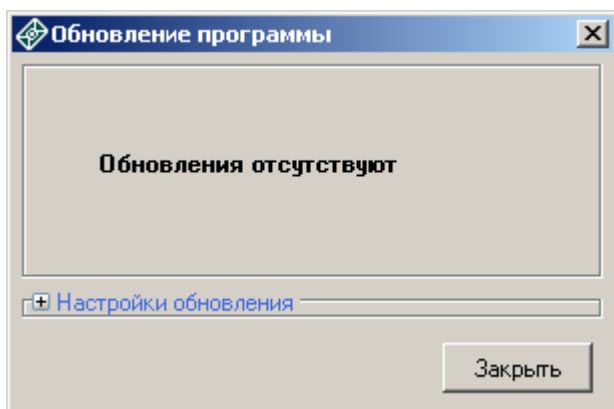


Рисунок 57. Используется последняя версия программы

Если обновления на сайте существуют, будет показано окно загрузки последней версии. Для запуска процесса обновления нажмите кнопку «Обновить».

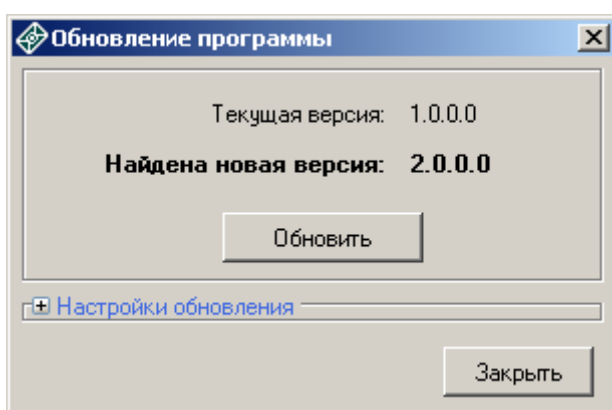


Рисунок 58. На сайте есть обновление программы

В процессе обновления будет загружена новая версия программы и запущена установка. Следует установить версию в соответствии с Руководством по установке. При этом действующая программа будет закрыта.

5.4. Параметры

С помощью пункта меню «Параметры» можно задать параметры, которые будут использоваться в программе.

Для того, чтобы добавить адрес службы штампов времени, на вкладке «Службы штампов времени» нажмите кнопку «Добавить» и укажите название и адрес службы (Рисунок 59).

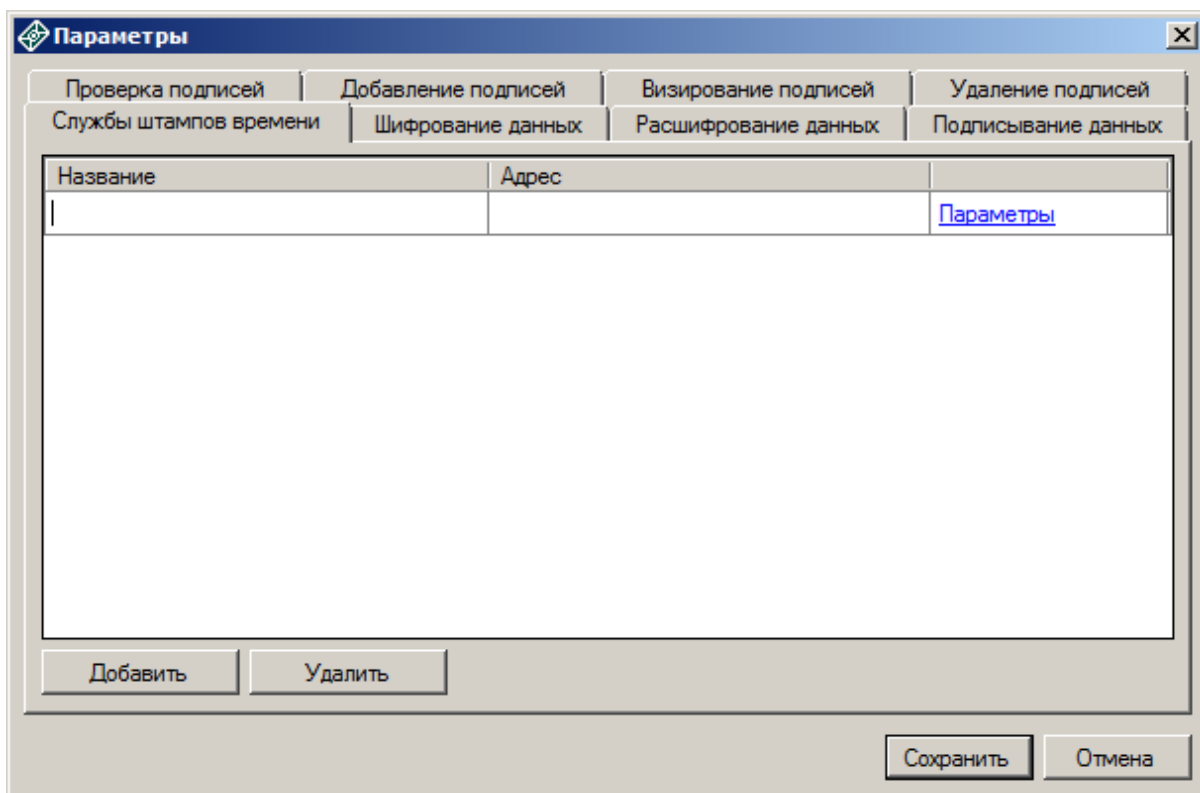


Рисунок 59. Параметры службы штампов времени

Для указания параметров подключения к службе штампов времени нажмите «Параметры», откроется окно (Рисунок 60). Укажите необходимые параметры и нажмите «ОК».

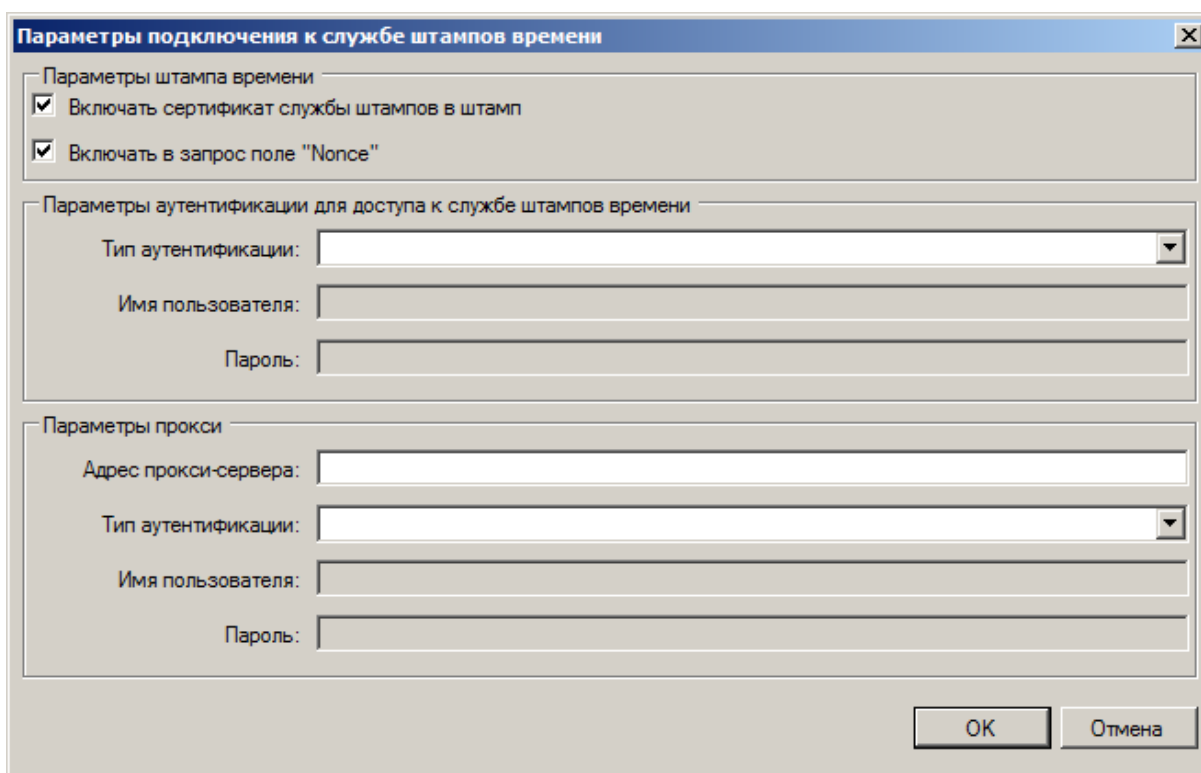


Рисунок 60. Параметры подключения к службе штампов времени

На вкладке «Шифрование данных» (Рисунок 61) можно указать сертификаты, используемые по умолчанию для шифрования файлов. Для этого нажмите кнопку «Добавить из хранилища...» и в

появившемся окне сертификатов выберите необходимые сертификаты. Также можно установить флажки «Показывать шаг «Приветствие»» и «Сохранять результаты в Base64».

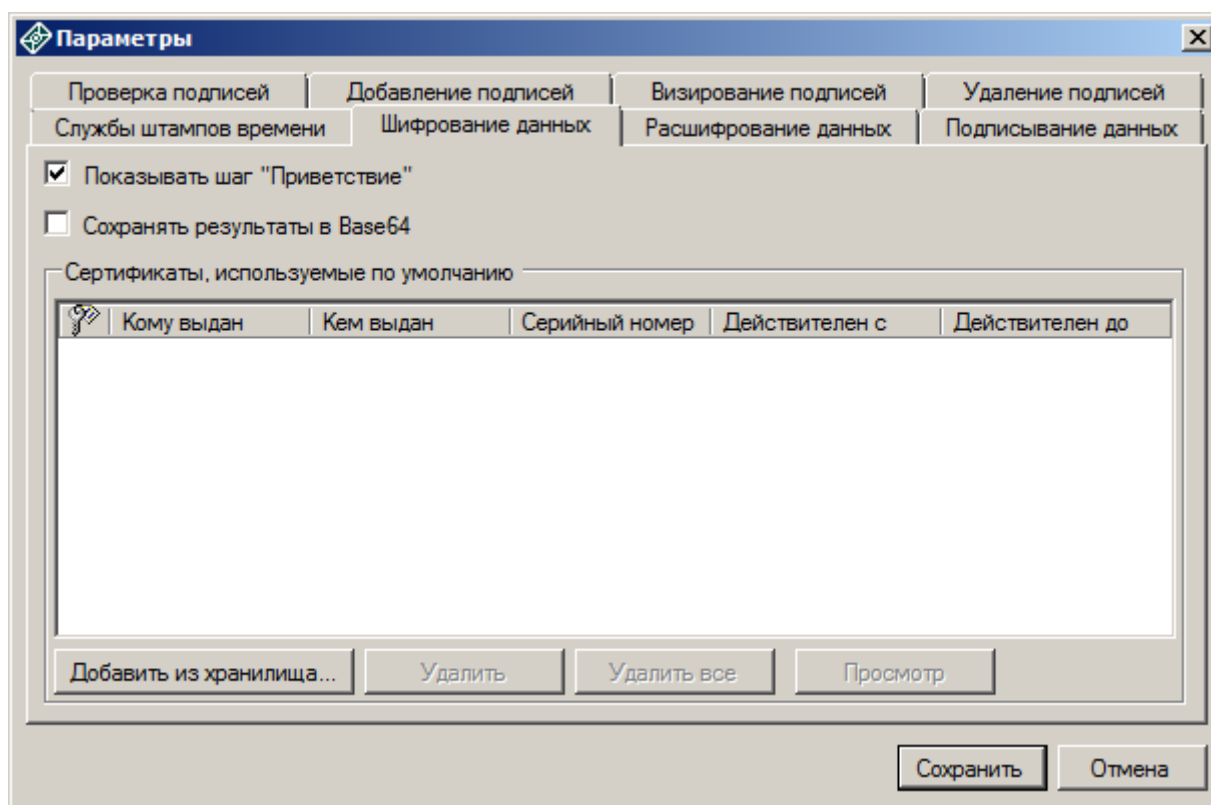


Рисунок 61. Параметры шифрования данных

На вкладке «Расшифрование данных» (Рисунок 62) указываются сертификаты, используемые по умолчанию для расшифрования данных. Для добавления сертификатов нажмите кнопку «Добавить из хранилища...» и выберите необходимые сертификаты. Чтобы не выводить шаг «Приветствие», снимите соответствующий флажок.

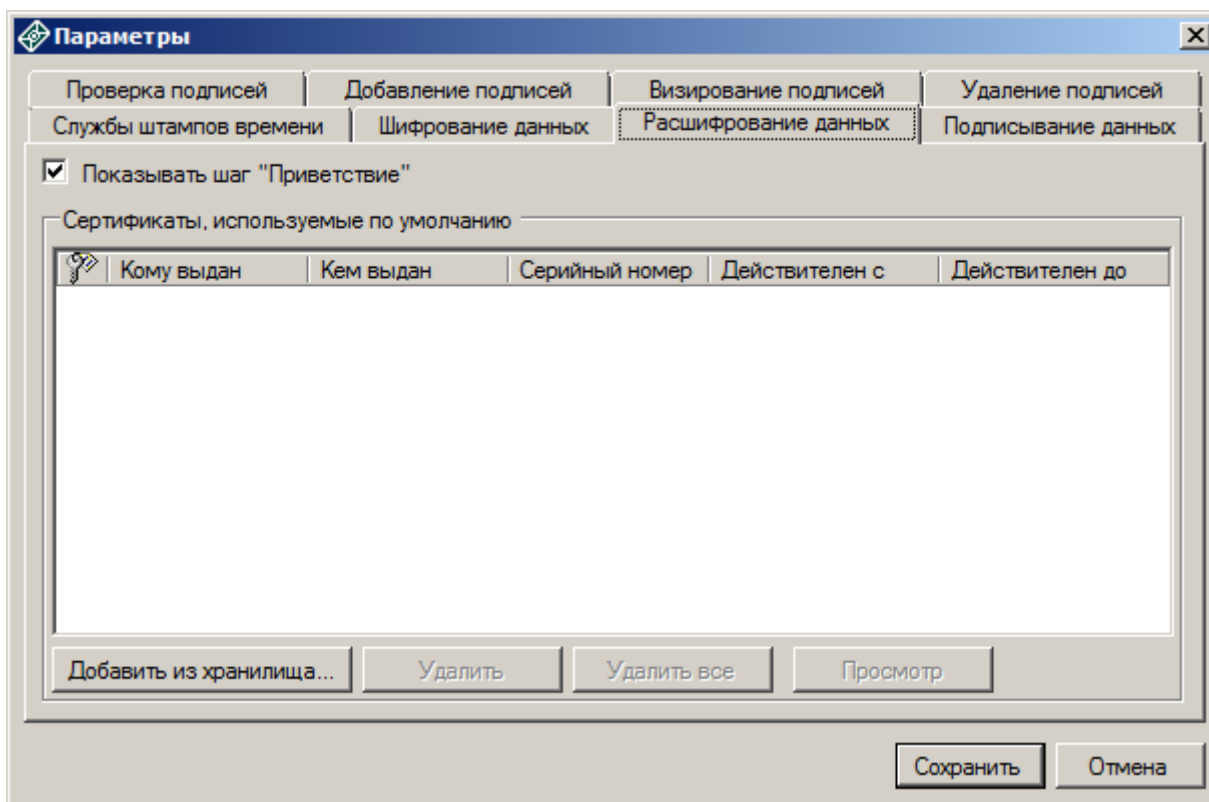


Рисунок 62. Параметры расшифрования данных

На вкладке «Подписывание данных» указываются параметры, используемые по умолчанию при подписи данных (Рисунок 63).

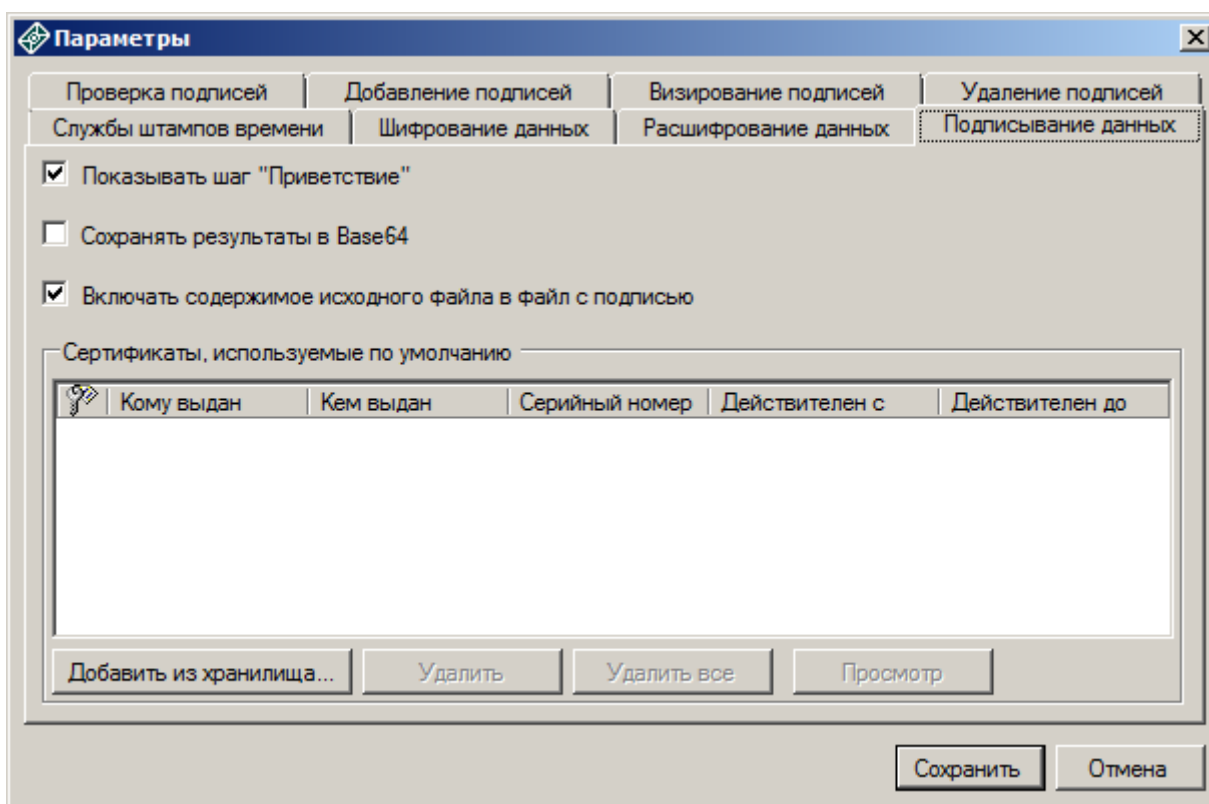


Рисунок 63. Параметры подписывания данных

Параметры для проверки подписи задаются на вкладке «Проверка подписей» (Рисунок 64).

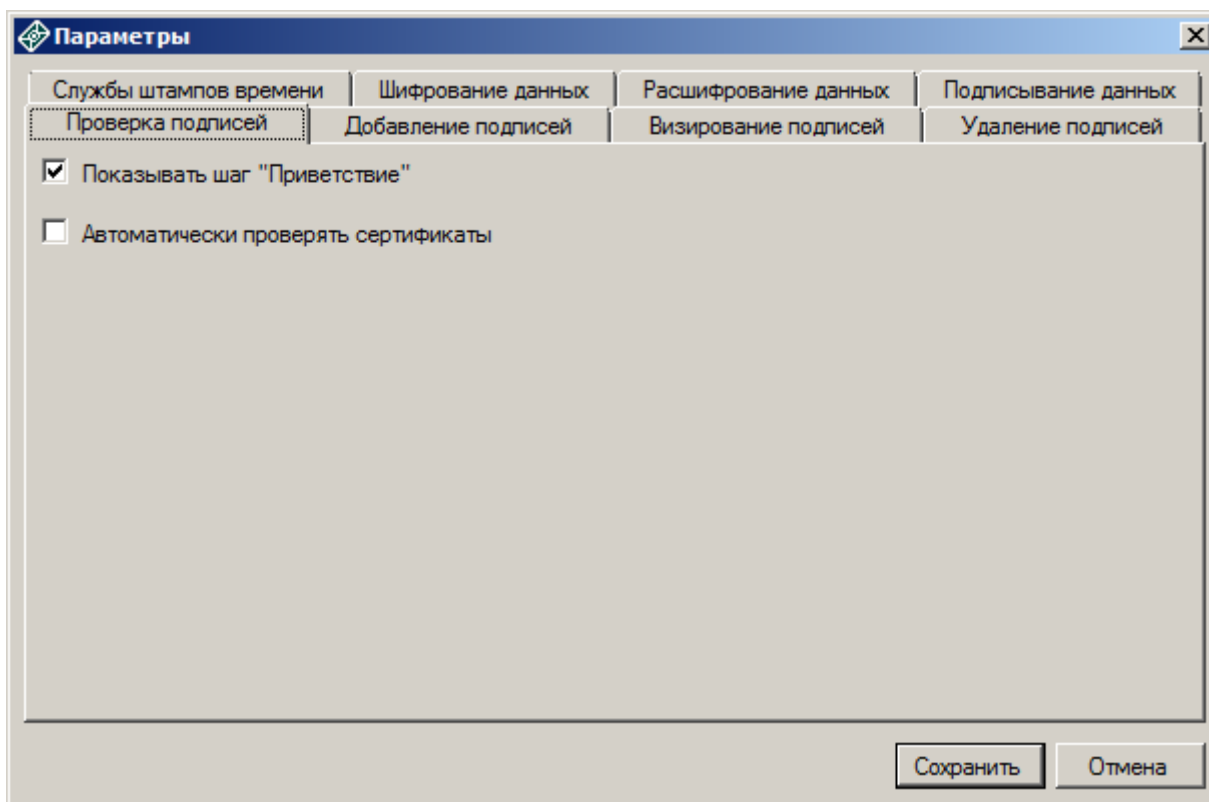


Рисунок 64. Параметры проверки подписей

На вкладке «Добавление подписей» можно указать параметры для добавления подписи к файлу с подписью (Рисунок 65).

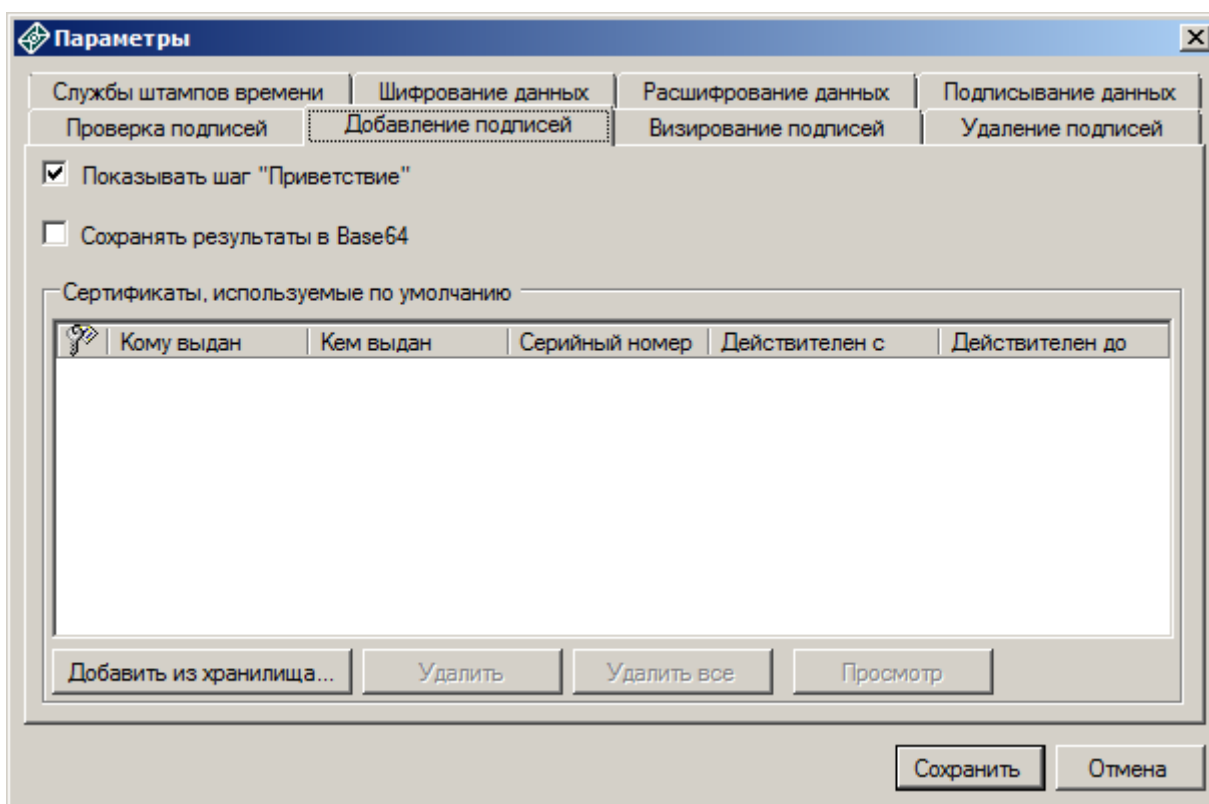


Рисунок 65. Параметры добавления подписей

Параметры для визирования подписей указываются на вкладке «Визирование подписей» (Рисунок 66).

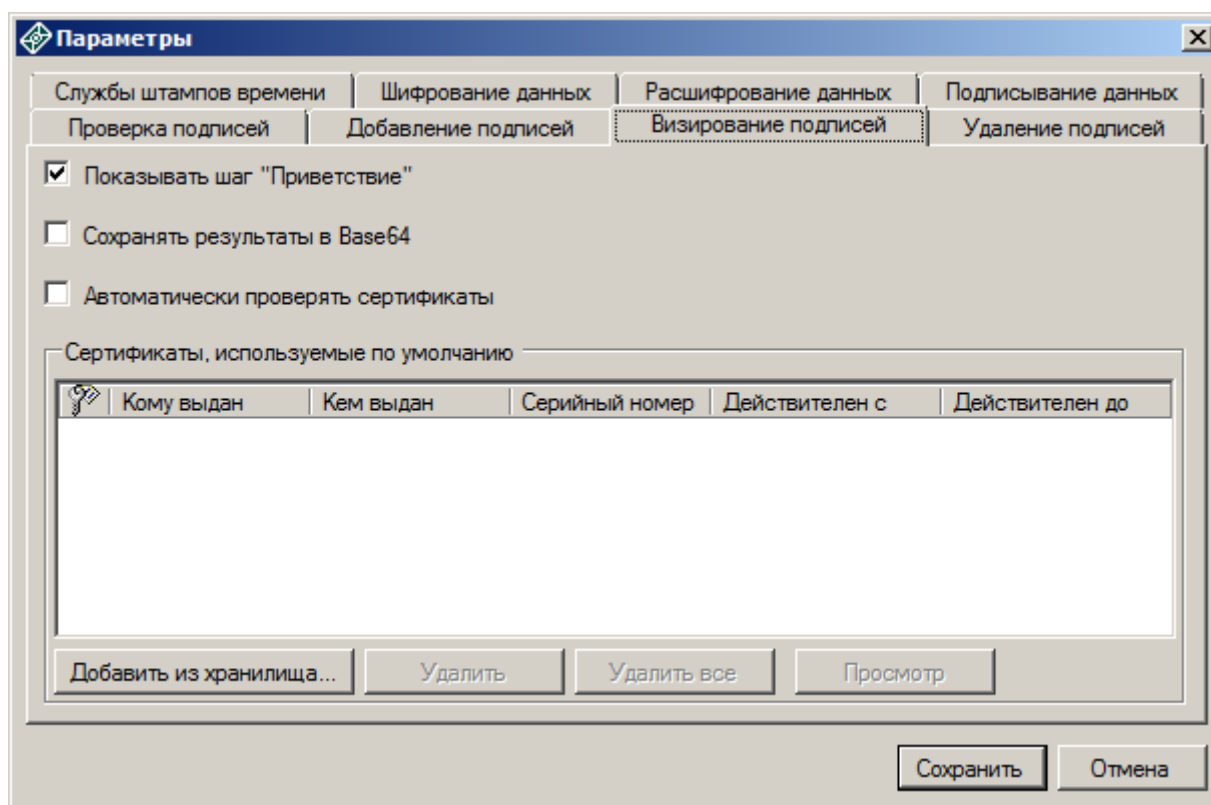


Рисунок 66. Параметры визирования подписей

Параметры для удаления подписей указываются на вкладке «Удаление подписей» (Рисунок 67).

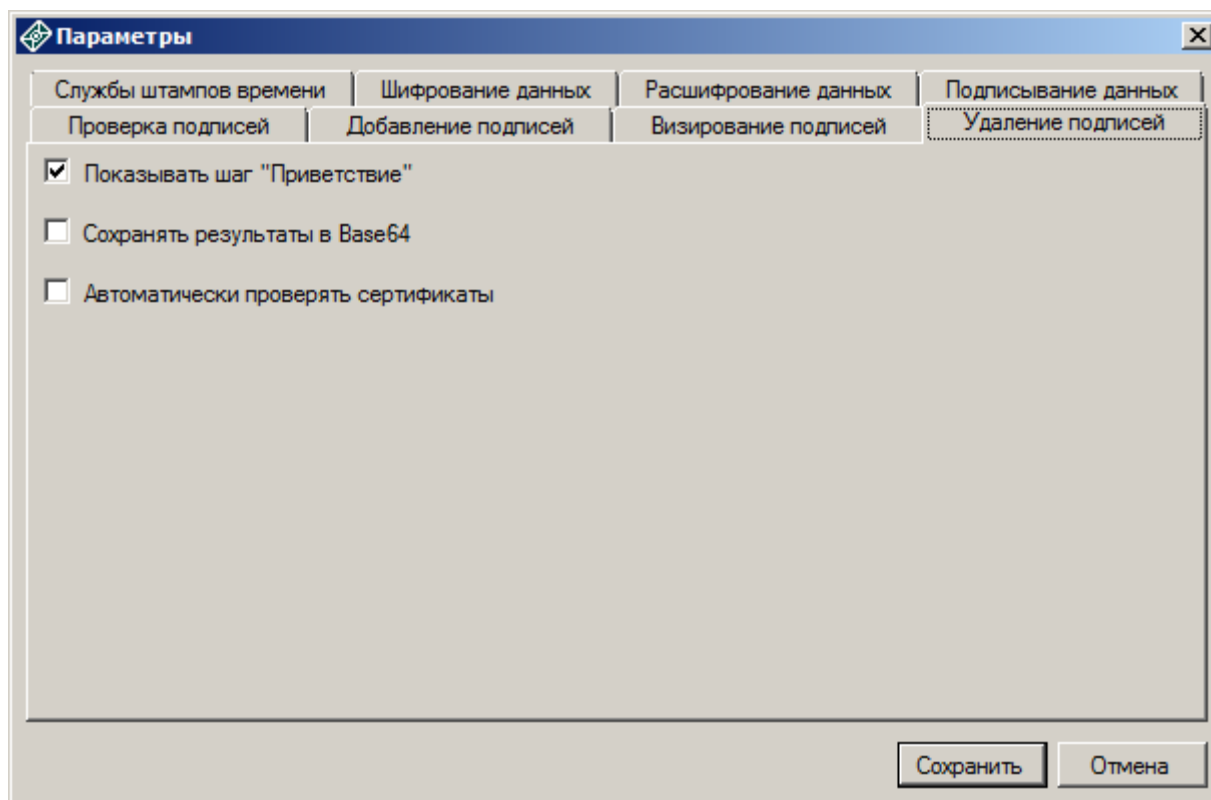


Рисунок 67. Параметры удаления подписей

6. Руководство по устранению неполадок

При возникновении любых нештатных ситуаций обращайтесь в службу поддержки компании «Русь-Телеком» по телефонам (495) 647-70-00 доб. 4602, (4812) 65-32-42 или по электронной почте, написав письмо на адрес support@rus-telecom.ru.