

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ  
(БАНК РОССИИ)

УТВЕРЖДЕН  
ВАМБ.00037-06-ЛУ

**СПЕЦИАЛИЗИРОВАННЫЙ АРХИВАТОР ЭЛЕКТРОННЫХ СООБЩЕНИЙ  
ВЕРСИЯ 6**

Руководство пользователя

ВАМБ.00037-06 92 01

**АННОТАЦИЯ**

Данный документ содержит сведения о назначении программного комплекса (ПК) ВАМБ.00037-06 «Специализированный архиватор электронных сообщений версия 6» (ПК САЭС), требования к аппаратно-программной среде функционирования, порядке запуска и настройки ПК САЭС, описаны процедуры загрузки и выгрузки ключа, криптографические операции над файлами, порядок протоколирования в ПК САЭС.

## СОДЕРЖАНИЕ

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>НАЗНАЧЕНИЕ ПК САЭС .....</b>  | <b>5</b>  |
| <b>2</b> | <b>ТРЕБОВАНИЯ К ОПЕРАЦИОННОЙ СРЕДЕ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ .....</b> | <b>6</b>  |
| <b>3</b> | <b>ЗАПУСК ПК САЭС .....</b>  | <b>7</b>  |
| <b>4</b> | <b>НАСТРОЙКА ПК САЭС .....</b>   | <b>9</b>  |
| 4.1      | ОБЩИЕ НАСТРОЙКИ ПК САЭС .....  | 9         |
| 4.2      | НАСТРОЙКИ БЕЗОПАСНОСТИ ПК САЭС.....                                    | 11        |
| 4.3      | ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ ПК САЭС .....                                 | 13        |
| 4.4      | СОХРАНЕНИЕ НАСТРОЕК В ФАЙЛ И ЗАГРУЗКА ИХ ИЗ ФАЙЛА.....                 | 15        |
| 4.5      | ПРОСМОТР ИНФОРМАЦИИ О ВЕРСИИ .....                                     | 16        |
| <b>5</b> | <b>ЗАГРУЗКА И ВЫГРУЗКА КЛЮЧА .....</b>                                 | <b>17</b> |
| <b>6</b> | <b>КРИПТОГРАФИЧЕСКИЕ ОПЕРАЦИИ НАД ФАЙЛАМИ .....</b>                    | <b>18</b> |
| 6.1      | СОЗДАНИЕ, ПРОВЕРКА И УДАЛЕНИЕ ЭП .....                                 | 18        |
| 6.1.1    | Создание ЭП.....   | 18        |
| 6.1.2    | Проверка ЭП.....   | 20        |
| 6.1.3    | Проверка и удаление ЭП.....  | 24        |
| 6.1.4    | Удаление ЭП без проверки .....   | 27        |
| 6.1.5    | Создание отсоединённой ЭП.....   | 29        |
| 6.1.6    | Проверка отсоединённой ЭП.....   | 31        |
| 6.2      | ЗАШИФРОВАНИЕ И РАСШИФРОВАНИЕ ФАЙЛОВ .....                              | 35        |
| 6.2.1    | Зашифрование .....   | 35        |
| 6.2.2    | Расшифрование.....   | 45        |
| 6.3      | ПОЛУЧЕНИЕ КРИПТОГРАФИЧЕСКОЙ ИНФОРМАЦИИ.....                            | 48        |
| 6.4      | ПРОСМОТР СТАТУСА OSCP .....  | 51        |
| 6.5      | УПРОЩЁННОЕ ПОЛУЧЕНИЕ КРИПТОГРАФИЧЕСКОЙ ИНФОРМАЦИИ.....                 | 52        |
| <b>7</b> | <b>ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИИ .....</b>                                    | <b>54</b> |
| 7.1      | ЗАКОДИРОВАНИЕ В ФОРМАТ BASE64 .....                                    | 54        |
| 7.2      | РАСКОДИРОВАНИЕ ИЗ ФОРМАТА BASE64.....                                  | 55        |
| 7.3      | ХЭШИРОВАНИЕ ФАЙЛОВ .....   | 57        |
| <b>8</b> | <b>ПРОТОКОЛИРОВАНИЕ В ПК САЭС .....</b>                                | <b>60</b> |
|          | <b>ПЕРЕЧЕНЬ РИСУНКОВ .....</b>   | <b>62</b> |

## 1 НАЗНАЧЕНИЕ ПК САЭС

Программный комплекс (ПК) ВАМБ.00037-06 «Специализированный архиватор электронных сообщений версия 6» (далее - ПК САЭС) – это программный модуль, встраивающийся в контекстное меню Проводника и позволяющий выполнять криптографические операции с группами файлов и каталогами. Для работы ПК САЭС требуется установка и настройка ПК ВАМБ.000107-06 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6» (далее – ПК «Средство КЗИ») и ВАМБ.00106-06 «СКАД «Сигнатура» версия 6. «Сигнатура-клиент» версия 6» (далее – ПК «Сигнатура-клиент»)).

### *Примечания*

*1 Операции "Зашифровать", "Расшифровать", "Создать ЭП", "Проверить ЭП", "Создать отсоединённую ЭП", "Проверить отсоединённую ЭП", "Проверить и удалить ЭП" и «Вычислить хэши (2012)» в ПК САЭС могут выполняться блочными или потоковыми функциями ПК ВАМБ.00104-06 «СКАД «Сигнатура» версия 6» (далее – СКАД «Сигнатура»), в зависимости от настроек ПК САЭС.*

*2 При выполнении этих операций блочными функциями для них действуют следующие ограничения на размер файлов: для 32-битной (x86) версии максимум до 400 Мбайт, а для 64-битных (x64) версий - объёмом максимум до 2 Гбайт. При этом данные величины могут быть уменьшены в зависимости от текущего использования и гранулированности виртуальной памяти вызывающего процесса.*

*3 При выполнении этих операций потоковыми функциями СКАД «Сигнатура» ограничения на размер файлов отсутствуют.*

## **2 ТРЕБОВАНИЯ К ОПЕРАЦИОННОЙ СРЕДЕ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ**

Минимальные требования к аппаратно-программной среде функционирования ПК САЭС:

- персональный компьютер (ЭВМ) с процессором Intel Pentium IV или более новым и объемом жесткого диска и оперативной памяти, удовлетворяющим минимальным требованиям для установленной на данной ЭВМ версии операционной системы (ОС) Microsoft Windows;
- при необходимости - сетевой адаптер и устройство резервного копирования информации на отчуждаемый носитель (например, CD-RW);
- средство защиты информации от несанкционированного доступа (СЗИ от НСД) - при необходимости;
- ОС семейства Windows. ПК САЭС работает под управлением ОС Windows (как в 32-битных (x86) ОС, так и в 64-битных (x64) ОС).

Перечень ОС, в которых функционирует ПК САЭС, приведен в документе ВАМБ.00107-06 30 01 «СКАД «Сигнатура» версия 6. АПК «Средство КЗИ СКАД «Сигнатура» версия 6». Формуляр».

### 3 ЗАПУСК ПК САЭС

Для запуска ПК САЭС запустите Проводник, выберите один или несколько файлов или каталогов и откройте контекстное меню (нажатием правой кнопки мыши). Выберите в контекстном меню пункт «САЭС версия 6» - откроется главное меню расширения проводника (Рисунок 1).

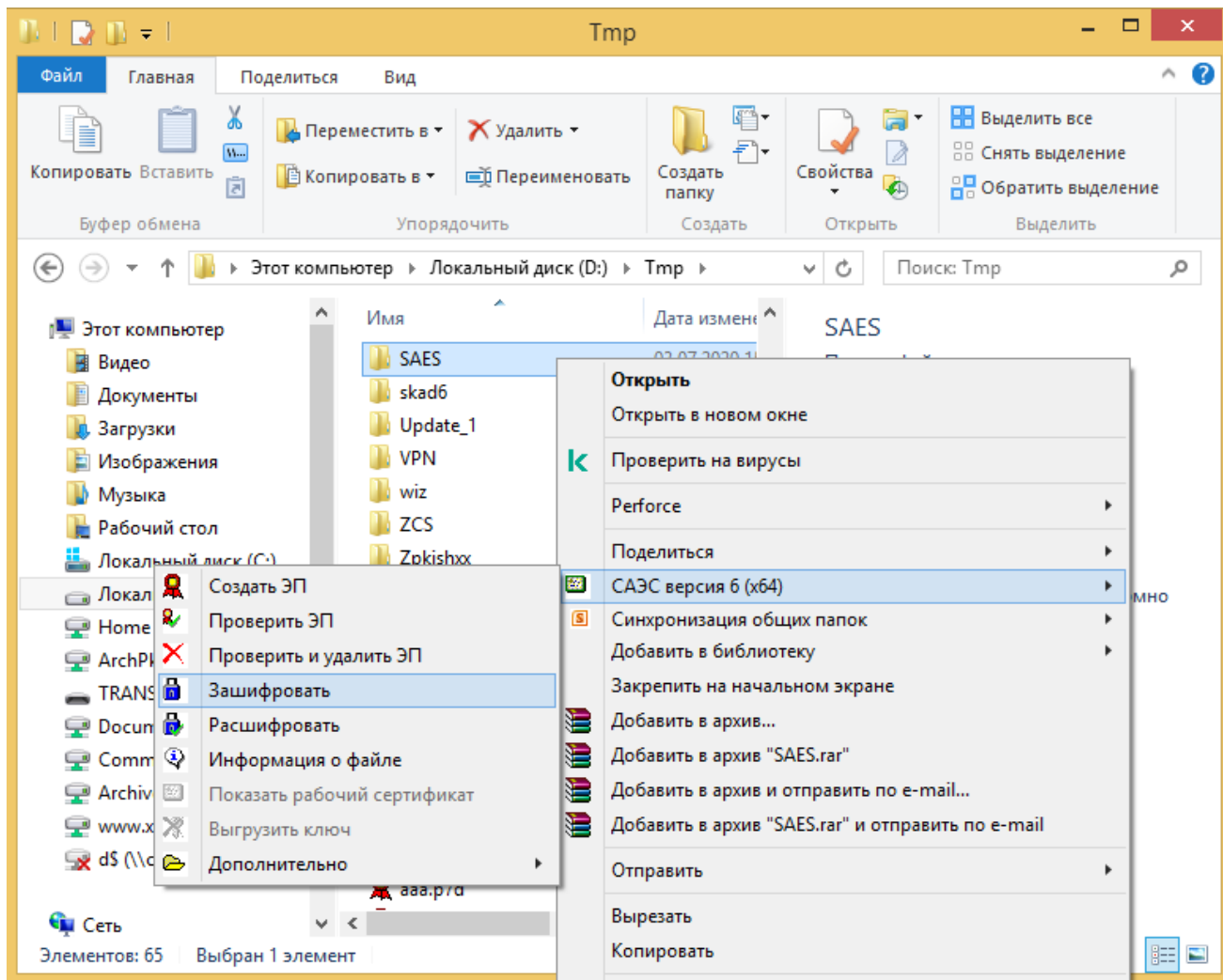


Рисунок 1 - Главное меню ПК САЭС

Большинство операций, выполняемых ПК САЭС, совершается над всеми выбранными файлами последовательно. В случае, если выбран один или несколько каталогов, операции совершаются над всеми файлами, расположенными в этих каталогах и их подкаталогах. Если вы попытаетесь выполнить какую-либо операцию ПК САЭС на ярлыке файла, вы получите сообщение об ошибке.

Однако если выбрать один или несколько ярлыков в составе группы файлов или каталогов, они будут обработаны как обычные файлы.

Часть операций, выполняемых ПК САЭС, - «Показать рабочий сертификат», «Выгрузить ключ» и «Настройки пользователя» - выполняется вне зависимости от того, какие файлы выбраны в Проводнике.

#### 4 НАСТРОЙКА ПК САЭС

Для настройки параметров ПК САЭС выберите в главном меню пункт «Дополнительно», подпункт «Настройки пользователя». Выберите одну из трёх закладок, измените настройки и нажмите кнопку «Применить» для сохранения внесённых изменений, кнопку «ОК» для закрытия окна настроек с сохранением внесённых изменений или кнопку «Отмена» для закрытия окна настроек без сохранения внесённых изменений.

*Примечание – значения по умолчанию устанавливаются в случае установки ПК САЭС 6 на ПЭВМ, на которой не был установлен ПК САЭС предыдущей версии. В противном случае конфигурационные установки наследуются от установки ПК САЭС предыдущей версии.*

##### 4.1 Общие настройки ПК САЭС

Общие настройки ПК САЭС (Рисунок 2) перечислены ниже (Таблица 1).

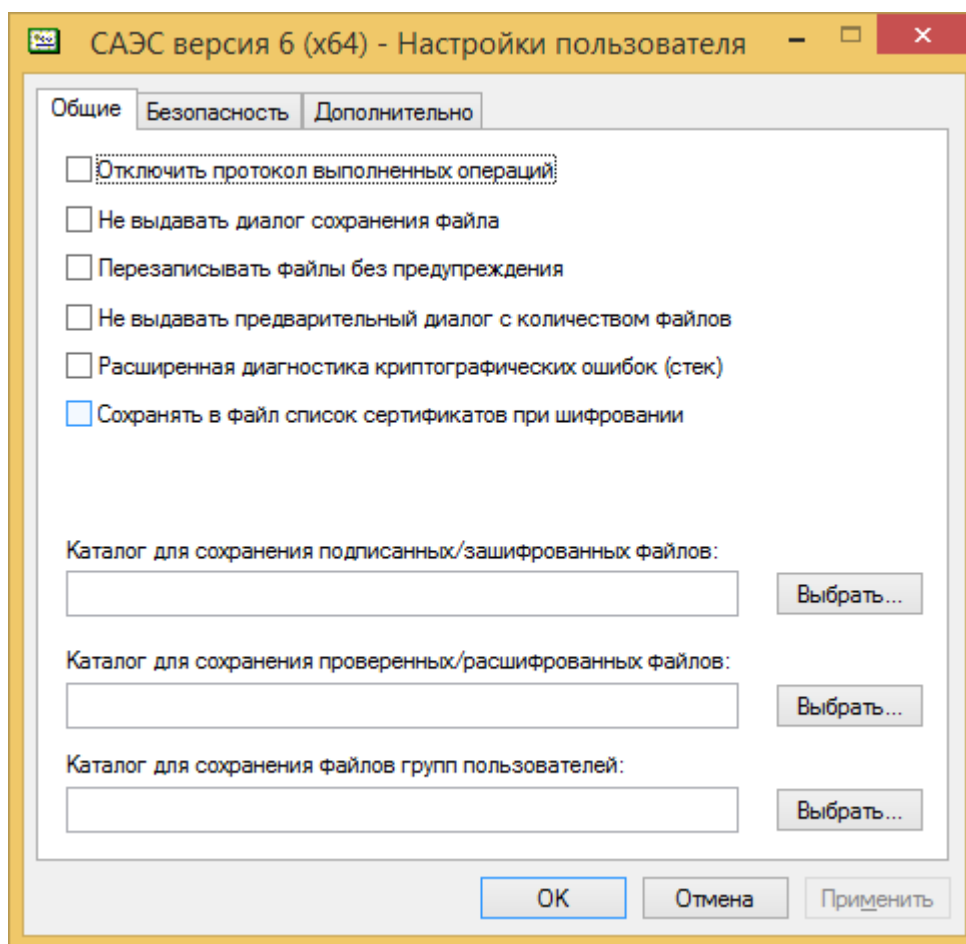


Рисунок 2 - Общие настройки ПК САЭС

Таблица 1 - Общие настройки ПК САЭС

| Название параметра | Описание | Значение по умолчанию<br>(после установки) |
|--------------------|----------|--|
|--------------------|----------|--|



| Название параметра  | Описание  | Значение по умолчанию (после установки) |
|---|---|---|
| Отключить протокол выполненных операций                   | Отключает протоколирование всех выполняемых операций в журнал приложений (Event Log) Windows  | Выключено                               |
| Не выдавать диалог сохранения файла                       | В случае, если при попытке записи файла файл с таким именем уже существует, отключает выдачу на экран стандартного диалога сохранения файла   | Выключено                               |
| Перезаписывать файлы без предупреждения                   | В случае, если при попытке записи файла файл с таким именем уже существует, отключает выдачу на экран предупреждения  | Выключено                               |
| Не выдавать предварительный диалог с количеством файлов   | Отключает выдачу предупреждения о предстоящей операции с указанием количества файлов, к которым эта операция будет применена (если количество файлов более одного)  | Выключено                               |
| Расширенная диагностика криптографических ошибок (стек)   | Добавляет к сообщению об ошибке криптографических функций содержимое стека ошибок   | Выключено                               |
| Сохранять в файл список сертификатов при шифровании       | После успешно выполненного шифрования создаёт текстовый файл с именем зашифрованного файла плюс расширение «txt» (в том же каталоге, где и зашифрованный файл), в который записываются имена владельцев и хэши издателя и серийного номера для всех сертификатов, на которые было выполнено шифрование.   | Выключено                               |
| Каталог для сохранения подписанных/ зашифрованных файлов  | Задаёт каталог, в который записываются результаты подписи и зашифрования. Если параметр не задан, результаты записываются в тот же каталог, в котором находится подписываемый или шифруемый файл.<br><i>Примечание – при заданном параметре не следует подписывать отсоединённой подписью группу файлов, содержащих файлы с одинаковым именем, лежащих в разных подкаталогах.</i>           | Не задан (пусто)                        |
| Каталог для сохранения проверенных/ расшифрованных файлов | Задаёт каталог, в который записываются результаты удаления подписей и расшифрования. Если параметр не задан, результаты записываются в тот же каталог, в котором находится подписанный или зашифрованный файл.<br><i>Примечание – при заданном параметре не следует проверять отсоединённую подпись группы файлов, содержащих файлы с одинаковым именем, лежащих в разных подкаталогах.</i> | Не задан (пусто)                        |

| Название параметра                                | Описание   | Значение по умолчанию (после установки) |
|---|--|---|
| Каталог для сохранения файлов групп пользователей | Задаёт каталог, в котором предлагается открывать и сохранять файлы групп пользователей – предполагаемых получателей зашифрованных сообщений. Также в этом каталоге хранятся файлы с информацией о последней операции шифрования. Если параметр не задан, используется пользовательский каталог для хранения данных приложений. | Не задан (пусто)                        |

## 4.2 Настройки безопасности ПК САЭС

Настройки безопасности ПК САЭС (Рисунок 3) приведены ниже (Таблица 2).

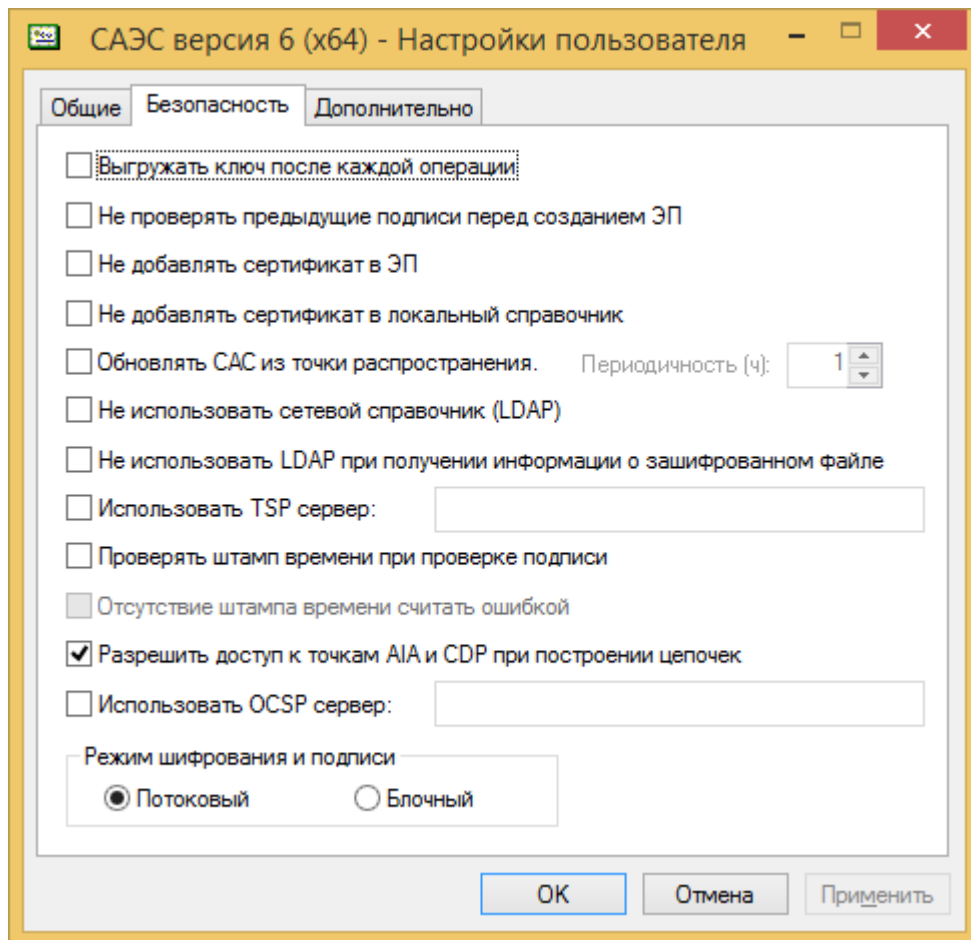


Рисунок 3 - Настройки безопасности ПК САЭС

Таблица 2 - Настройки безопасности ПК САЭС

Изменения настроек безопасности вступают в силу только после выгрузки и последующей загрузки ключа.

| Название параметра  | Описание   | Значение по умолчанию (после установки) |
|---|--|---|
| Выгружать ключ после каждой операции                                | После завершения любой операции с одним или несколькими файлами выгружать ключ, что потребует его повторной загрузки при выполнении следующей операции   | Выключено                               |
| Не проверять предыдущие подписи перед созданием ЭП                  | Отключить проверку всех ЭП файла (если они уже есть) перед созданием следующей ЭП  | Выключено                               |
| Не добавлять сертификат в ЭП  | Отключить режим включения в ЭП сертификата, на котором создаётся ЭП  | Выключено                               |
| Не добавлять сертификат в локальный справочник                      | Отключить режим добавления сертификата, найденного в сетевом справочнике (а также объектов цепочки – сертификатов ЦС и САС при включённой опции «Разрешить доступ к точкам AIA и CDP при построении цепочек») в базу сертификатов Справочника сертификатов. Рекомендуется включать данную опцию (т.е. отключать режим добавления) перед поиском в ЕСК во избежание копирования в справочник всех найденных сертификатов. | Выключено                               |
| Обновлять САС из точки распространения                              | Включить режим обновления САС из точки распространения при инициализации криптоконтекста (загрузке ключа). Обновление производится, только если со времени предыдущего обновления прошло больше времени, чем указано в параметре "Периодичность".  | Выключено                               |
| Периодичность (ч)   |  | 1 час                                   |
| Не использовать сетевой справочник (LDAP)                           | Отключить использование сетевого справочника, указанного в настройках Справочника сертификатов, при операциях проверки подписи и поиска сертификатов.  | Выключено                               |
| Не использовать LDAP при получении информации о зашифрованном файле | Отключить использование сетевого справочника, указанного в настройках Справочника сертификатов, при поиске сертификатов для отображения списка получателей в диалоге с информацией о зашифрованном файле.  | Выключено                               |
| Использовать TSP сервер (выключатель)                               | При создании подписи добавлять в неё штамп времени с сервера, адрес которого задаётся следующим параметром   | Выключено                               |
| Использовать TSP сервер (строка ввода)                              | Адрес TSP сервера. Доступен для редактирования только при включённом предыдущем параметре  | Пустая строка                           |
| Проверять штамп времени при проверке подписи                        | При проверке каждой подписи пытаться проверить для неё штамп времени. Ошибка проверки штампа времени считается ошибкой проверки подписи  | Выключено                               |

| Название параметра   | Описание   | Значение по умолчанию<br>(после установки) |
|--|--|--|
| Отсутствие штампа времени считать ошибкой                  | Требовать наличие штампа времени. Отсутствие штампа времени хотя бы одной из подписей считается ошибкой проверки подписи. Доступен для изменения только при включённом предыдущем параметре  | Выключено                                  |
| Разрешить доступ к точкам AIA и CDP при построении цепочек | При построении цепочек использовать адреса для поиска сертификатов ЦС и САС, указанные в полях сертификата "Информация доступа к Центру" (AIA) и "Точка распространения САС" (CDP)   | Включено                                   |
| Использовать OCSP сервер (выключатель)                     | При просмотре сертификата показывать его статус с сервера, адрес которого задаётся следующим параметром. В случае, если адрес сервера в следующем параметре не задан, он берётся из расширения «Информация доступа к Центру» просматриваемого сертификата. | Выключено                                  |
| Использовать OCSP сервер (строка ввода)                    | Адрес OCSP сервера. Доступен для редактирования только при включённом предыдущем параметре   | Пустая строка                              |
| Режим шифрования и подписи                                 | Выбор набора функций СКАД Сигнатуры (блочный или потоковый) используемый при выполнении криптографических операций   | Потоковый                                  |

#### 4.3 Дополнительные настройки ПК САЭС

Дополнительные настройки ПК САЭС (Рисунок 4) приведены ниже (Таблица 3).

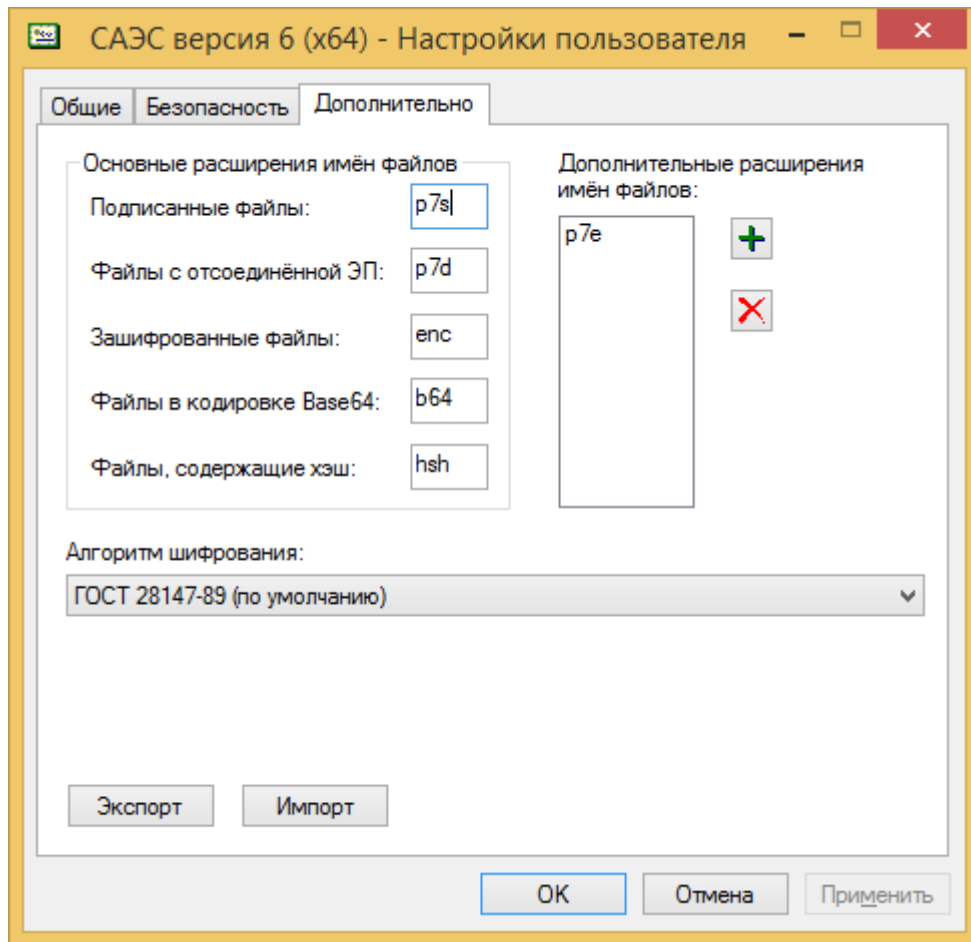



Рисунок 4 - Дополнительные настройки ПК САЭС

Таблица 3 - Дополнительные настройки ПК САЭС

| Название параметра                    | Описание  | Значение по умолчанию<br>(после установки) |
|---------------------------------------|---|--|
| Подписанные файлы                     | Расширение, которое добавляется к файлу при создании присоединённой ЭП и снимается при удалении ЭП  | p7s  |
| Файлы с отсоединённой ЭП              | Расширение, которое добавляется к файлу при создании отсоединённой ЭП   | p7d  |
| Зашифрованные файлы                   | Расширение, которое добавляется к файлу при зашифровании и снимается при расшифровании  | enc  |
| Файлы в кодировке Base64              | Расширение, которое добавляется к файлу при преобразовании в кодировку Base64 зашифровании и снимается при преобразовании из кодировки Base64 | b64  |
| Файлы, содержащие хэш                 | Расширение, которое добавляется к файлу при сохранении хэша   | hsh  |
| Дополнительные расширения имён файлов | Список расширений, которые снимаются с файлов при удалении ЭП или расшифровании   | p7e  |
| Алгоритм шифрования                   | Алгоритм, используемый при  | ГОСТ 28147-89                              |

| Название параметра | Описание   | Значение по умолчанию<br>(после установки) |
|--------------------|------------|--|
|                    | шифровании |  |

Для добавления дополнительного расширения в список нажмите кнопку , введите расширение в диалоге и нажмите кнопку «ОК» (Рисунок 5).

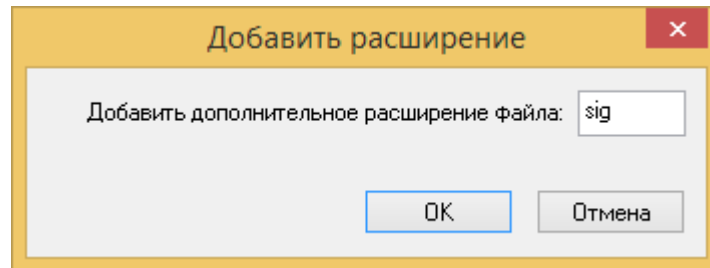



Рисунок 5 - Диалог добавления дополнительного расширения

Для удаления дополнительного расширения выберите его в списке и нажмите кнопку .

*Примечание – для обеспечения обратной совместимости в части расширений имён файлов при совместном использовании САЭС версия 6 и САЭС версия 5 (ВАМБ. 00037-02) рекомендуется на рабочих местах с ПК САЭС версия 5 изменить настройки пользователя – на вкладке «Дополнительно» в список «Дополнительные расширения имён файлов» добавить значение «**eps**».*

#### 4.4 Сохранение настроек в файл и загрузка их из файла

Для сохранения настроек ПК САЭС в файл выберите в главном меню пункт «Дополнительно», подпункт «Настройки пользователя», выберите закладку «Дополнительно» и нажмите кнопку «Экспорт». В стандартном диалоге сохранения файла укажите имя конфигурационного файла и нажмите кнопку «Сохранить».

*Примечание - Сохраняются параметры, отображаемые на экране. Если Вы внесли изменения в конфигурацию САЭС, но не нажали кнопку «Применить», в файл будут сохранены изменённые параметры.*

Для загрузки настроек ПК САЭС из файла выберите в главном меню пункт «Дополнительно», подпункт «Настройки пользователя», выберите закладку «Дополнительно» и нажмите кнопку «Импорт». В стандартном диалоге открытия файла выберите имя конфигурационного файла и нажмите кнопку «Открыть».

*Примечание - Загруженные параметры отображаются на экране; но не сохраняются автоматически. Для сохранения загруженных параметров конфигурации САЭС нажмите кнопку «ОК» или «Применить».*

#### 4.5 Просмотр информации о версии

Для просмотра информации о версии ПК САЭС выберите в главном меню пункт «Дополнительно», подпункт «Настройки пользователя» и в системном меню диалога выберите пункт «О программе...» (Рисунок 6).

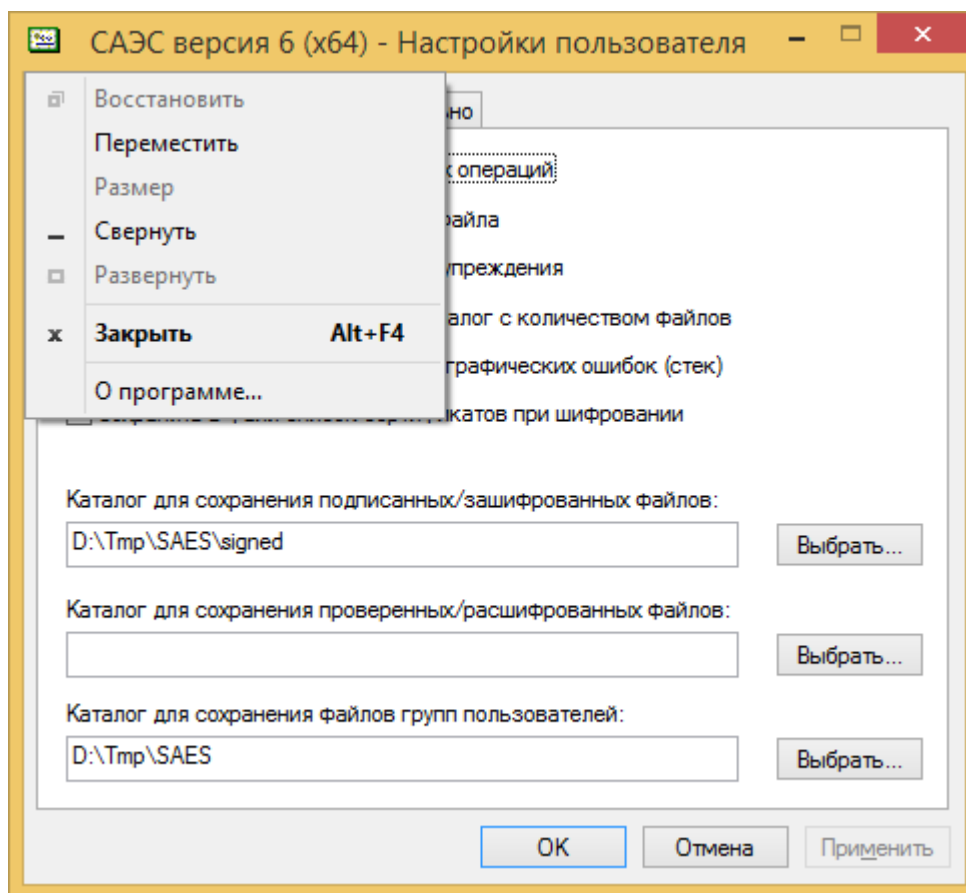


Рисунок 6. Выбор пункта меню «О программе...»

На экране появится диалог с информацией о версии ПК САЭС (Рисунок 7).

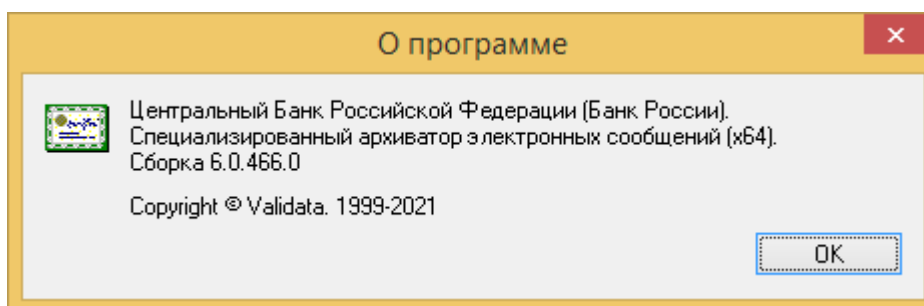


Рисунок 7. Диалог с информацией о версии программы

## 5 ЗАГРУЗКА И ВЫГРУЗКА КЛЮЧА

Для выполнения любой криптографической операции над одним или несколькими файлами необходимо загрузить ключ. Загрузка ключа в ПК САЭС производится в случае, если он ещё не загружен, после предупреждения о предстоящей операции с указанием количества файлов (если оно появляется) и до начала собственно операции. В процессе загрузки ключа может потребоваться выбор профиля пользователя, ключевого носителя, выбор ключа, задание пароля ключа, ПИН-кода ключевого носителя, инициализация датчика случайных чисел – в зависимости от настроек ПК «Сигнатура-клиент».

В случае если опция «Выгружать ключ после каждой операции» в настройках выключена, ключ останется загруженным в памяти до закрытия данного экземпляра (окна) Проводника. Принудительно выгрузить ключ, не закрывая окно Проводника, можно, выбрав в главном меню пункт «Выгрузить ключ». Просмотреть информацию о рабочем сертификате (и загруженном ключе) можно, выбрав в главном меню пункт «Показать рабочий сертификат».

Если опция «Выгружать ключ после каждой операции» включена, ключ будет выгружен сразу после завершения операции над всеми выбранными файлами.

В случае если одновременно загружено несколько экземпляров Проводника, в них могут быть загружены разные ключи.

*Примечание – Если в программе конфигурации ПК «Средство КЗИ» установлен режим «Кэшировать закрытые ключи», то ключ, загруженный в ПК САЭС, не будет выгружен ни по завершении операции, ни при закрытии окна Проводника, ни по пункту меню «Выгрузить ключ», а только после завершения процесса Проводника. Для этого необходимо либо перезагрузить ОС Windows, либо в Диспетчере Задач выполнить по отношению к Проводнику действие «Перезапустить» («Снять задачу»).*

Сразу после загрузки ключа производится подключение к сетевому справочнику (LDAP), если в настройках пользователя не установлен режим «Не использовать сетевой справочник (LDAP)». В случае, если при подключении к сетевому справочнику произошла ошибка, на экран выводится диалог (возможно, после таймаута).

Нажатие кнопки «ОК» приводит к продолжению работы без сетевого справочника, нажатие кнопки «Отмена» - к выгрузке ключа и отказу от операции.

Если в настройках пользователя не установлен режим «Не обновлять САС из точки распространения», будет произведено обновление справочника аннулированных сертификатов (САС). В случае ошибки на экран выводится диалог (возможно, после таймаута).

Нажатие кнопки «ОК» приводит к продолжению работы без обновления САС из точки распространения, нажатие кнопки «Отмена» - к выгрузке ключа и отказу от операции.



## **6 КРИПТОГРАФИЧЕСКИЕ ОПЕРАЦИИ НАД ФАЙЛАМИ**

### **6.1 Создание, проверка и удаление ЭП**

#### **6.1.1 Создание ЭП**

Для того чтобы создать присоединённую ЭП в формате CMS/PKCS#7, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПК САЭС пункт «Создать ЭП». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа. Перед созданием ЭП будет произведена проверка уже имеющихся в файле присоединённых ЭП в формате CMS/PKCS#7 (если они там есть), при условии, что в настройках пользователя не установлен режим «Не проверять предыдущие подписи перед созданием ЭП». Если проверка существующих ЭП не была успешной, создание новой ЭП не происходит. Подпись выполняется в блочном или потоковом режиме, в зависимости от значения конфигурационного параметра «Режим шифрования и подписи».

*Примечание – В случае подписи файла, уже подписанного присоединённой подписью, новая подпись устанавливается в том режиме (блочный - потоковый), в котором установлена уже имеющаяся подпись. В этом случае значение конфигурационного параметра «Режим шифрования и подписи» игнорируется.*

Подписанный файл сохраняется в каталог, заданный в параметре «Каталог для сохранения подписанных/ зашифрованных файлов» в настройках пользователя (или в каталог, где находится подписываемый файл, если этот параметр не задан). При этом к имени файла добавляется расширение, заданное в параметре «Основные расширения имён файлов - Подписанные файлы» в настройках пользователя. В случае, когда файл уже имеет такое расширение, второй раз оно не добавляется. Если при записи подписанного файла оказывается, что файл с таким именем уже существует (за исключением случая, когда происходит добавление подписи в уже подписанный файл), выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках пользователя не установлен режим «Не выдавать диалог сохранения файла»). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»).

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - пропуску операции с текущим файлом, кнопки «Отмена» - прекращению операции со всеми оставшимися файлами.

Если операция создания ЭП производится с одним файлом, после создания ЭП на экран выдаётся сообщение об успехе или сообщение об ошибке.

Если в настройках пользователя установлен режим «Использовать TSP сервер» и задан адрес TSP сервера, при создании ЭП в неё будет добавлен штамп времени (TSP). Если при добавлении штампа времени произошла ошибка, вся операция считается неуспешной, подписанный файл не создаётся.

Если операция создания ЭП производится с несколькими файлами, сначала на экран выдаётся запрос на создание ЭП (Рисунок 8) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

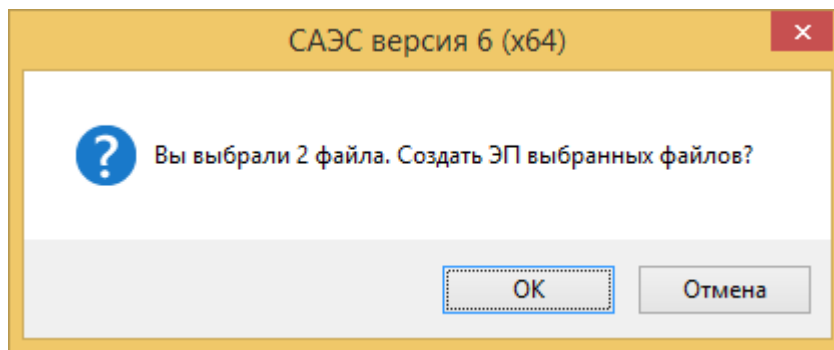


Рисунок 8 - Запрос на создание ЭП

Затем на экран выдаётся диалог создания ЭП файлов (Рисунок 9).

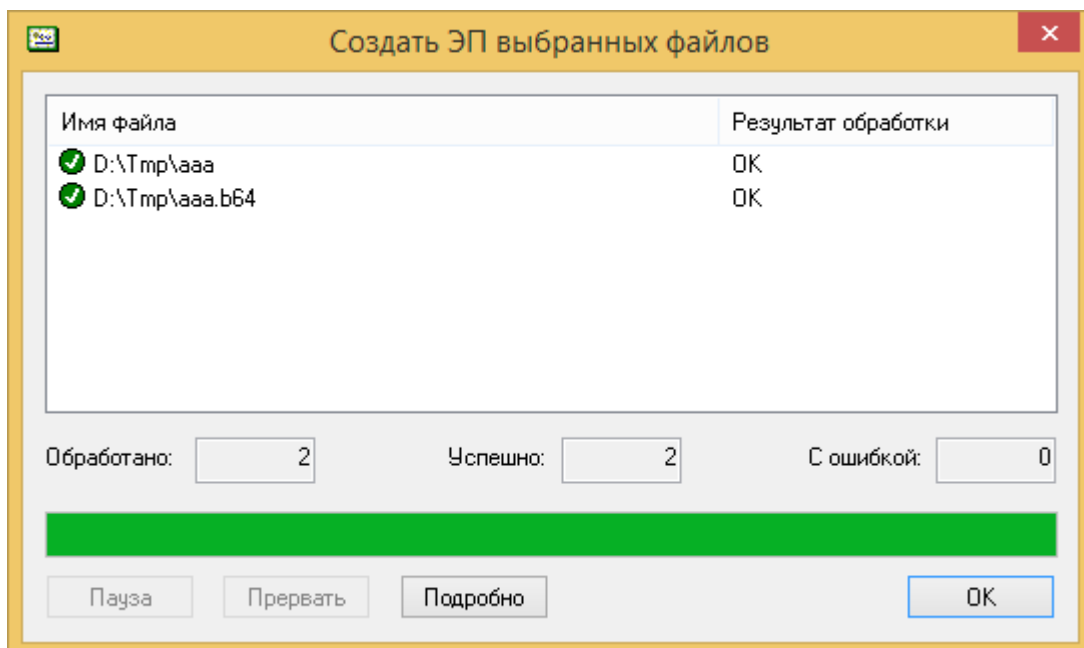


Рисунок 9 - Диалог создания ЭП файлов

Во второй колонке списка выводится краткая информация о результате создания ЭП. Для отображения полной информации выделите строку с файлом и нажмите кнопку «Подробнее» (или сделайте двойной клик «мышью») (Рисунок 10).

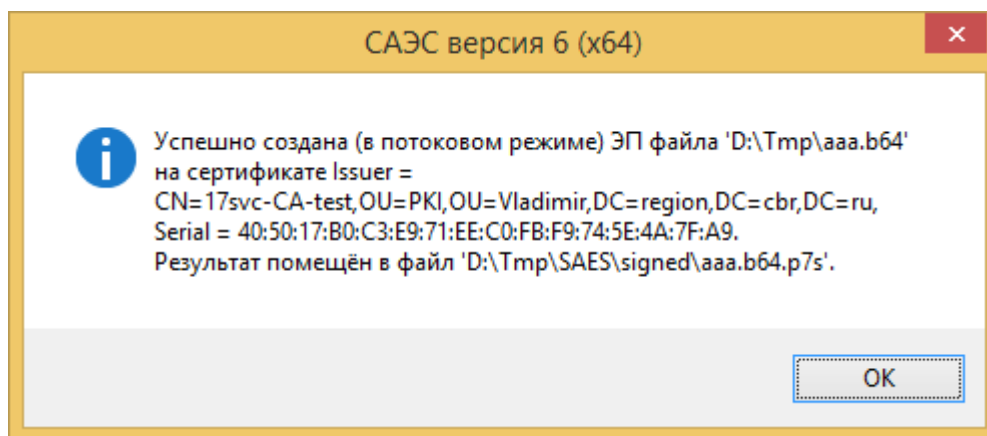


Рисунок 10 - Полная информация о создании ЭП

В процессе обработки вы можете приостановить или прервать создание ЭП нажатием кнопок «Пауза» или «Прервать».

#### 6.1.2 Проверка ЭП

Для того чтобы проверить присоединённую ЭП, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПК САЭС пункт «Проверить ЭП». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. раздел 5). Проверка подписи выполняется в блочном или потоковом режиме, в зависимости от значения конфигурационного параметра «Режим шифрования и подписи».

Если операция проверки ЭП производится с одним файлом, после проверки ЭП на экран выдаётся диалог с информацией о проверке ЭП (Рисунок 11).

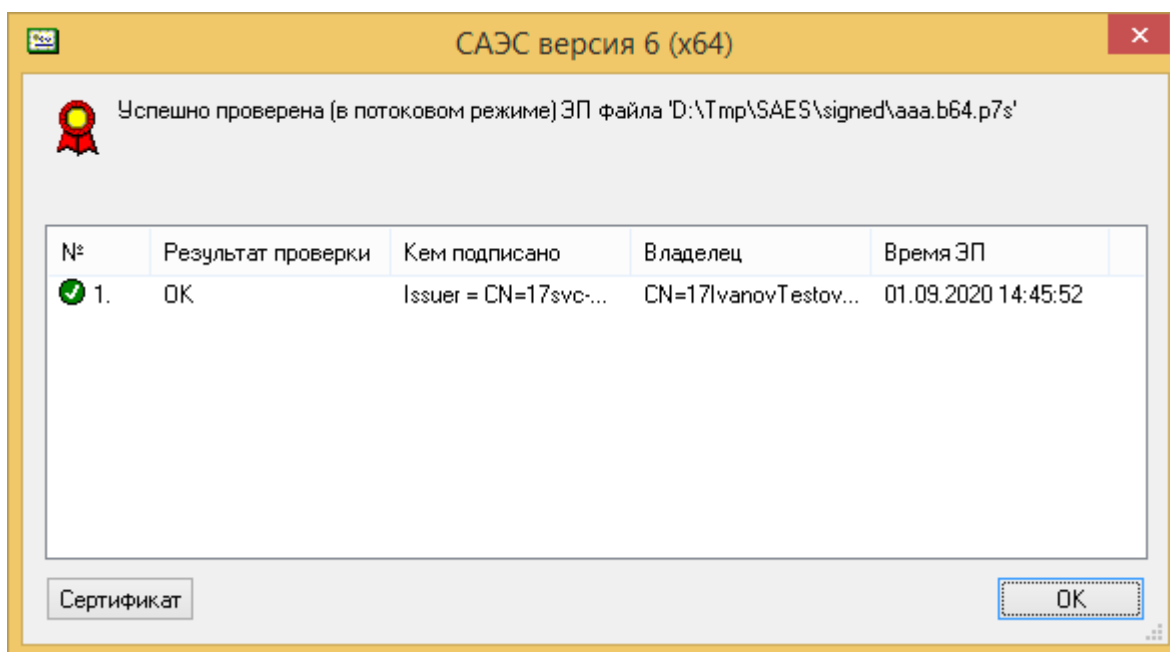


Рисунок 11 - Диалог с информацией о проверке ЭП

Первая колонка содержит номер ЭП и иконку – признак успешной или неуспешной проверки, вторая колонка – описание результата проверки этой подписи, третья – имя издателя и серийный номер сертификата, на котором создана ЭП, четвёртая – имя владельца сертификата и пятая – время создания ЭП. Чтобы подробно просмотреть сертификат (Рисунок 12), выделите подпись и нажмите кнопку «Сертификат» (или сделайте двойной клик «мышью»).

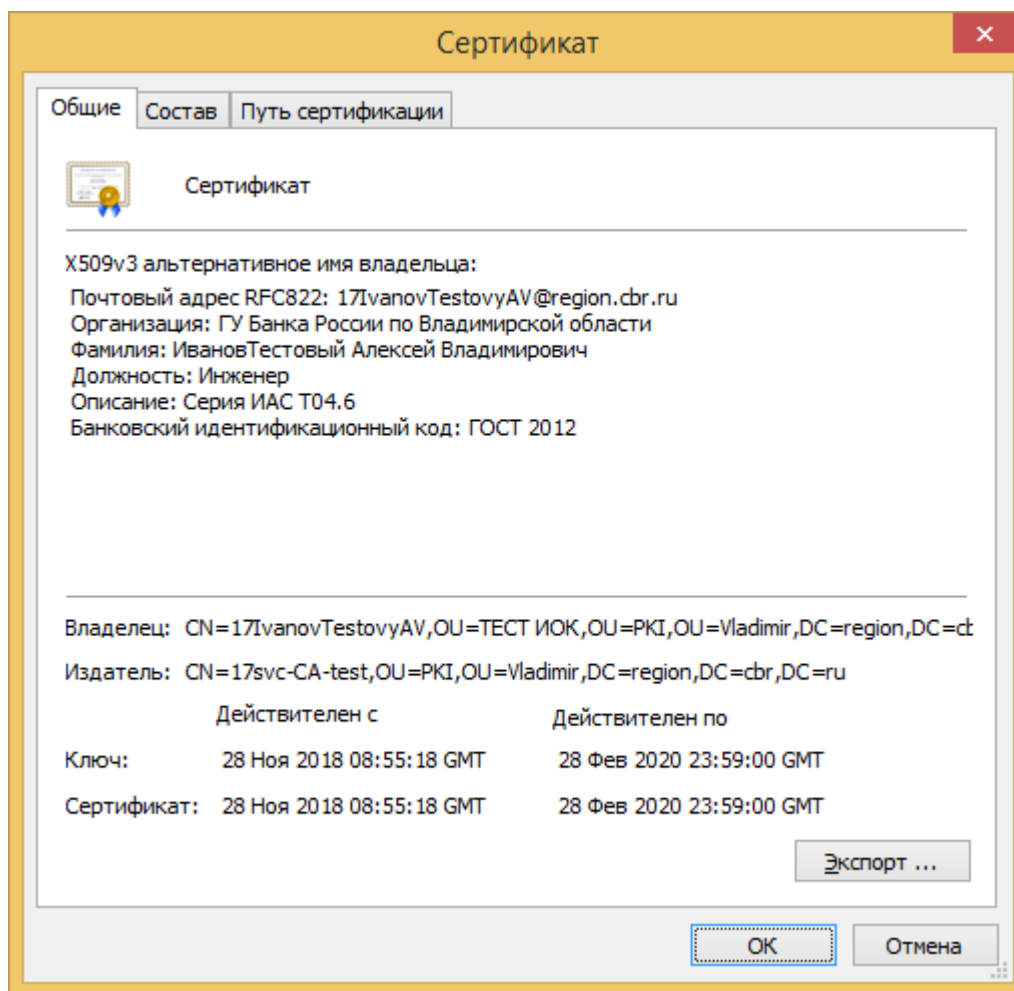


Рисунок 12 - Диалог просмотра сертификата

В случае если хоть одна подпись не была успешно проверена, результат проверки файла является отрицательным (Рисунок 13).

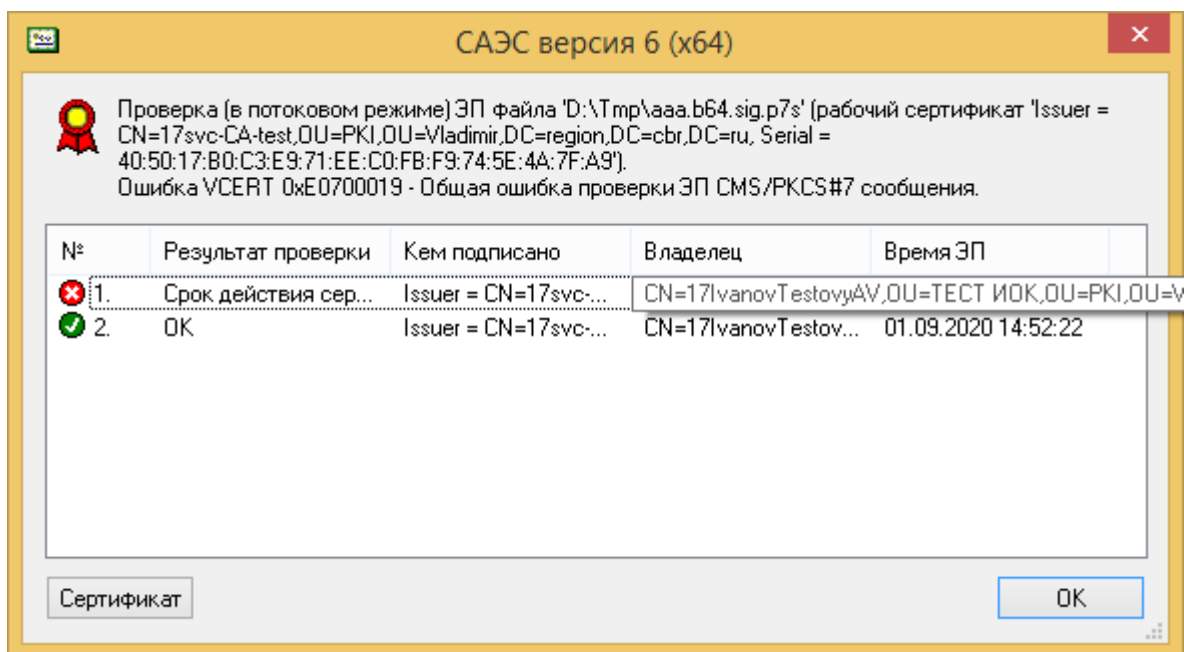


Рисунок 13 - Диалог с информацией об ошибке при проверке ЭП

Если в настройках пользователя установлен режим «Проверять штамп времени при проверке подписи», при проверке каждой ЭП производится поиск штампа времени (TSP) и его проверка (в случае обнаружения). В диалоге с информацией о проверке ЭП информация о проверке штампа времени ЭП содержится под строчкой, содержащей информацию о проверке этой ЭП и содержит аналогичную информацию (Рисунок 14).

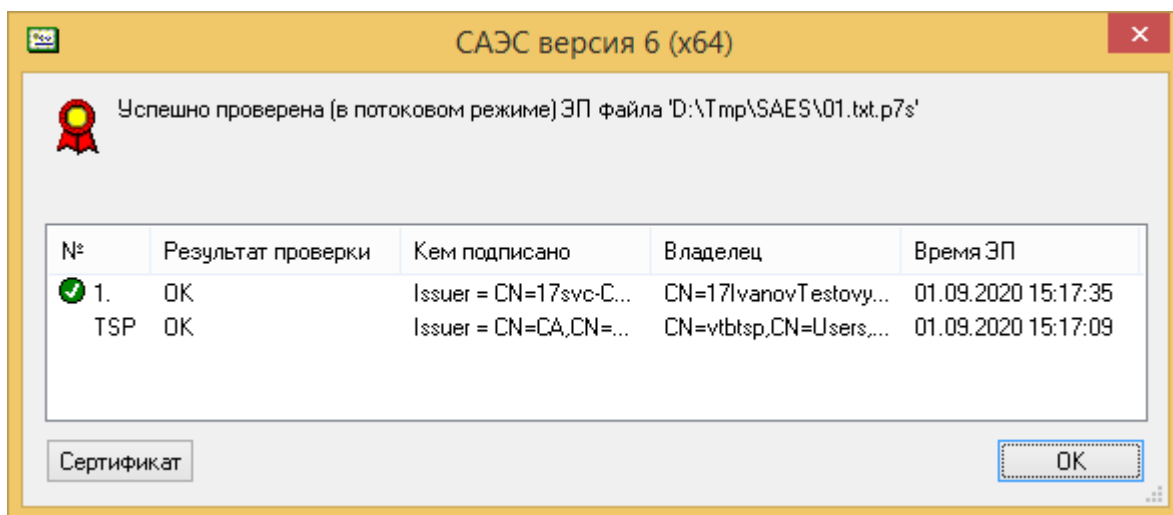


Рисунок 14 - Диалог с информацией о проверке ЭП со штампом времени

В случае возникновения ошибки при проверке штампа времени проверка подписи считается неудачной. Если в настройках пользователя не установлен режим «Отсутствие штампа времени считать ошибкой», информация об отсутствии штампа времени не выводится. Если в настройках пользователя установлен режим «Отсутствие штампа времени

считать ошибкой», отсутствующие штампы времени отображаются отдельной строкой (Рисунок 15).

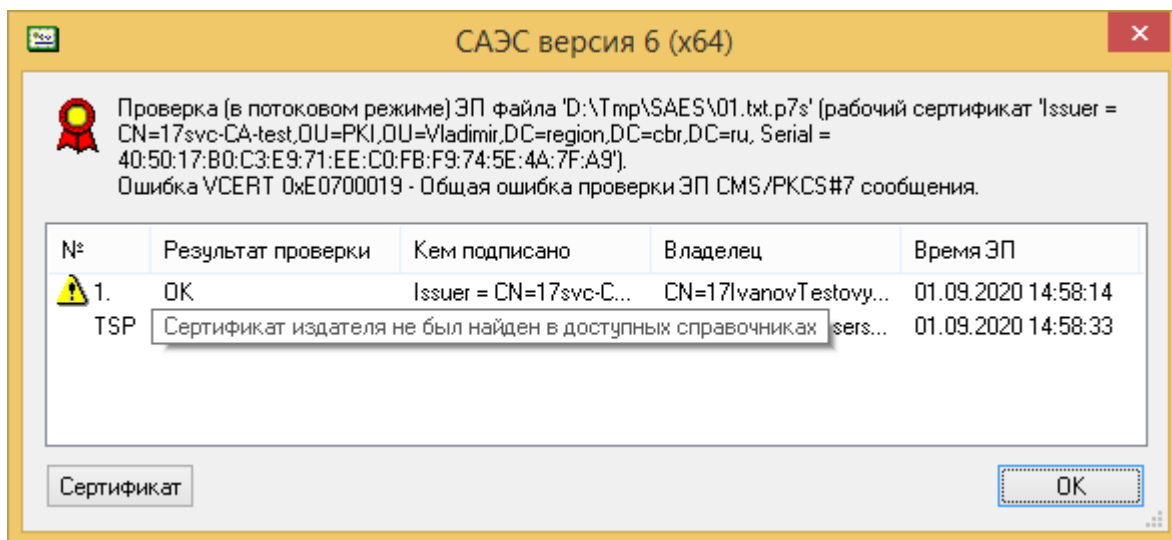


Рисунок 15 - Диалог с информацией о проверке ЭП с отсутствующим штампом времени

Если операция проверки ЭП производится с несколькими файлами, сначала на экран выдаётся запрос на проверку ЭП (Рисунок 16) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

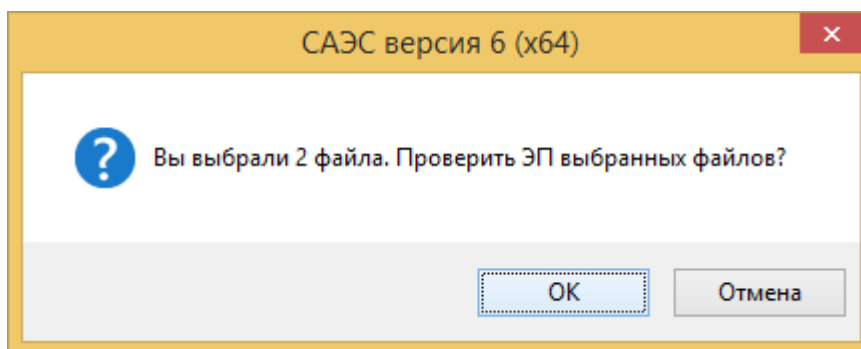


Рисунок 16 - Запрос на проверку ЭП

Затем на экран выдаётся диалог проверки ЭП файлов (Рисунок 17).

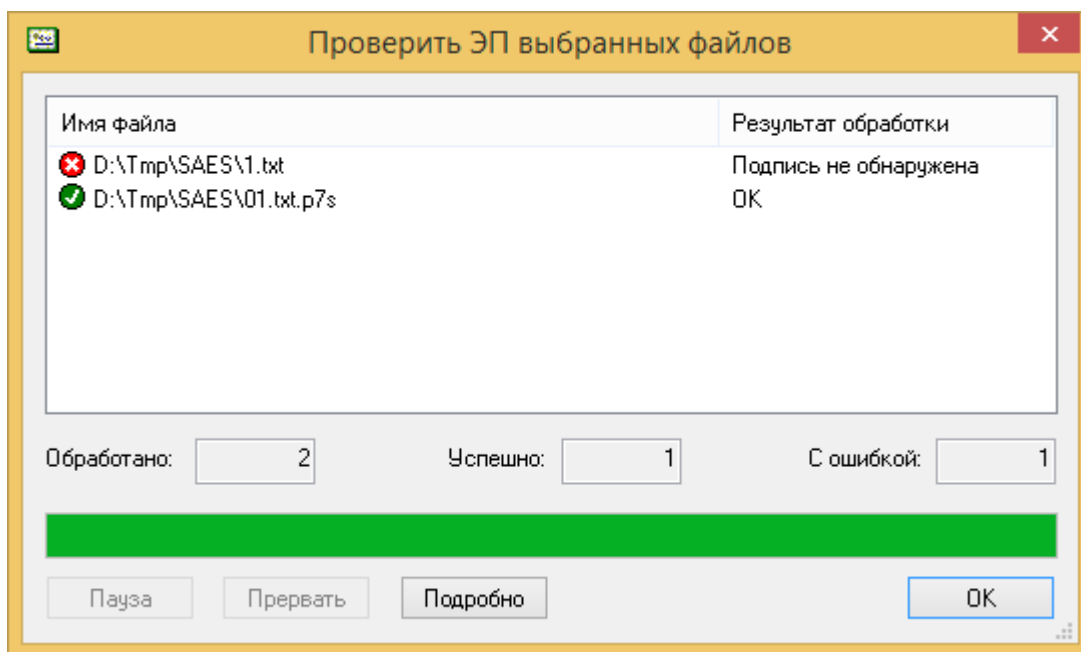


Рисунок 17 - Диалог проверки ЭП файлов

Во второй колонке списка выводится краткая информация о результате проверки ЭП. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробнее» (или сделайте двойной клик «мышью»).

В процессе обработки вы можете приостановить или прервать проверку ЭП нажатием кнопок «Пауза» или «Прервать».

### 6.1.3 Проверка и удаление ЭП

Для того чтобы проверить присоединённую ЭП и удалить из файла одну или несколько подписей, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПК САЭС пункт «Проверить и удалить ЭП». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа. Затем на экране появится диалог подтверждения удаления ЭП (Рисунок 18). Диалог будет выдан независимо от количества выбранных файлов и от выбора режима «Не выдавать предварительный диалог с количеством файлов» в настройках пользователя.

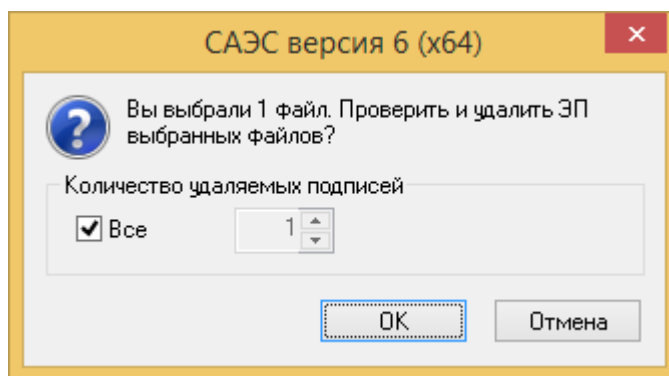


Рисунок 18 - Диалог удаления ЭП

Чтобы удалить не все подписи, а несколько (начиная с конца), снимите опцию «Все» и выберите количество удаляемых подписей. Удаление и проверка подписи выполняется в блочном или потоковом режиме, в зависимости от значения конфигурационного параметра «Режим шифрования и подписи».

*Примечание – В потоковом режиме возможно удаление с проверкой только всех подписей.*

Удаление ЭП производится только в случае успешной проверки всех подписей файла. Файл, полученный в результате удаления подписей, сохраняется в каталог, заданный в параметре «Каталог для сохранения проверенных/ расшифрованных файлов» в настройках пользователя (или в каталог, где находится проверяемый файл, если этот параметр не задан). При этом если удаляются все подписи, а файл имеет расширение, заданное в параметре «Основные расширения имён файлов - Подписанные файлы» или в параметре «Дополнительные расширения имён файлов» в настройках пользователя, это расширение будет удалено. В случае, когда файл не имеет такого расширения, и в случае, когда удаляются не все подписи, имя файла не меняется. Если при записи файла с удалёнными ЭП оказывается, что файл с таким именем уже существует (за исключением случая, когда происходит удаление не всех ЭП, и результат записывается в исходный файл), выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках пользователя не установлен режим «Не выдавать диалог сохранения файла»). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»).

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - к пропуску операции с текущим файлом, кнопки «Отмена» - к прекращению операции со всеми оставшимися файлами.



Если операция проверки и удаления ЭП производится с одним файлом, после выполнения операции на экран выдаётся диалог с информацией о проверенных и удалённых ЭП (Рисунок 19).

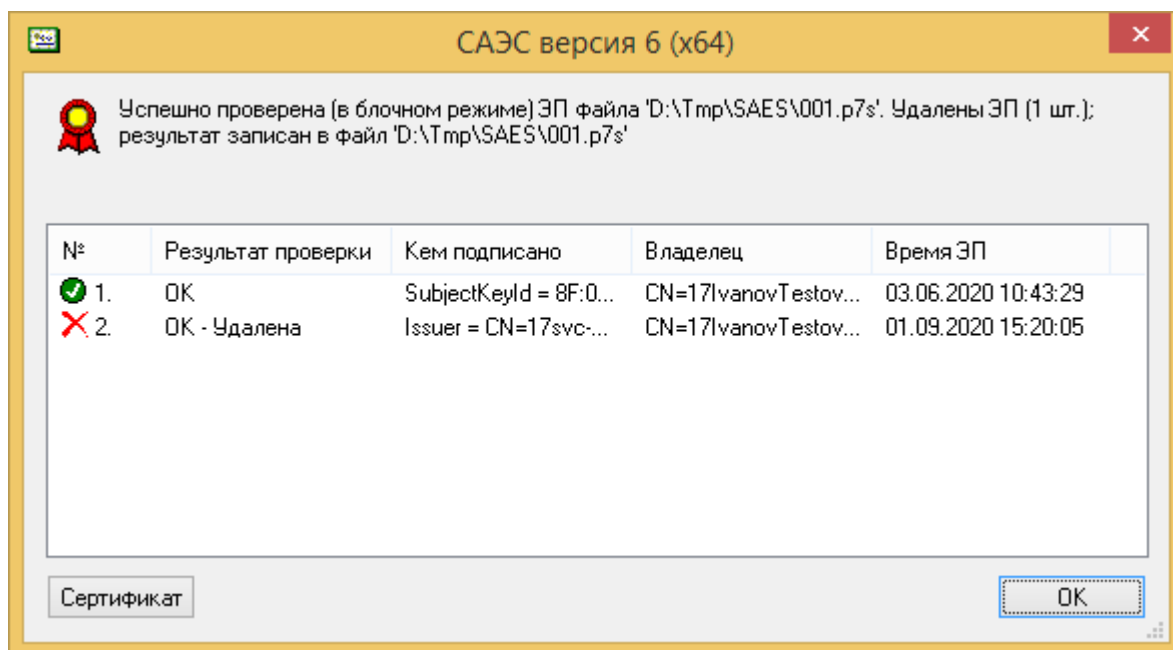


Рисунок 19 - Диалог с информацией об удалении и проверке ЭП

Первая колонка содержит номер ЭП и иконку – признак удаления или успешной (неуспешной) проверки, вторая колонка – описание результата операции, третья – имя издателя и серийный номер сертификата, на котором создана ЭП, четвертая – имя владельца сертификата и пятая – время создания ЭП. Чтобы подробно просмотреть сертификат выделите подпись и нажмите кнопку «Сертификат» (или сделайте двойной клик «мышью»).

Если операция проверки ЭП производится с несколькими файлами, на экран выдаётся диалог проверки и удаления ЭП файлов (Рисунок 20).

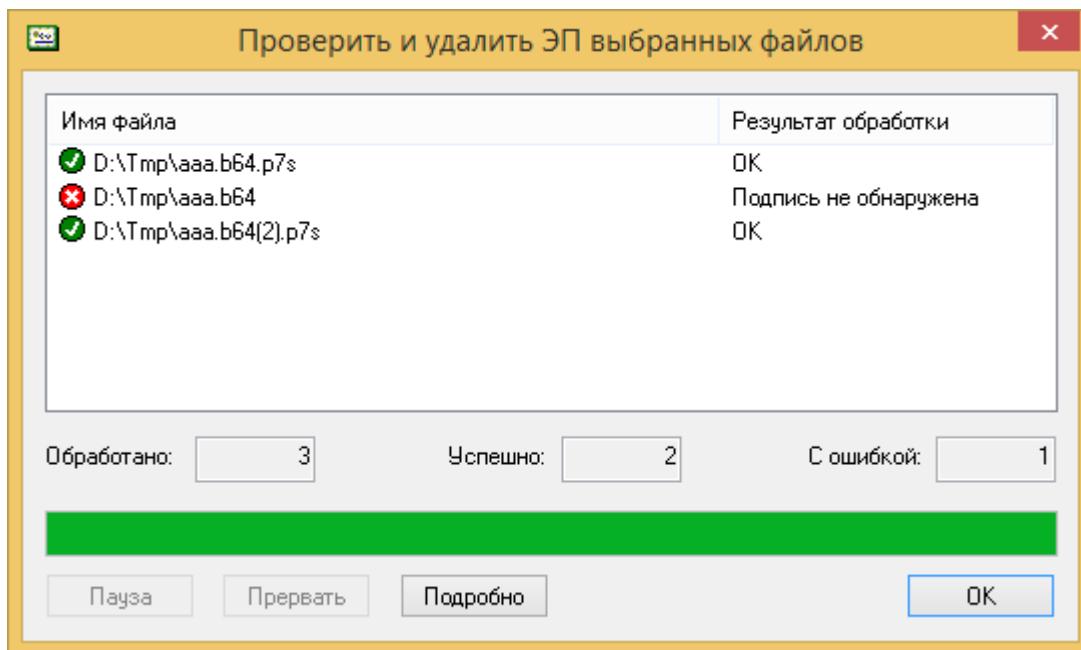


Рисунок 20 - Диалог проверки и удаления ЭП файлов

Во второй колонке списка выводится краткая информация о результате операции. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробнее» (или сделайте двойной клик «мышью»).

В процессе обработки вы можете приостановить или прервать выполнение операции нажатием кнопок «Пауза» или «Прервать».

#### 6.1.4 Удаление ЭП без проверки

Для того чтобы удалить из файлов все ЭП, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПК САЭС пункт «Дополнительно», подпункт «Удалить ЭП без проверки». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. раздел 5).

Файл, полученный в результате удаления всех подписей, сохраняется в каталог, заданный в параметре «Каталог для сохранения проверенных/ расшифрованных файлов» в настройках пользователя (или в каталог, где находится подписанный файл, если этот параметр не задан). При этом если файл имеет расширение, заданное в параметре «Основные расширения имён файлов - Подписанные файлы» или в параметре «Дополнительные расширения имён файлов» в настройках пользователя, это расширение будет удалено. В случае, когда файл не имеет такого расширения, имя файла не меняется. Если при записи файла с удалёнными ЭП оказывается, что файл с таким именем уже существует, выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках пользователя не установлен режим «Не выдавать диалог сохранения

файла)). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»).

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - к пропуску операции с текущим файлом, кнопки «Отмена» - к прекращению операции со всеми оставшимися файлами.

Если операция удаления ЭП производится с одним файлом, после проверки ЭП на экран выдаётся сообщение об успехе или сообщение об ошибке.

Если операция удаления ЭП производится с несколькими файлами, сначала на экран выдаётся запрос на удаление ЭП (Рисунок 21) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

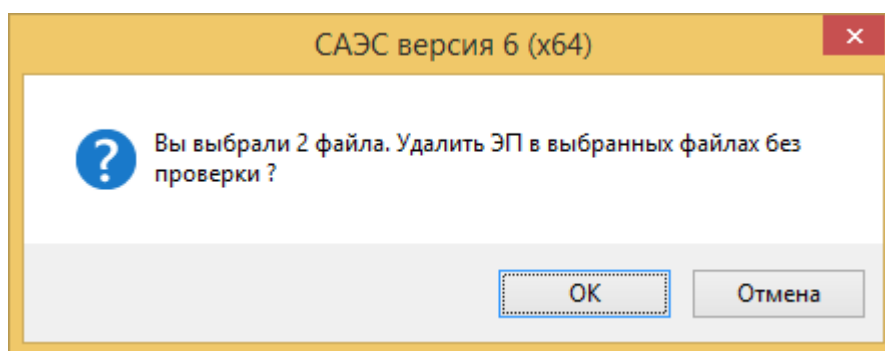


Рисунок 21 - Запрос на удаление ЭП

Затем на экран выдаётся диалог удаления ЭП (Рисунок 22).

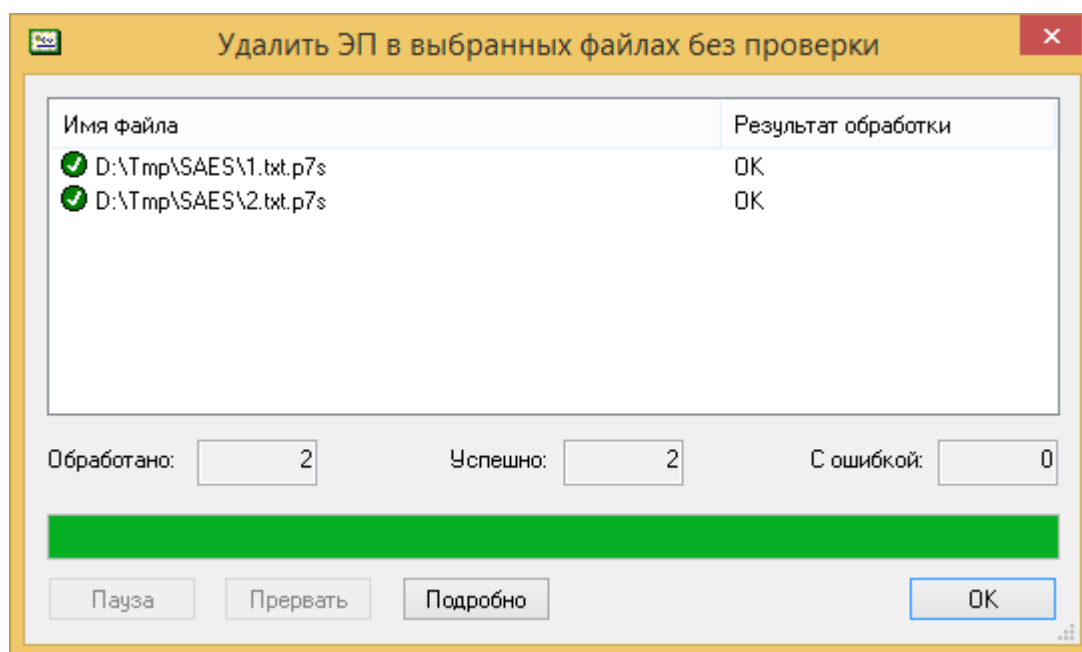


Рисунок 22 - Диалог удаления ЭП

Во второй колонке списка выводится краткая информация о результате операции. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробнее» (или сделайте двойной клик «мышью»).

В процессе обработки вы можете приостановить или прервать выполнение операции нажатием кнопок «Пауза» или «Прервать».

#### 6.1.5 Создание отсоединённой ЭП

Для того чтобы создать отсоединённую (detached) ЭП в формате PKCS#7, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПК САЭС пункт «Дополнительно», подпункт «Создать отсоединённую ЭП». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. раздел 5). Файл с отсоединённой подписью сохраняется в каталог, заданный в параметре «Каталог для сохранения подписанных/ зашифрованных файлов» в настройках пользователя (или в каталог, где находится подписываемый файл, если этот параметр не задан). При этом к имени файла добавляется расширение, заданное в параметре «Основные расширения имён файлов – Файлы с отсоединённой ЭП» в настройках пользователя. В случае, когда файл уже имеет такое расширение, второй раз оно не добавляется. Если при записи подписанного файла оказывается, что файл с таким именем уже существует (за исключением случая, когда файл содержит отсоединённую ЭП), выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках пользователя не установлен режим «Не выдавать диалог сохранения файла»). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»).

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - к пропуску операции с текущим файлом, кнопки «Отмена» - к прекращению операции со всеми оставшимися файлами.

В случае если параметр «Каталог для сохранения подписанных/ зашифрованных файлов» в настройках пользователя не задан, при попытке создать отсоединённую ЭП для файла, имеющего расширение, заданное в параметре «Основные расширения имён файлов – Файлы с отсоединённой ЭП» в настройках пользователя, будет выдана ошибка.

В такой ситуации для создания отсоединённой ЭП необходимо изменить расширение подписываемого файла.

Перед созданием отсоединённой ЭП будет произведена проверка уже имеющихся подписей в файле с отсоединённой ЭП (если они там есть) при условии, что в настройках

пользователя не установлен режим «Не проверять предыдущие подписи перед созданием ЭП». Если проверка существующих отсоединённых ЭП не была успешной, создание новой отсоединённой ЭП не происходит.

Если операция создания отсоединённой ЭП производится с одним файлом, после создания ЭП на экран выдаётся сообщение об успехе (Рисунок 23) или сообщение об ошибке (Рисунок 24).

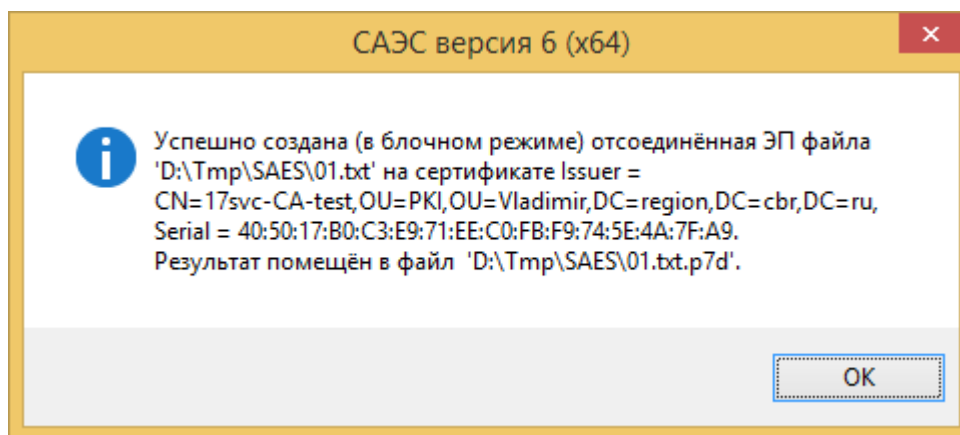


Рисунок 23 - Сообщение об успешном создании отсоединённой ЭП

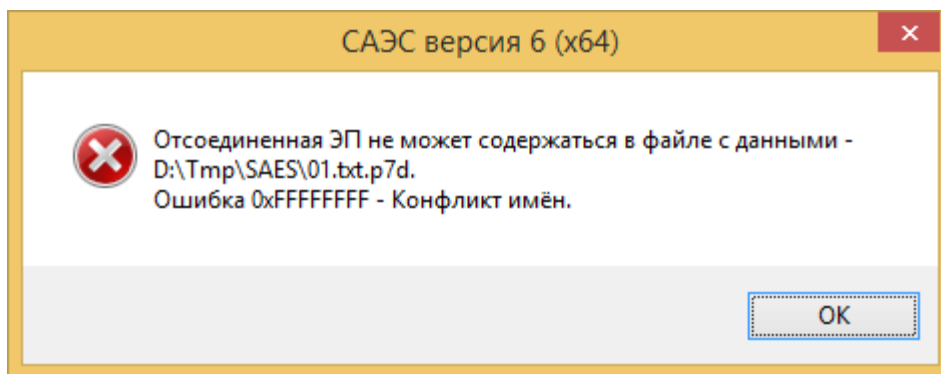


Рисунок 24 - Сообщение об ошибке при создании отсоединённой ЭП

Если в настройках пользователя установлен режим «Использовать TSP сервер» и задан адрес TSP сервера, при создании отсоединённой ЭП в неё будет добавлен штамп времени (TSP). Если при добавлении штампа времени произошла ошибка, вся операция считается неуспешной, файл с отсоединённой ЭП не создаётся.

Если операция создания отсоединённой ЭП производится с несколькими файлами, сначала на экран выдаётся запрос на создание отсоединённой ЭП при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов» (Рисунок 25).

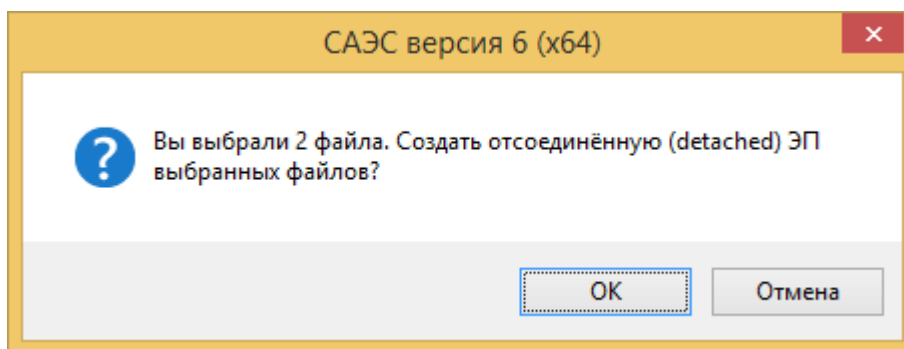


Рисунок 25 - Запрос на создание отсоединённой ЭП

Затем на экран выдаётся диалог создания отсоединённой ЭП файлов (Рисунок 26).

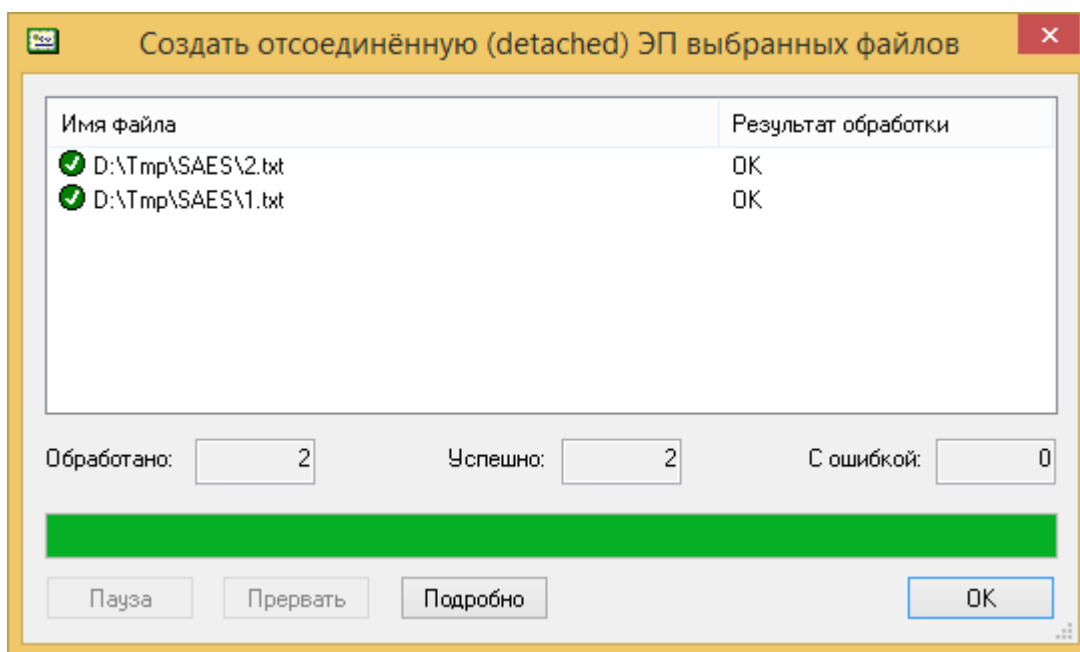


Рисунок 26 - Диалог создания отсоединённой ЭП файлов

Во второй колонке списка выводится краткая информация о результате создания отсоединённой ЭП. Для отображения полной информации выделите строку с файлом и нажмите кнопку «Подробнее» (или сделайте двойной клик «мышью»).

В процессе обработки вы можете приостановить или прервать создание отсоединённой ЭП нажатием кнопок «Пауза» или «Прервать».

#### 6.1.6 Проверка отсоединённой ЭП

Для того чтобы проверить отсоединённую ЭП выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПК САЭС пункт «Дополнительно», подпункт «Проверить отсоединённую ЭП». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. раздел 5).

**ВНИМАНИЕ:** для проверки отсоединённой ЭП надо выбирать в Проводнике файлы с подписанными данными, а не файлы отсоединённых подписей. Для каждого файла с данными файл с отсоединённой подписью ищется в каталоге, заданном в параметре «Каталог для сохранения подписанных/ зашифрованных файлов» в настройках пользователя (или в каталоге, где находится подписанный файл, если этот параметр не задан). При этом к имени файла с данными добавляется расширение, заданное в параметре «Основные расширения имён файлов – Файлы с отсоединённой ЭП» в настройках пользователя (в случае, когда файл уже имеет такое расширение, второй раз оно не добавляется).

В случае если параметр «Каталог для сохранения подписанных/ зашифрованных файлов» в настройках пользователя не задан, при попытке проверить отсоединённую ЭП для файла, имеющего расширение, заданное в параметре «Основные расширения имён файлов – Файлы с отсоединённой ЭП» в настройках пользователя, будет выдана ошибка (Рисунок 27).

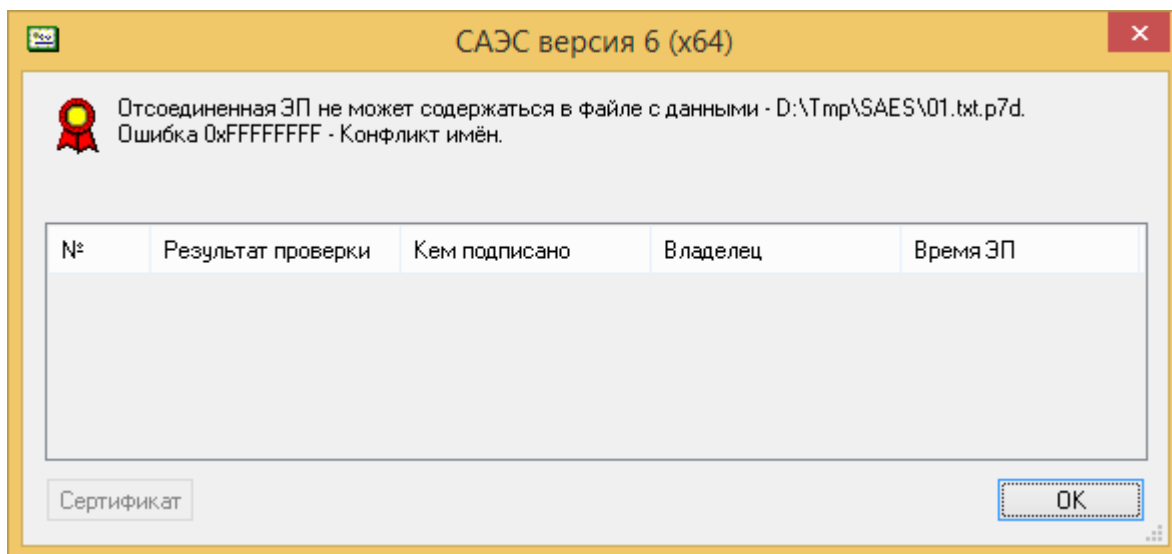


Рисунок 27 - Сообщение о конфликте имён при проверке отсоединённой ЭП

Если операция проверки отсоединённой ЭП производится с одним файлом, после проверки ЭП на экран выдаётся диалог с информацией о проверенных ЭП (Рисунок 28).

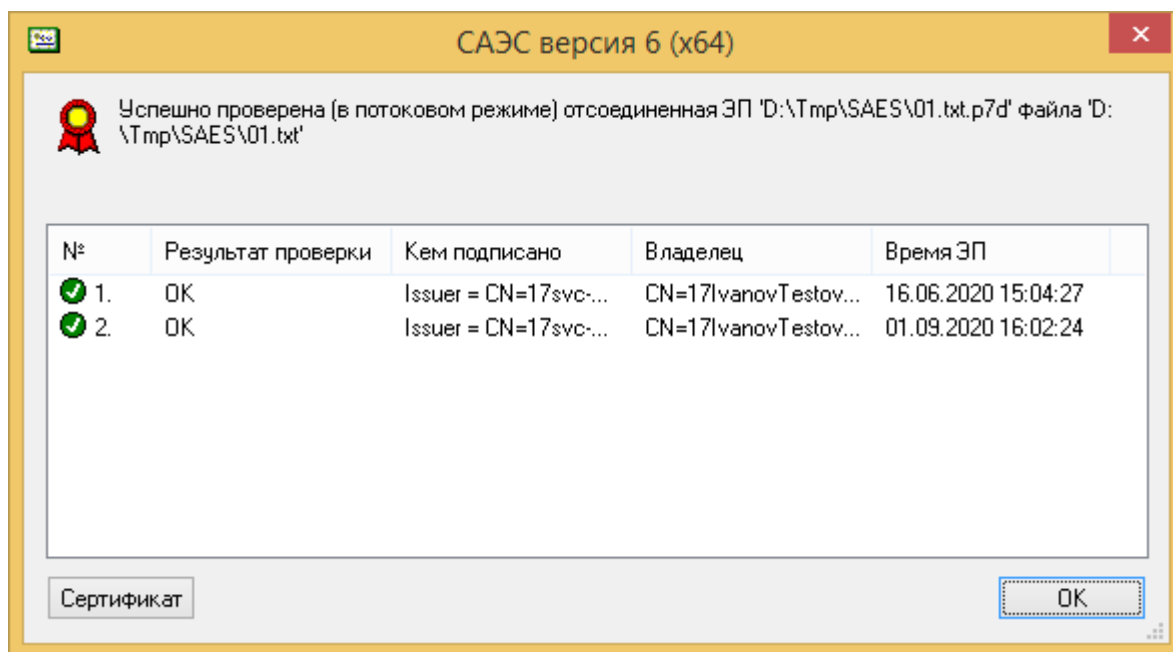


Рисунок 28 - Диалог с информацией о проверке отсоединённой ЭП

Первая колонка содержит номер ЭП и иконку – признак успешной или неуспешной проверки, вторая колонка – описание результата проверки этой подписи, третья – имя издателя и серийный номер сертификата, на котором создана ЭП, четвёртая – имя владельца сертификата и пятая – время создания ЭП. Чтобы подробно просмотреть сертификат (Рисунок 29), выделите подпись и нажмите кнопку «Сертификат» (или сделайте двойной клик «мышью»).



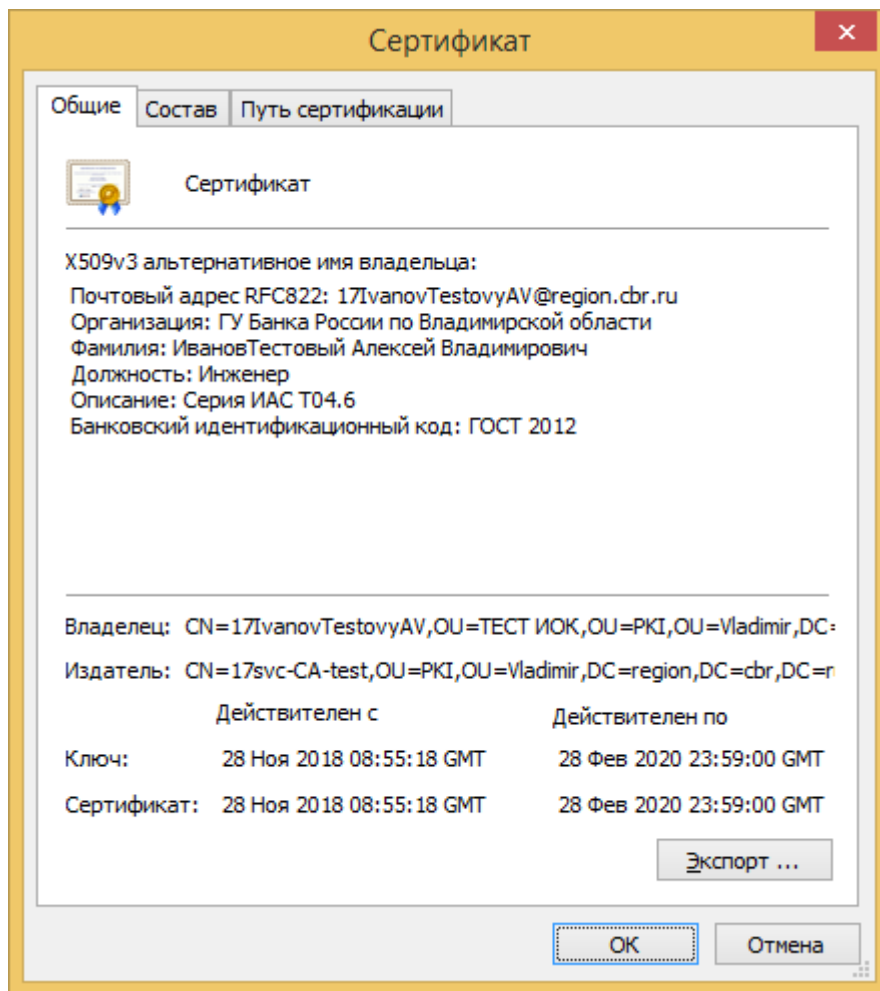


Рисунок 29 - Диалог просмотра сертификата

В случае если хоть одна подпись не была успешно проверена, результат проверки файла является отрицательным.

Если в настройках пользователя установлен режим «Проверять штамп времени при проверке подписи», при проверке каждой отсоединённой ЭП производится поиск штампа времени (TSP) и его проверка (в случае обнаружения). В диалоге с информацией о проверке отсоединённой ЭП информация о проверке штампа времени ЭП содержится под строчкой, содержащей информацию о проверке этой ЭП и содержит аналогичную информацию (если в настройках пользователя не установлен режим «Отсутствие штампа времени считать ошибкой», информация об отсутствии штампа времени не выводится).

В случае возникновения ошибки при проверке штампа времени, проверка подписи считается неудачной. Если в настройках пользователя установлен режим «Отсутствие штампа времени считать ошибкой», отсутствующие штампы времени отображаются отдельной строкой.

Если операция проверки отсоединённой ЭП производится с несколькими файлами, сначала на экран выдаётся запрос на проверку отсоединённой ЭП (Рисунок 30) при условии,

что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

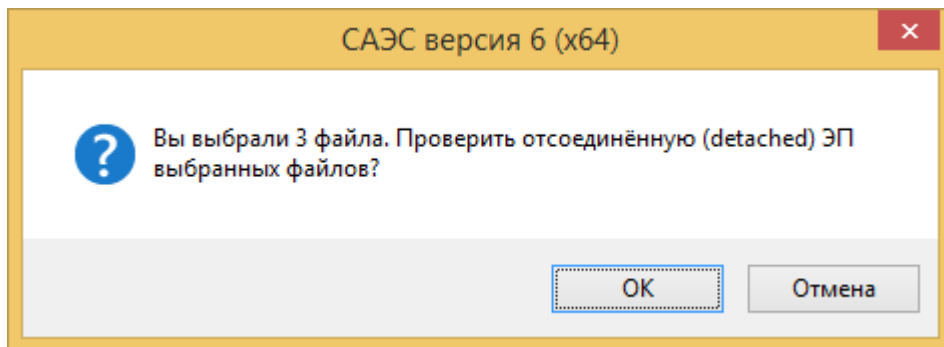


Рисунок 30 - Запрос на проверку отсоединённой ЭП

Затем на экран выдаётся диалог проверки отсоединённой ЭП файлов (Рисунок 31).

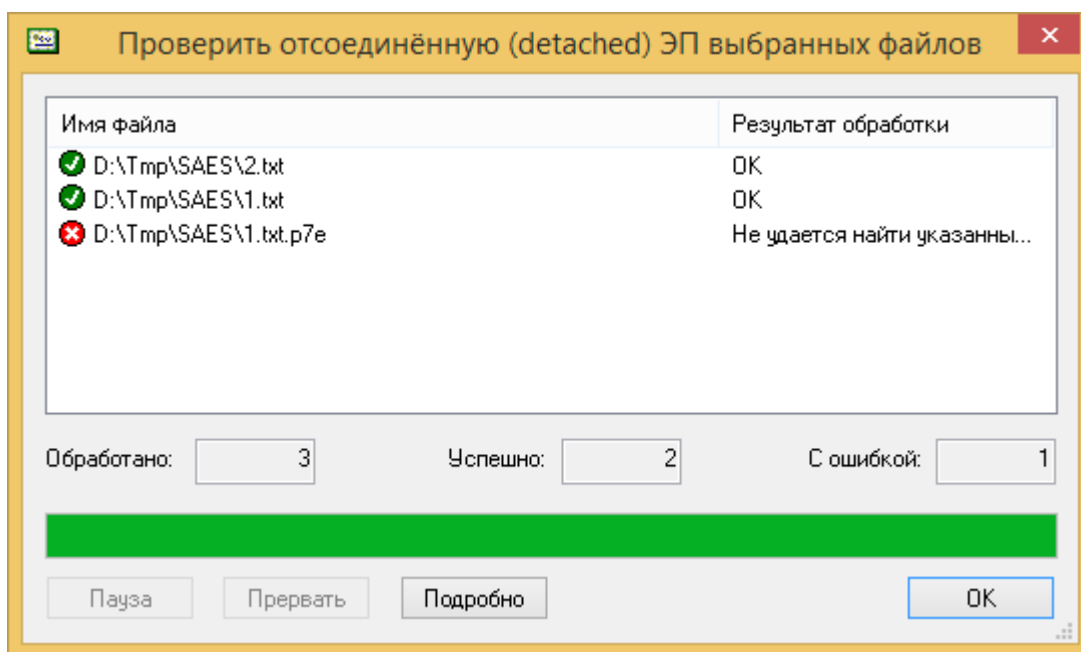


Рисунок 31 - Диалог проверки отсоединённой ЭП файлов

Во второй колонке списка выводится краткая информация о результате проверки ЭП. Для отображения полной информации выделите строку с файлом и нажмите кнопку «Подробнее» (или сделайте двойной клик «мышью»).

В процессе обработки вы можете приостановить или прервать проверку отсоединённой ЭП нажатием кнопок «Пауза» или «Прервать».

## 6.2 Зашифрование и расшифрование файлов

### 6.2.1 Зашифрование

Для зашифрования выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПК САЭС пункт «Зашифровать». Если ранее в этом экземпляре

Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. раздел 5). Прежде, чем начать шифрование, необходимо задать список получателей зашифрованного сообщения. Для этого на экран выдаётся диалог выбора получателей зашифрованного сообщения (Рисунок 32).

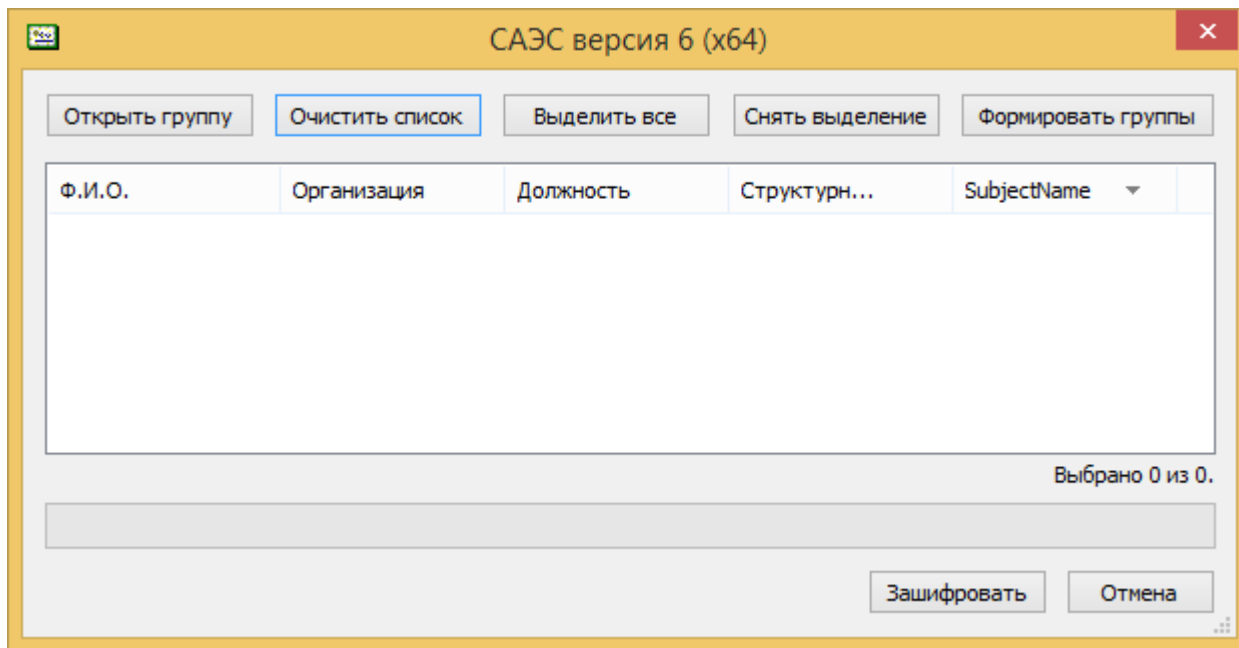


Рисунок 32 - Пустой диалог выбора получателей

Изначально список получателей пуст. Необходимо задать список получателей (пользователей, для которых шифруется файл). Для удобства выбора получателей зашифрованного сообщения можно создавать поименованные списки получателей – группы (возможно также создание одной безымянной группы). При следующем открытии диалога выбора получателей список заполняется получателями, на которых последний раз выполнялось шифрование.

#### 6.2.1.1 Создание групп получателей

Для создания (или изменения) групп получателей нажмите кнопку «Формировать группы», на экран будет выдано диалоговое окно (Рисунок 33).

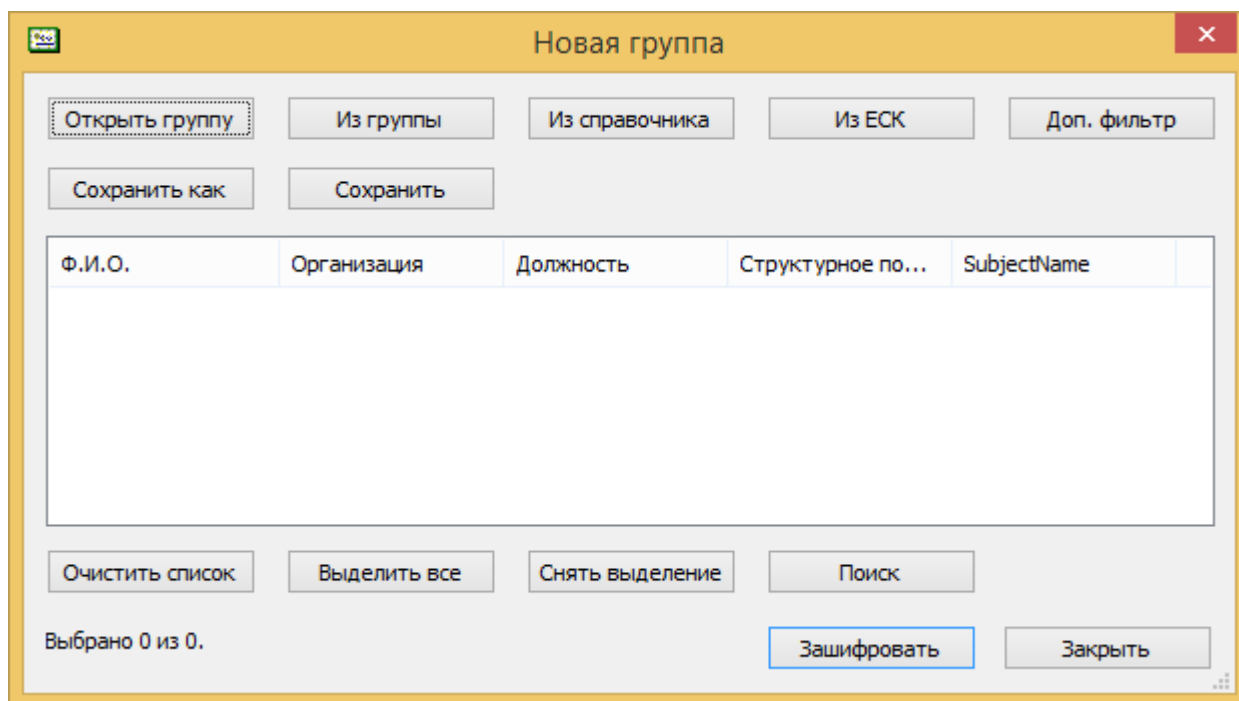


Рисунок 33 - Диалог формирования групп получателей

Для открытия существующей группы нужно нажать кнопку «Открыть группу», после чего в стандартном диалоге открытия файла выбрать файл группы (с расширением “cgr”). Для создания новой группы надо заполнить список получателей (пользователей). Самый простой способ создать группу - это нажать кнопку «Из справочника» (Рисунок 34). При этом отображается список всех пользователей, включенных в Локальный справочник.

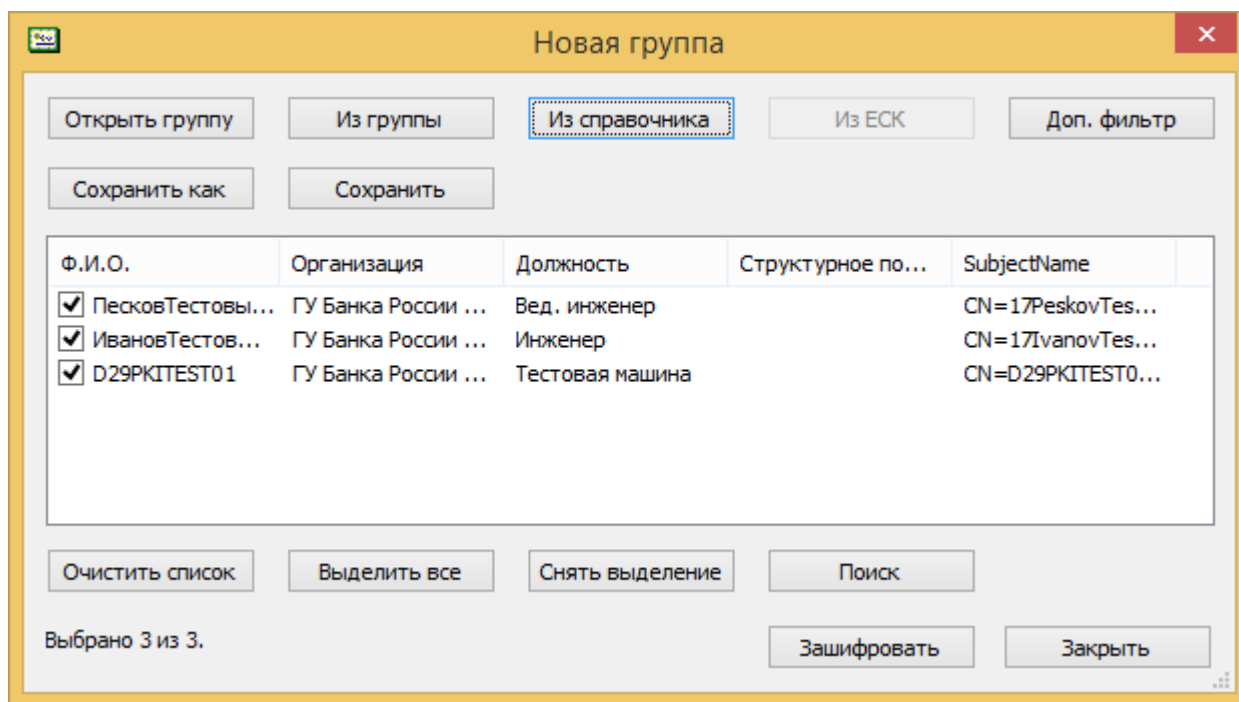


Рисунок 34 - Список получателей из Справочника сертификатов

Теперь в этом списке получателей надо выделить тех, которые войдут в формируемую группу. Это можно сделать либо вручную, мышкой, отметив галочкой, либо с помощью кнопки «Поиск», предварительно сняв выделение со всех получателей в списке. После нажатия на кнопку «Поиск» на экране отображается диалоговое окно поиска (Рисунок 35).

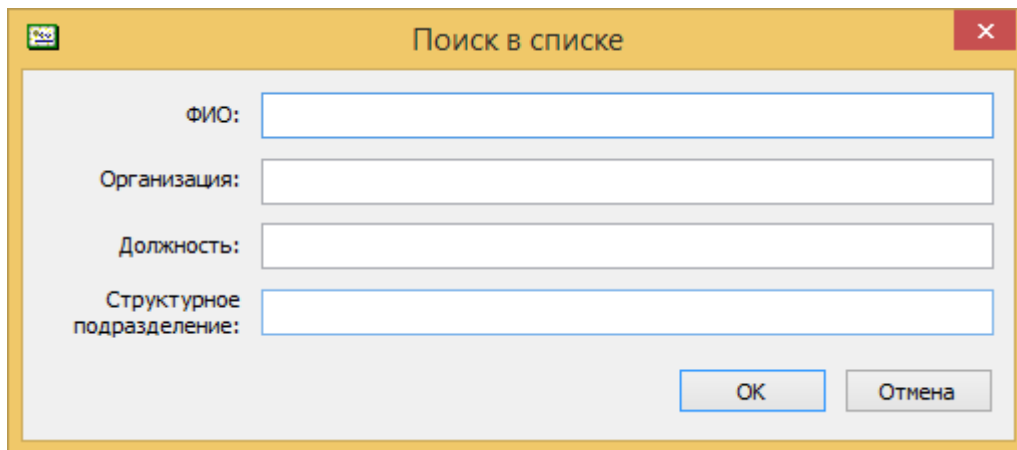


Рисунок 35 - Диалог поиска в списке

Задайте шаблон поиска для одного или нескольких полей (условия поиска складываются как логическое «И»). Шаблон поиска может включать специальные символы '?' и '\*' обозначающие - один произвольный символ и произвольное число произвольных символов, соответственно (как в файловом шаблоне). Строчные и прописные буквы считаются эквивалентными (Рисунок 36).

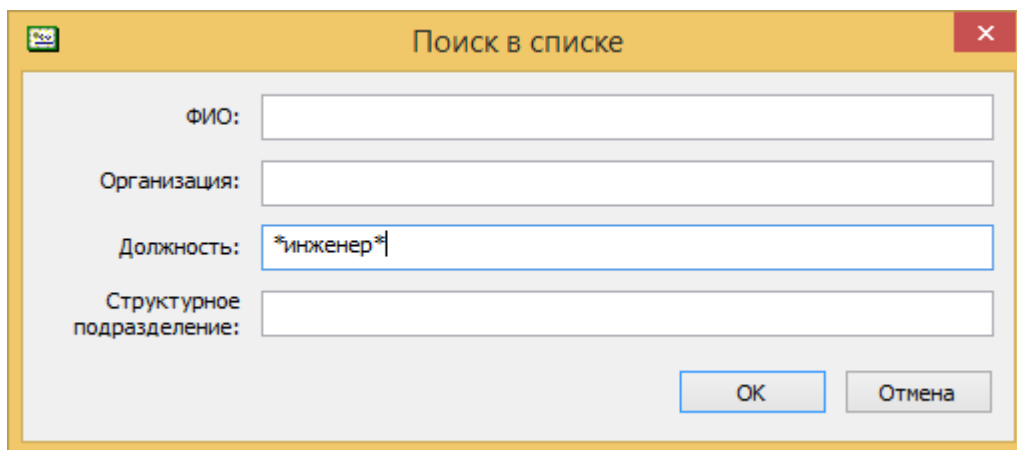


Рисунок 36 - Шаблон для поиска в списке

Нажмите кнопку «ОК». Получатели, соответствующие введённому шаблону, будут помечены галочками (Рисунок 37).

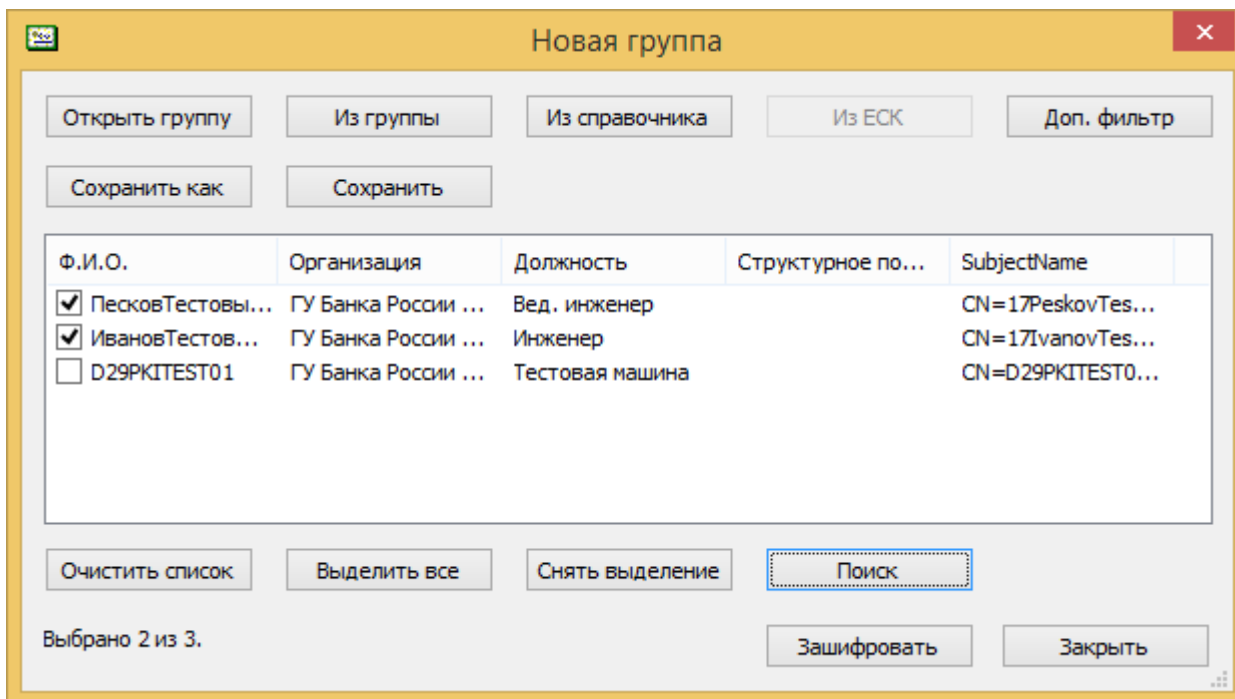


Рисунок 37 - Результат поиска в списке

Выделение с помощью поиска можно выполнять несколько раз подряд, в этом случае вновь найденные пользователи добавляются к ранее найденным. Чтобы выделить всех пользователей или убрать выделение со всего списка, нажмите кнопки «Выделить все» и «Снять выделение», соответственно. Для удаления всех пользователей из списка нажмите кнопку «Очистить список».

Для поиска сертификатов в глобальном справочнике (Единая система каталогов Банка России, далее – ЕСК) надо нажать кнопку «Из ЕСК». На экране отобразится диалоговое окно поиска. Задайте шаблоны для поиска (шаблон на поиск в ЕСК не может содержать специальный символ '?', поскольку он не поддерживается протоколом LDAP) (Рисунок 38).

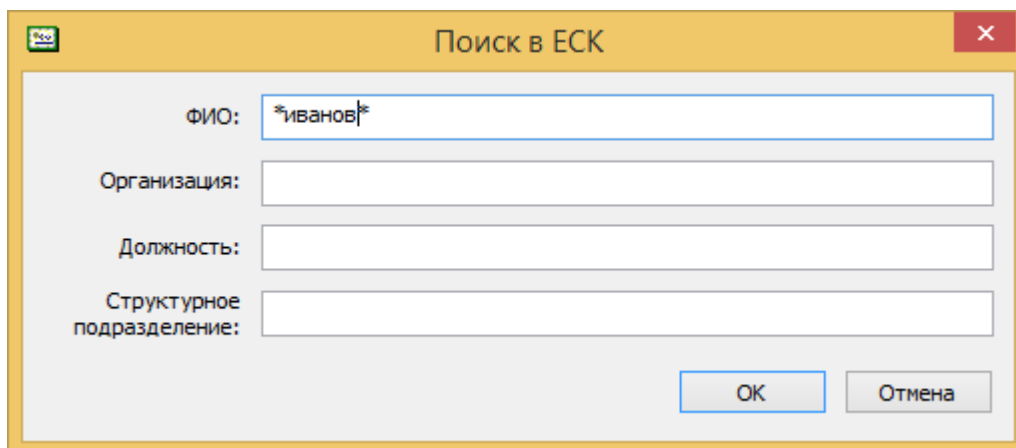


Рисунок 38 - Шаблон для поиска в ЕСК

Нажмите кнопку «ОК». В список будут внесены все, найденные в ЕСК пользователи, соответствующие заданному шаблону (Рисунок 39).

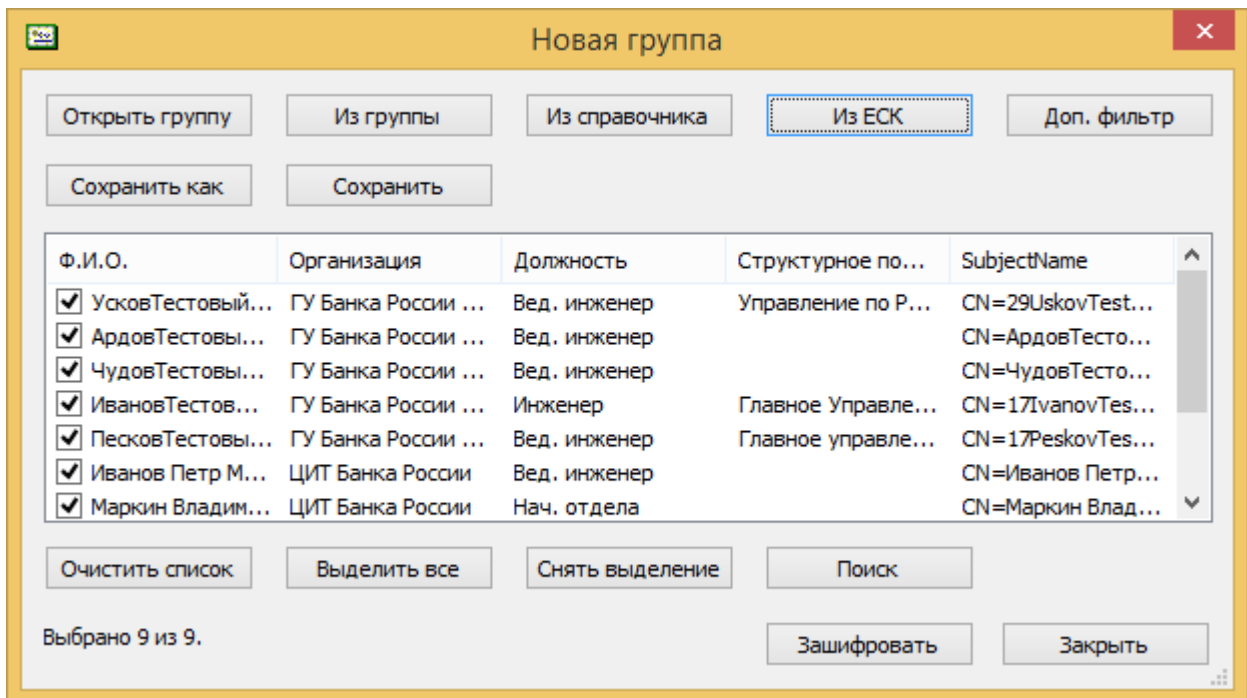


Рисунок 39 - Результат поиска в ЕСК

Обратите внимание, что в списке оказались не только пользователи с фамилией Иванов, но и другие, содержащие данную подстроку, например, Маркин Владимир Иванович.

Для того, чтобы отсеять пользователей, у которых в данный момент нет сертификатов, на которые можно шифровать, нажмите кнопку «Доп. фильтр». Все пользователи в списке будут проверены, и выделенными останутся только те, у которых есть хотя бы один неотозванный сертификат с действующим (неистекшим) ключом шифрования для той ключевой системы, на которой был загружен ключ (профиль).

**ВНИМАНИЕ:** эта операция может занять много времени, т.к. она требует разбора, проверки и построения цепочки для каждого проверяемого сертификата.

Чтобы сохранить выделенных в списке пользователей как группу, нажмите кнопку «Сохранить» и укажите имя файла в стандартном диалоге сохранения. Название группы отображается в заголовке окна.

Кнопка «Из группы» добавляет содержимое указанной группы к списку пользователей, что позволяет сливать две и более групп в одну.

Нажатие на кнопку «Закреть» просто возвращает в диалоговое окно выбора получателей.

Нажатие на кнопку «Зашифровать» возвращает в предыдущее диалоговое окно и переносит список выделенных получателей (Рисунок 40).

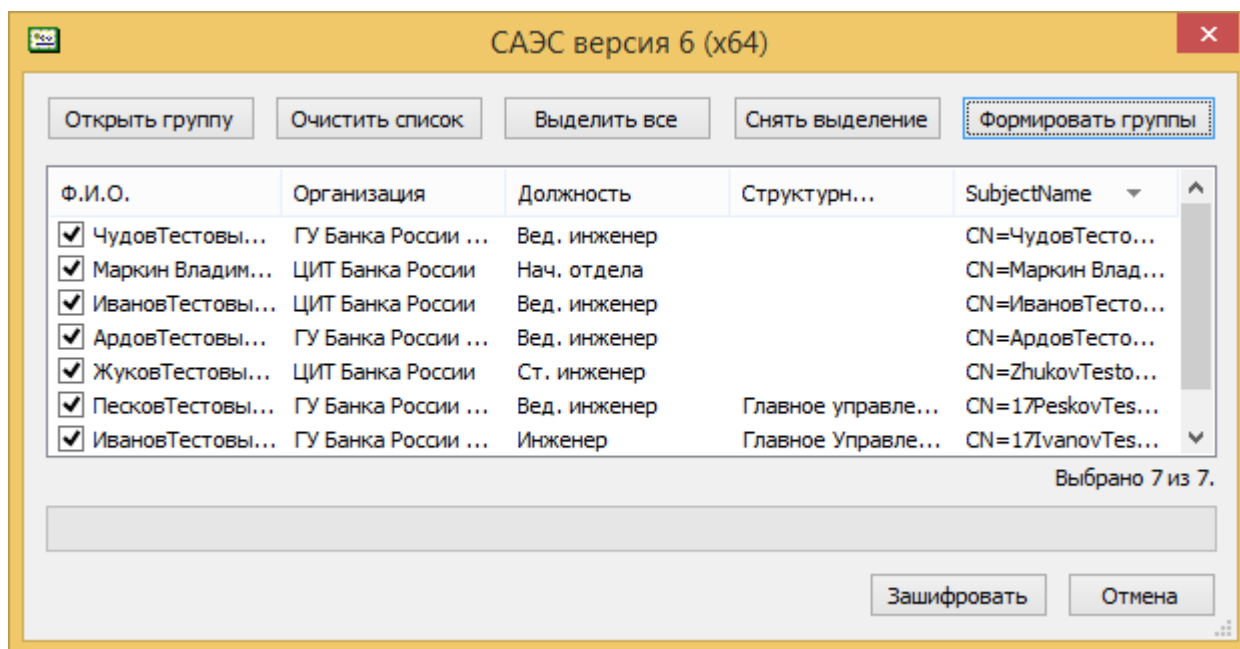


Рисунок 40 - Диалог выбора получателей со списком из безымянной группы

После этого можно сразу перейти к шифрованию, а можно открыть ранее созданные группы.

#### 6.2.1.2 Выбор получателей для шифрования из ранее созданных групп

Чтобы выбрать получателей шифрования из ранее созданных групп, нажмите кнопку «Открыть группу» и выберите в стандартном диалоге открытия файлов файл группы. Содержимое группы отобразится в списке, все пользователи будут помечены галочкой (Рисунок 41).

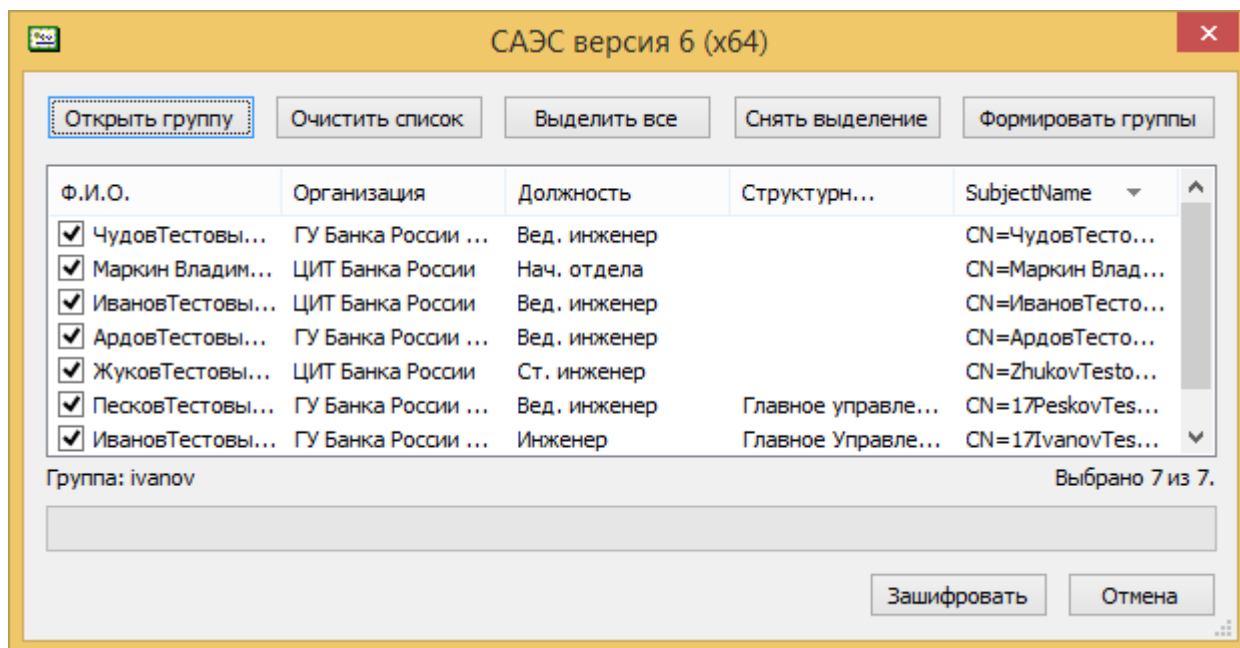


Рисунок 41 - Диалог со списком из группы "ivanov"



Одновременно можно открыть несколько групп, все пользователи будут внесены в список, любого пользователя можно удалить из списка на шифрование, убрав галочку.

Для очистки списка, выделения всех получателей списка и снятия выделения со всех получателей нажмите кнопки «Очистить список», «Выделить все» и «Снять выделение» соответственно.

#### 6.2.1.3 Выполнение шифрования

После выбора списка получателей нажмите кнопку «Зашифровать». Сначала происходит поиск сертификатов для всех выбранных получателей (один получатель может иметь несколько сертификатов, шифрование производится на все действительные сертификаты пользователя, предназначенные для шифрования). Процесс поиска отображается в линейке прогресса в диалоговом окне (Рисунок 42).

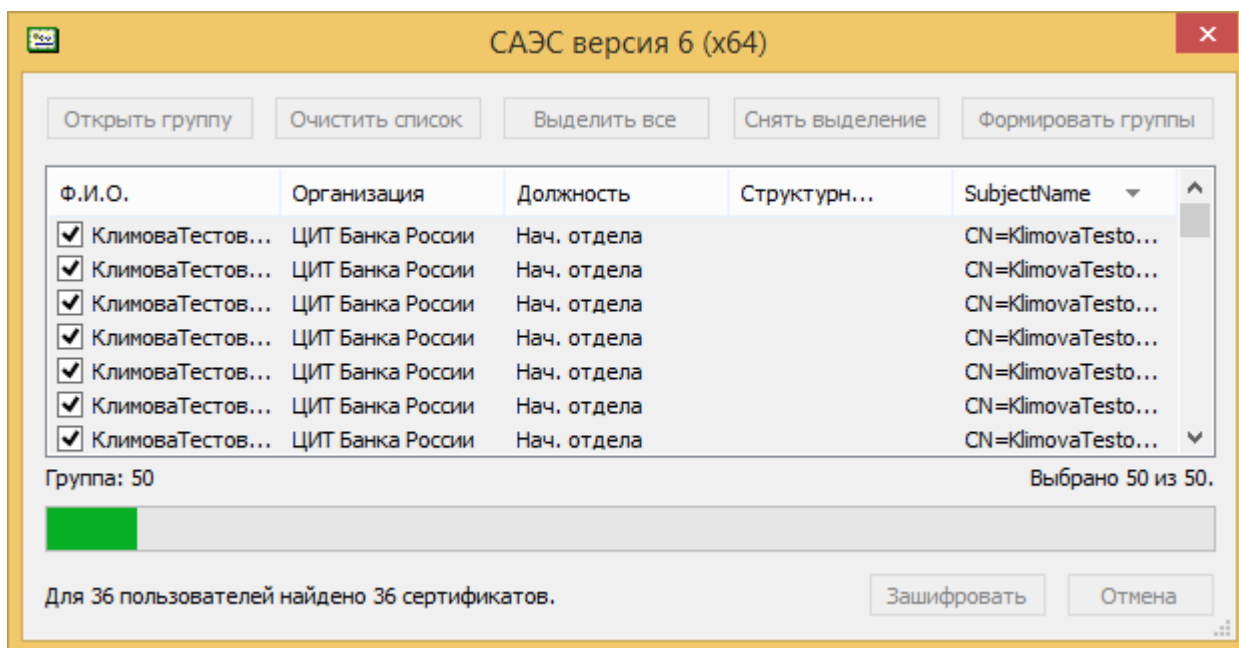


Рисунок 42 - Процесс поиска сертификатов получателей

Если для какого-либо получателя из списка не найдено ни одного сертификата, на экран выдаётся предупреждение (Рисунок 43).

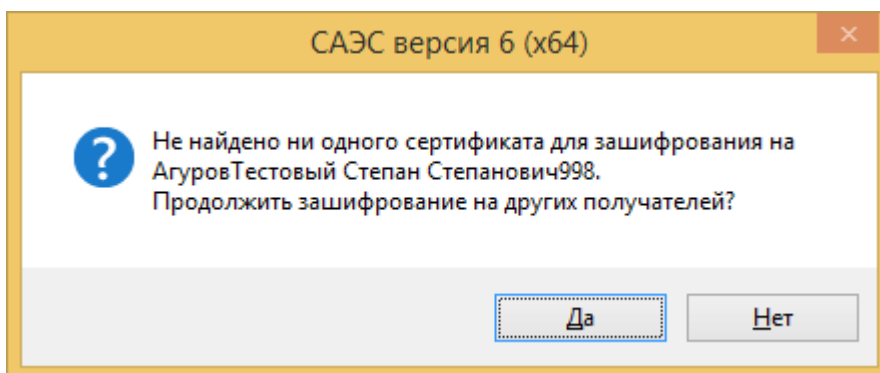


Рисунок 43 - Предупреждение об отсутствии сертификатов у получателя

Нажатие кнопки «Да» исключает получателя из списка, нажатие кнопки «Нет» прекращает операцию.

Если файл, к которому применяется операция зашифрования, уже зашифрован, на экран выдаётся предупреждение (Рисунок 44 или Рисунок 45).

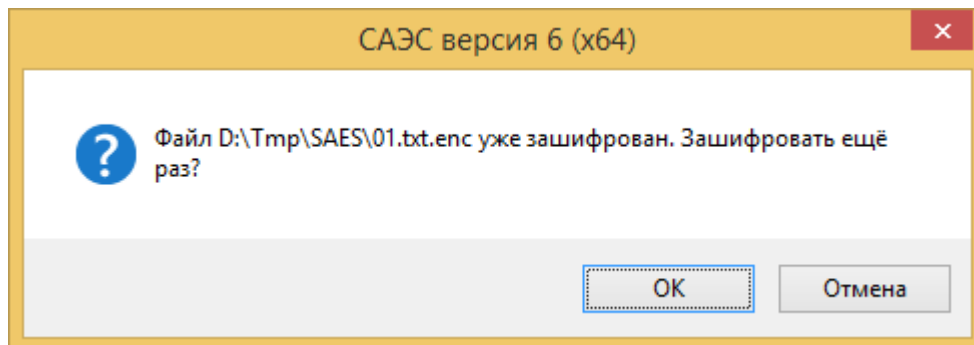


Рисунок 44 - Предупреждение о том, что файл уже зашифрован  
(при шифровании одного файла)

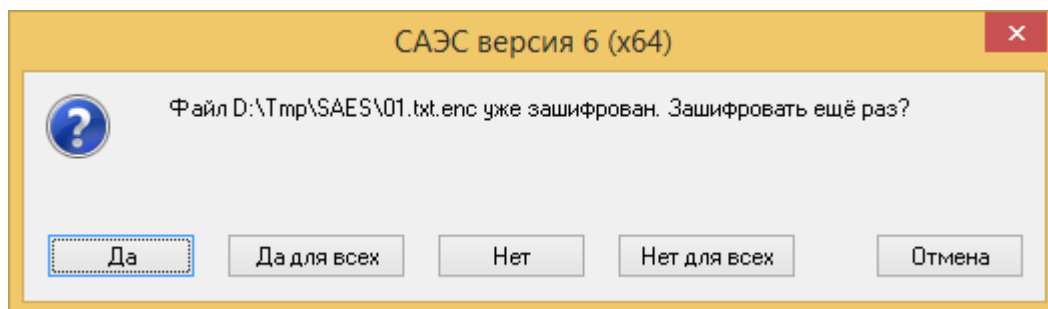


Рисунок 45 - Предупреждение о том, что файл уже зашифрован  
(при шифровании нескольких файлов)

Нажмите кнопку «Да», чтобы разрешить повторное зашифрование файла, кнопка «Да для всех» разрешает повторное зашифрование указанного файла и всех остальных файлов, выбранных для данной операции. Нажатие на кнопку «Нет» приводит к пропуску данного файла, «Нет для всех» - к пропуску всех зашифрованных файлов, выбранных для данной операции. Кнопка «Отмена» прекращает операцию (в случае, если для зашифрования выбран только один файл, в этом диалоге будут только две кнопки – «ОК» и «Отмена»).

Зашифрованный файл сохраняется в каталог, заданный в параметре «Каталог для сохранения подписанных/ зашифрованных файлов» в настройках пользователя (или в каталог, где находится шифруемый файл, если этот параметр не задан). При этом к имени файла добавляется расширение, заданное в параметре «Основные расширения имён файлов - Зашифрованные файлы» в настройках пользователя. В случае когда файл уже имеет такое расширение, второй раз оно не добавляется. Если при записи зашифрованного файла оказывается, что файл с таким именем уже существует (за исключением случая, когда происходит зашифрование уже зашифрованного файла), выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках

пользователя не установлен режим «Не выдавать диалог сохранения файла»). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»).

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - пропуску операции с текущим файлом, кнопки «Отмена» - прекращению операции со всеми оставшимися файлами.

Если операция зашифрования производится с одним файлом, после выполнения операции на экран выдаётся сообщение об успехе (Рисунок 46) либо сообщение об ошибке (Рисунок 47).

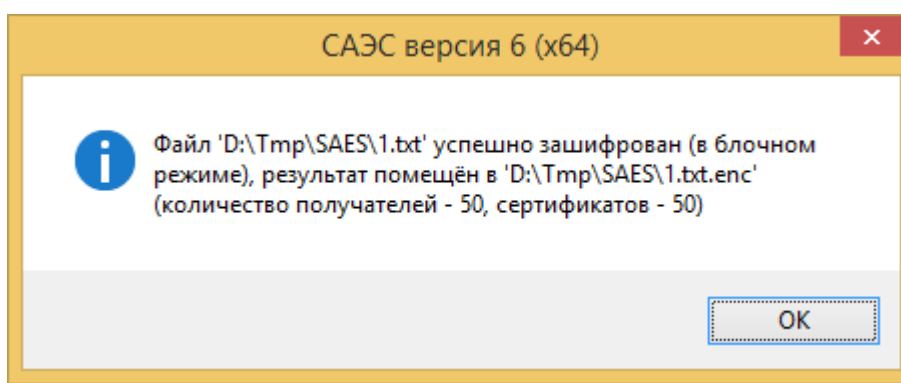


Рисунок 46 - Сообщение об успешном зашифровании файла

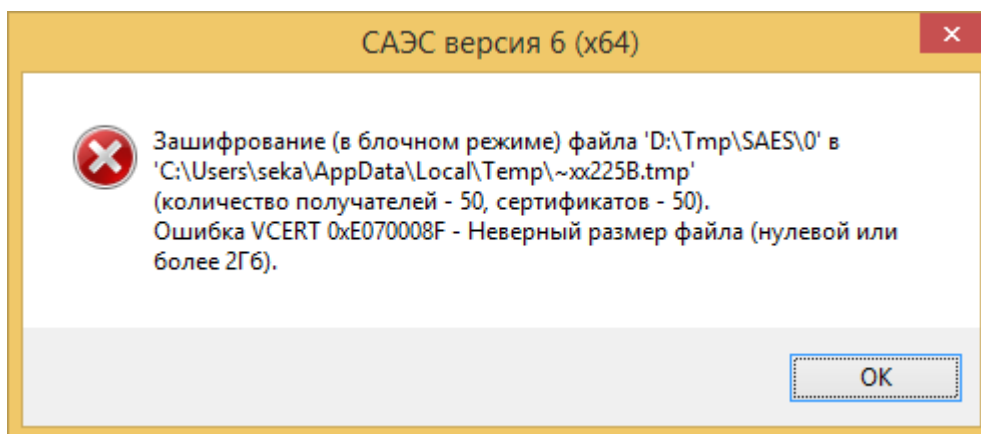


Рисунок 47 - Сообщение об ошибке при зашифровании файла

Если операция зашифрования производится с несколькими файлами, сначала на экран выдаётся запрос на зашифрование (Рисунок 48) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

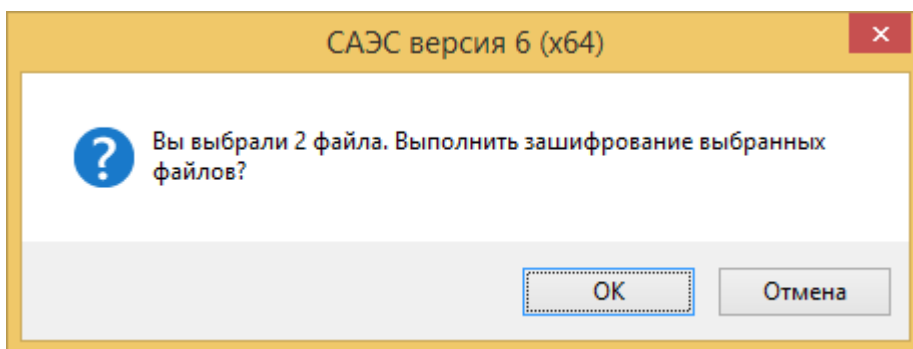


Рисунок 48 - Запрос на зашифрование

Затем на экран выдаётся диалог зашифрования файлов (Рисунок 41), а затем, после нажатия кнопки «Зашифровать», диалог результатов зашифрования (Рисунок 49).

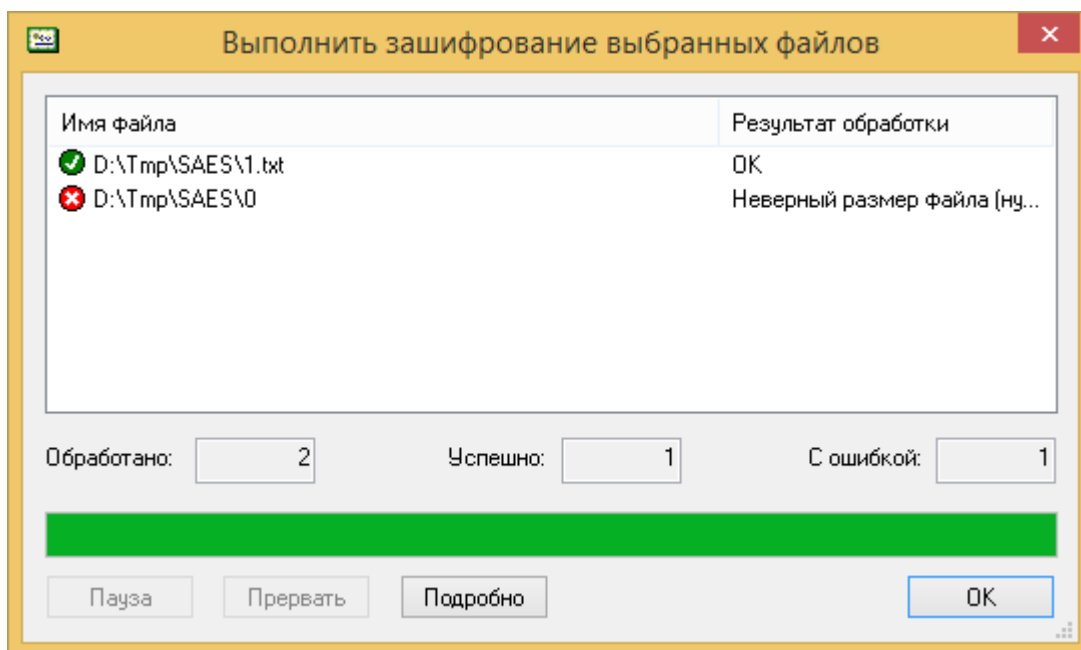


Рисунок 49 – Диалог результатов зашифрования файлов

Во второй колонке списка выводится краткая информация о результате зашифрования. Для отображения полной информации выделите строку с файлом и нажмите кнопку «Подробнее» (или сделайте двойной клик «мышью»).

В процессе обработки вы можете приостановить или прервать зашифрование нажатием кнопок «Пауза» или «Прервать».

### 6.2.2 Расшифрование

Для расшифрования выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПК САЭС пункт «Расшифровать». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. раздел 5).

Расшифрованный файл сохраняется в каталог, заданный в параметре «Каталог для сохранения проверенных/ расшифрованных файлов» в настройках пользователя (или в каталог, где находится зашифрованный файл, если этот параметр не задан). При этом если файл имеет расширение, заданное в параметре «Основные расширения имён файлов - Зашифрованные файлы» или в параметре «Дополнительные расширения имён файлов» в настройках пользователя, это расширение будет удалено. В случае когда файл не имеет такого расширения, имя файла не меняется. Если при записи расшифрованного файла оказывается, что файл с таким именем уже существует, выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках пользователя не установлен режим «Не выдавать диалог сохранения файла»). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»).

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - к пропуску операции с текущим файлом, кнопки «Отмена» - к прекращению операции со всеми оставшимися файлами.

Если операция расшифрования производится с одним файлом, после выполнения операции на экран выдаётся сообщение об успехе (Рисунок 50) или сообщение об ошибке (Рисунок 51).

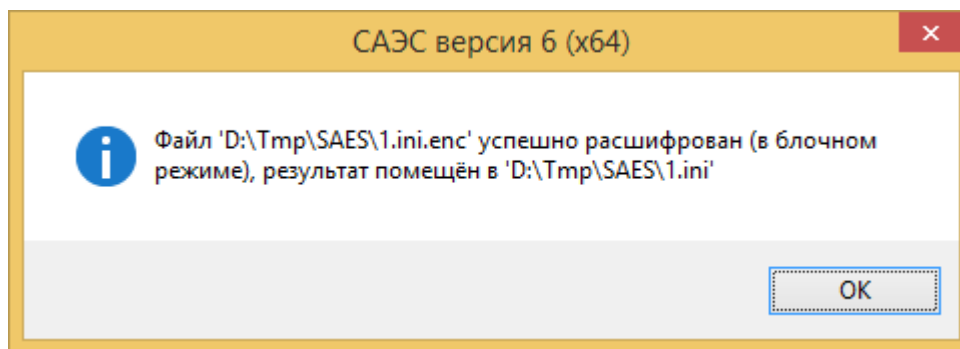


Рисунок 50 - Сообщение об успешном расшифровании файла

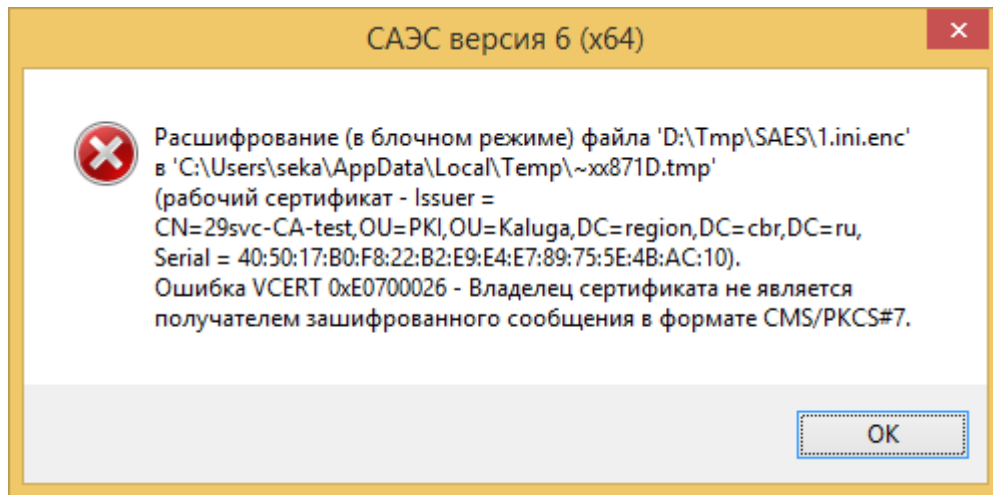


Рисунок 51 - Сообщение об ошибке при расшифровании файла

Если операция расшифрования производится с несколькими файлами, сначала на экран выдаётся запрос на расшифрование (Рисунок 52) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

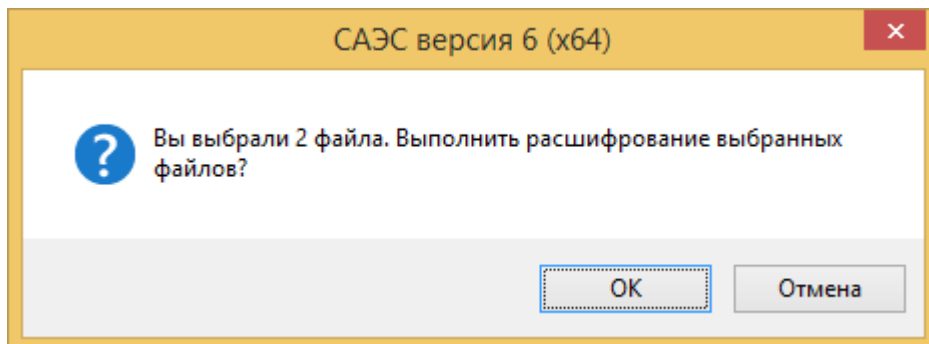


Рисунок 52 - Запрос на расшифрование

Затем на экран выдаётся диалог расшифрования файлов (Рисунок 53).

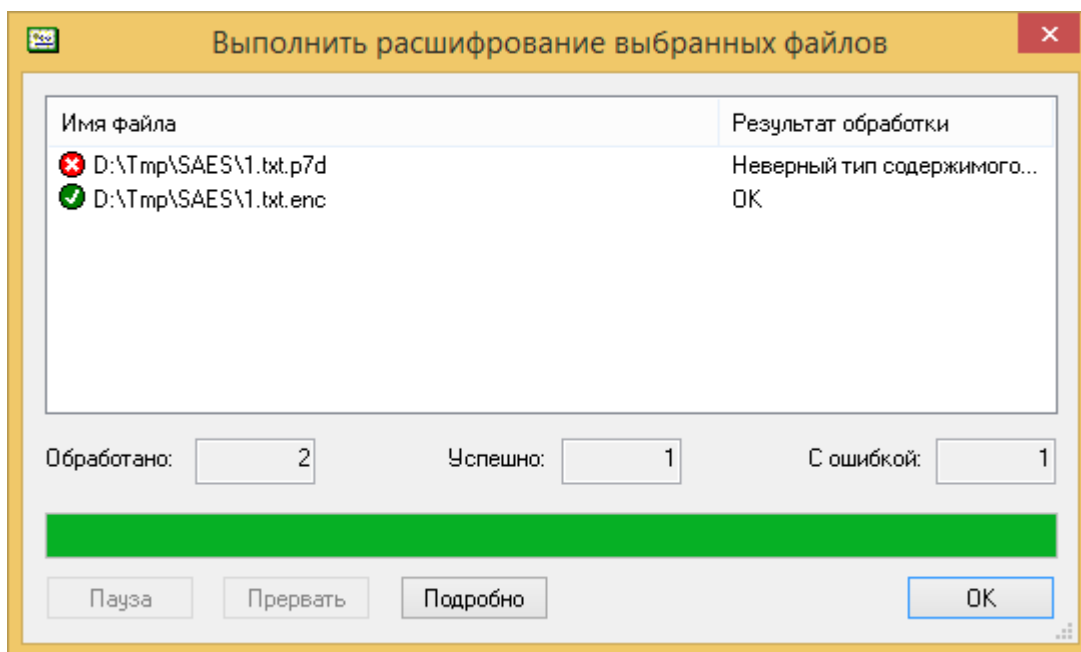


Рисунок 53 - Диалог расшифрования файлов

Во второй колонке списка выводится краткая информация о результате расшифрования. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробнее» (или сделайте двойной клик «мышью»).

В процессе обработки вы можете приостановить или прервать расшифрование нажатием кнопок «Пауза» или «Прервать».

### 6.3 Получение криптографической информации

Для того чтобы получить информацию о зашифрованных или содержащих ЭП файлах, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПК САЭС пункт «Информация о файле». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. раздел 5).

Если операция производится с одним файлом, то для зашифрованного файла на экран будет выдан диалог (Рисунок 54) с информацией о зашифрованном файле, содержащий список получателей (на кого зашифрован файл).

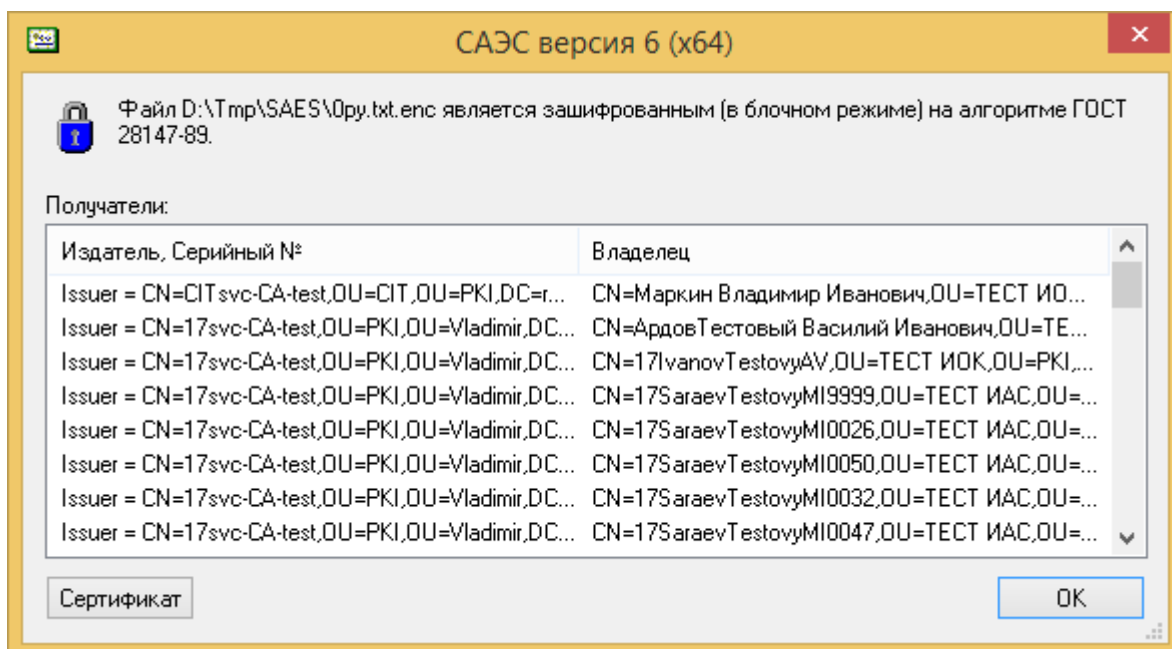


Рисунок 54 - Диалог с информацией о зашифрованном файле

Чтобы подробно посмотреть сертификат получателя, выделите его и нажмите кнопку «Сертификат» (или сделайте двойной клик «мышью»).

Для файла, содержащего ЭП, будет выдан диалог с информацией об ЭП (Рисунок 55).

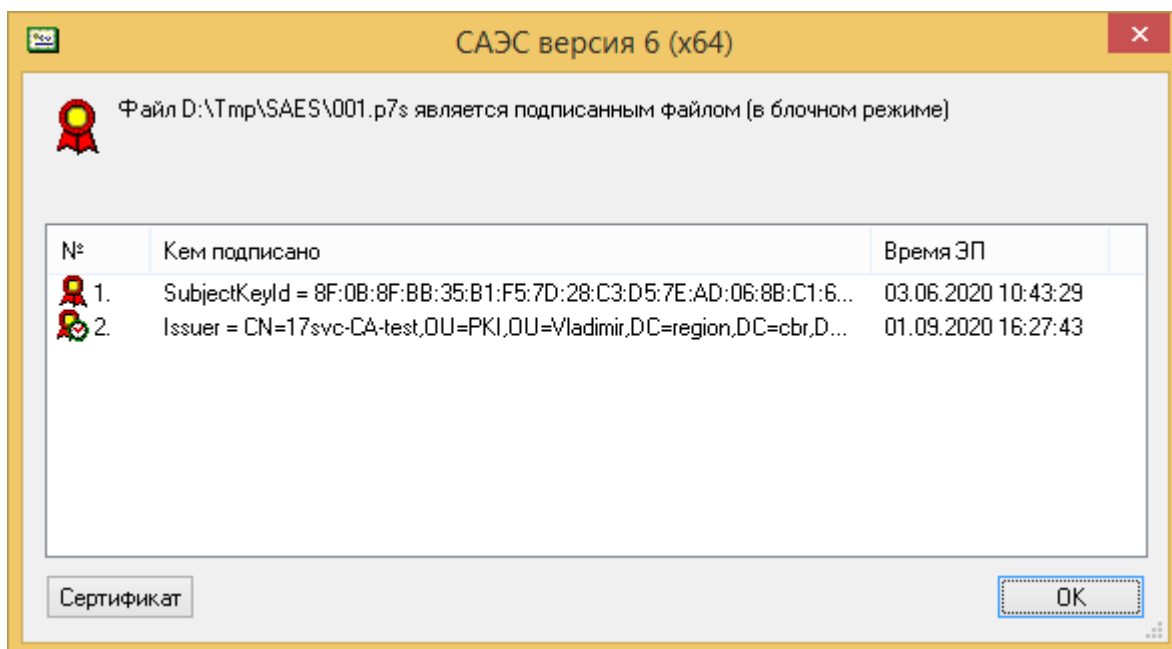




Рисунок 55 - Диалог с информацией об ЭП

В отличие от диалога с информацией о проверке подписи, здесь не отображается информация о сертификате и времени установки штампа времени, а только факт его существования: если подпись содержит штамп времени, он помечается иконкой , а если не содержит - .



Чтобы подробно просмотреть сертификат, на котором выполнена подпись, выделите его и нажмите кнопку «Сертификат» (или сделайте двойной клик «мышью»).

**ВНИМАНИЕ:** для получения информации об отсоединённой ЭП надо выбирать в Проводнике файлы отсоединённых подписей, а не файлы с подписанными данными.

Для файла, не содержащего ЭП и не зашифрованного, будет выдано сообщение (Рисунок 56).

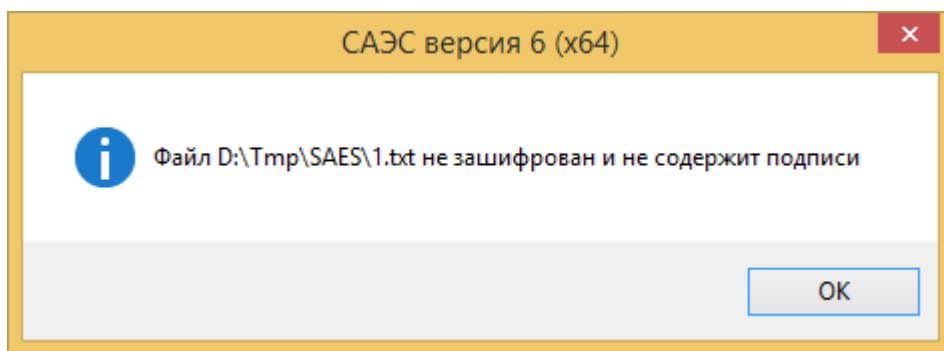


Рисунок 56 - Сообщение о незашифрованном файле, не содержащем ЭП

Если операция производится с несколькими файлами, сначала на экран выдаётся запрос на отображение криптографической информации (Рисунок 57) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

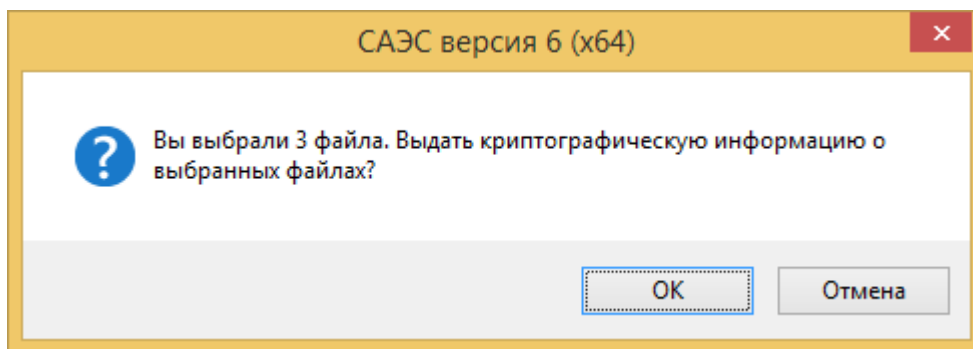


Рисунок 57 - Запрос на отображение криптографической информации о файлах

Затем на экран выдаётся диалог отображения криптографической информации о файлах (Рисунок 58).

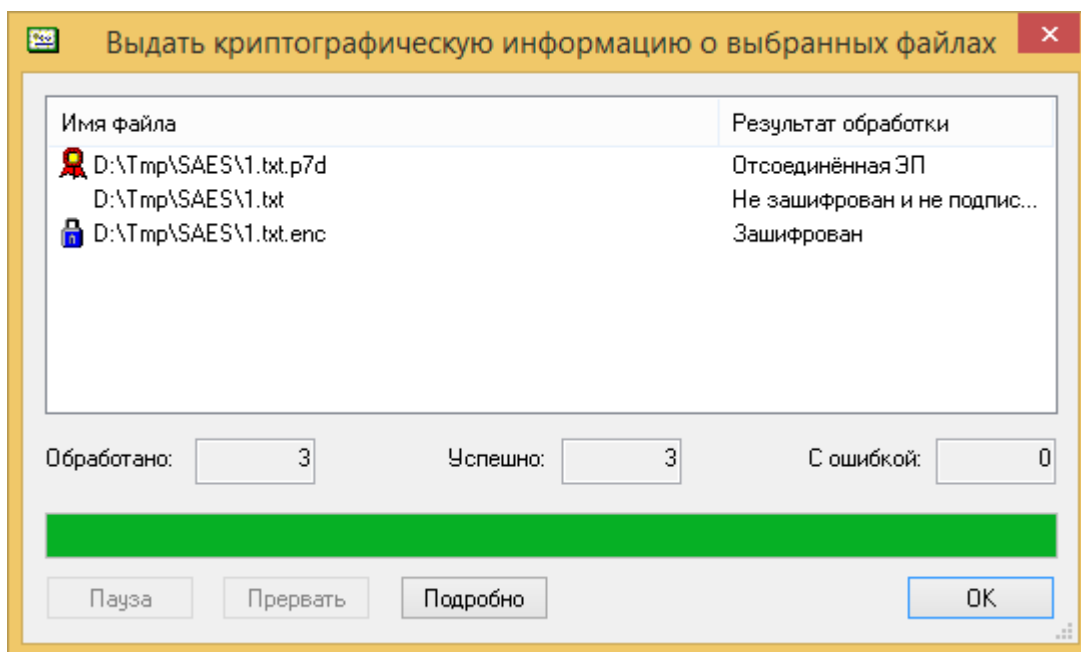


Рисунок 58 - Диалог отображения криптографической информации о файлах

Во второй колонке списка выводится краткая информация о файле. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробнее» (или сделайте двойной клик «мышью»).

В процессе обработки вы можете приостановить или прервать операцию нажатием кнопок «Пауза» или «Прервать».

#### 6.4 Просмотр статуса OCSP

Если в настройках пользователя установлен режим «Использовать OCSP сервер», то из диалога подробного просмотра сертификата (вызванного из выше описанных диалоговых окон) можно просмотреть статус отзыва цифрового сертификата (Online Certificate Status Protocol). Нажмите кнопку «ОК», на экране появится диалоговое окно со статусом отзыва (Рисунок 59) или сообщение об ошибке (Рисунок 60).

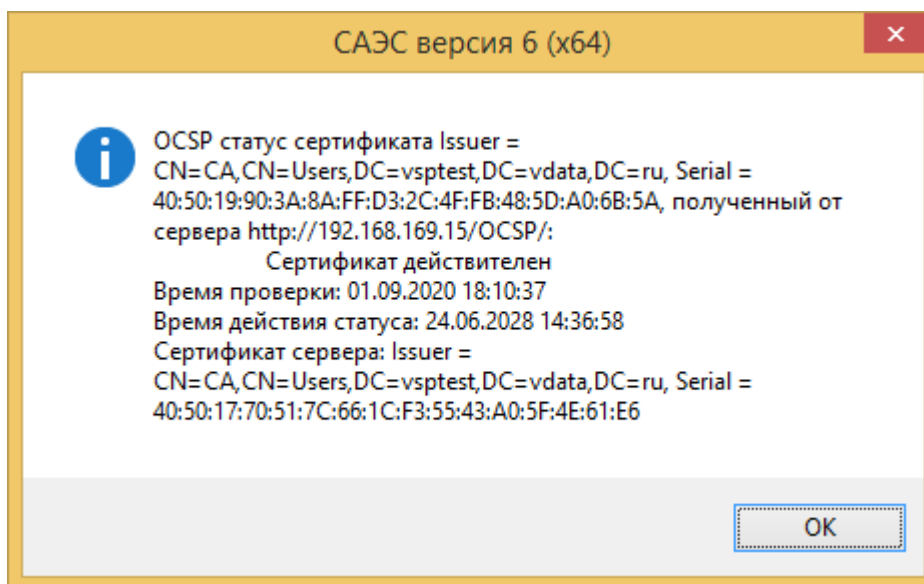


Рисунок 59 – Диалог, отображающий статус OSCP

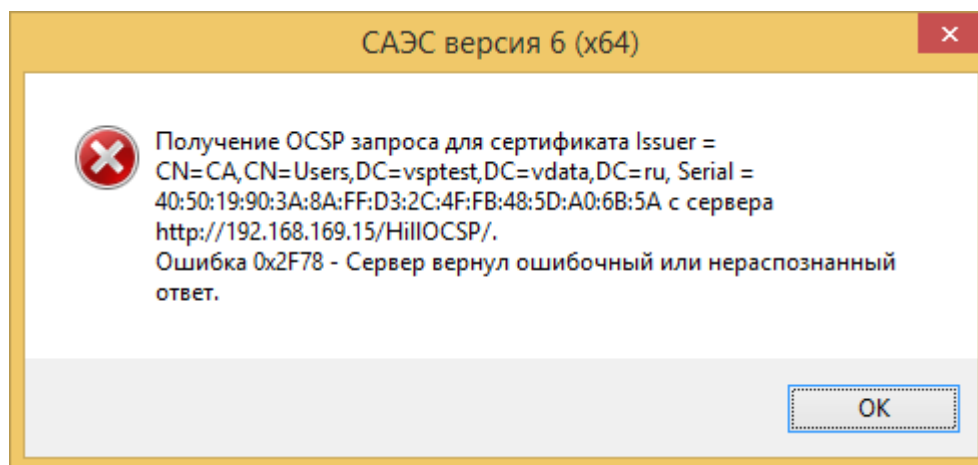


Рисунок 60 – Сообщение об ошибке при получения статуса OSCP

## 6.5 Упрощённое получение криптографической информации

Двойное нажатие (double click) мыши на файлах с расширениями \*.p7s, \*.p7d, \*.p7e и \*.enc вызывает упрощённые диалоги отображения криптографической информации (Рисунок 61 и Рисунок 62).

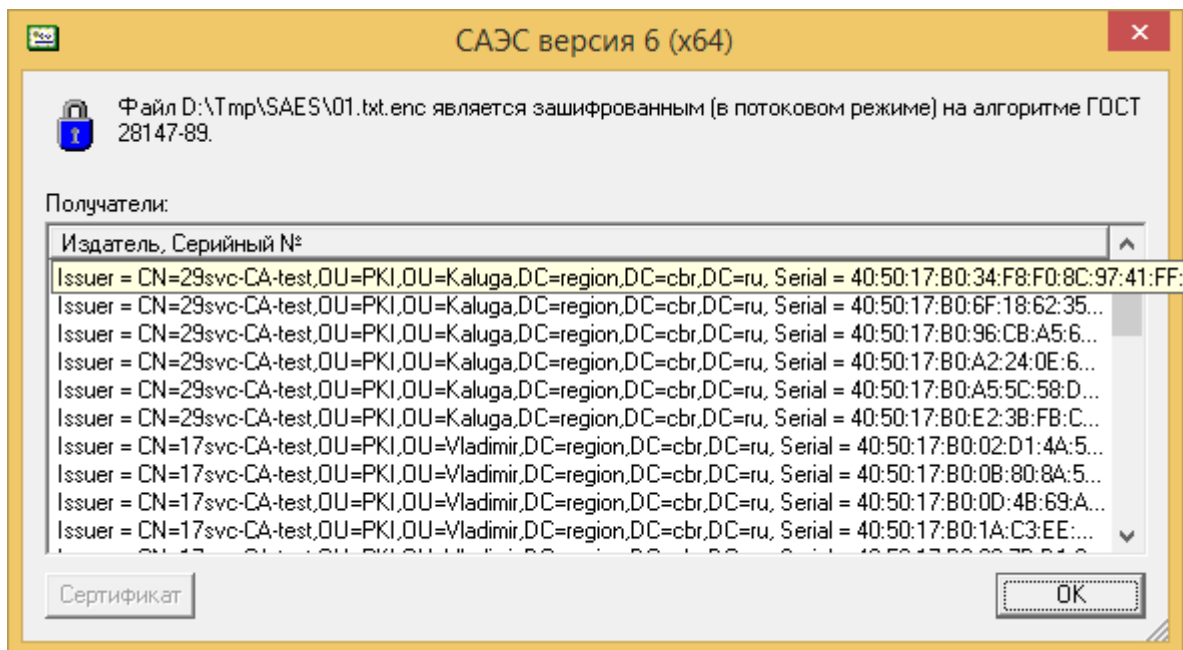


Рисунок 61 – Упрощённый диалог с информацией о зашифрованном файле

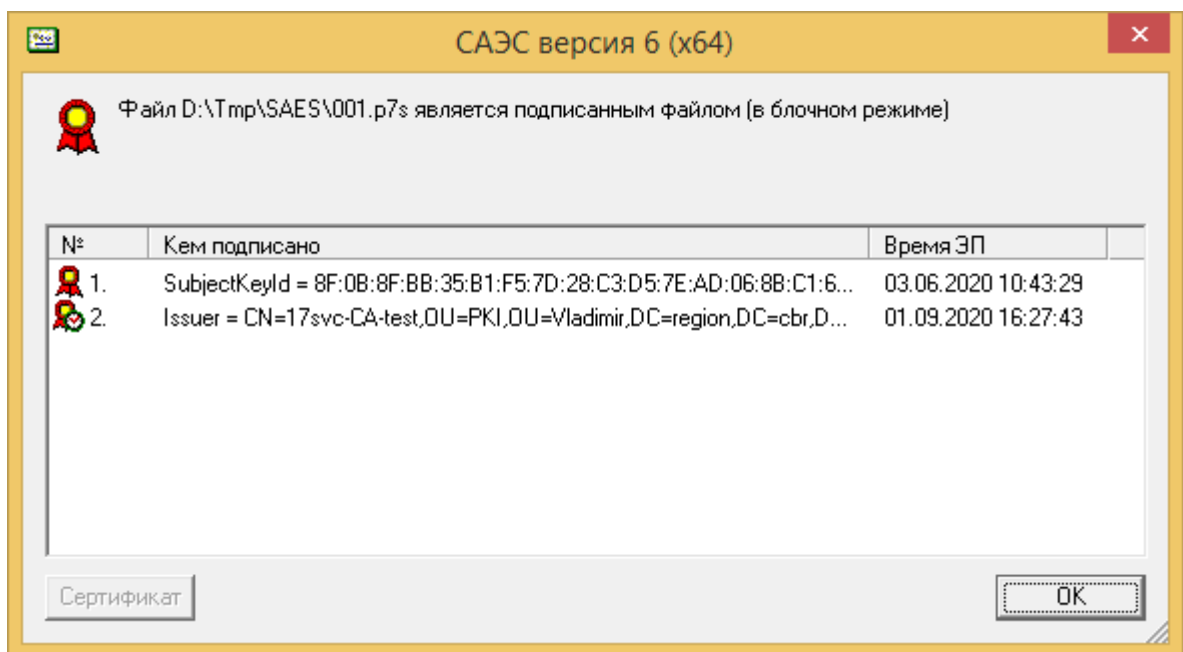


Рисунок 62 – Упрощённый диалог с информацией об ЭП

При просмотре криптографической информации через упрощённые диалоги не происходит загрузки криптографического профиля и ключа, поэтому просмотр сертификата (и имени владельца) невозможен.

**ВНИМАНИЕ:** при изменении расширений имён файла в настройках ПК САС набор расширений файлов, для которых возможно упрощённое получение криптографической информации не изменяется.

## 7 ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИИ

### 7.1 Закодирование в формат Base64

Для того чтобы закодировать в формат Base64, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПК САЭС пункт «Дополнительно», подпункт «Закодировать в Base64». Для выполнения этой операции загрузка ключа не требуется.

Файл, полученный в результате закодирования в формат Base64, сохраняется в каталог, где находится кодируемый файл. При этом к имени файла добавляется расширение, заданное в параметре «Основные расширения имён файлов - Файлы в кодировке Base64» в настройках пользователя. В случае, когда файл уже имеет такое расширение, второй раз оно не добавляется.

Если операция закодирования в формат Base64 производится с одним файлом, на экран выдаётся сообщение об успехе (Рисунок 63) или сообщение об ошибке.

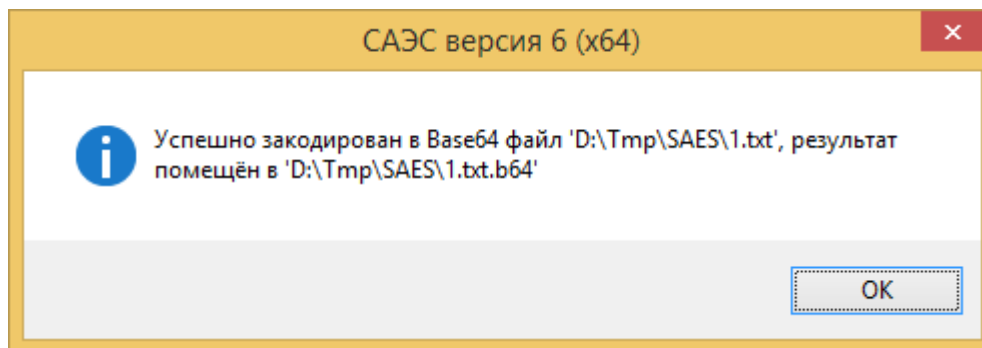


Рисунок 63 - Сообщение об успешном кодировании файла в Base64

Если операция закодирования в формат Base64 производится с несколькими файлами, сначала на экран выдаётся запрос на закодирование (Рисунок 64) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

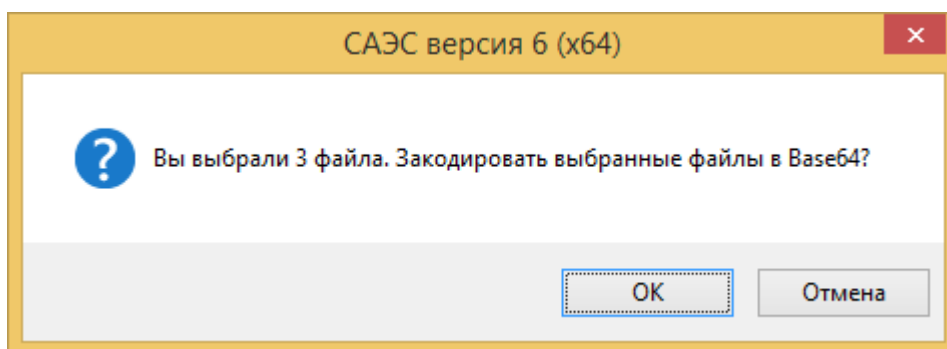


Рисунок 64 - Запрос на закодирование в формат Base64

Затем на экран выдаётся диалог закодирования в формат Base64 (Рисунок 65).

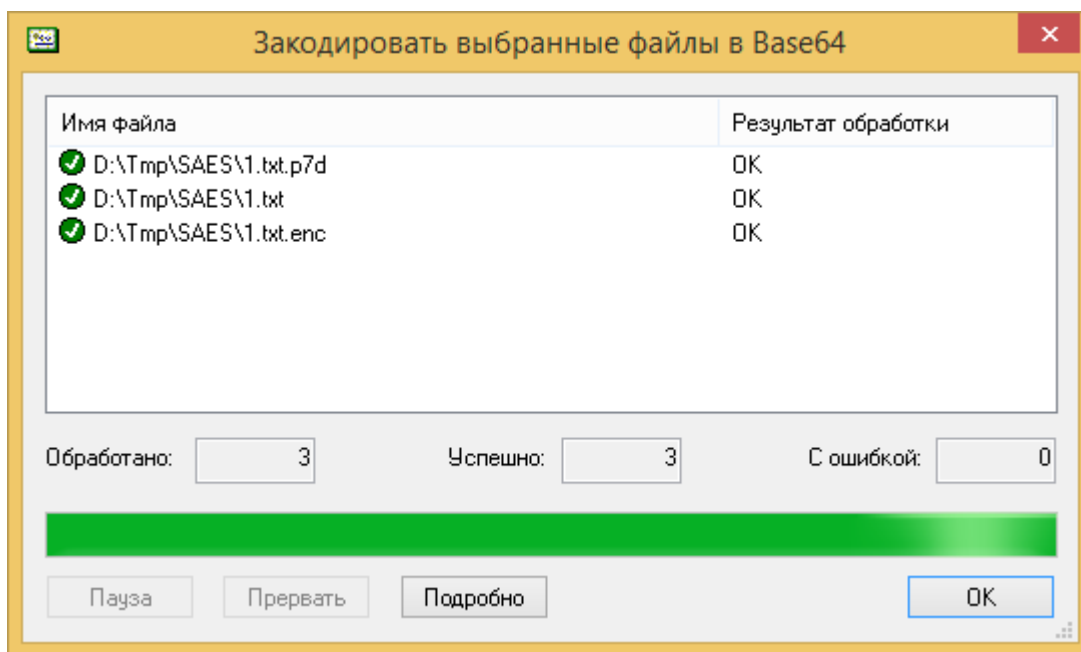


Рисунок 65 - Диалог закодирования в формат Base64

Во второй колонке списка выводится краткая информация о результате операции. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробнее» (или сделайте двойной клик «мышью»).

В процессе обработки вы можете приостановить или прервать выполнение операции нажатием кнопок «Пауза» или «Прервать».

## 7.2 Раскодирование из формата Base64

Для того чтобы раскодировать из формата Base64, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПК САЭС пункт «Дополнительно», подпункт «Раскодировать из Base64». Для выполнения этой операции загрузка ключа не требуется.

Файл, полученный в результате раскодирования из формата Base64, сохраняется в каталог, где находится закодированный файл. При этом если в параметре «Основные расширения имён файлов - Файлы в кодировке Base64» задано расширение, оно добавляется к имени файла. В случае, когда такое расширение не задано, имя файла не меняется.

Если при записи раскодированного файла оказывается, что файл с таким именем уже существует, выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках пользователя не установлен режим «Не выдавать диалог сохранения файла»). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»).

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - к пропуску операции с текущим файлом, кнопки «Отмена» - к прекращению операции со всеми оставшимися файлами.

Если операция раскодирования из формата Base64 производится с одним файлом, после неё на экран выдаётся сообщение об успехе или сообщение об ошибке (Рисунок 66, Рисунок 67).

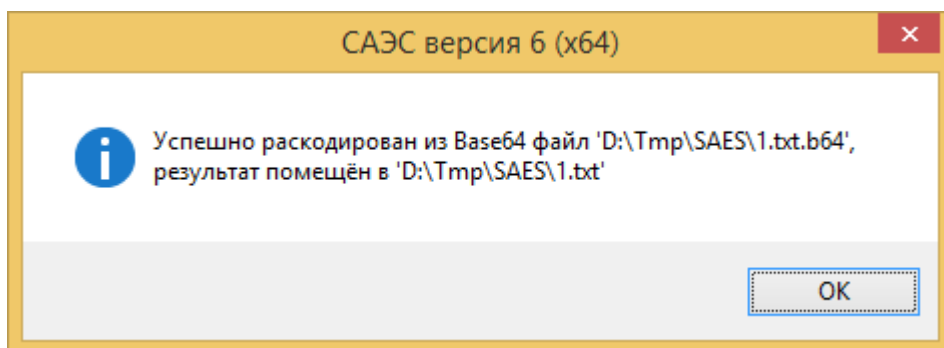


Рисунок 66 - Сообщение об успешном раскодировании файла из Base64

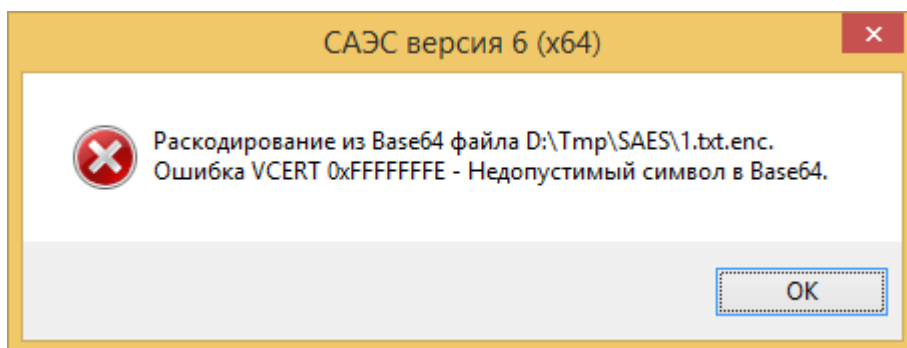


Рисунок 67 - Сообщение об ошибке при раскодировании файла из Base64

Если операция раскодирования из формата Base64 производится с несколькими файлами, сначала на экран выдаётся запрос на раскодирование (Рисунок 68) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

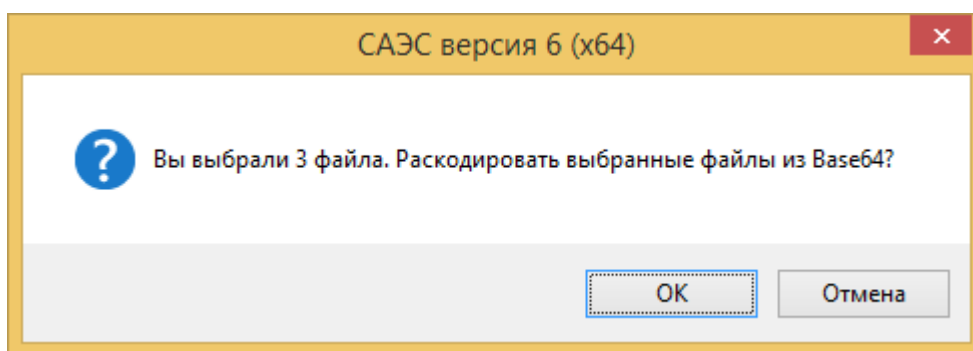


Рисунок 68 - Запрос на раскодирование из формата Base64

Затем на экран выдаётся диалог раскодирования из формата Base64 (Рисунок 69).

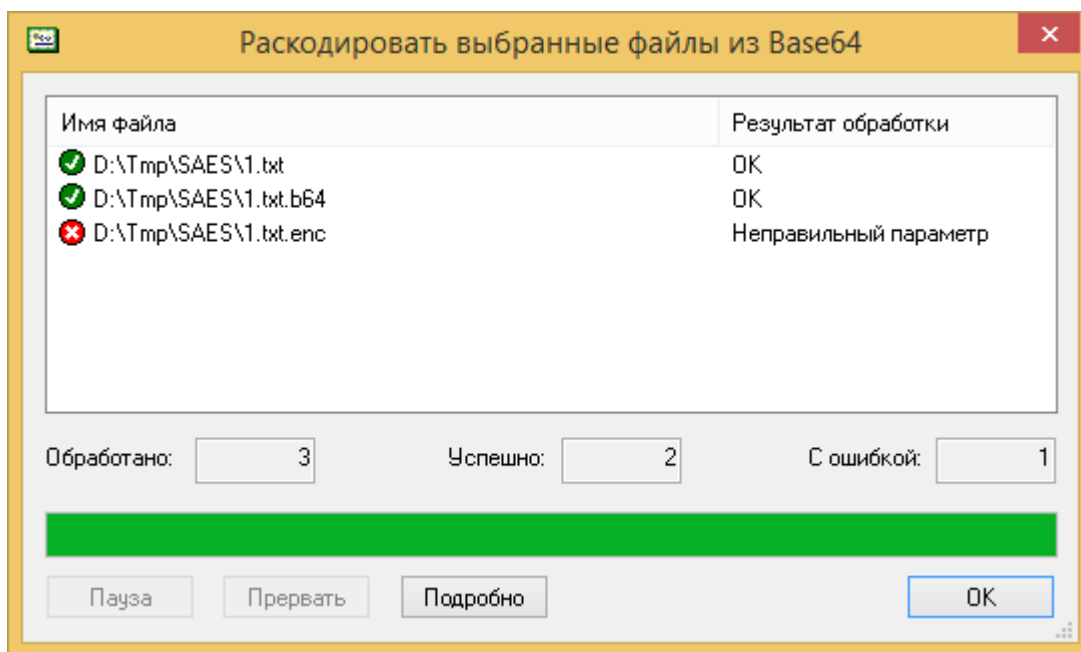


Рисунок 69 - Диалог раскодирования из формата Base64

Во второй колонке списка выводится краткая информация о результате операции. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробно» (или сделайте двойной клик «мышью»).

В процессе обработки вы можете приостановить или прервать выполнение операции нажатием кнопок «Пауза» или «Прервать».

### 7.3 Хэширование файлов

Для того чтобы вычислить хэш по ГОСТ 34.11-2012 (256 бит), выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПК САЭС пункт «Дополнительно», подпункт «Вычислить хэш (2012)». Для выполнения этой операции загрузка ключа не требуется.

Если операция хэширования производится с одним файлом, на экран выдаётся диалоговое окно с результатом (Рисунок 70) или сообщение об ошибке.





Рисунок 70 - Диалог с результатом хэширования

Хэш представлен в трёх форматах. Формат № 1 является простым побайтовым шестнадцатеричным представлением. Формат № 2 отличается от него только порядком полубайт (нибблов) в байте и отображается для совместимости с другими средствами хэширования. Формат № 3 отличается от Формата № 1 обратным порядком байт и соответствует требованиям ГОСТ 34.11-2012 «Информационные технологии. Криптографическая защита информации. Функция хэширования».

Для сохранения вычисленного значения хэша в файл нажмите кнопку «Сохранить» и укажите имя файла в стандартном диалоге сохранения.

Если операция хэширования производится с несколькими файлами, сначала на экран выдаётся запрос на хэширование (Рисунок 71) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

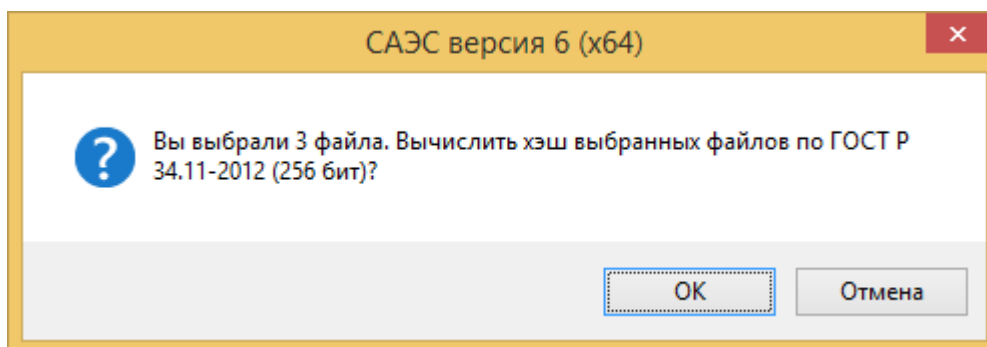


Рисунок 71 - Запрос на хэширование

Затем на экран выдаётся диалог вычисления хэша (Рисунок 72).

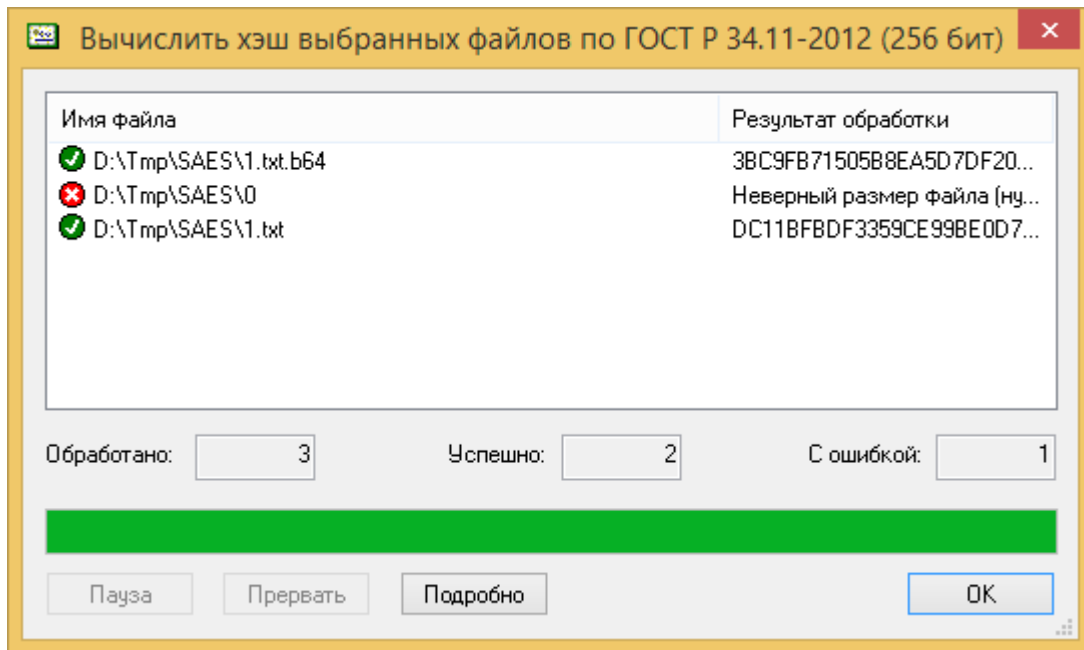


Рисунок 72 - Диалог вычисления хэша

Во второй колонке списка выводится результат операции. Для отображения полной информации выделите строку с файлом и нажмите кнопку «Подробнее» (или сделайте двойной клик «мышью»).

В процессе обработки вы можете приостановить или прервать выполнение операции нажатием кнопок «Пауза» или «Прервать».

## 8 ПРОТОКОЛИРОВАНИЕ В ПК САЭС

В случае если в настройках пользователя не включён режим «Отключить протокол выполненных операций», ПК САЭС протоколирует в журнал приложений (Event Log) Windows все криптографические операции и все ошибки, возникшие в процессе их выполнения. В качестве кода события всегда указывается «1», источника события – «SPKISHXX», а категория отсутствует. В описании события указывается программный модуль (spkishxx.dll), идентификаторы процесса и потока и текстовое описание события или ошибки, совпадающее с сообщениями, выдаваемыми в экранных диалогах (однако длинные сообщения обрезаются до длины 16 Кбайт). В случае если в настройках включён режим «Расширенная диагностика криптографических ошибок (стек)», текстовое описание может содержать стек ошибок (Рисунок 73, Рисунок 74).

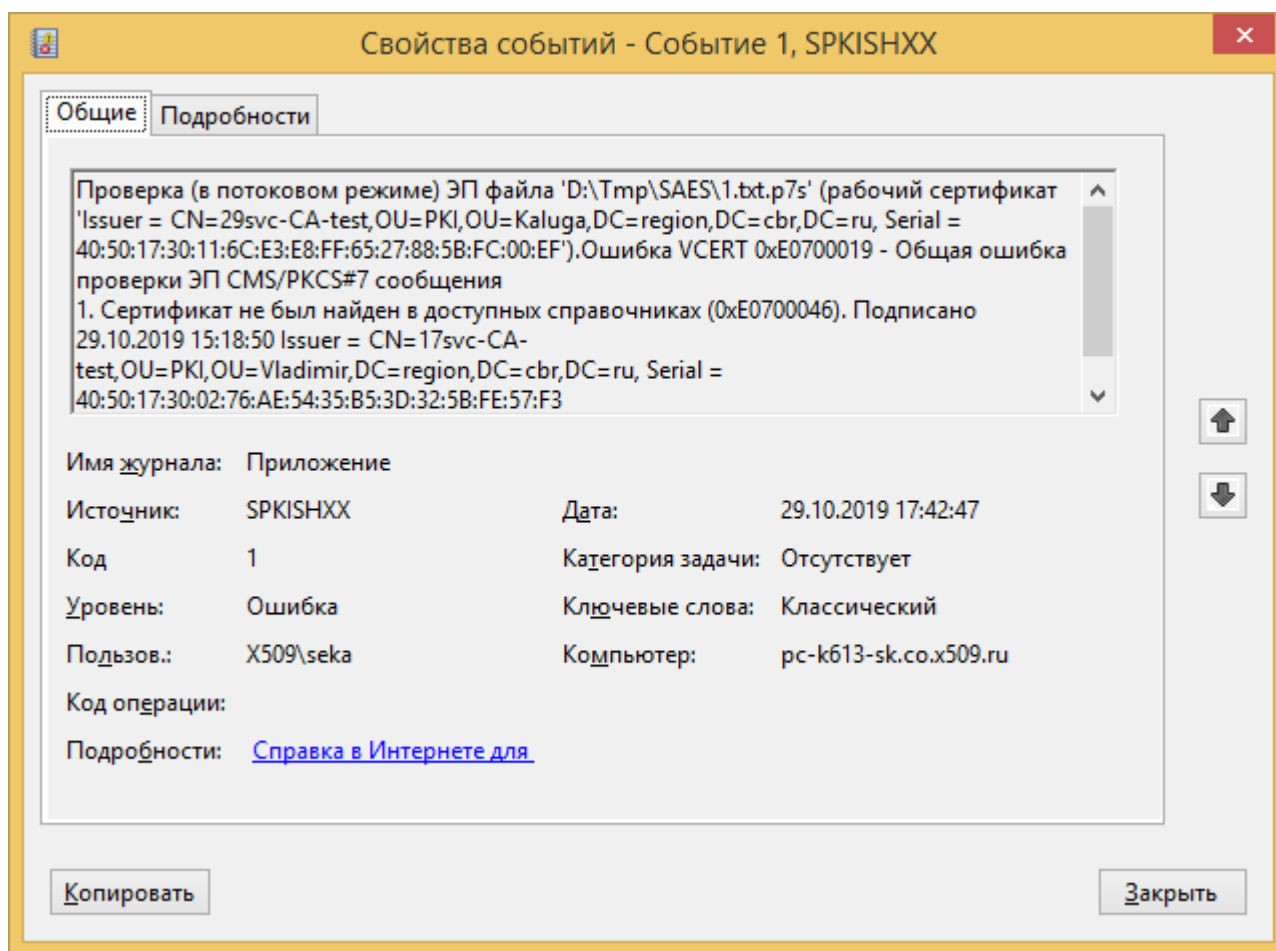


Рисунок 73 - Описание ошибки проверки подписи без стека ошибок

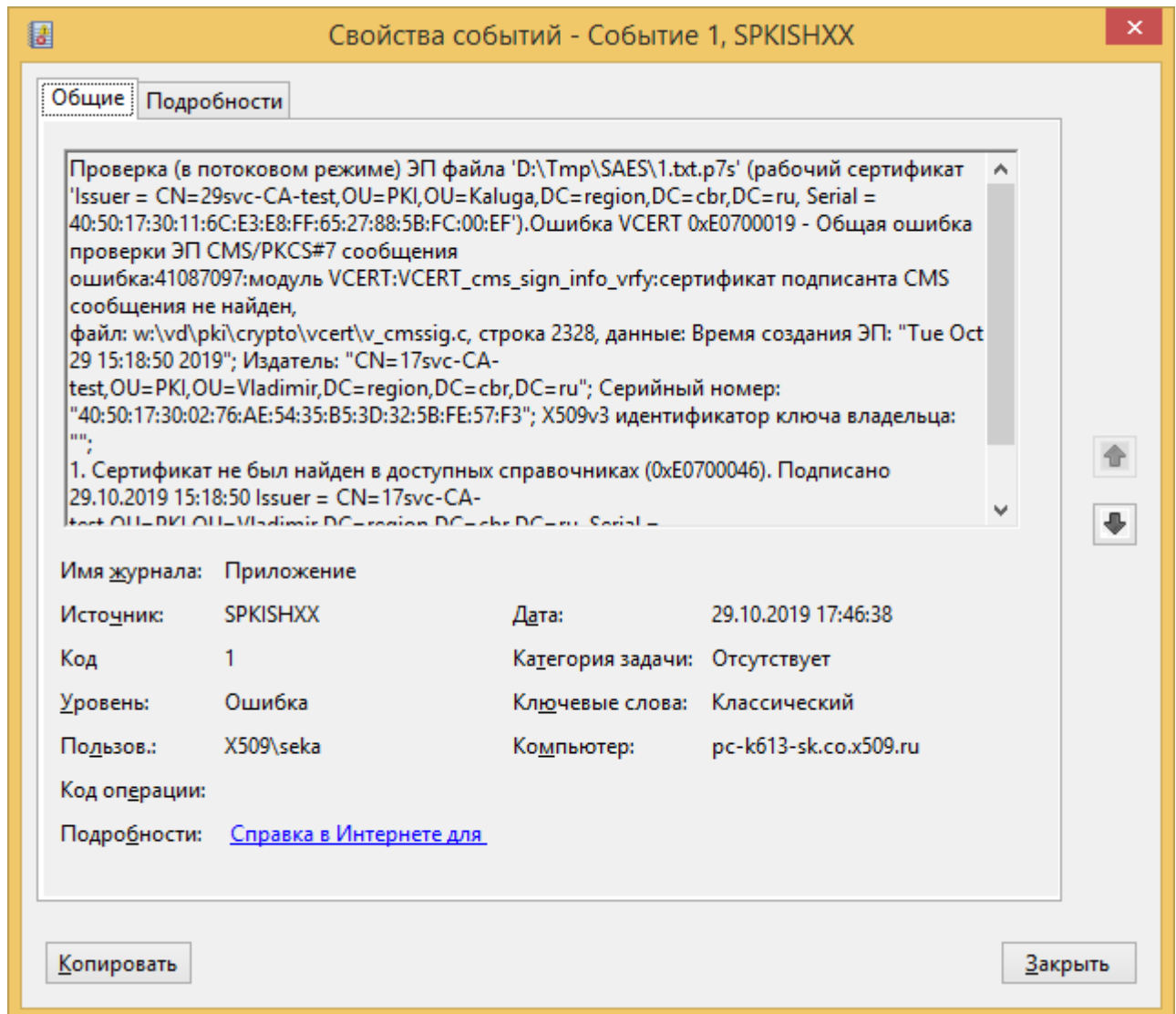


Рисунок 74 - Описание ошибки проверки подписи со стеком ошибок

## ПЕРЕЧЕНЬ РИСУНКОВ

|   |    |
|---|----|
| Рисунок 1 - Главное меню ПК САЭС .....  | 7  |
| Рисунок 2 - Общие настройки ПК САЭС .....   | 9  |
| Рисунок 3 - Настройки безопасности ПК САЭС.....                                       | 11 |
| Рисунок 4 - Дополнительные настройки ПК САЭС .....                                    | 14 |
| Рисунок 5 - Диалог добавления дополнительного расширения .....                        | 15 |
| Рисунок 6. Выбор пункта меню «О программе...».....                                    | 16 |
| Рисунок 7. Диалог с информацией о версии программы .....                              | 16 |
| Рисунок 8 - Запрос на создание ЭП.....  | 19 |
| Рисунок 9 - Диалог создания ЭП файлов.....  | 19 |
| Рисунок 10 - Полная информация о создании ЭП .....                                    | 20 |
| Рисунок 11 - Диалог с информацией о проверке ЭП.....                                  | 20 |
| Рисунок 12 - Диалог просмотра сертификата.....  | 21 |
| Рисунок 13 - Диалог с информацией об ошибке при проверке ЭП.....                      | 22 |
| Рисунок 14 - Диалог с информацией о проверке ЭП со штампом времени .....              | 22 |
| Рисунок 15 - Диалог с информацией о проверке ЭП с отсутствующим штампом времени ..... | 23 |
| Рисунок 16 - Запрос на проверку ЭП .....  | 23 |
| Рисунок 17 - Диалог проверки ЭП файлов .....  | 24 |
| Рисунок 18 - Диалог удаления ЭП.....  | 25 |
| Рисунок 19 - Диалог с информацией об удалении и проверке ЭП.....                      | 26 |
| Рисунок 20 - Диалог проверки и удаления ЭП файлов .....                               | 27 |
| Рисунок 21 - Запрос на удаление ЭП .....  | 28 |
| Рисунок 22 - Диалог удаления ЭП.....  | 28 |
| Рисунок 23 - Сообщение об успешном создании отсоединённой ЭП.....                     | 30 |
| Рисунок 24 - Сообщение об ошибке при создании отсоединённой ЭП.....                   | 30 |
| Рисунок 25 - Запрос на создание отсоединённой ЭП .....                                | 31 |
| Рисунок 26 - Диалог создания отсоединённой ЭП файлов .....                            | 31 |
| Рисунок 27 - Сообщение о конфликте имён при проверке отсоединённой ЭП .....           | 32 |
| Рисунок 28 - Диалог с информацией о проверке отсоединённой ЭП .....                   | 33 |
| Рисунок 29 - Диалог просмотра сертификата.....  | 34 |
| Рисунок 30 - Запрос на проверку отсоединённой ЭП.....                                 | 35 |
| Рисунок 31 - Диалог проверки отсоединённой ЭП файлов.....                             | 35 |
| Рисунок 32 - Пустой диалог выбора получателей .....                                   | 36 |
| Рисунок 33 - Диалог формирования групп получателей.....                               | 37 |
| Рисунок 34 - Список получателей из Справочника сертификатов.....                      | 37 |
| Рисунок 35 - Диалог поиска в списке.....  | 38 |
| Рисунок 36 - Шаблон для поиска в списке .....   | 38 |
| Рисунок 37 - Результат поиска в списке .....  | 39 |
| Рисунок 38 - Шаблон для поиска в ЕСК.....   | 39 |
| Рисунок 39 - Результат поиска в ЕСК.....  | 40 |
| Рисунок 40 - Диалог выбора получателей со списком из безымянной группы .....          | 41 |

|  |    |
|--|----|
| Рисунок 41 - Диалог со списком из группы "all" .....   | 41 |
| Рисунок 42 - Процесс поиска сертификатов получателей .....   | 42 |
| Рисунок 43 - Предупреждение об отсутствии сертификатов у получателя.....                           | 42 |
| Рисунок 44 - Предупреждение о том, что файл уже зашифрован (при шифровании одного файла).....      | 43 |
| Рисунок 45 - Предупреждение о том, что файл уже зашифрован (при шифровании нескольких файлов)..... | 43 |
| Рисунок 46 - Сообщение об успешном зашифровании файла.....   | 44 |
| Рисунок 47 - Сообщение об ошибке при зашифровании файла .....                                      | 44 |
| Рисунок 48 - Запрос на зашифрование.....   | 45 |
| Рисунок 49 – Диалог результатов зашифрования файлов.....   | 45 |
| Рисунок 50 - Сообщение об успешном расшифровании файла.....  | 46 |
| Рисунок 51 - Сообщение об ошибке при расшифровании файла .....                                     | 47 |
| Рисунок 52 - Запрос на расшифрование .....   | 47 |
| Рисунок 53 - Диалог расшифрования файлов .....   | 48 |
| Рисунок 54 - Диалог с информацией о зашифрованном файле .....                                      | 49 |
| Рисунок 55 - Диалог с информацией об ЭП .....  | 49 |
| Рисунок 56 - Сообщение о незашифрованном файле, не содержащем ЭП .....                             | 50 |
| Рисунок 57 - Запрос на отображение криптографической информации о файлах .....                     | 50 |
| Рисунок 58 - Диалог отображения криптографической информации о файлах .....                        | 51 |
| Рисунок 59 – Диалог, отображающий статус OCSP .....  | 52 |
| Рисунок 60 – Сообщение об ошибке при получения статуса OCSP .....                                  | 52 |
| Рисунок 61 – Упрощённый диалог с информацией о зашифрованном файле .....                           | 53 |
| Рисунок 62 – Упрощённый диалог с информацией об ЭП .....   | 53 |
| Рисунок 63 - Сообщение об успешном кодировании файла в Base64 .....                                | 54 |
| Рисунок 64 - Запрос на закодирование в формат Base64 .....   | 54 |
| Рисунок 65 - Диалог закодирования в формат Base64 .....  | 55 |
| Рисунок 66 - Сообщение об успешном раскодировании файла из Base64.....                             | 56 |
| Рисунок 67 - Сообщение об ошибке при раскодировании файла из Base64 .....                          | 56 |
| Рисунок 68 - Запрос на раскодирование из формата Base64.....                                       | 56 |
| Рисунок 69 - Диалог раскодирования из формата Base64.....  | 57 |
| Рисунок 70 - Диалог с результатом хэширования.....   | 58 |
| Рисунок 71 - Запрос на хэширование .....   | 58 |
| Рисунок 72 - Диалог вычисления хэша .....  | 59 |
| Рисунок 73 - Описание ошибки проверки подписи без стека ошибок.....                                | 60 |
| Рисунок 74 - Описание ошибки проверки подписи со стеком ошибок .....                               | 61 |

[illegible][illegible]