ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00077-06–ЛУ

«ВАЛИДАТА КЛИЕНТ» ВЕРСИЯ 4

РАСШИРЕНИЕ ПРОВОДНИКА

Руководство пользователя

ВАМБ.00077-06 92 07

2020

Аннотация

Настоящий документ содержит описание программного модуля «Расширение проводника» (далее — Расширение проводника) для операционной системы (ОС) Windows.

Документ предназначен для пользователей программного комплекса (ПК) ВАМБ.00077-06 «“Вадидата Клиент” версия 4» как руководство по эксплуатации Расширения проводника.

Содержание

1 РАСШИРЕНИЕ ПРОВОДНИКА

Расширение проводника — это программный модуль, встраивающийся в контекстное меню Проводника и позволяющий выполнять криптографические операции с группами файлов и каталогами. Для работы Расширения проводника требуется установленный и настроенный ПК «Справочник сертификатов».

Примечание — Операции “Зашифровать”, “Расшифровать”, “Создать ЭП”, “Проверить ЭП”, “Создать отсоединённую ЭП”, “Проверить отсоединённую ЭП”, “Проверить и удалить ЭП” и “Вычислить хэш (2012)” в Расширении проводника могут выполняться блочными или потоковыми функциями средства криптографической защиты информации (далее — СКЗИ), в зависимости от настроек Расширении проводника.

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.

При выполнении этих операций потоковыми функциями СКЗИ ограничения на размер файлов отсутствуют.

1.1 Запуск Расширения проводника

Для запуска Расширения проводника запустите Проводник, выберите один или несколько файлов или каталогов и откройте контекстное меню (нажатием правой кнопки мыши). Выберите в контекстном меню пункт «Расширение проводника» — откроется главное меню Расширения проводника (Рисунок 1).

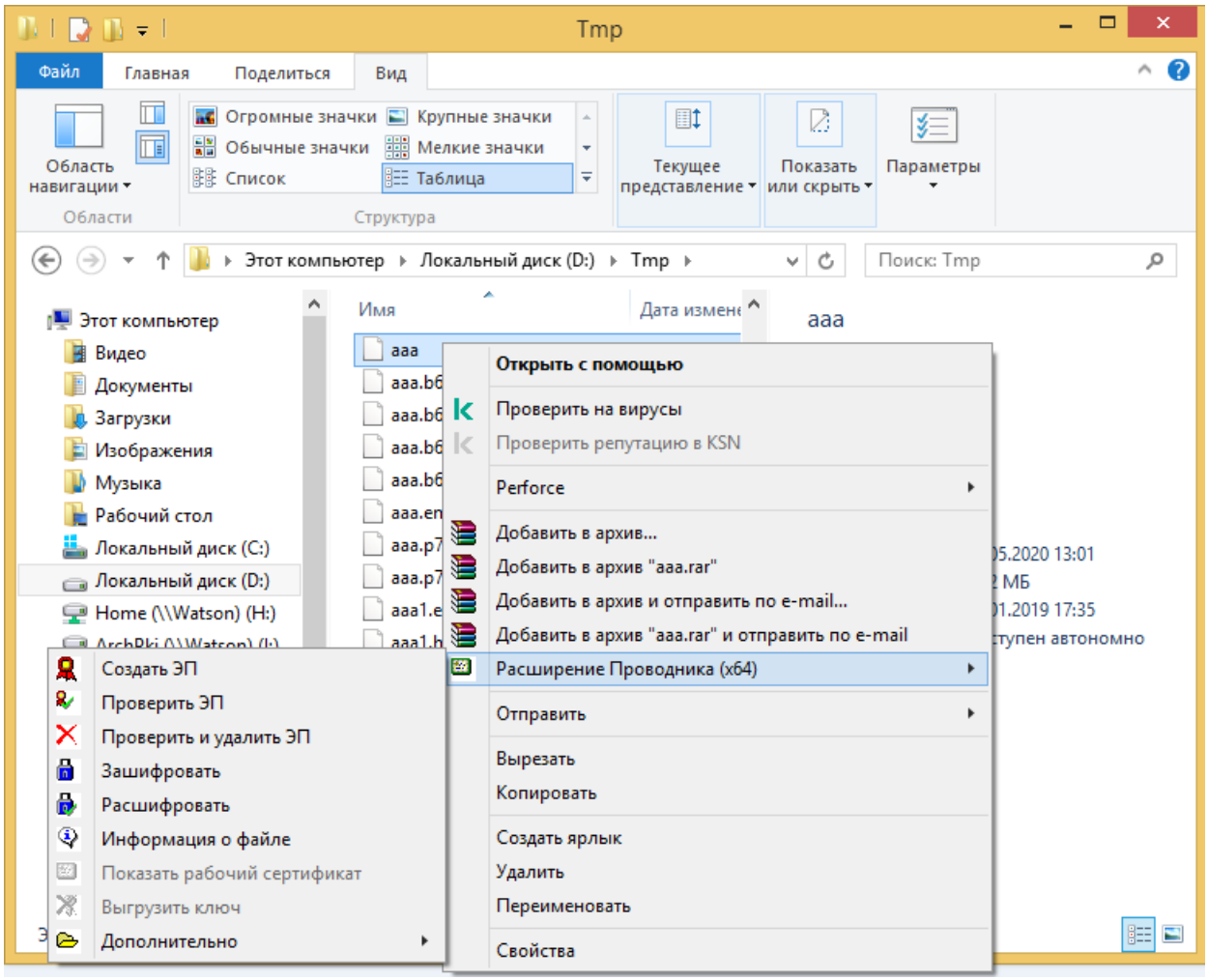

Рисунок 1 – Главное меню Расширения проводника

Большинство операций, выполняемых Расширением проводника, 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 Расширения проводника 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 Расширением проводника, — «Показать рабочий сертификат», «Выгрузить ключ» и «Настройки пользователя» — выполняется вне зависимости от того, какие файлы выбраны в Проводнике.

1.2 Настройка Расширения проводника

Для настройки параметров Расширения проводника 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.

1.2.1 Общие настройки Расширения проводника

Общие настройки Расширения проводника (Рисунок 2) перечислены ниже (Таблица 1).

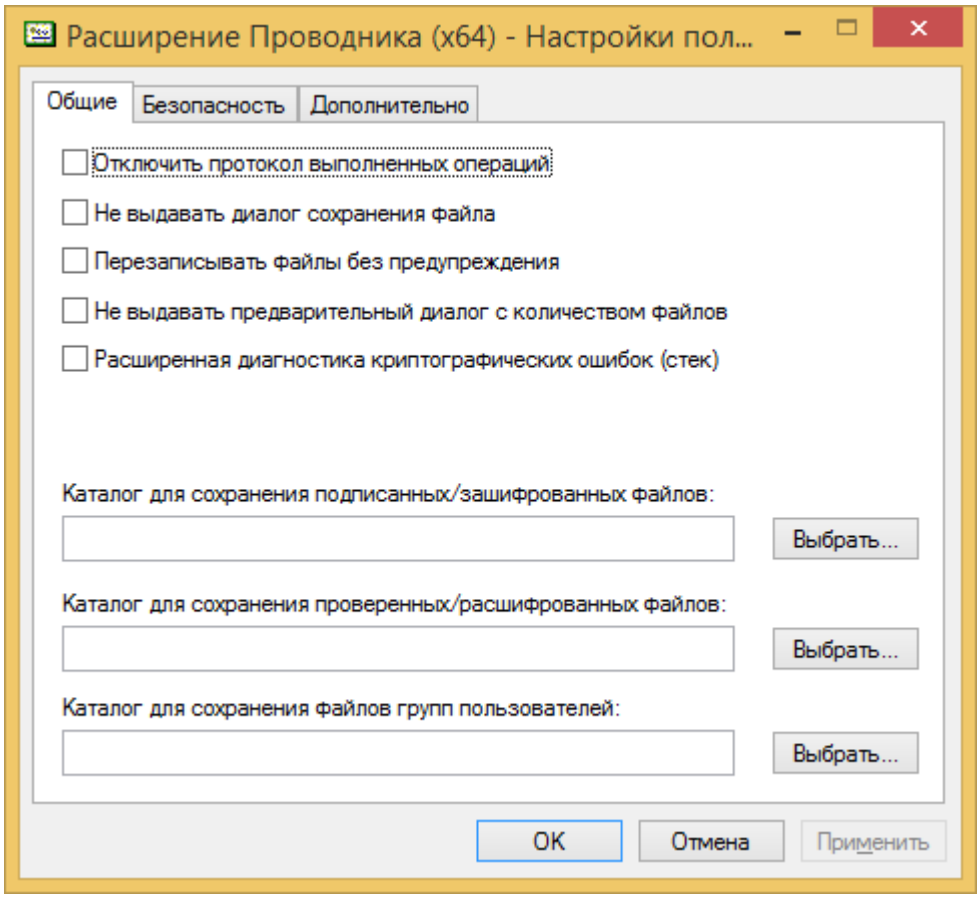

Рисунок 2 – Общие настройки Расширения проводника

Таблица 1 – Общие настройки Расширения проводника

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

Название параметра	Описание	Значение по умолчанию (после установки)
Расширенная диагностика криптографических ошибок (стек)	Добавляет к сообщению об ошибке криптографических функций содержимое стека ошибок	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	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	Не задан (пусто)
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)

1.2.2 Настройки безопасности Расширения проводника

Настройки безопасности Расширения проводника (Рисунок 3) приведены ниже (Таблица 2).

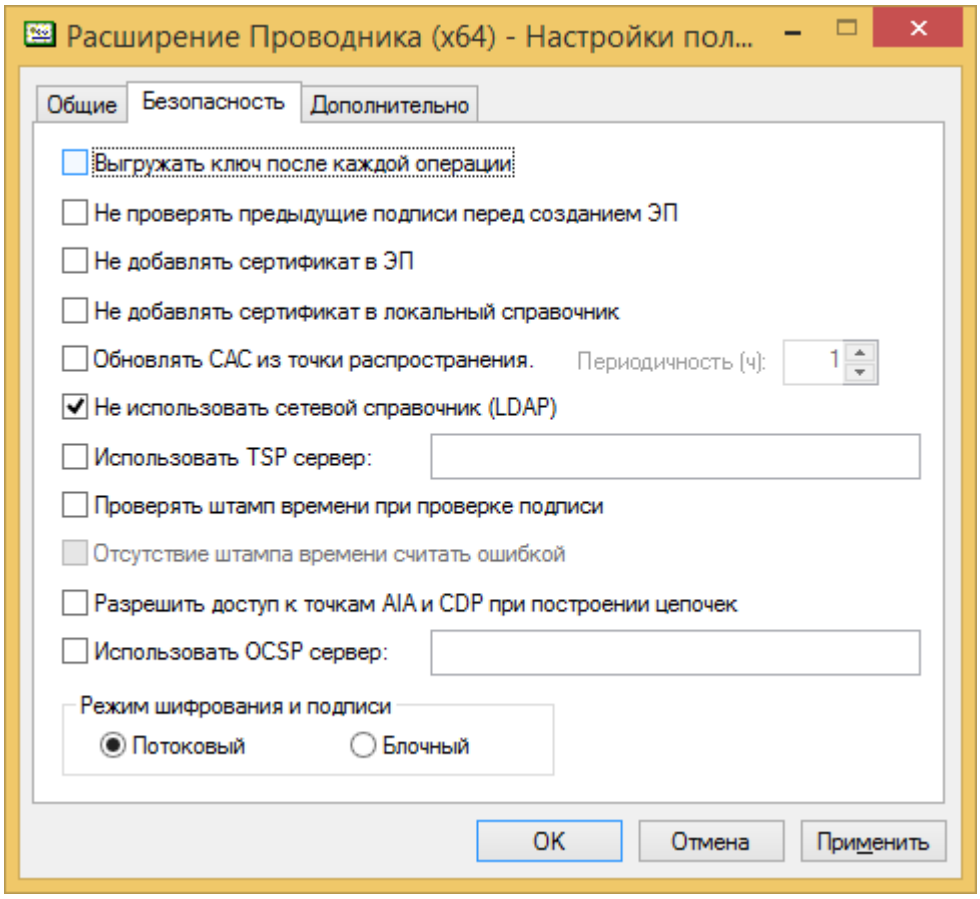

Рисунок 3 – Настройки безопасности Расширения проводника

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

Таблица 2 – Настройки безопасности Расширения проводника

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 электронных подписей (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 в базу сертификатов Справочника сертификатов. Рекомендуется включать данную опцию (т.е. отключать режим добавления) перед поиском в сетевом справочнике во избежание копирования в справочник всех найденных сертификатов	Выключено

Название параметра	Описание	Значение по умолчанию (после установки)
Обновлять CAC из точки распространения	Включить режим обновления списков аннулированных сертификатов (CAC) 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 для зашифрования	Включено
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
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 Центра сертификации и CAC, указанные в полях сертификата «Информация доступа к Центру» (AIA) и «Точка распространения CAC» (CDP)	Выключено
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 ПК «Валидата Клиент» (блочный или потоковый) используемый при выполнении криптографических операций	Потоковый

1.2.3 Дополнительные настройки Расширения проводника

Дополнительные настройки Расширения проводника (Рисунок 4) приведены ниже (Таблица 3).

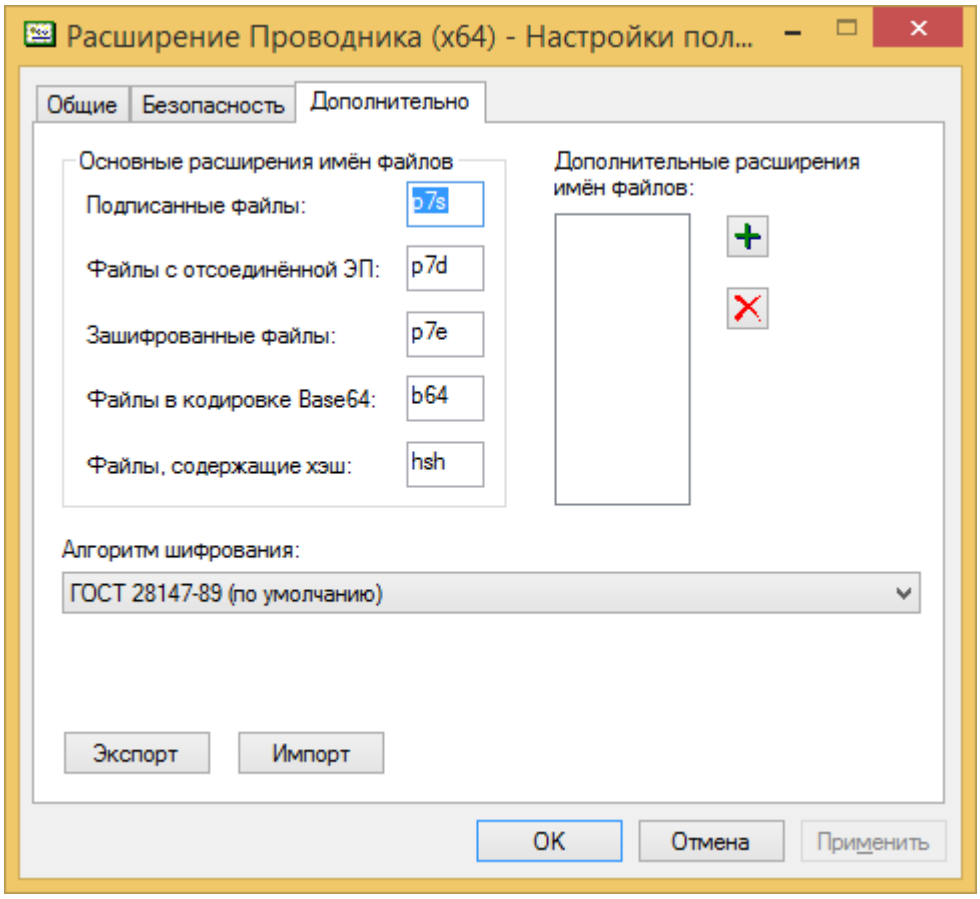

Рисунок 4 – Дополнительные настройки Расширения проводника

Таблица 3 – Настройки безопасности Расширения проводника

Название параметра	**Описание**	**Значение по умолчанию (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	p7e
Файлы в кодировке Base64	Расширение, которое добавляется к файлу при преобразовании в кодировку Base64 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	Пустой список
Алгоритм шифрования	Алгоритм, используемый при шифровании	ГОСТ 28147-89

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

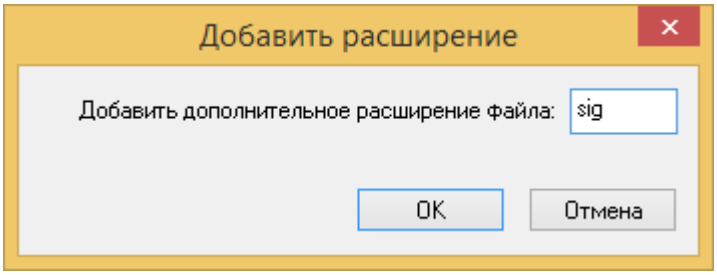

Рисунок 5 – Диалог добавления дополнительного расширения

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

1.2.4 Сохранение настроек в файл и загрузка их из файла

Для сохранения настроек Расширения проводника 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 Расширения проводника, но не нажали кнопку «Применить», в файл будут сохранены изменённые параметры.

Для загрузки настроек Расширения проводника 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 Расширения проводника нажмите кнопку «ОК» или «Применить».

1.2.5 Просмотр информации о сборке

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

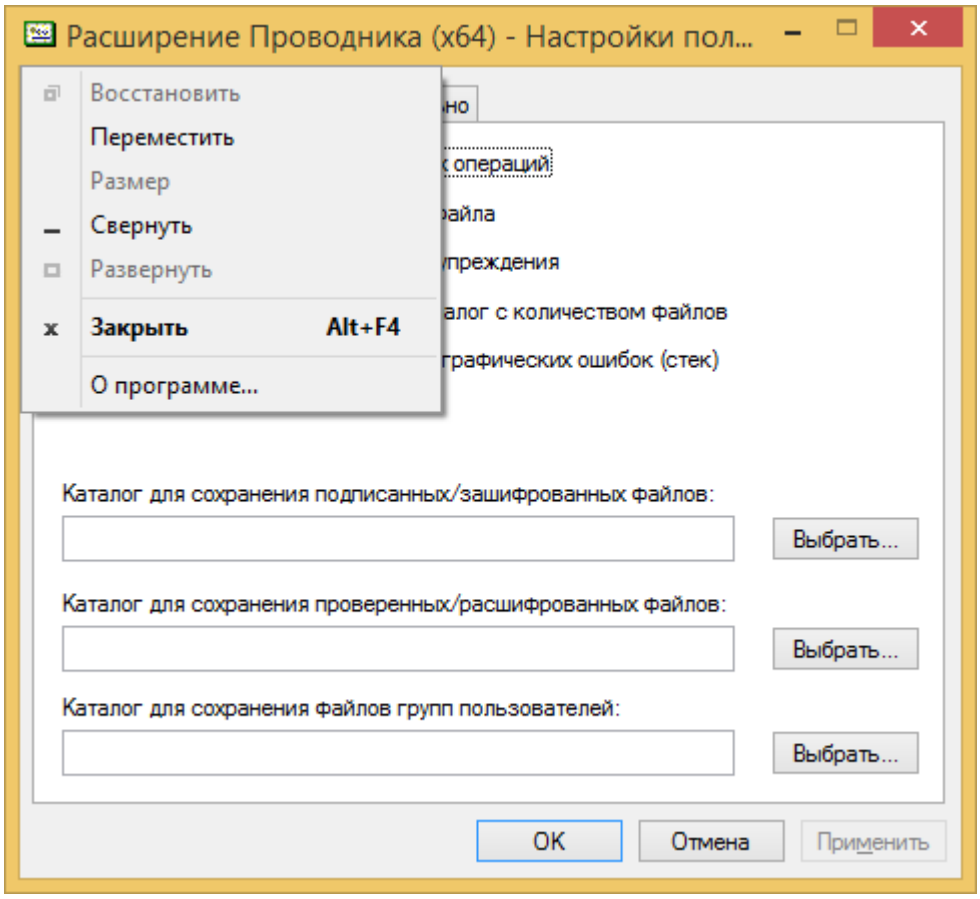

Рисунок 6 – Выбор пункта меню «О программе. . . »

На экране появится диалог с информацией о сборке Расширения проводника (Рисунок 7).

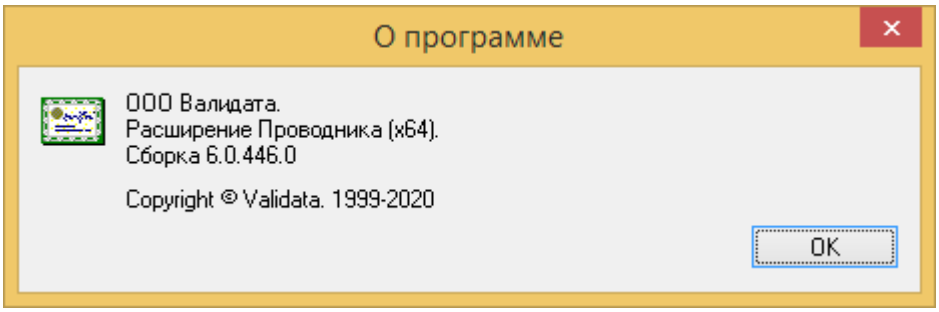

Рисунок 7 – Диалог с информацией о сборке программы

1.3 Загрузка и выгрузка ключа

Для выполнения любой криптографической операции над одним или несколькими файлами необходимо загрузить ключ. Загрузка ключа в Расширение проводника 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 «Справочник сертификатов» и конфигурационной программы.

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.

Если одновременно загружено несколько экземпляров Проводника, в них могут быть загружены разные ключи.

Примечание — Если в программе конфигурации СКЗИ установлен режим «Кэшировать закрытые ключи», то ключ, загруженный в Расширение проводника, 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 перегрузить операционную систему (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)». Если при подключении к LDAP произошла ошибка, на экран выводится диалог (возможно, после таймаута) (Рисунок 8).

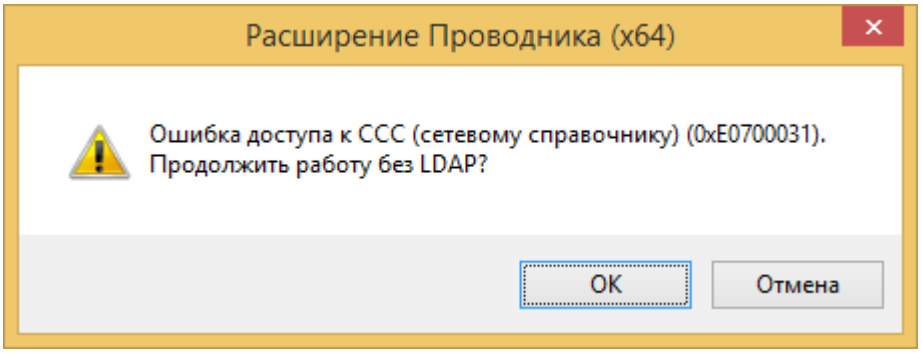

Рисунок 8 – Диалог с сообщением об ошибке подключения к LDAP

Нажатие кнопки «OK» 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 CAC из точки распространения», будет произведено обновление CAC. В случае ошибки на экран выводится диалог (возможно, после таймаута) (Рисунок 9).

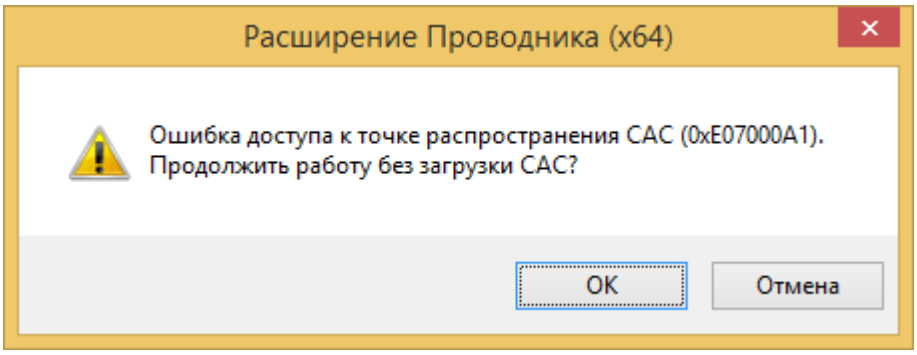

Рисунок 9 – Диалог с сообщением об ошибке при обновлении CAC

Нажатие кнопки «OK» приводит к продолжению работы без обновления CAC из точки распространения, нажатие кнопки «Отмена» — к выгрузке ключа и отказу от операции.

1.4 Криптографические операции над файлами

1.4.1 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 Расширения проводника 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» — к пропуску операции с текущим файлом, кнопки «Отмена» — к 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 подтверждение (Рисунок 10) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

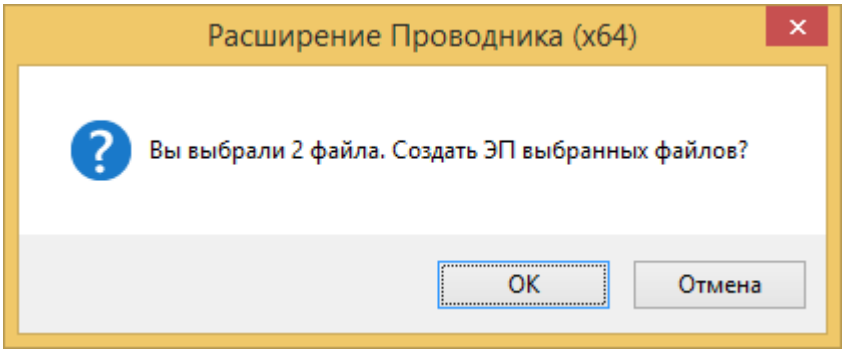

Рисунок 10 – Запрос на создание ЭП

Затем на экран выдаётся диалог создания ЭП файлов (Рисунок 11).

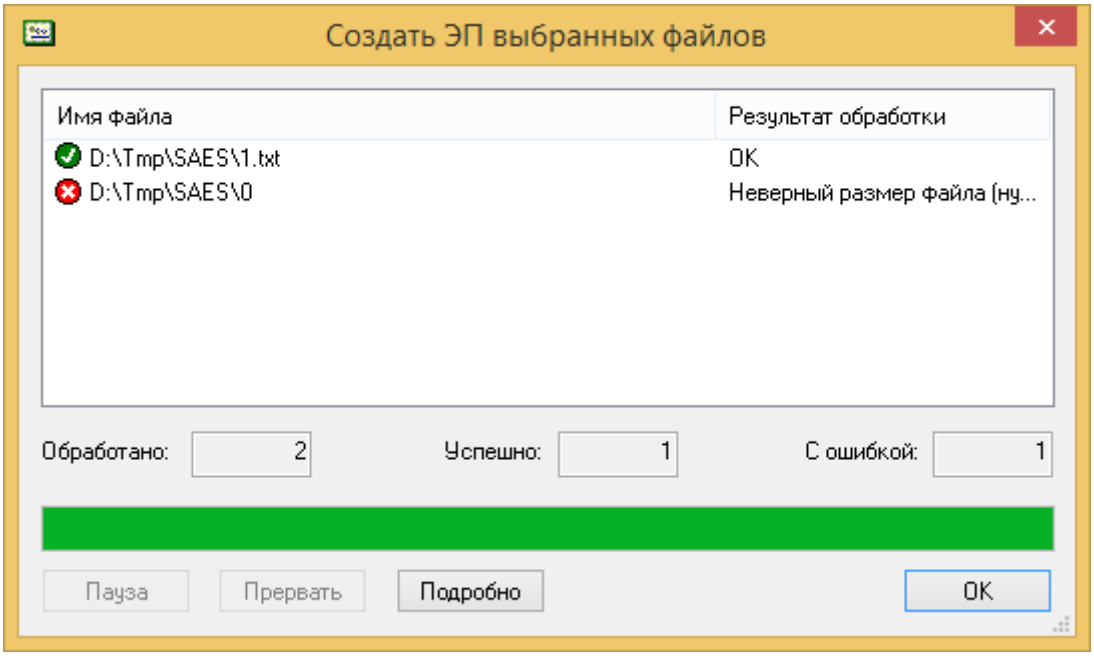

Рисунок 11 – Диалог создания ЭП файлов

Во второй колонке списка выводится краткая информация о результате создания ЭП. Для отображения полной информации выделите строчку с файлом

и нажмите кнопку «Подробно» (или сделайте двойной клик «мышью») (Рисунок 12).

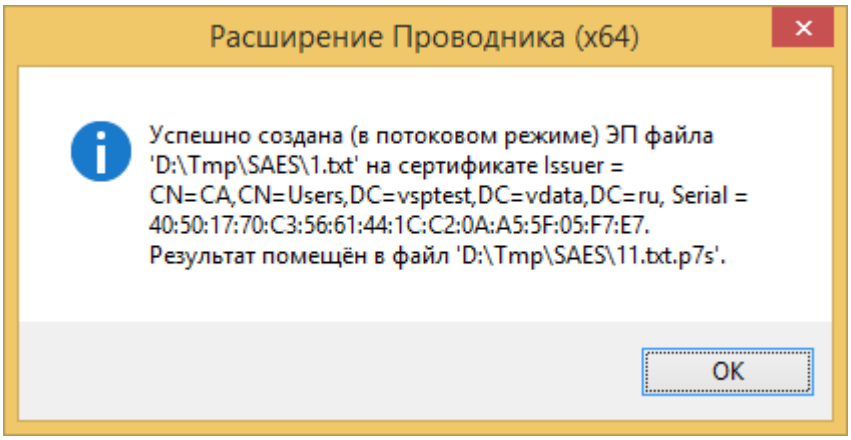

Рисунок 12 – Полная информация о создании ЭП

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

1.4.2 Проверка ЭП

Для того чтобы проверить присоединённую ЭП, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню Расширения проводника пункт «Проверить ЭП». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. раздел 1.3). 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 13).

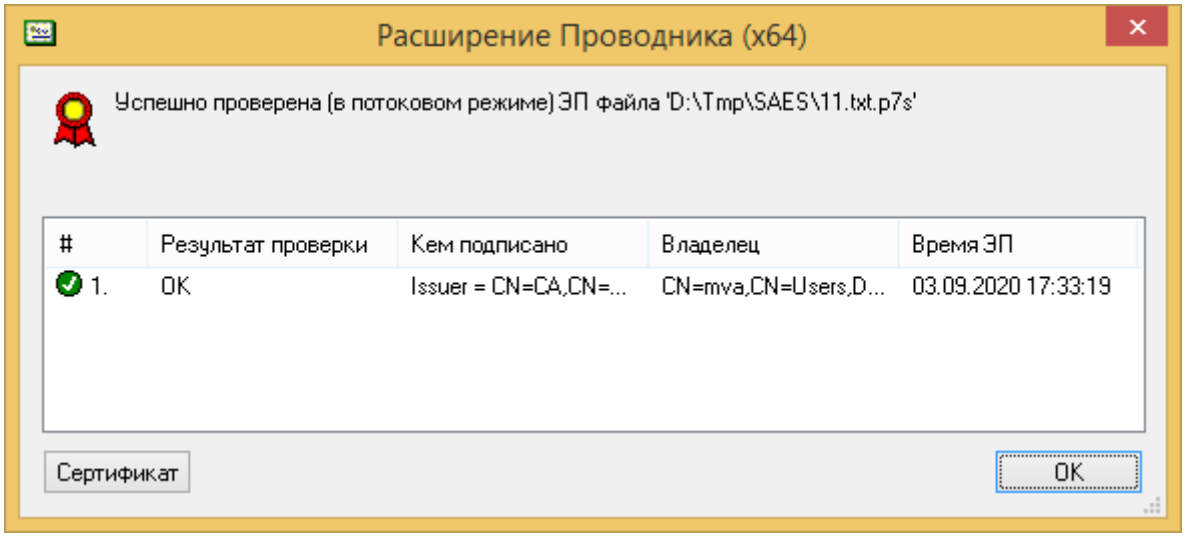

Рисунок 13 – Диалог с информацией о проверке ЭП

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 14), выделите подпись и нажмите кнопку «Сертификат» (или сделайте двойной клик «мышью»).

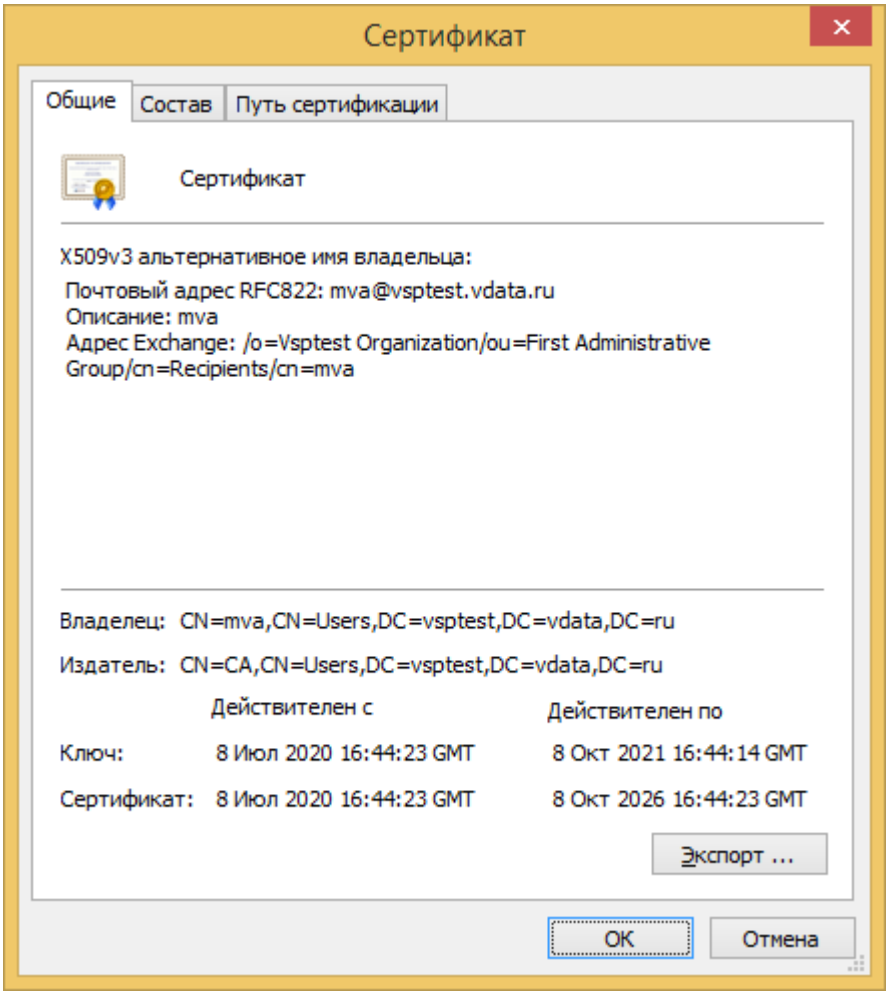

Рисунок 14 – Диалог просмотра сертификата

В случае если хоть одна подпись не была успешно проверена, результат проверки файла является отрицательным (Рисунок 15).

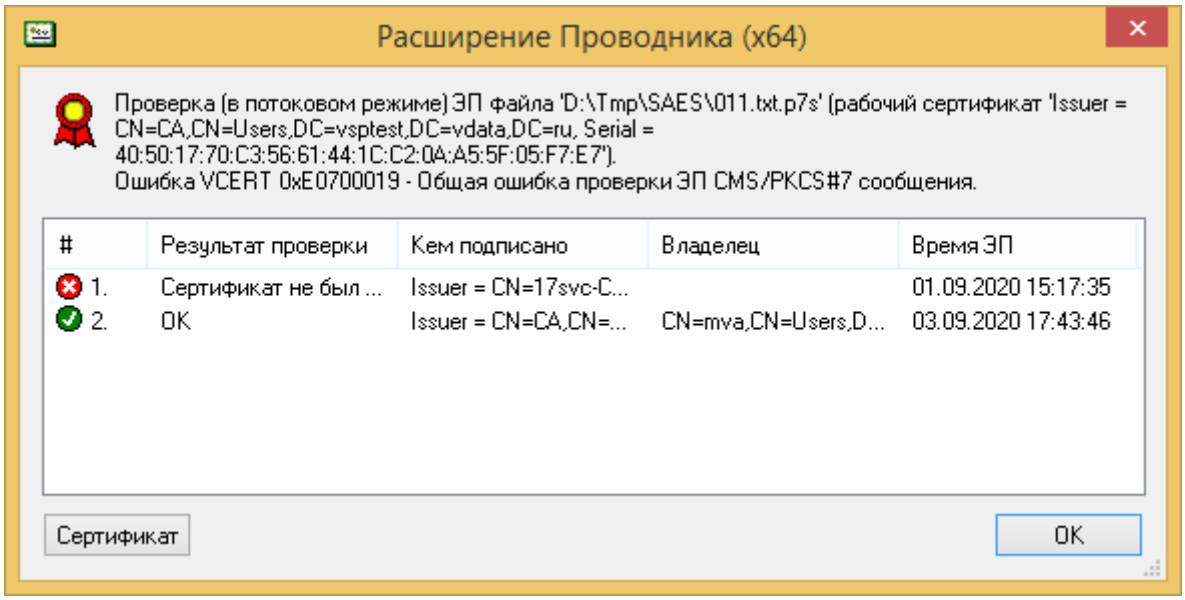

Рисунок 15 – Диалог с информацией об ошибке при проверке ЭП

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 (Рисунок 16) под информацией о проверке ЭП содержится информация о проверке соответствующего штампа времени.

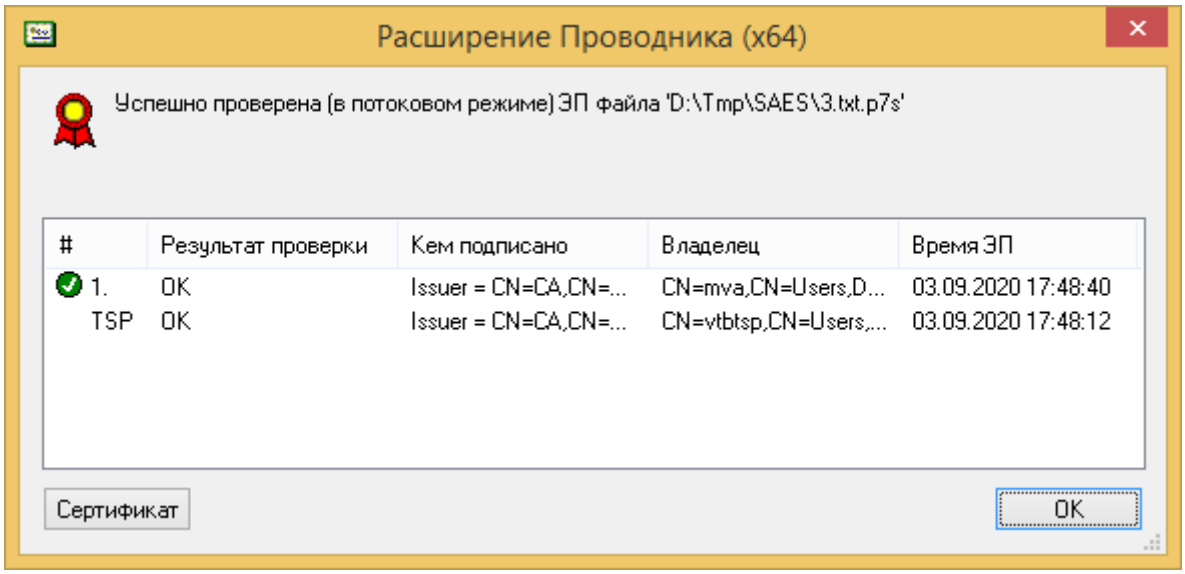

Рисунок 16 – Диалог с информацией о проверке ЭП со штампом времени

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 17).

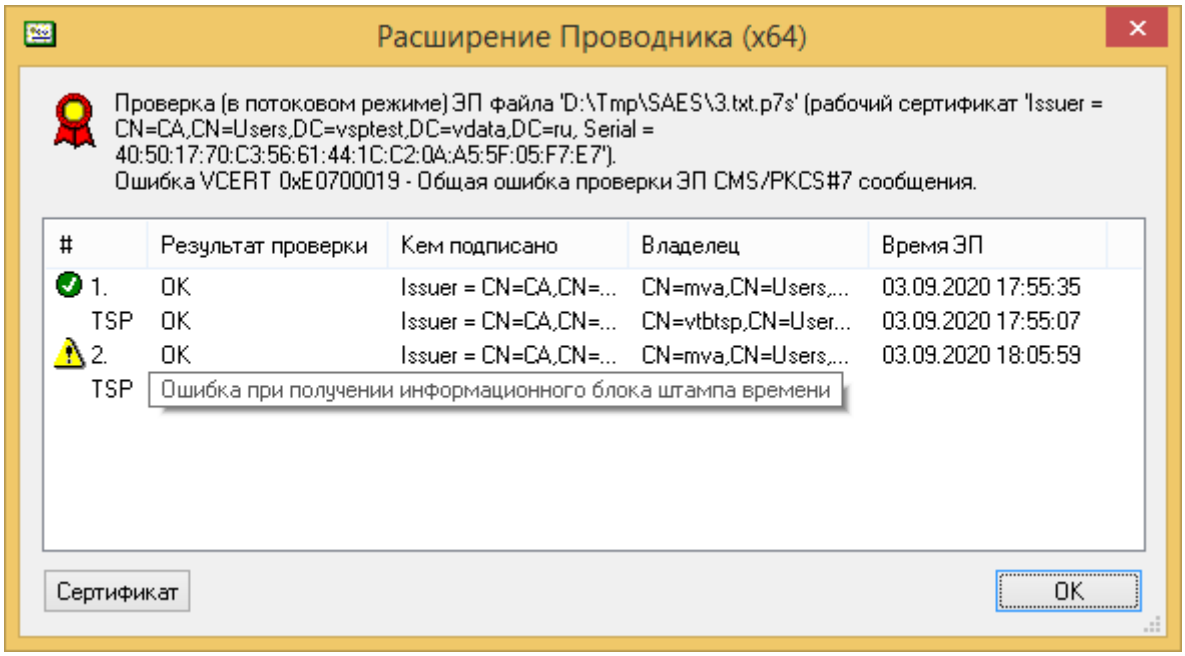

Рисунок 17 – Диалог с информацией о проверке ЭП с отсутствующим штампом времени

Если операция проверки ЭП производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение (Рисунок 18) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

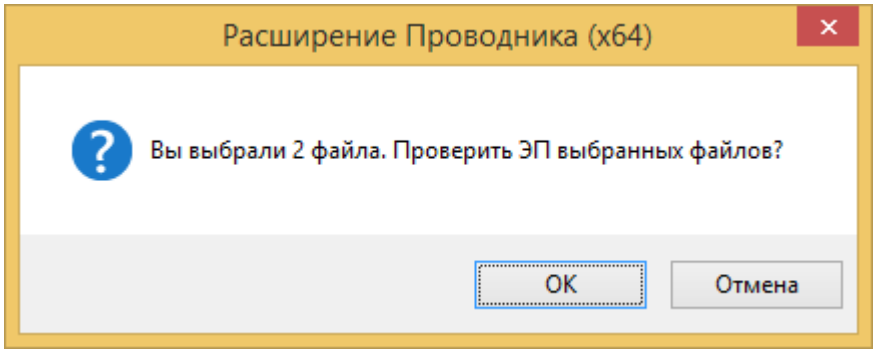

Рисунок 18 – Запрос на проверку ЭП

Затем на экран выдаётся диалог проверки ЭП файлов (Рисунок 19).

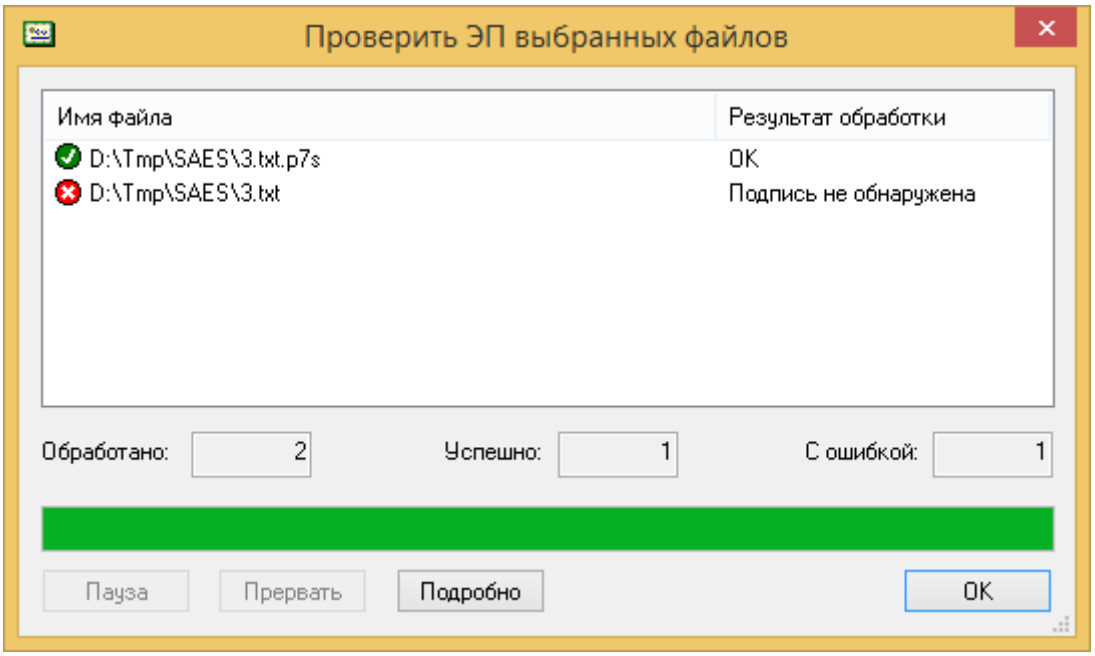

Рисунок 19 – Диалог проверки ЭП файлов

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

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

1.4.3 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 Расширения проводника 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 20). Диалог будет выдан независимо от количества выбранных файлов и от выбора режима «Не выдавать предварительный диалог с количеством файлов» в настройках пользователя.

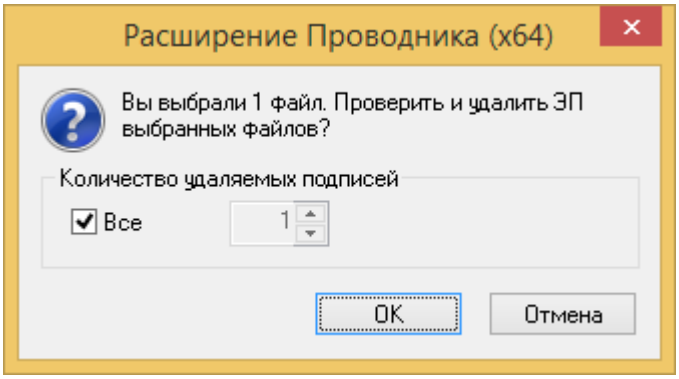

Рисунок 20 – Диалог удаления ЭП

Чтобы удалить не все подписи, а несколько (начиная с конца), снимите опцию

«Все» и выберите количество удаляемых подписей. Удаление и проверка подписи выполняются 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 21).

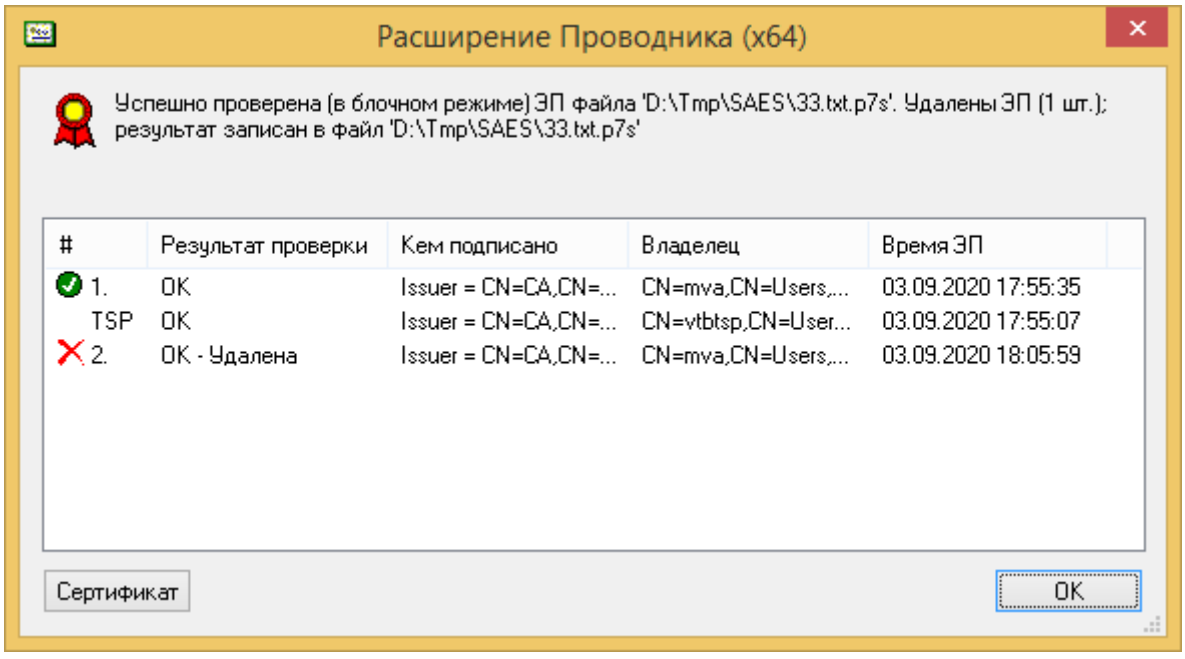

Рисунок 21 – Диалог с информацией об удалении и проверке ЭП

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, четвёртая — имя владельца сертификата, а 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 22).

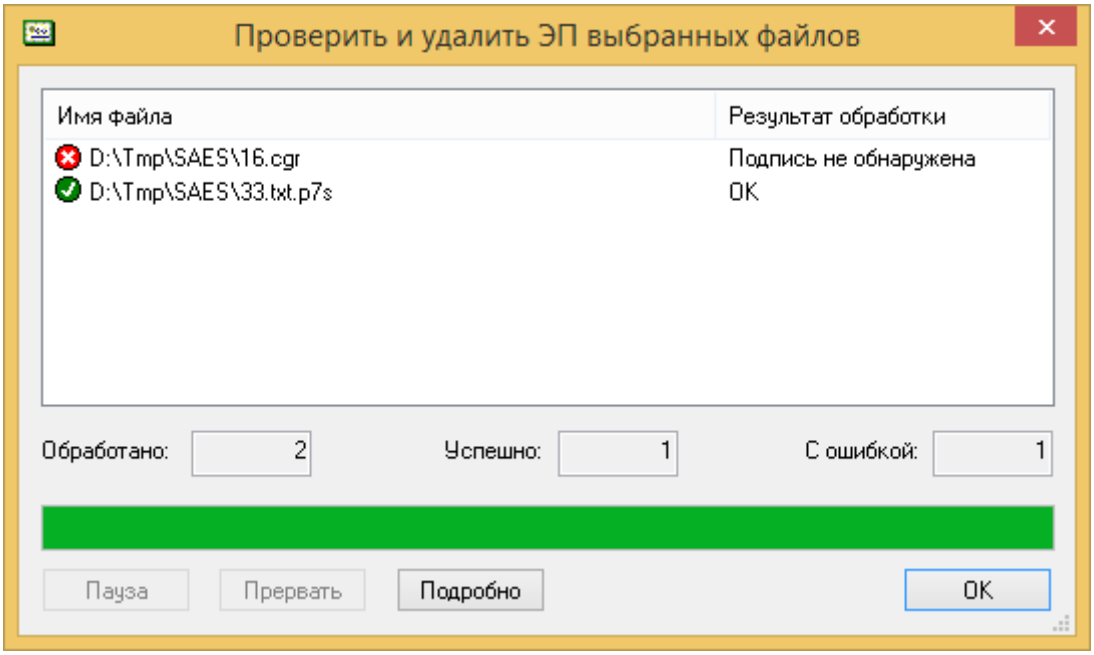

Рисунок 22 – Диалог проверки и удаления ЭП файлов

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

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

1.4.4 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 Расширения проводника 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 1.3).

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 подтверждение (Рисунок 23) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

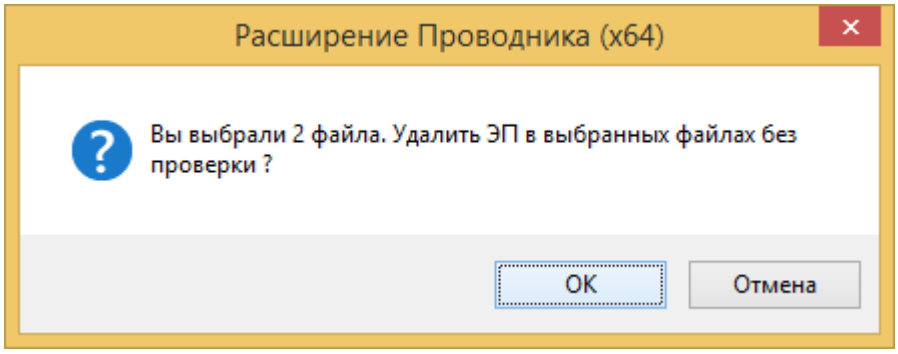

Рисунок 23 – Запрос на удаление ЭП

Затем на экран выдаётся диалог удаления ЭП (Рисунок 24).

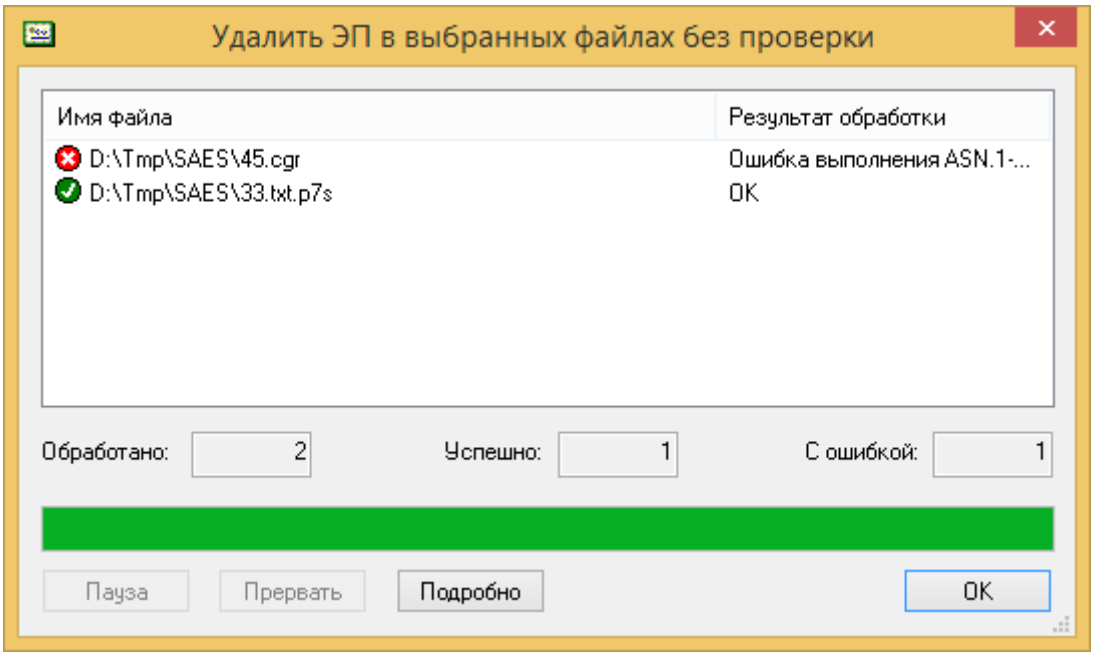

Рисунок 24 – Диалог удаления ЭП

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».

1.4.5 Создание отсоединённой ЭП

Для того чтобы создать отсоединённую (detached) ЭП в формате CMS/PKCS#7, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню Расширения проводника пункт «Дополнительно», подпункт «Создать отсоединённую ЭП». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. раздел 1.3). 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 25) или сообщение об ошибке (Рисунок 26).

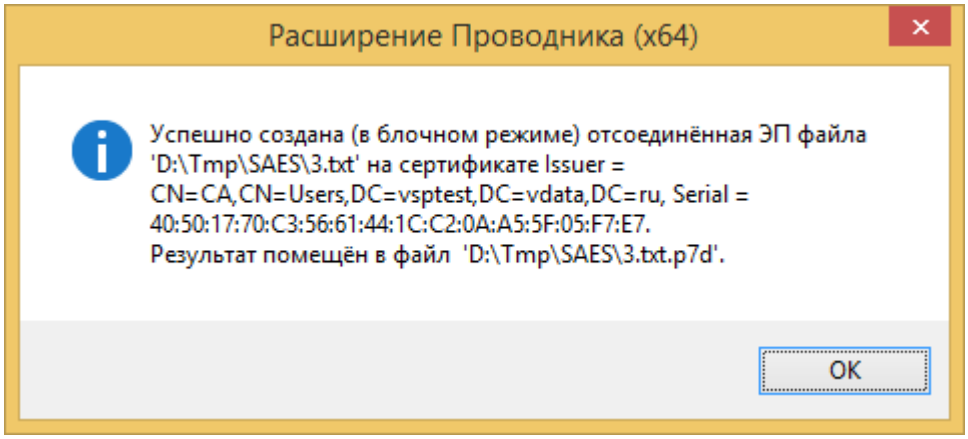

Рисунок 25 – Сообщение об успешном создании отсоединённой ЭП

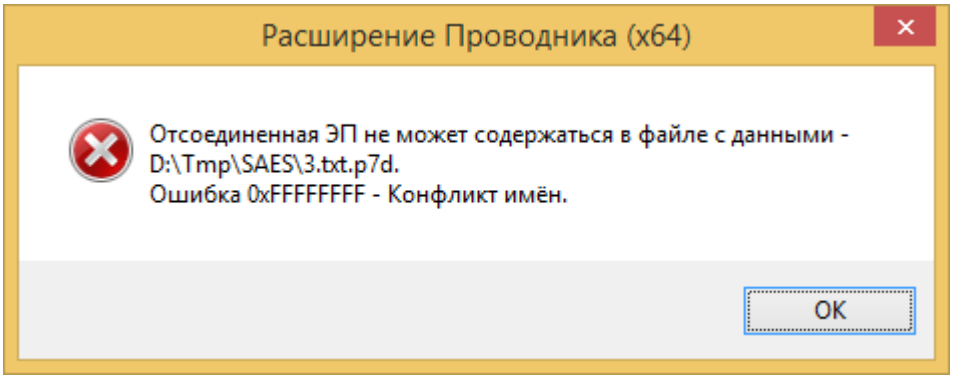

Рисунок 26 – Сообщение об ошибке при создании отсоединённой ЭП

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 подтверждение при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов» (Рисунок 27).

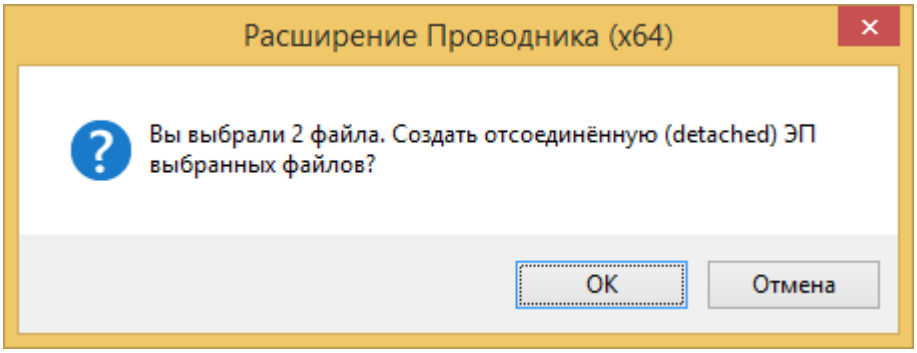

Рисунок 27 – Запрос на создание отсоединённой ЭП

Затем на экран выдаётся диалог создания отсоединённой ЭП файлов (Рисунок 28).

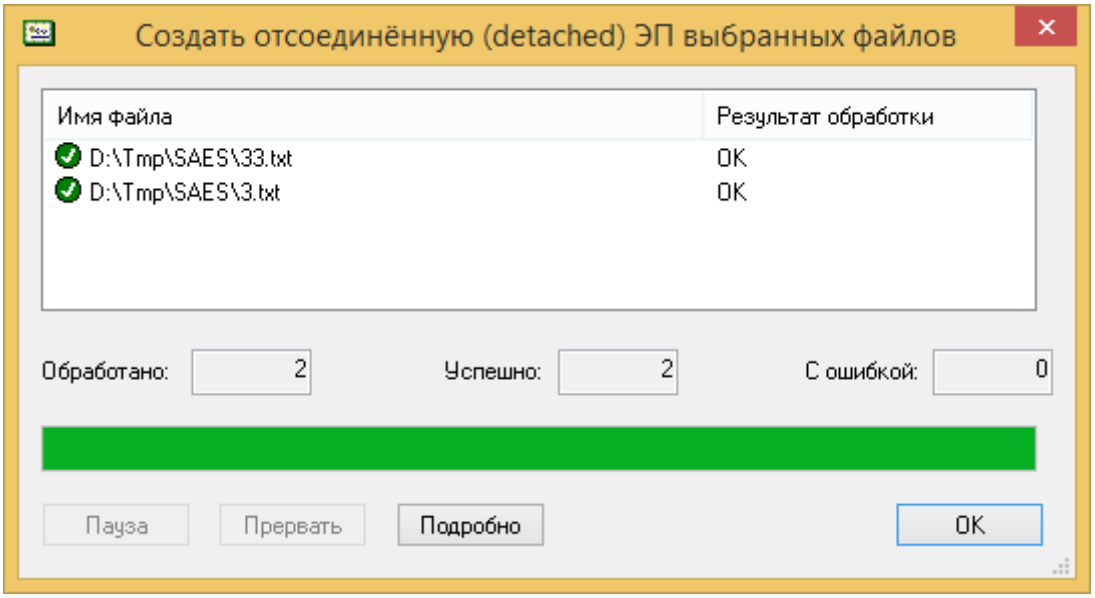

Рисунок 28 – Диалог создания отсоединённой ЭП файлов

Во второй колонке списка выводится краткая информация о результате создания отсоединённой ЭП. 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 создание отсоединённой ЭП нажатием кнопок «Пауза» или «Прервать».

1.4.6 Проверка отсоединённой ЭП

Для того чтобы проверить отсоединённую ЭП выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню Расширения проводника пункт «Дополнительно», подпункт «Проверить отсоединённую ЭП».

Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. раздел 1.3).

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 29).

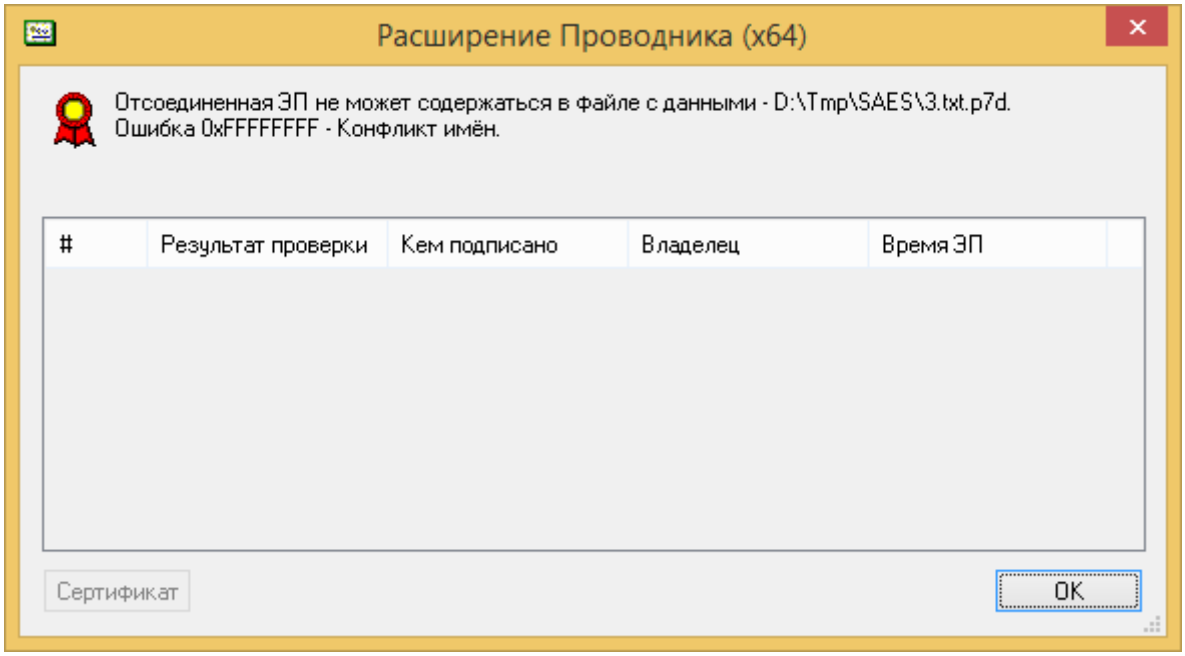

Рисунок 29 – Сообщение о конфликте имён при проверке отсоединённой ЭП

Если операция проверки отсоединённой ЭП производится с одним файлом, после проверки ЭП на экран выдаётся диалог с информацией о проверенных ЭП (Рисунок 30).

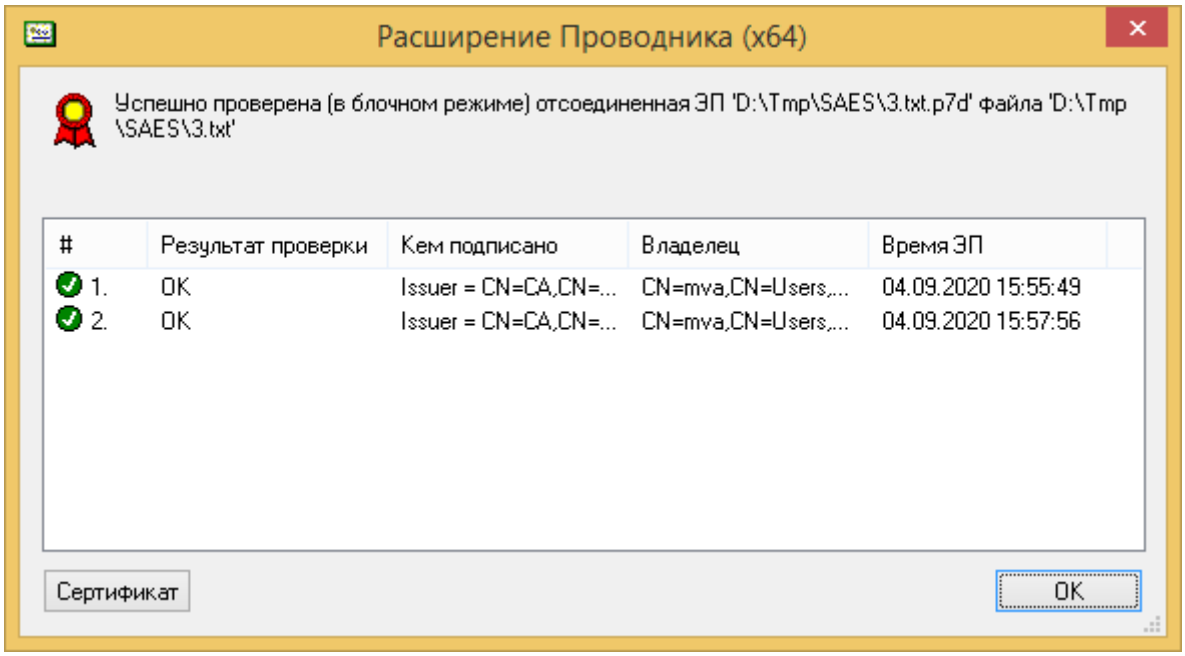

Рисунок 30 – Диалог с информацией о проверке отсоединённой ЭП

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, а пятая — время создания ЭП. Чтобы подробно просмотреть сертификат (Рисунок 14), выделите подпись и нажмите кнопку «Сертификат» (или сделайте двойной клик «мышью»).

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 подтверждение (Рисунок 31) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

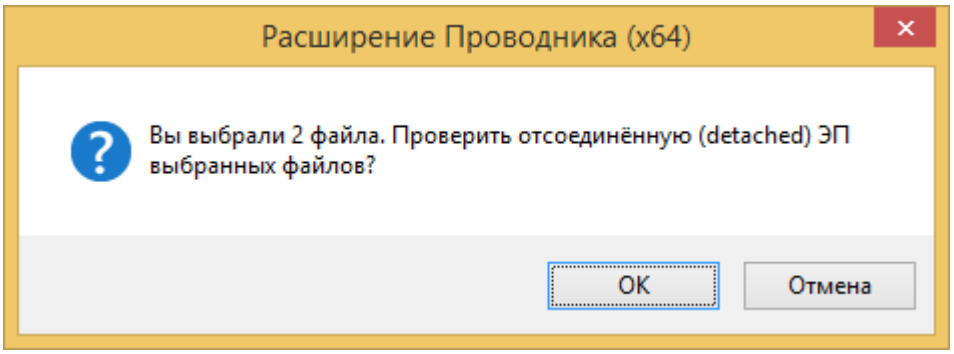

Рисунок 31 – Запрос на проверку отсоединённой ЭП

Затем на экран выдаётся диалог проверки отсоединённой ЭП файлов (Рисунок 32).

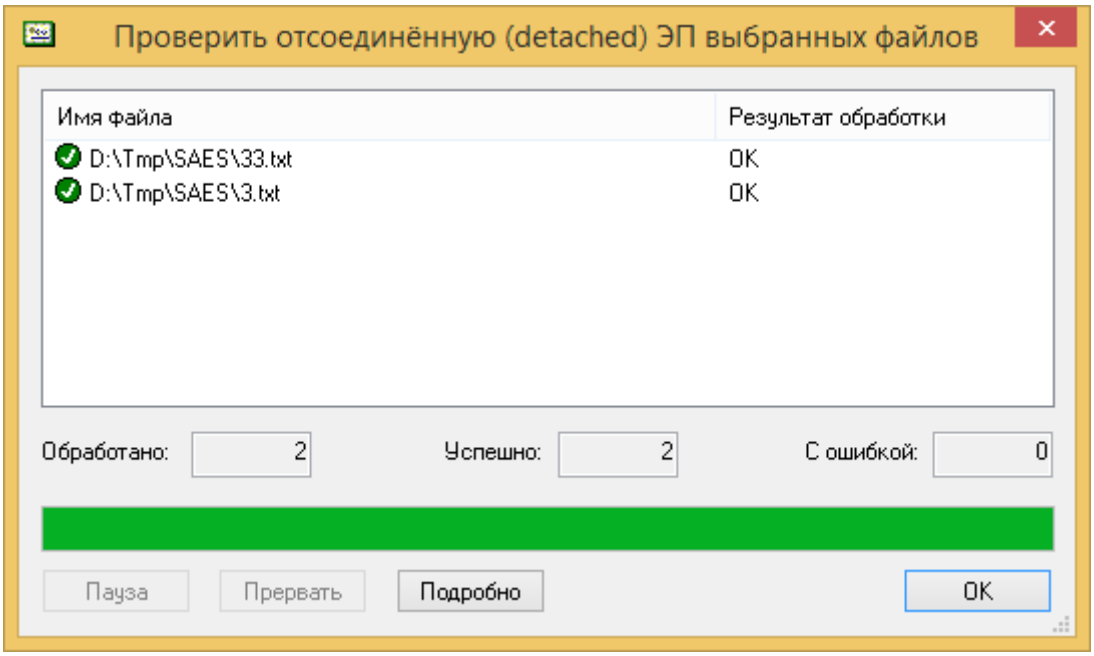

Рисунок 32 – Диалог проверки отсоединённой ЭП файлов

Во второй колонке списка выводится краткая информация о результате проверки ЭП. 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 проверку отсоединённой ЭП нажатием кнопок «Пауза» или «Прервать».

1.4.7 Зашифрование

Для зашифрования выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню Расширения проводника пункт «Зашифровать». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. раздел 1.3). Прежде, чем начать шифрование, необходимо задать список получателей зашифрованного сообщения. Для этого на экран выдаётся диалог выбора получателей зашифрованного сообщения (Рисунок 33).

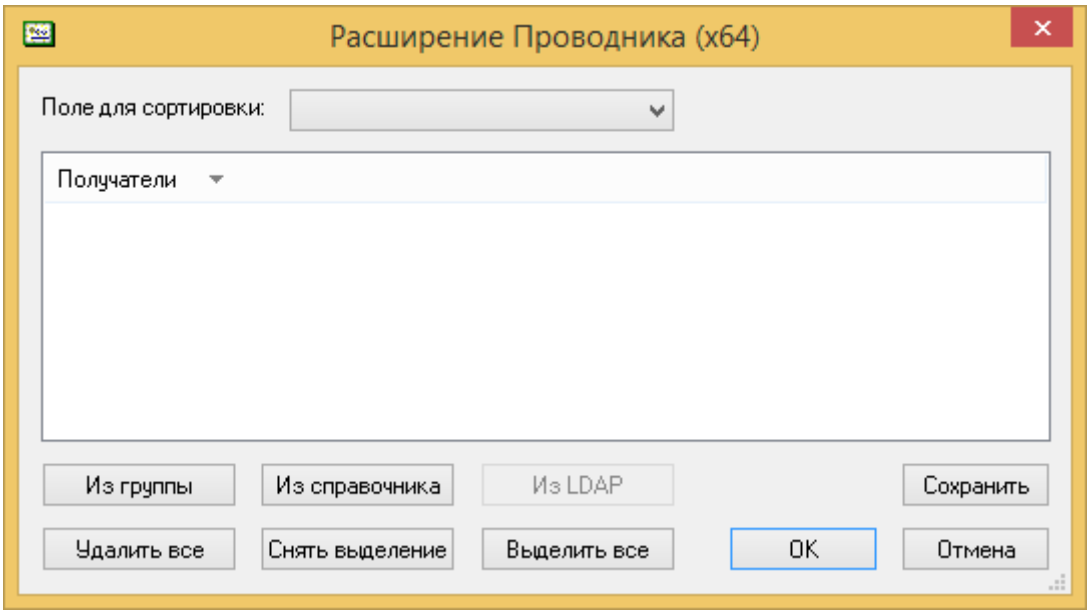

Рисунок 33 – Пустой диалог выбора получателей

Изначально список получателей пуст. Необходимо задать список получателей (пользователей, для которых шифруется файл). Нажмите кнопку «Из справочника», чтобы внести в список всех владельцев сертификатов, предназначенных для шифрования, содержащихся в Справочнике сертификатов. Найденные имена пользователей добавляются к списку получателей и отмечаются «галочками» (Рисунок 34).

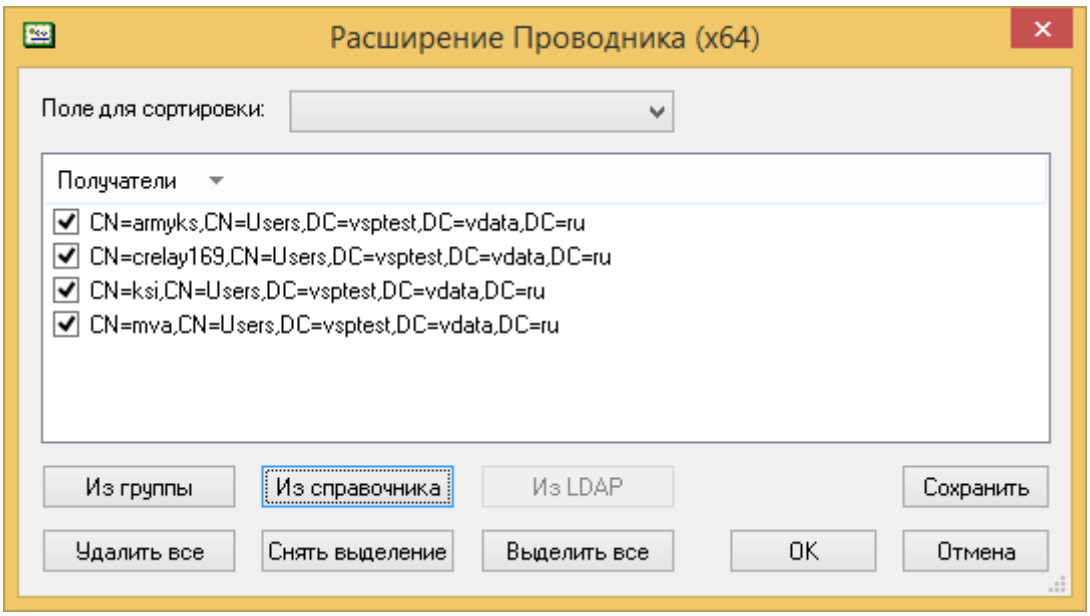

Рисунок 34 – Заполненный диалог выбора получателей

Чтобы просмотреть имя владельца сертификата целиком, сделайте на нём двойной клик мышью.

Если в настройках пользователя отключён режим «Не использовать сетевой справочник (LDAP)», будет доступна кнопка «Из LDAP». Для поиска сертифи-

катов в сетевом справочнике нажмите её. На экране появится диалог поиска в LDAP (Рисунок 35).

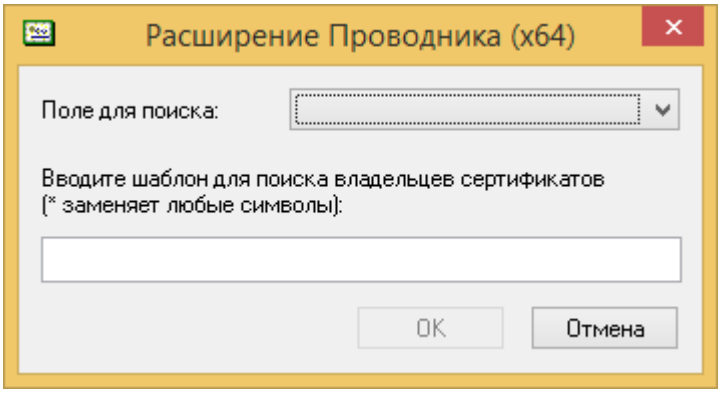

Рисунок 35 – Диалог поиска в LDAP

Задайте поле (часть имени владельца сертификата) для поиска и шаблон поиска — строку, в которой символ * (звёздочка) заменяет любой набор символов (регистр букв при поиске значения не имеет). Например, для поиска всех пользователей с доменным именем, содержащим подстроку **data**, поиск должен выглядеть следующим образом (Рисунок 36).

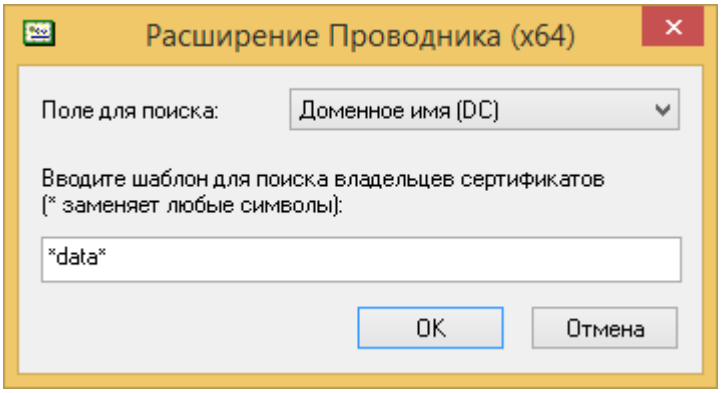

Рисунок 36 – Поиск по названию населённого пункта

В качестве поля для поиска можно выбрать режим «Поиск по всему имени» (Рисунок 37).

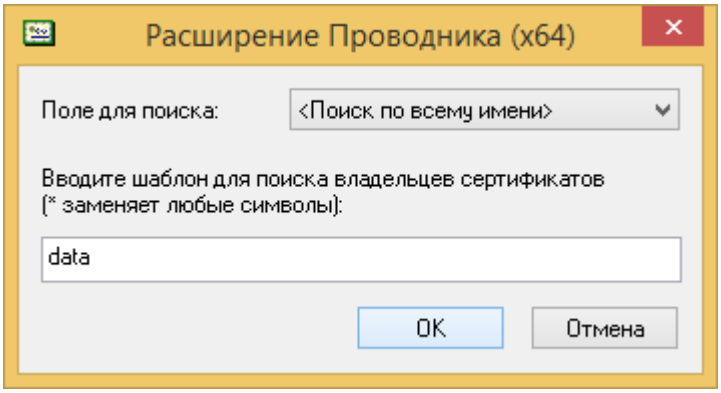

Рисунок 37 – Поиск в LDAP по всему имени

В этом режиме символы * в начале и в конце шаблона поиска ставятся автоматически. При заданных на рисунке выше (Рисунок 37) параметрах поиска будут найдены не только пользователи с доменным именем, содержащим подстроку **data**, но и те, у кого подстрока **data** содержится в другой части имени, например в фамилии.

Найденные имена пользователей добавляются к списку получателей и отмечаются «галочками». Список получателей может быть отсортирован по любому полю (части имени владельца сертификата). Для сортировки выберите поле в раскрывающемся списке; нажатие на заголовок списка (там, где слово «Получатели») переключает порядок сортировки — по возрастанию / по убыванию (Рисунок 38).

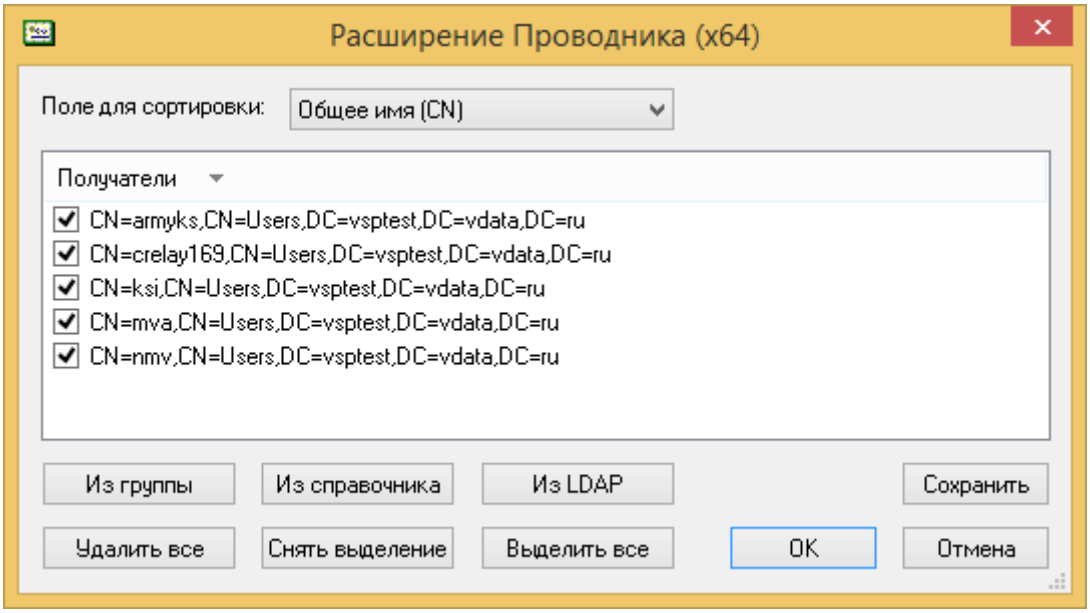

Рисунок 38 – Список, отсортированный по должности

Чтобы сохранить группу получателей, отметьте их в списке «галочками» и нажмите кнопку «Сохранить». Выберите имя для файла группы в стандартном диалоге сохранения файла (если в настройках пользователя задан параметр «Каталог для сохранения файлов групп пользователей», этот каталог будет предложен для сохранения файла). Для удобства выделения «галочками» имён пользователей используйте кнопки «Выделить все» и «Снять выделение». Нажатие на кнопку «Удалить все» после подтверждения очищает список.

Чтобы открыть ранее созданную группу, нажмите кнопку «Из группы» и выберите имя файла в стандартном диалоге открытия файла (если в настройках пользователя задан параметр «Каталог для сохранения файлов групп пользователей», этот каталог будет предложен для открытия файла). Имена пользователей, содержащиеся в открытой группе, добавляются к списку получателей и отмечаются «галочками».

После того, как список сформирован, для зашифрования на всех получателей из списка, отмеченных «галочками», нажмите кнопку «OK». При этом будет сформирован список сертификатов для выполнения зашифрования (один пользователь может иметь несколько сертификатов, зашифрование производится на все действующие сертификаты пользователя, предназначенные для шифрова-

ния). Если для какого-либо получателя из списка не найдено ни одного сертификата, на экран выдаётся предупреждение (Рисунок 39).

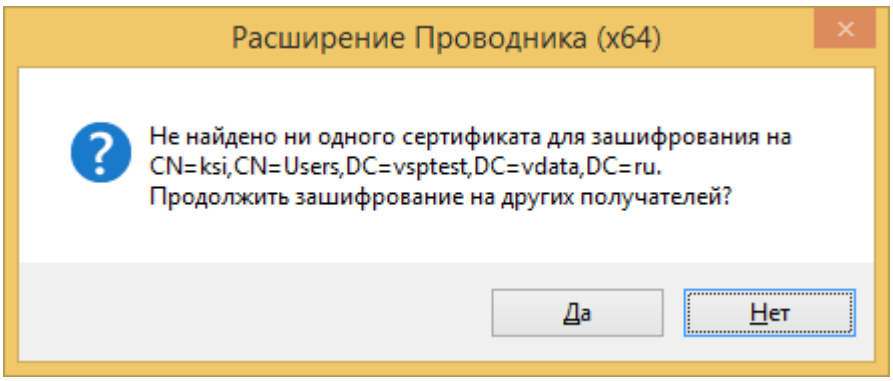

Рисунок 39 – Предупреждение об отсутствии сертификатов для шифрования

Нажатие кнопки «Да» исключает получателя из списка, нажатие кнопки «Нет» прекращает операцию. Список получателей, для которых найден хотя бы один сертификат для шифрования, сохраняется (но не более 256 получателей) и предлагается пользователю при следующем открытии диалога выбора получателей.

Если файл, к которому применяется операция зашифрования, уже зашифрован, на экран выдаётся предупреждение (Рисунок 40).

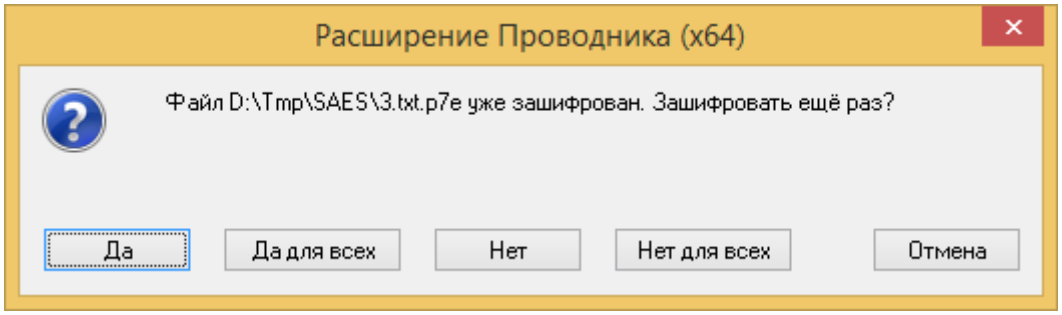

Рисунок 40 – Предупреждение о том, что файл уже зашифрован

Нажмите кнопку «Да», чтобы разрешить повторное зашифрование файла. Нажатие на кнопку «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») (Рисунок 41).

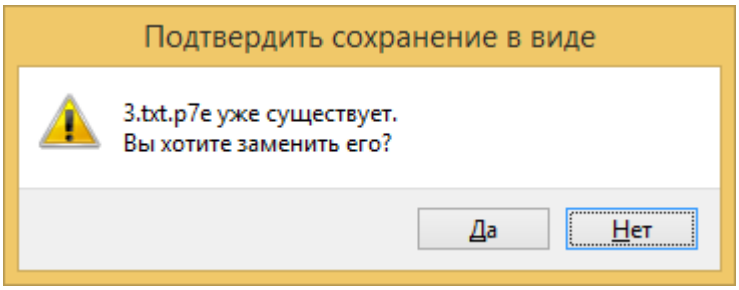

Рисунок 41 – Диалог подтверждения перезаписи файла

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 зашифрования производится с одним файлом, после выполнения операции на экран выдаётся сообщение об успехе (Рисунок 42) или об ошибке (Рисунок 43).

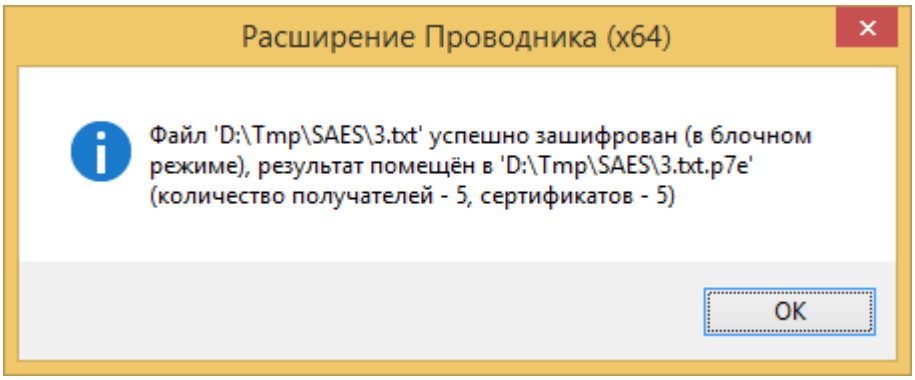

Рисунок 42 – Сообщение об успешном зашифровании файла

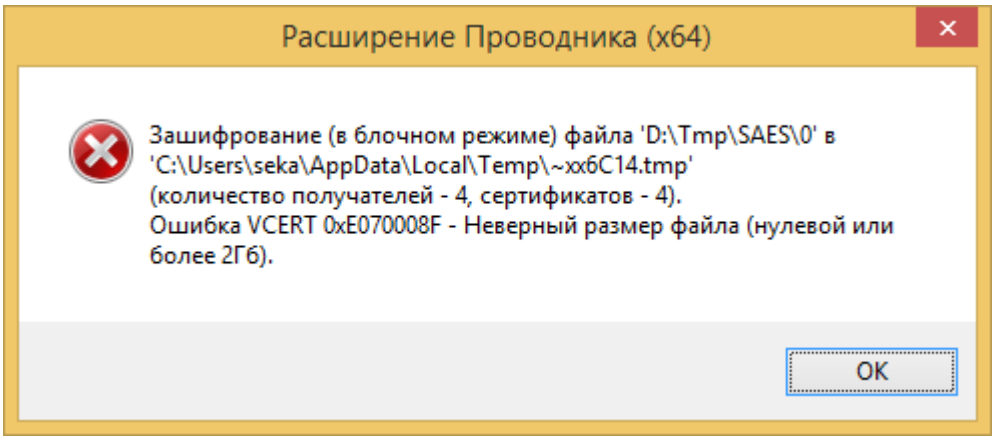

Рисунок 43 – Сообщение об ошибке при зашифровании файла

Если операция зашифрования производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов» (Рисунок 44).

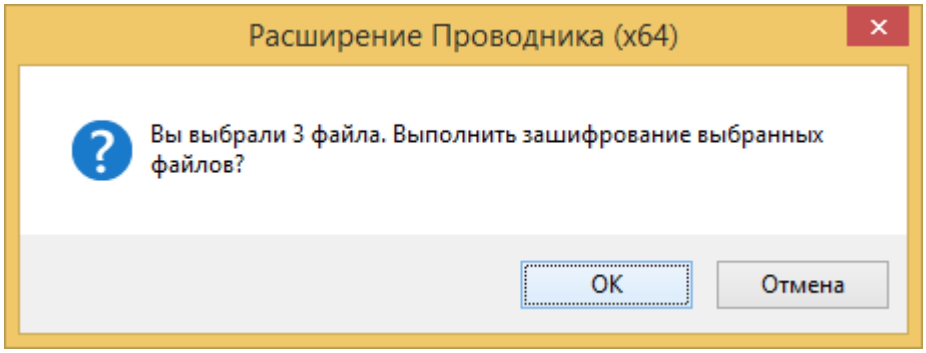

Рисунок 44 – Запрос на шифрование файлов

Затем на экран выдаётся диалог зашифрования файлов (Рисунок 45).

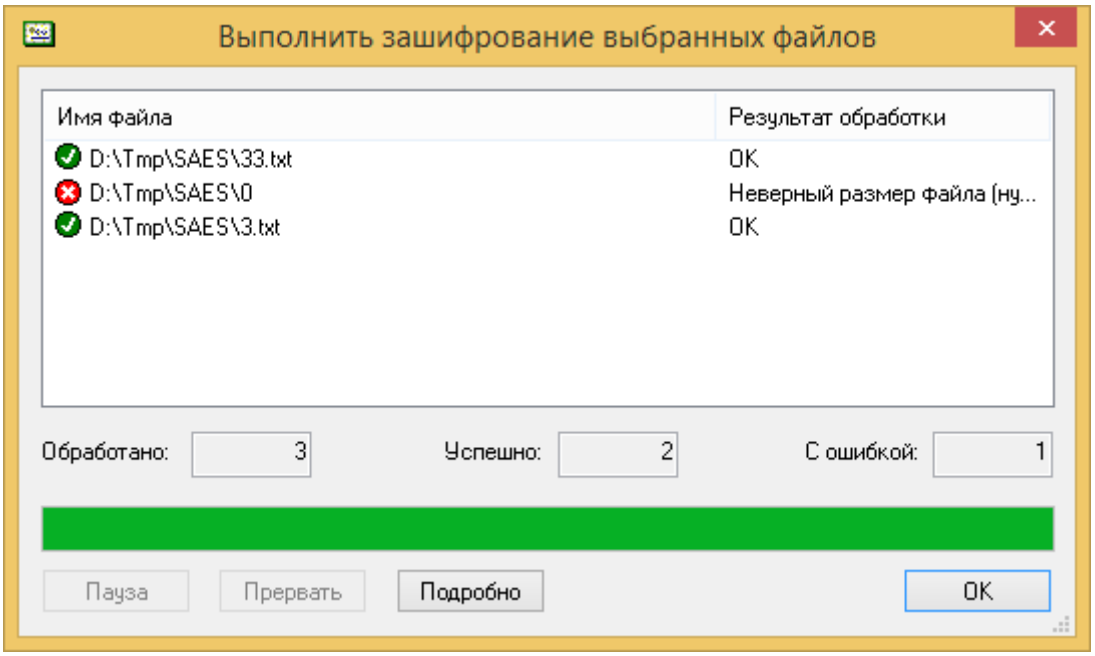

Рисунок 45 – Диалог зашифрования файлов

Во второй колонке списка выводится краткая информация о результате зашифрования. 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 зашифрование нажатием кнопок «Пауза» или «Прервать».

1.4.8 Расшифрование

Для расшифрования выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню Расширения проводника пункт «Расшифровать». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. раздел 1.3).

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») (Рисунок 41).

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 46) или сообщение об ошибке (Рисунок 47).

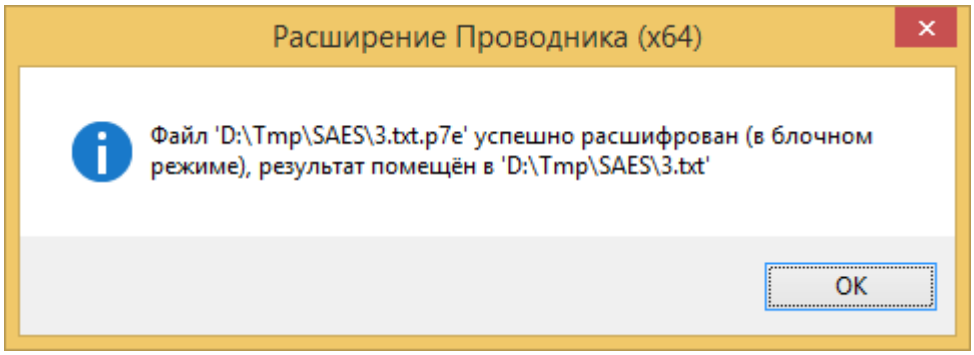

Рисунок 46 – Сообщение об успешном расшифровании файла

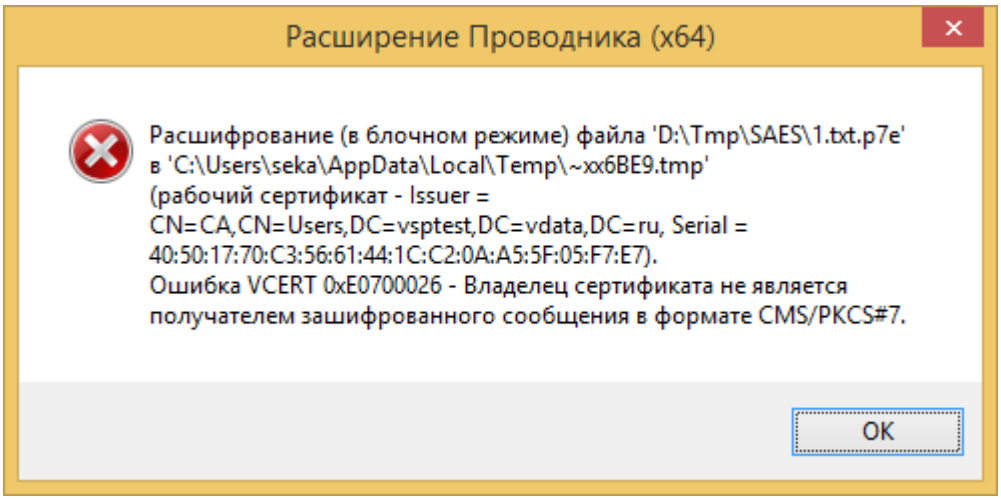

Рисунок 47 – Сообщение об ошибке при расшифровании файла

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

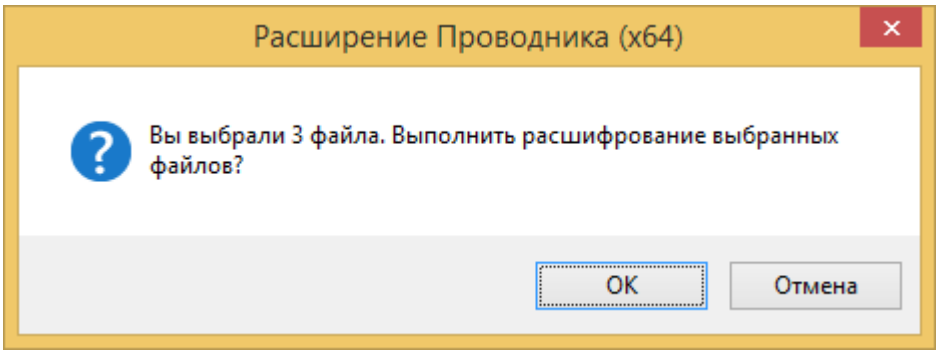

Рисунок 48 – Запрос на расшифрование

Затем на экран выдаётся диалог расшифрования файлов (Рисунок 49).

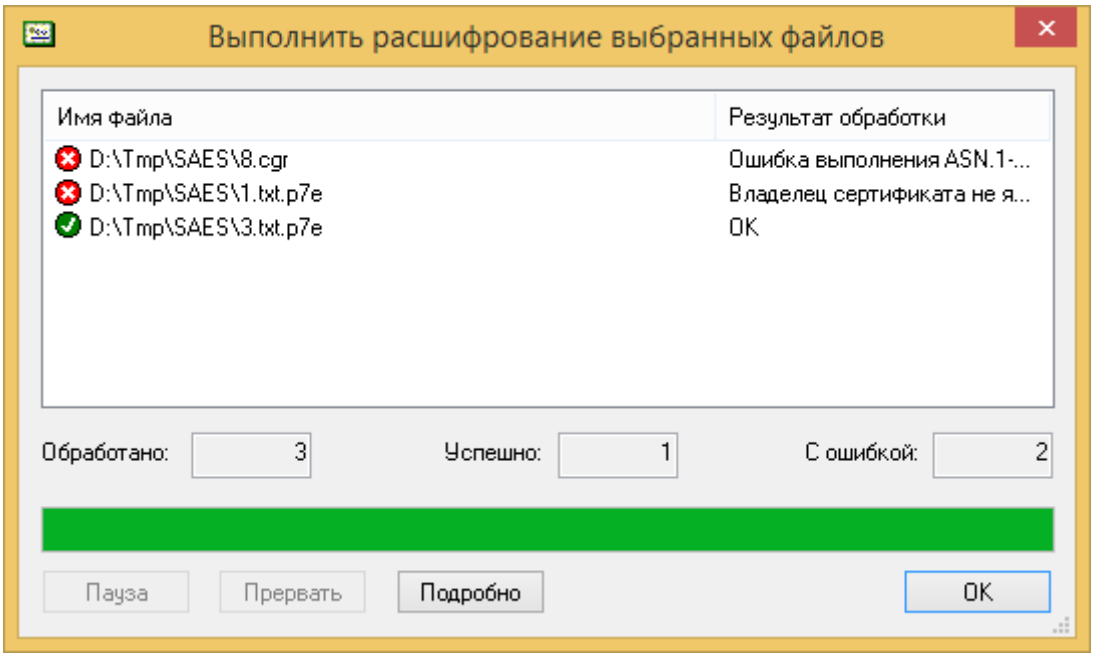

Рисунок 49 – Диалог расшифрования файлов

Во второй колонке списка выводится краткая информация о результате расшифрования. 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 расшифрование нажатием кнопок «Пауза» или «Прервать».

1.4.9 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 Расширения проводника пункт «Информация о файле». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. раздел 1.3).

Если операция производится с одним файлом, то для зашифрованного файла на экран будет выдан диалог (Рисунок 50) с информацией о зашифрованном файле, содержащий список получателей (на кого зашифрован файл).

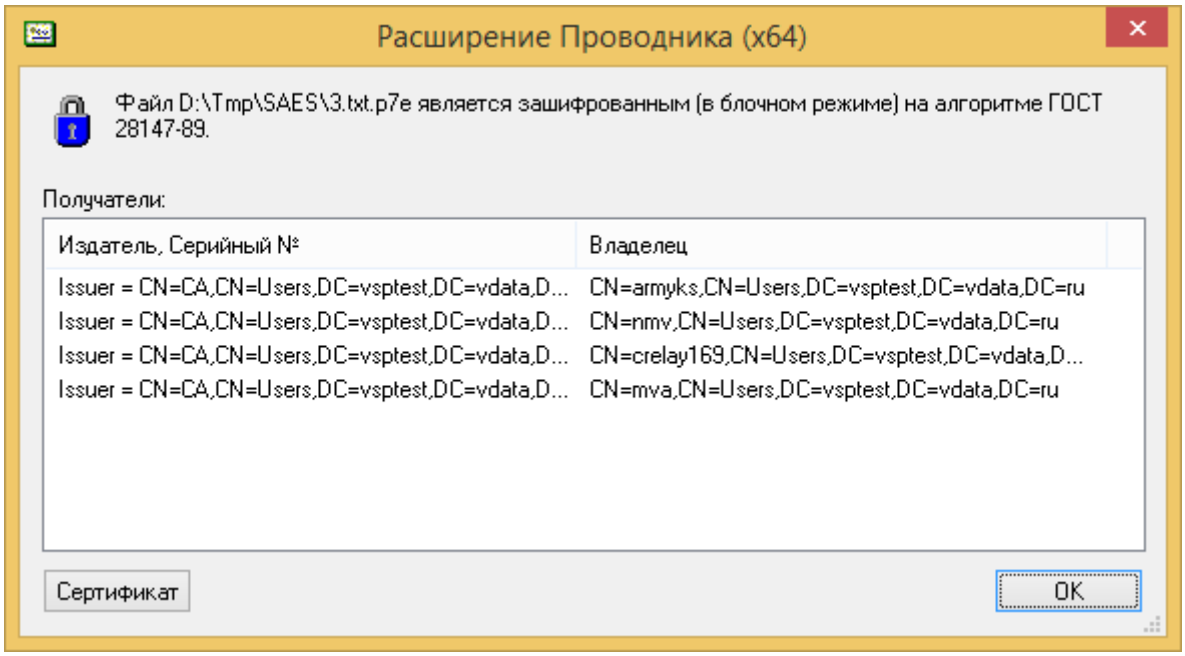

Рисунок 50 – Диалог с информацией о зашифрованном файле

Чтобы подробно просмотреть 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 51).

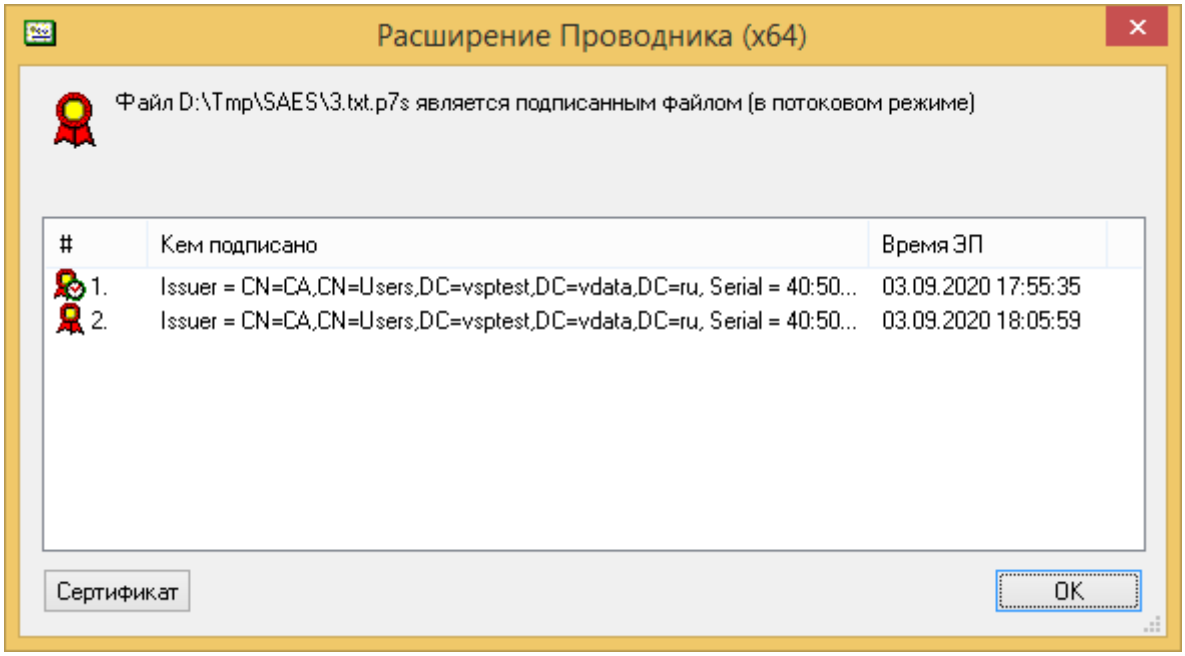

Рисунок 51 – Диалог с информацией об ЭП

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 52).

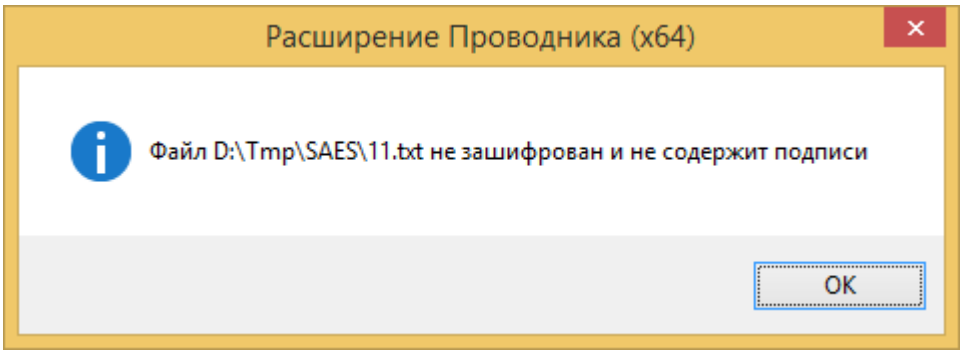

Рисунок 52 – Сообщение о незашифрованном файле, не содержащем ЭП

Если операция производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение (Рисунок 53) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

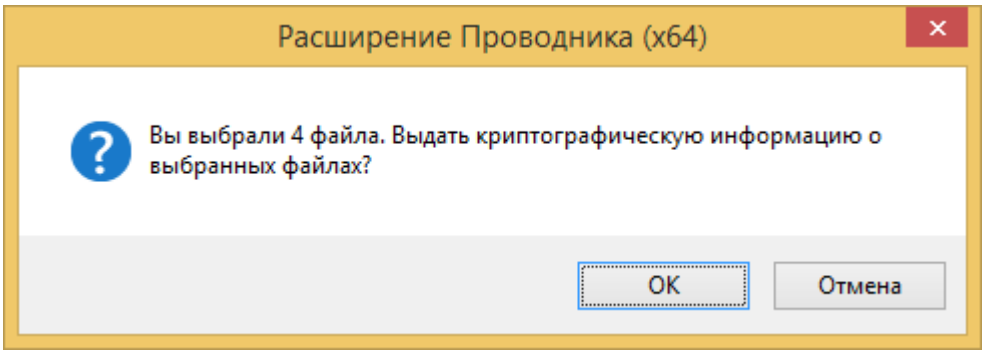

Рисунок 53 – Запрос на отображение криптографической информации о файлах

Затем на экран выдаётся диалог отображения криптографической информации о файлах (Рисунок 54).

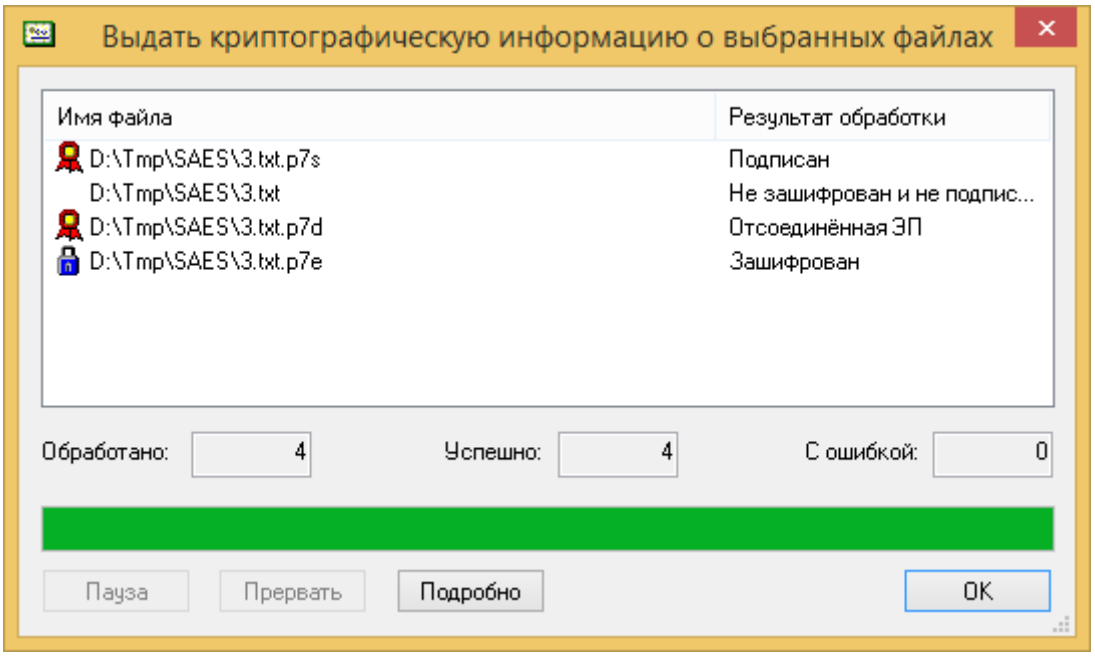

Рисунок 54 – Диалог отображения криптографической информации о файлах

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

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

1.4.10 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 проверки сертификата (Online Certificate Status Protocol). Нажмите кнопку «OK», на экране появится диалоговое окно со статусом сертификата (Рисунок 55) или сообщение об ошибке (Рисунок 56).

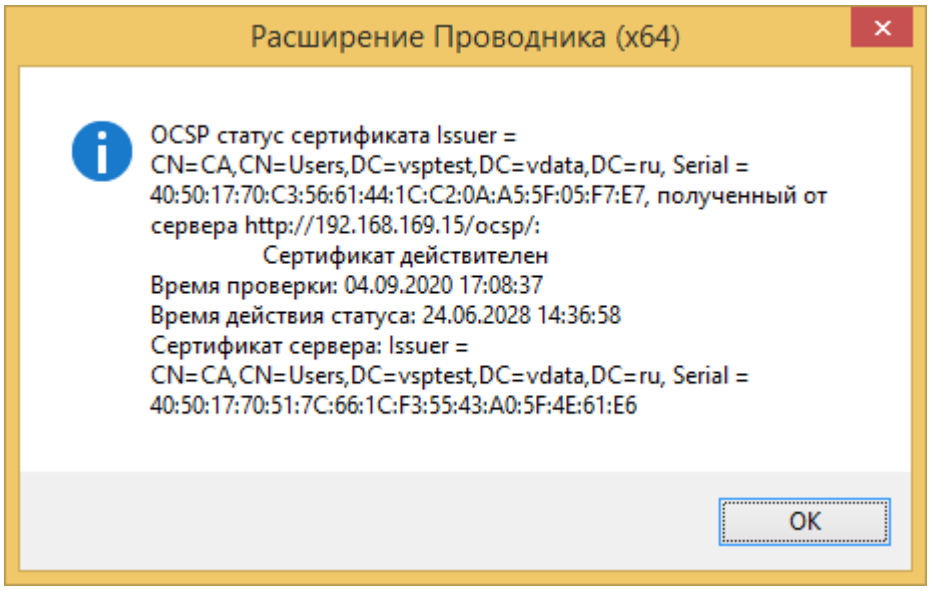

Рисунок 55 – Диалог, отображающий статус OCSP

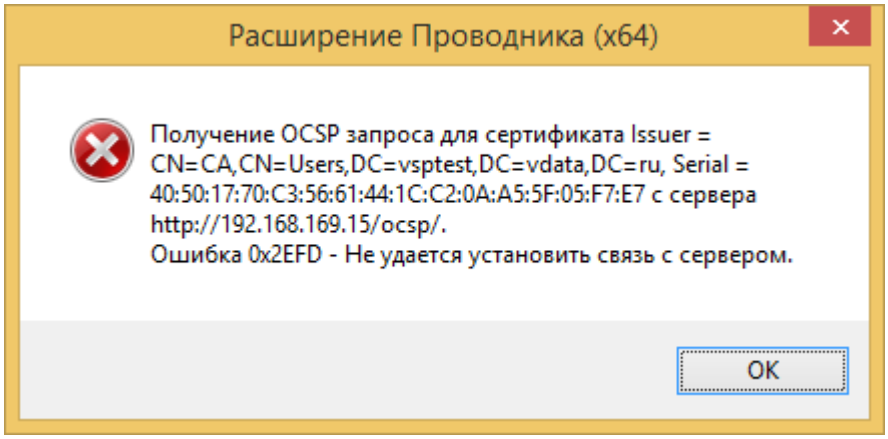

Рисунок 56 – Сообщение об ошибке при получения статуса OCSP

1.4.11 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 57, Рисунок 58).

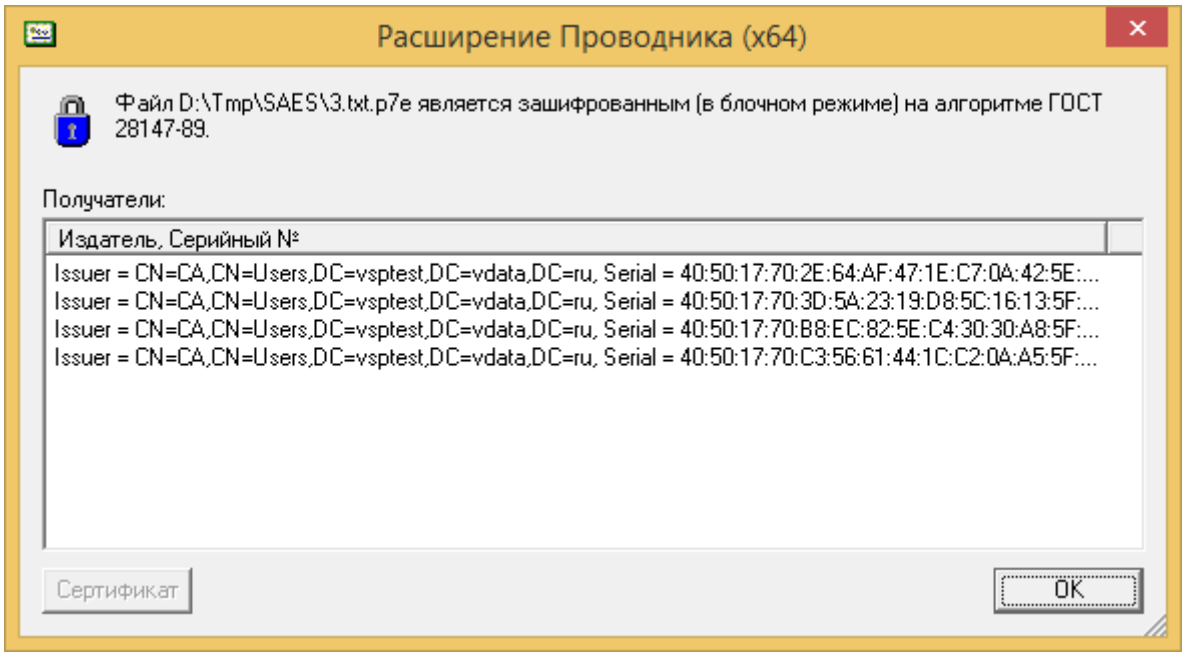

Рисунок 57 – Упрощённый диалог с информацией о зашифрованном файле

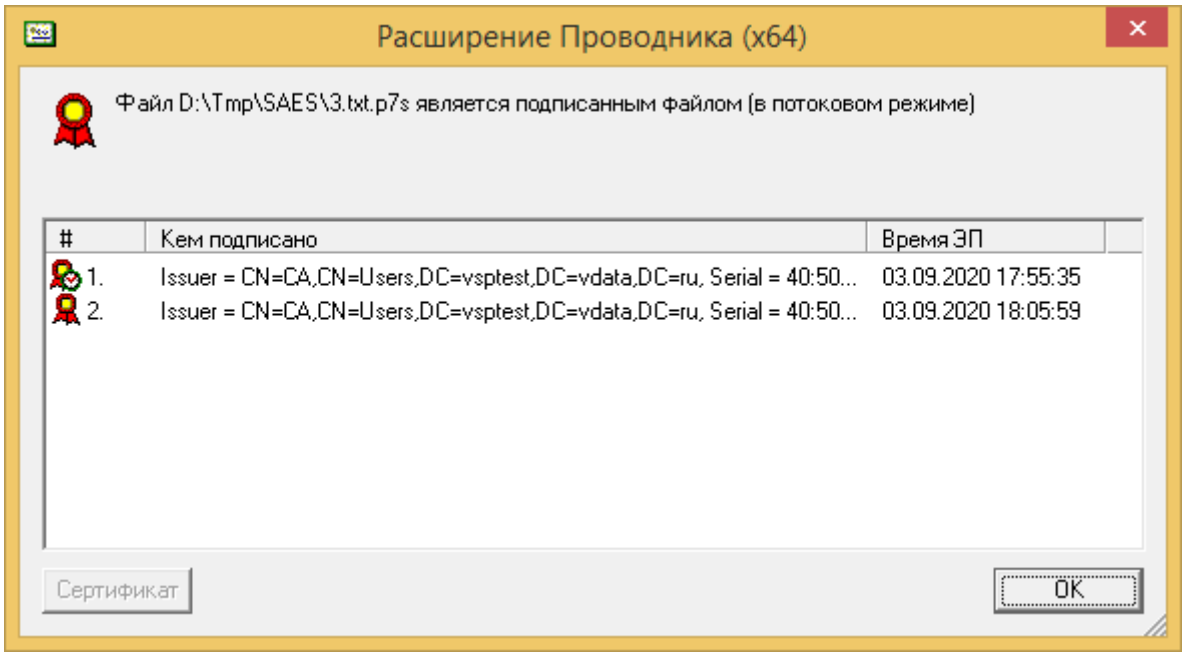

Рисунок 58 – Упрощённый диалог с информацией об ЭП

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 Расширения проводника набор расширений файлов, для которых возможно упрощённое получение криптографической информации, не изменяется.

1.5 Дополнительные функции

1.5.1 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 Расширения проводника 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 59) или сообщение об ошибке.

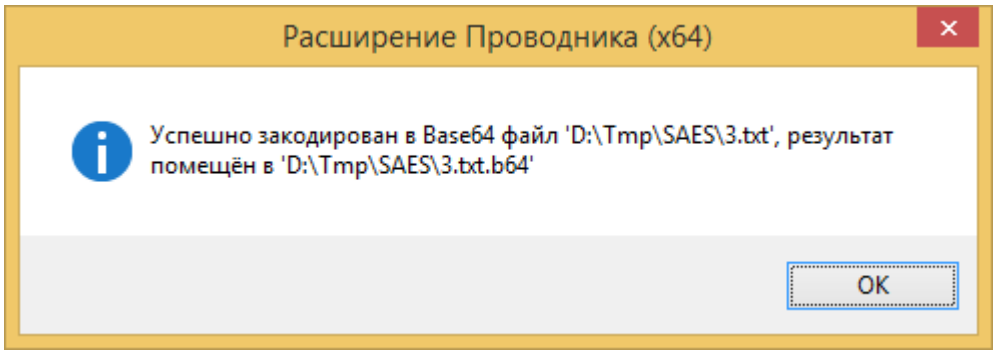

Рисунок 59 – Сообщение об успешном кодировании файла в Base64

Если операция закодирования в формат Base64 производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение (Рисунок 60) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

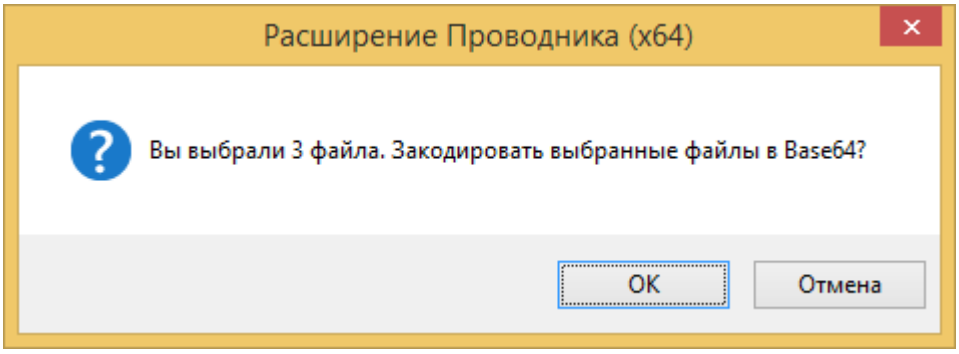

Рисунок 60 – Запрос на закодирование в формат Base64

Затем на экран выдаётся диалог закодирования в формат Base64 (Рисунок 61).

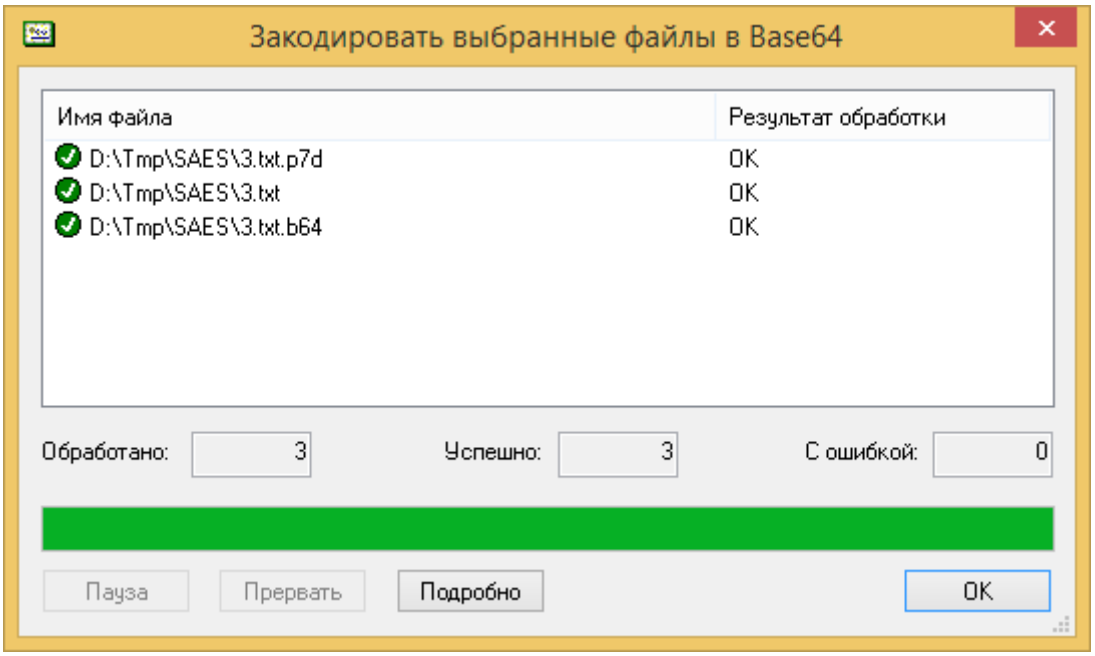

Рисунок 61 – Диалог закодирование в формат Base64

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».

1.5.2 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 Расширения проводника 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 62, Рисунок 63).

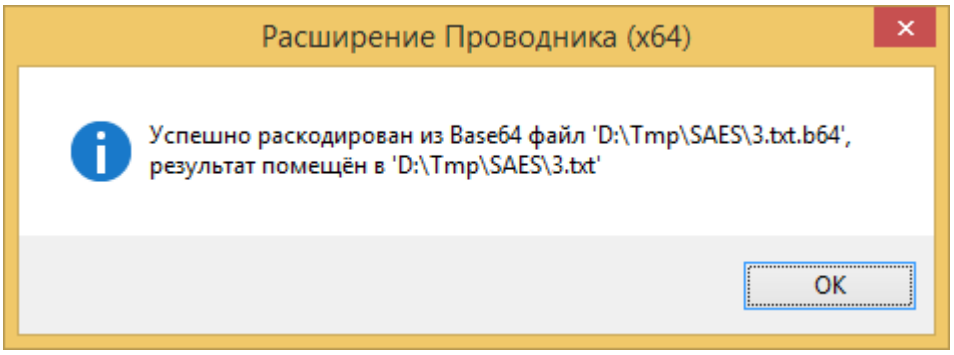

Рисунок 62 – Сообщение об успешном раскодировании файла из Base64

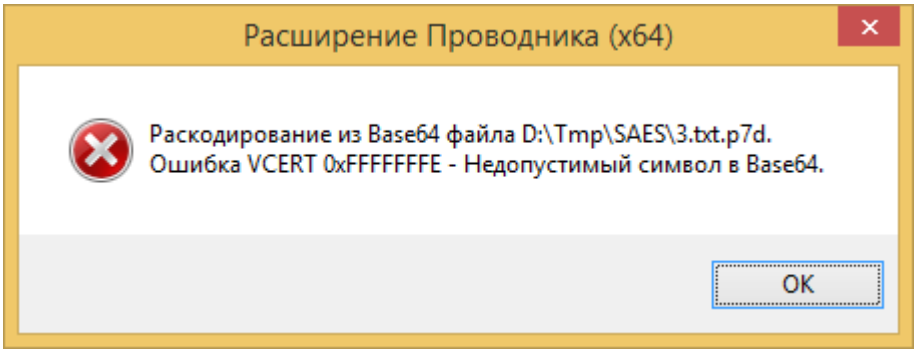

Рисунок 63 – Сообщение об ошибке при раскодировании файла из Base64

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

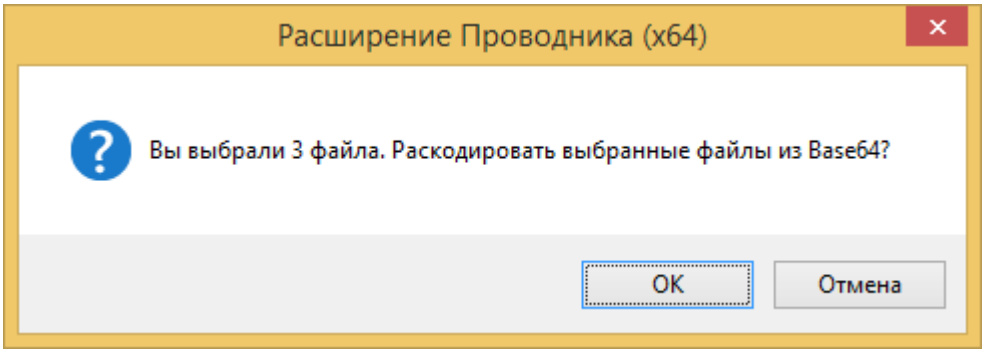

Рисунок 64 – Запрос на раскодирование из формата Base64

Затем на экран выдаётся диалог раскодирования из формата Base64 (Рисунок 65).

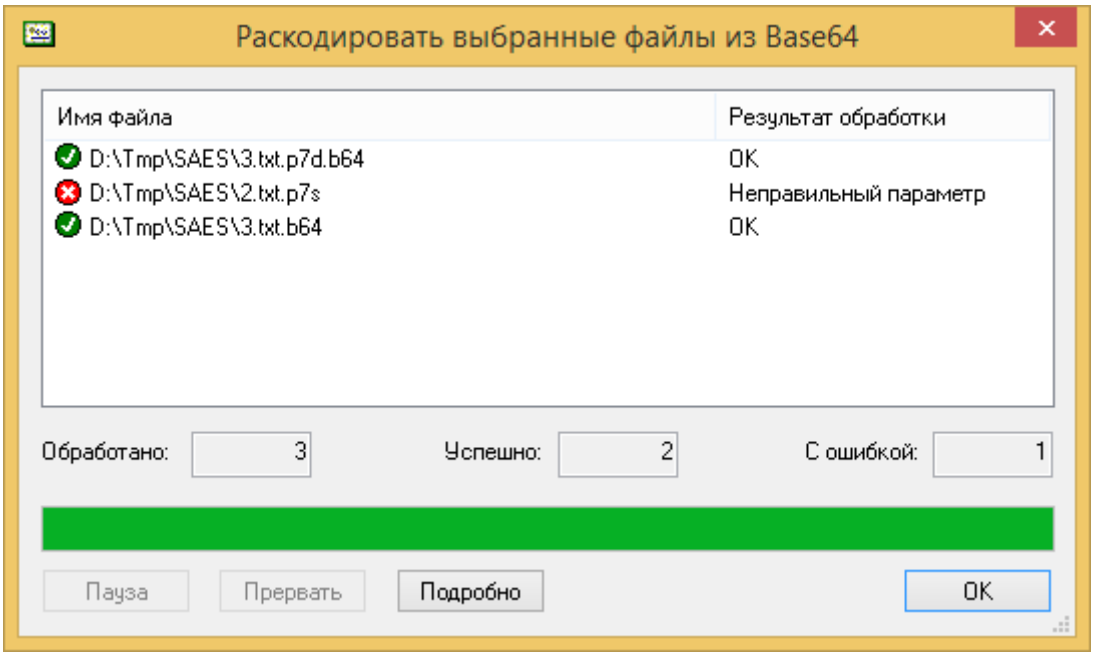

Рисунок 65 – Диалог раскодирования из формата Base64

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».

1.6 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 Расширения проводника пункт «Дополнительно», подпункт «Вычислить хэш». Для выполнения этой операции загрузка ключа не требуется.

Если операция хэширования производится с одним файлом, на экран выдаётся диалоговое окно с результатом (Рисунок 66) или сообщение об ошибке.

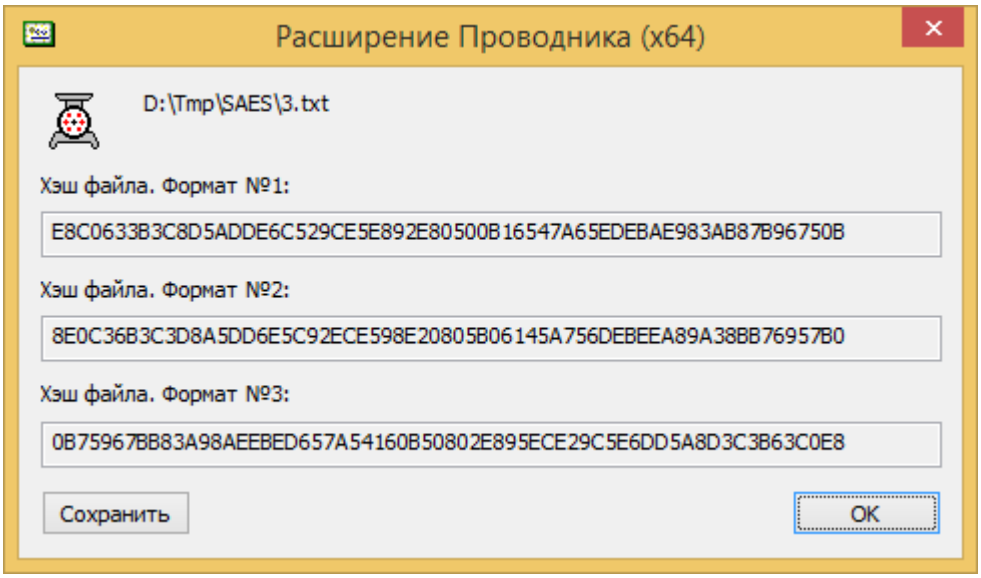

Рисунок 66 – Диалог с результатом хэширования

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.

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 подтверждение (Рисунок 67) при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов».

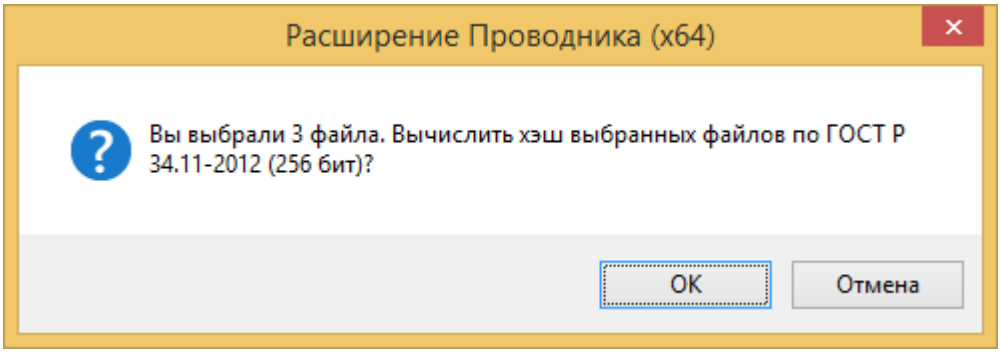

Рисунок 67 – Запрос на хэширование

Затем на экран выдаётся диалог вычисления хэша (Рисунок 68).

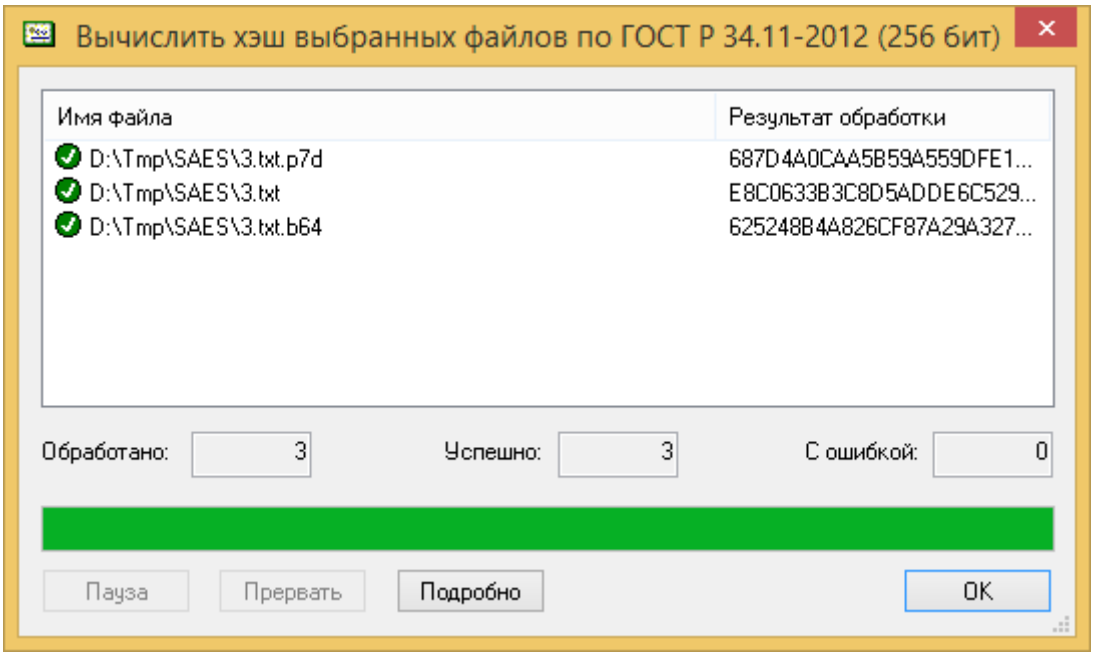

Рисунок 68 – Диалог вычисления хэша

Во второй колонке списка выводится результат 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».

2 ПРОТОКОЛИРОВАНИЕ В РАСШИРЕНИИ ПРОВОДНИКА

В случае если в настройках пользователя не включён режим «Отключить протокол выполненных операций», Расширение проводника 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 — «CPKISHXX», а категория отсутствует. В описании события указывается программный модуль (cpkishxx.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 69, Рисунок 70).

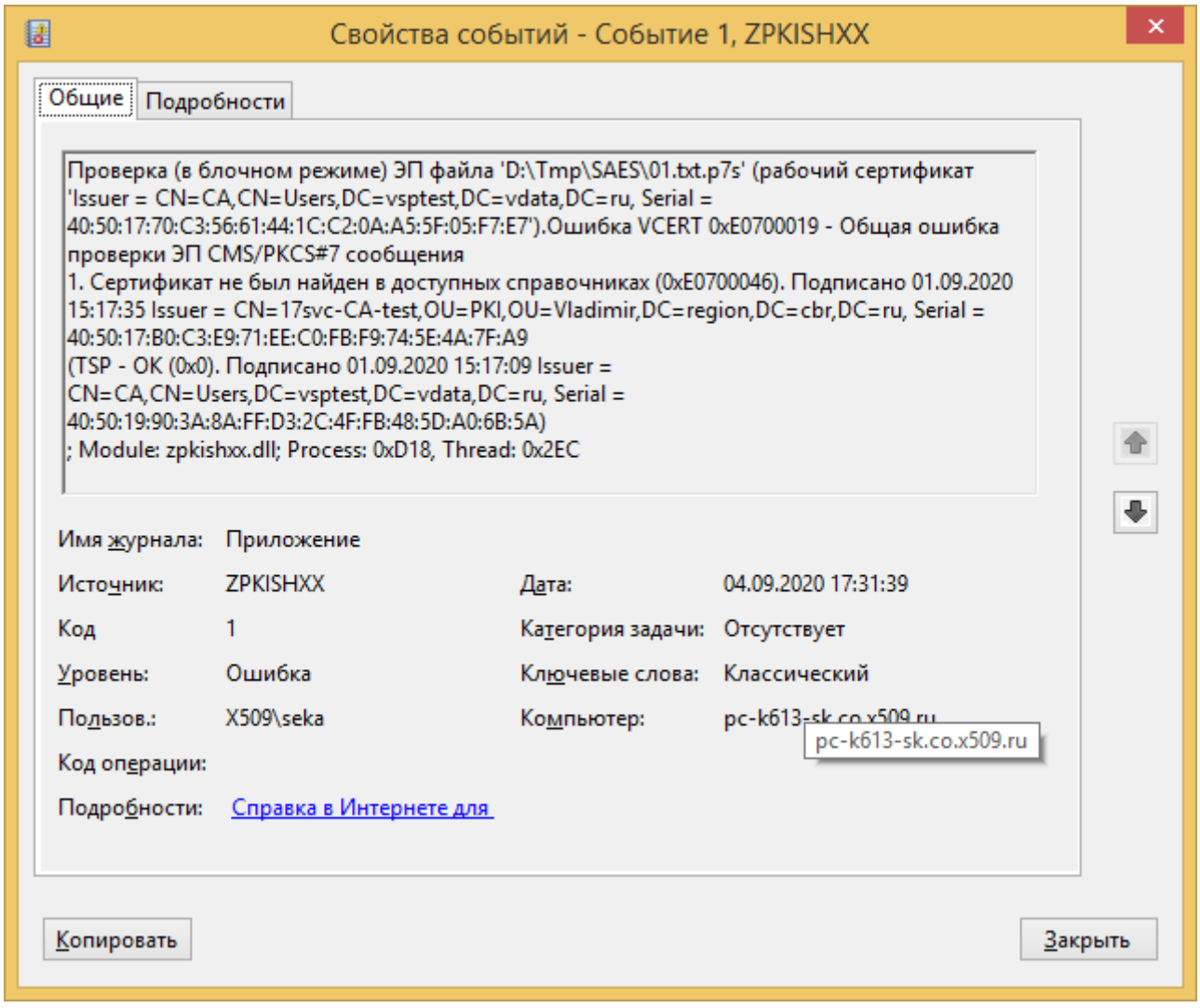

Рисунок 69 – Описание ошибки проверки подписи без стека ошибок

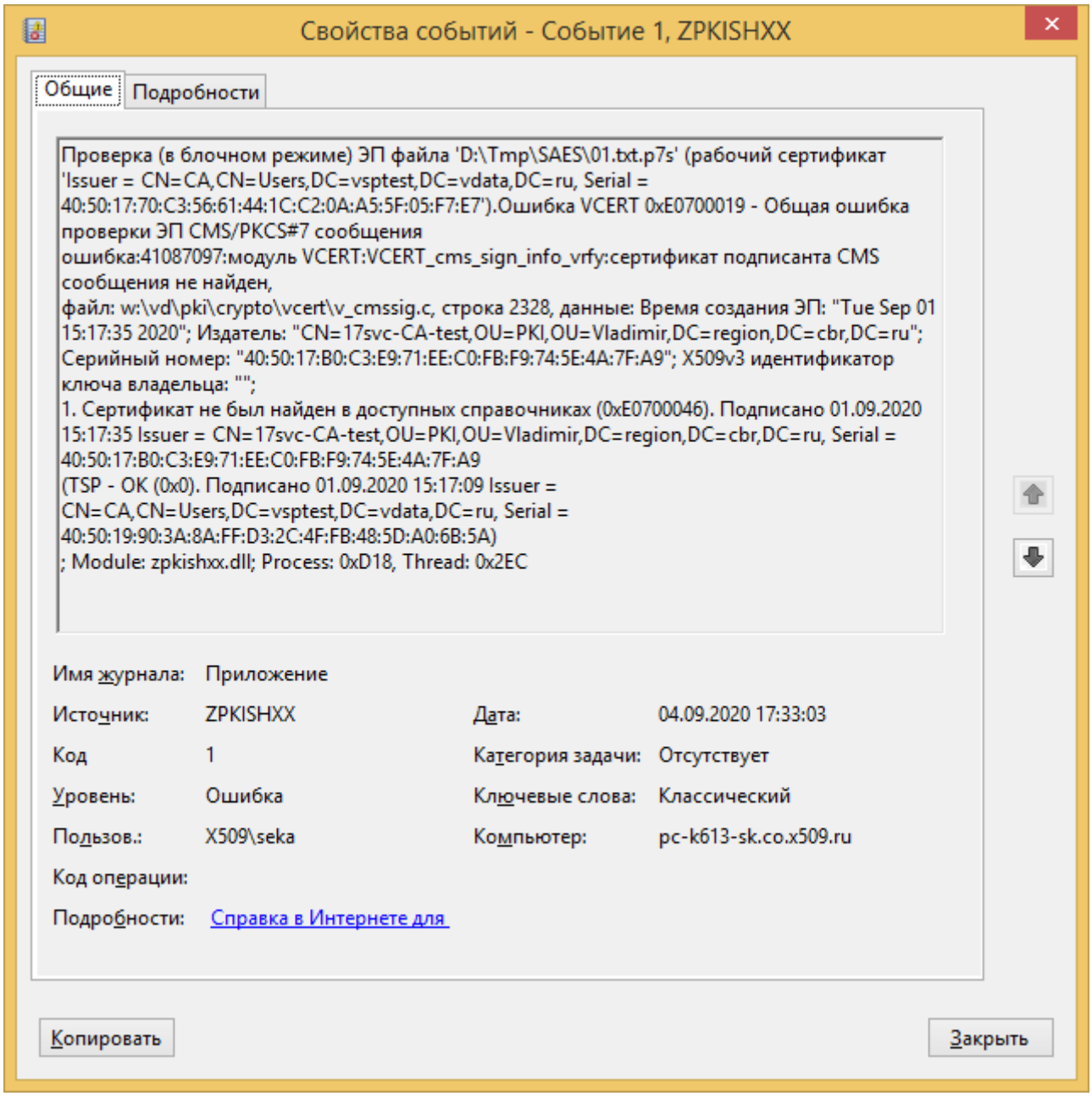

Рисунок 70 – Описание ошибки проверки подписи со стеком ошибок

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ОС	Операционная система (Operating System)
ПК	Программный комплекс
САС	Список аннулированных сертификатов (Certificate Revocation List)
СКЗИ	Средство криптографической защиты информации
ЭП	Электронная подпись (Digital Signature)

ПЕРЕЧЕНЬ РИСУНКОВ

ПЕРЕЧЕНЬ ТАБЛИЦ

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум	№ документа	Входящий № сопроводительного докум и дата	Подп	Дата
Изм	изменённых	заменённых	новых	аннулированных					