УТВЕРЖДЕН

РБ.ЮСКИ.08034-02 34 01-ЛУ

ПРОГРАММНОЕ СРЕДСТВО
«AVEST PERSONAL CRYPTOKIT»
AvPCK

Руководство оператора

РБ.ЮСКИ.08034-02 34 01

Листов 31

Подп. и дата	
Инв.№ дубл	
Взам. инв.№	
Подп. и дата	
Инв.№ подл.	

2015

АННОТАЦИЯ

Настоящий документ содержит описание эксплуатации программного продукта Avest Personal CryptoKit (далее – AvPCK), использующего средства криптографической защиты информации.

Руководство предназначено для широкого круга пользователей: в нем объясняются основные понятия в области криптографической защиты информации, подробно описываются способы решения различных криптографических задач. Описание сопровождается примерами и иллюстрациями.

В документе содержится информация о назначении программы, необходимых условиях ее эксплуатации, приведена последовательность действий оператора, обеспечивающих установку, запуск, выполнение и завершение программы, приведено описание функций, формата и возможных режимов работы программы, а также приведены тексты сообщений, выдаваемых в ходе выполнения программы, описание их содержания и соответствующих действий оператора.

Функциональность программы позволяет решать задачи, связанные с работой с выработкой/проверкой ЭЦП, зашифрованием/расшифрованием файлов с использованием криптопровайдера AvCSP и сертификатов открытых ключей.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ

Программа AvPCK используется совместно с программой «Персональный менеджер сертификатов Авест» и является логическим компонентом инфраструктуры открытых ключей системы криптографической защиты информации (СКЗИ) и, совместно с программой «Центр цифровых сертификатов Авест», обеспечивает организацию системы доверия к открытым ключам участвующих в обмене электронными документами пользователей.

Программа Avest Personal CryptoKit создает удобный пользовательский интерфейс для выполнения криптографических операций шифрования данных, их подписи и проверки корректности ЭЦП.

Функциональные возможности программы:

- формирование и проверка корректности ЭЦП;
- зашифрование и расшифрование файлов;
- добавление подписи к подписанному файлу;
- пакетный режим обработки данных (возможность обработки группы файлов).

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

Программа AvPCK выполняется в среде 32-х разрядных операционных систем Microsoft Windows 98 Second Edition, Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows 7. Требуется также установленный Microsoft Internet Explorer версии не ниже 6.0.

Для использования программы в операционных системах Windows 2000, Windows XP и Windows 2003, Windows Vista, Windows 7 пользователь должен иметь права «Администратор» либо «Пользователь».

Для установки и использования программы требуется наличие нам ПЭВМ пользователя установленных программных продуктов: криптопровайдер AvCSP и Персональный менеджер сертификатов Авест.

3. ИНСТАЛЛЯЦИЯ AVPCK

Для установки программы Avest Personal CryptoKit необходимо:

- проверить наличие установленных на компьютере криптопровайдера AvCSP и программы «Персональный менеджер сертификатов Авест» («Пуск» →«Программы» → «Авест»);
- необходимо иметь право производить установку программного обеспечения в среде операционной системы, т.е. принадлежать к группе «Администраторы».

Действия по установке программы Avest Personal CryptoKit:

Запустите программу avpck_setup.exe с дистрибутивного компакт-диска. Для запуска программы воспользуйтесь пунктом «Выполнить» в основном меню Windows «Пуск», либо сделайте это с помощью возможностей стандартного приложения Windows «Проводник».

В начале установки выводится стандартное окно с информацией о предлагаемом к установке программном обеспечении (см. Рисунок 1).

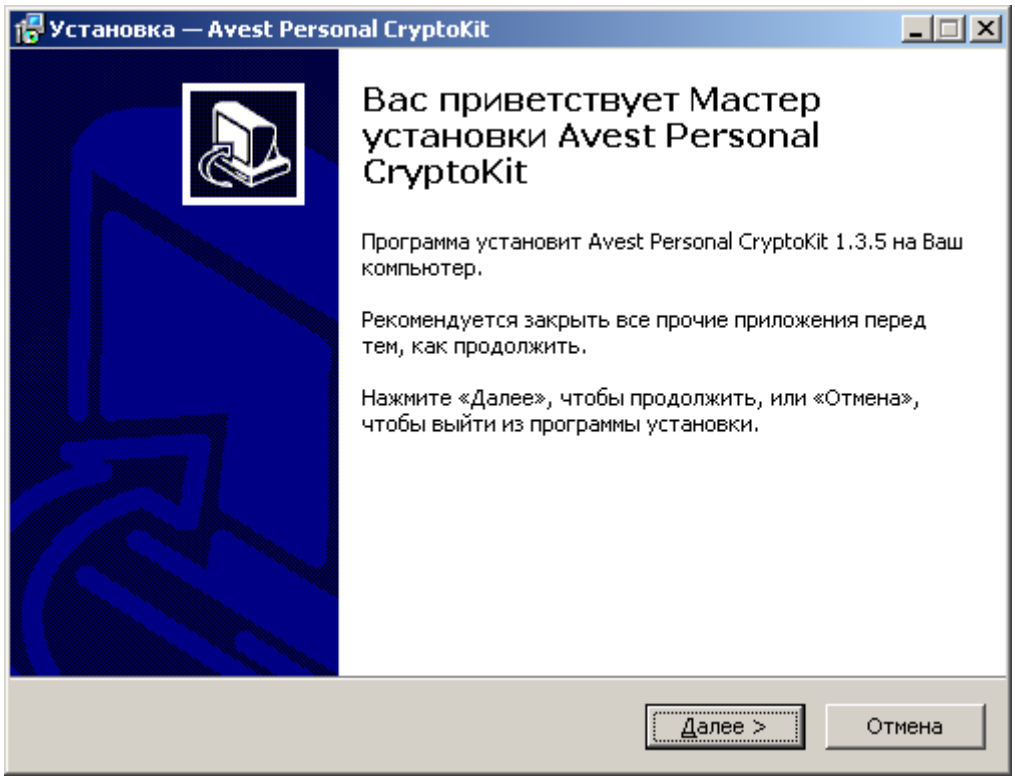

Рисунок 1 Начало установки Avest Personal CryptoKit

В следующем окне будет приведено лицензионное соглашение, условия которого рекомендуется принять и нажать кнопку «Далее» для продолжения процедуры инсталляции программы на Ваш компьютер (см. Рисунок 2).

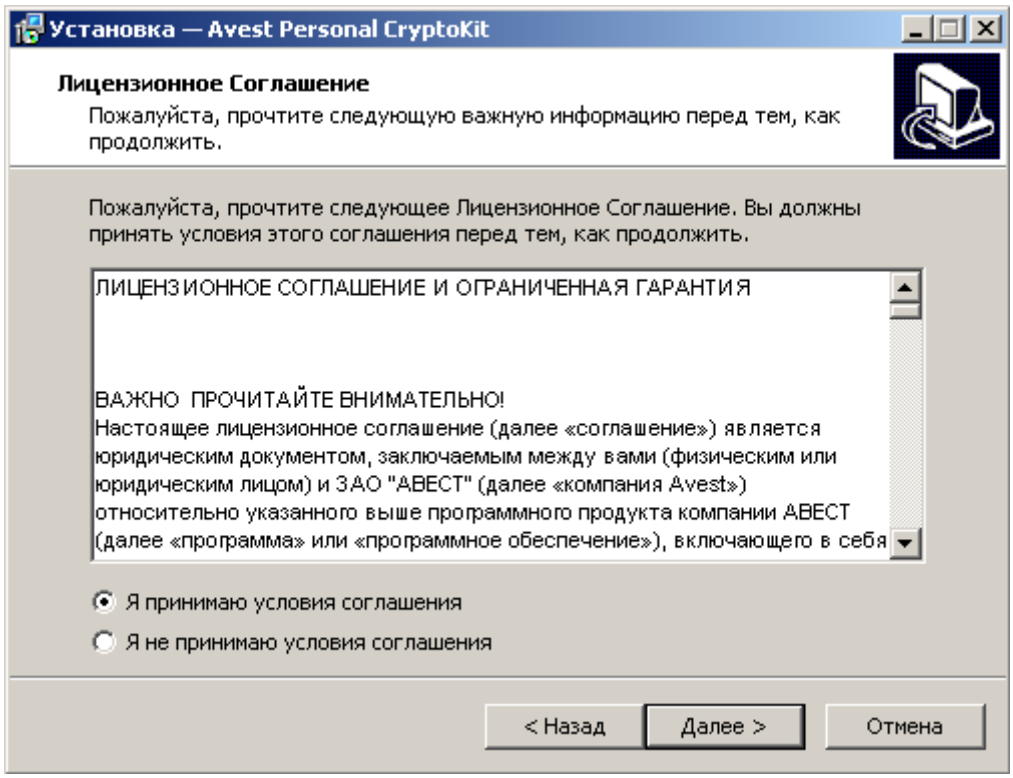

Рисунок 2 Лицензионное соглашение

В случае если Вы не согласны с условиями соглашения, нажмите кнопку «Отмена» для выхода из программы установки.

Далее следует выбрать папку в меню «Пуск», в которой программа создаст необходимые ярлыки (см. Рисунок 3

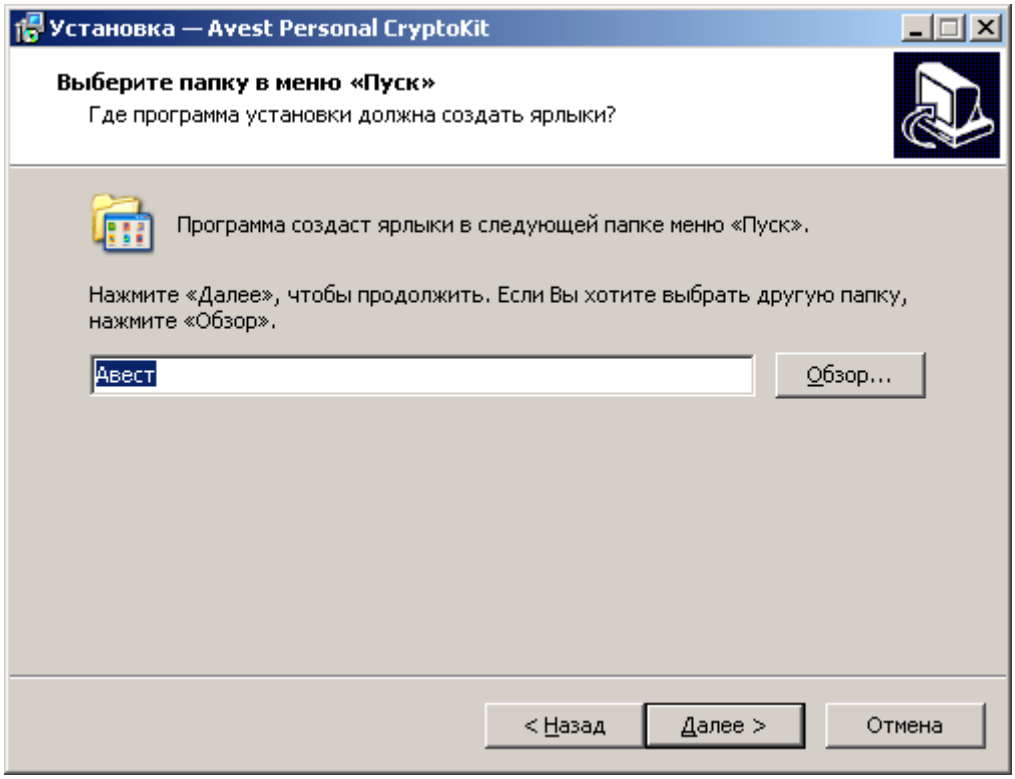

Рисунок 3 Выбор папки в меню «Пуск»

После этого следует выбрать персональный менеджер сертификатов, для которого предназначена установка AvPCK. Если на компьютере установлено несколько версий менеджеров, то в выпадающем списке можно выбрать нужный. Проконтролировать правильность выбора можно просмотрев информацию о пути установки программного обеспечения (см. Рисунок 4).

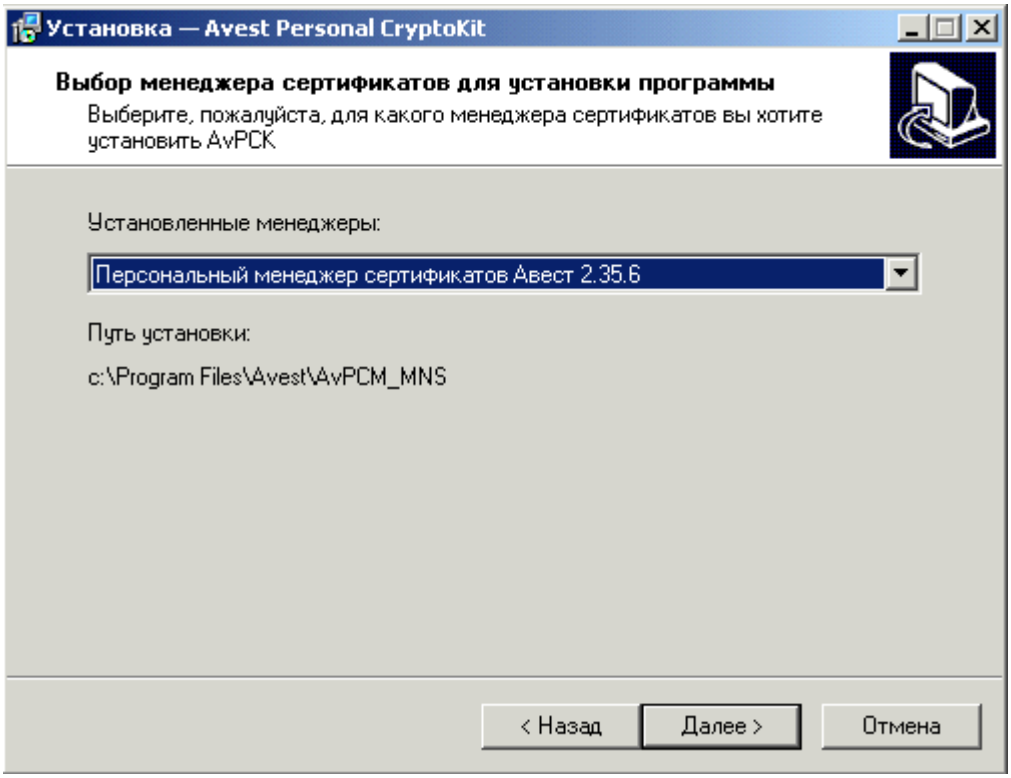

Рисунок 4 Выбор персонального менеджера

После этого всё готово к установке Avest Personal CryptoKit. Нажмите «Установить», чтобы проинсталлировать программу, или «Назад», если нужно изменить опции установки (см. Рисунок 5).

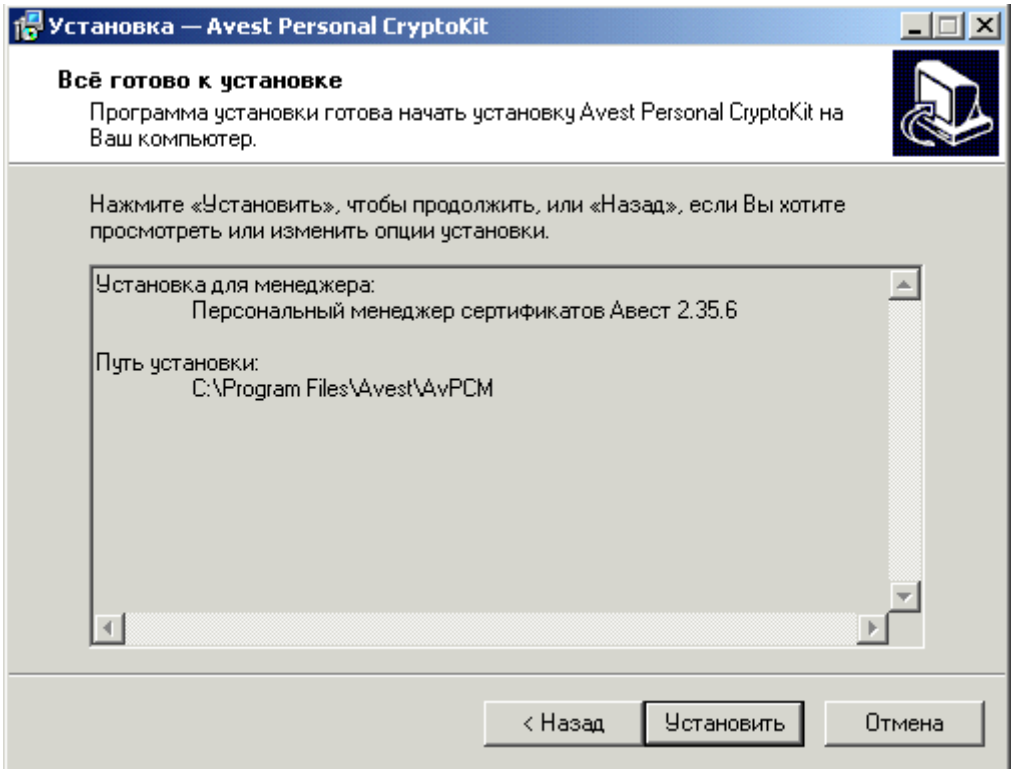

Рисунок 5 Всё готово к установке Avest Personal CryptoKit

После нажатия кнопки «Установить» начнёт процесс установки программы. В процессе утсановки в окне мастера установки отображается информация о текущем этапе и выполняемых действиях (см. Рисунок 6).

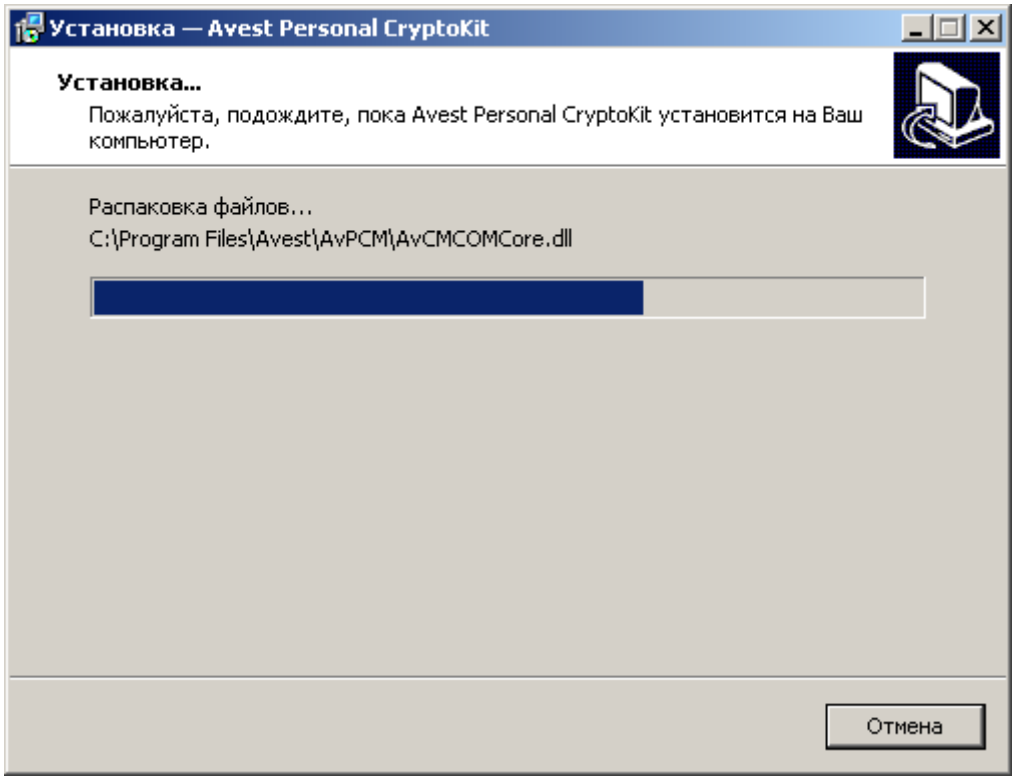

Рисунок 6 Установка

Когда работа мастера установки будет завершена, об это сообщается в последнем окне мастера установки программы. В последнем окне мастера установки программы надо нажать кнопку «Завершить» (см. Рисунок 7).

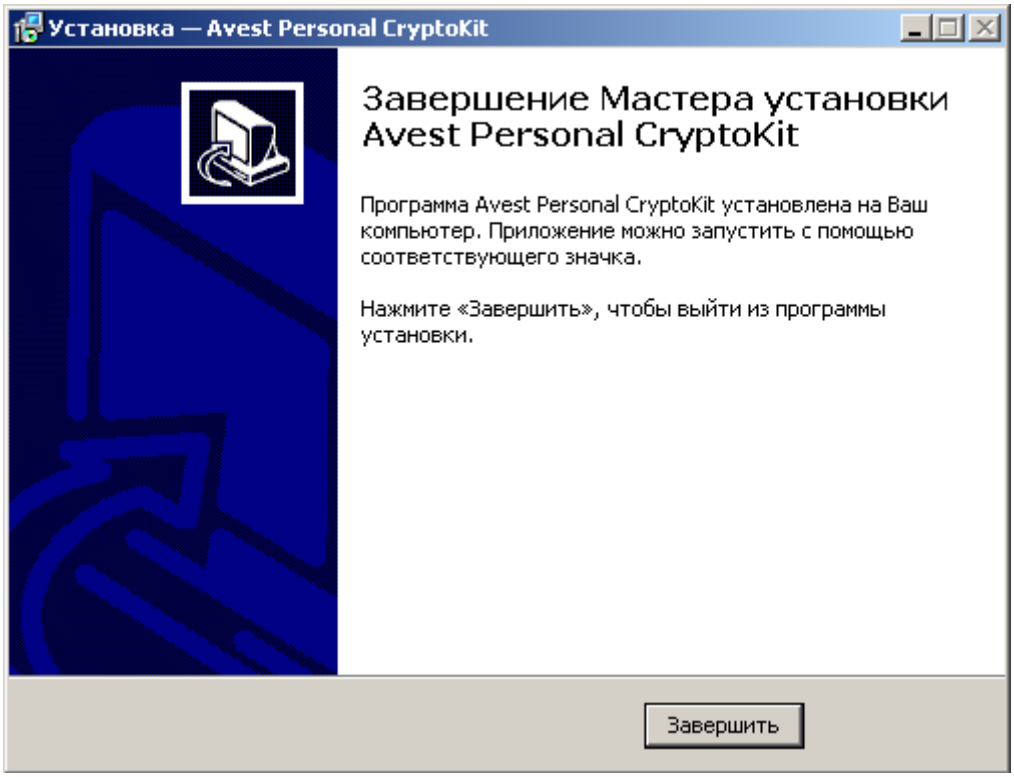

Рисунок 7 Завершение работы мастера установки

4. ЗАПУСК И ОСТАНОВКА ПРОГРАММЫ AVPCK

После того как компонент AvPCK был успешно установлен на компьютер, пользователь может произвести активизацию (запуск) программы и получить доступ к опциям Avest Personal CryptoKit двумя способами:

1. щелкнув по какому - либо из файлов в диалоговых окнах ОС Windows и выбрав нужный пункт в контекстном меню, где после установки появились четыре новые команды (см. Рисунок 8):

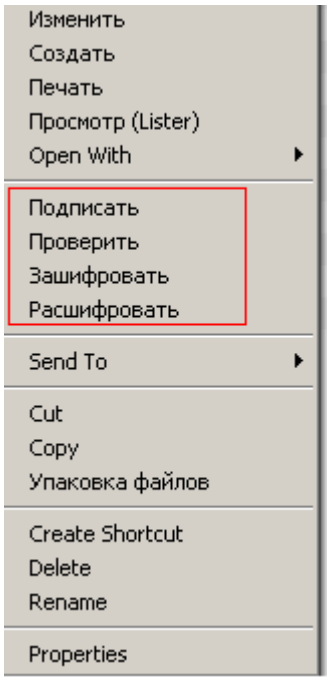

Рисунок 8 Новые команды

2. Выполнив команду Пуск →Программы →Авест → Personal CryptoKit монитор.

В системном трее появится значок запущенной программы Avest Personal CryptoKit.exe. Щёлкнув по нему правой клавишей мыши можно вызвать меню программы (см. Рисунок 9).

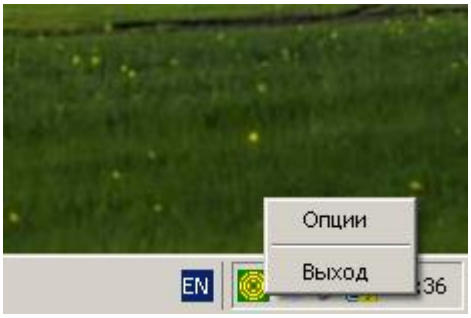

Рисунок 9 Меню программы Avest Personal CryptoKit

Для того чтобы выйти из программы Avest Personal CryptoKit, нужно вызвать меню программы, как описано выше, и выбрать Выход (см. Рисунок 9). Программа завершит свою работу.

5. НАСТРОЙКИ AVPCK

Запустив программу одним из способов, описанных в разделе Запуск и остановка программы AvPCK, пользователь получает возможность изменить настройки программы. Для этого нужно нажать правой кнопкой мыши на значок программы в системном трее и в появившемся меню (см. Рисунок 9) выбрать пункт Опции.

В появившемся окне настроек программы AvPCK (см. Рисунок 10) пользователь может поменять настройки программы или ознакомится с содержимым журнала работы. Подробное описание настроек программы по вкладкам окна даётся ниже.

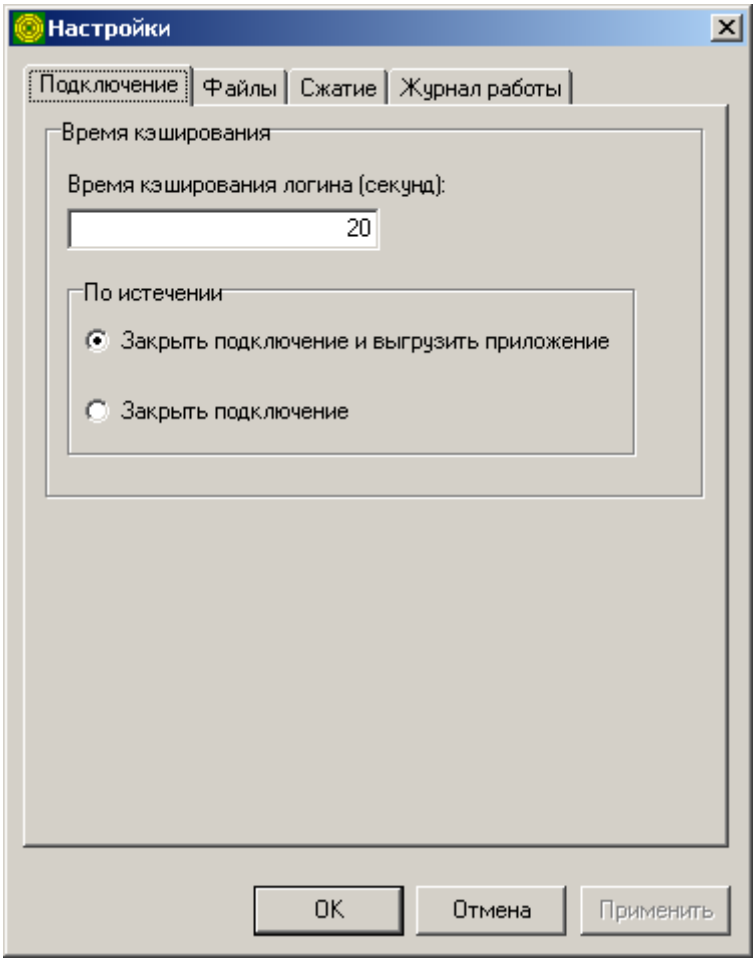

Рисунок 10 Окно настроек AvPCK

5.1 Вкладка «Подключение»

Вкладка Подключение (см. Рисунок 10) позволяет задать время кэширования логина (в секундах) – время, на которое система «запоминает» введённый пароль для контейнера с личным ключом.

Также на этой вкладке возможен выбор действия программы по истечении времени кэширования: программа может закрыть подключение к личному ключу, либо закроет подключение и закончит работу программы, выгрузив её из памяти.

После указания желаемых настроек нужно нажать кнопку «Применить».

5.2 Вкладка «Файлы»

На вкладке Файлы (см. Рисунок 11) можно поменять настройки, касающиеся работы AvPCK с файлами:

- Выбор режима подписи (подпись и исходный файл в одном файле или подпись в отдельном файле) определяет каким образом будет происходить подпись: будет ли подпись сохранена вместе с исходным файлом в один общий файл с расширением *.sgn или будет сохранена отдельно (см. раздел ***6.1 Выработка ЭЦП***)
- `Помещать всю цепочку сертификатов в подписанный файл` – сохранется ли цепочка сертификат в файл при подписи;
- `Удалять исходный файл после зашифрования` – нужно ли удалять исходный файл после того, как он был зашифрован;
- `Запрашивать подтверждение на перезапись` (по умолчанию включена) - позволяет пользователю выбрать нужно ли перезаписывать выходной файл, если он уже существует. Если опция отключена – файл по всегда переписывается без запроса подтверждения;
- `Временные файлы` – определяет где будут хранится создаваемые программой в процессе работы временные файлы. Кроме того, можно очистить данную папку с помощью кнопки Очистить папку.

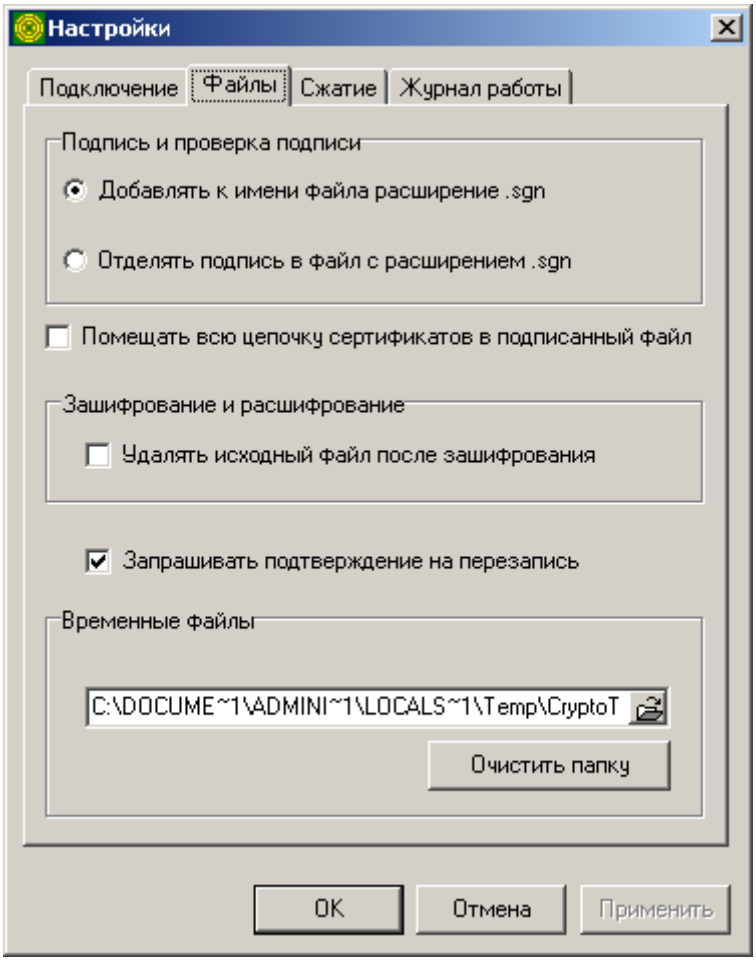

Рисунок 11 Вкладка Файлы

После указания желаемых настроек нужно нажать кнопку «Применить».

5.3 Вкладка «Сжатие»

На вкладке Сжатие (см. Рисунок 12) можно выбрать степень сжатия при шифровании: Не сжимать, Быстрое, Среднее и Максимальное.

В строке Не сжимать файлы с расширением через точку с запятой можно указать расширения файлов, к которым процедура сжатия применятся не будет. По умолчанию там указаны наиболее распространённые расширения архивных файлов.

Примечание. При зашифровании файлов, размер которых превышает 700 МБ, необходимо в настройках выставить опцию «**Не сжимать**», в противном случае будет выдаваться ошибка «Файл имеет слишком большой размер».

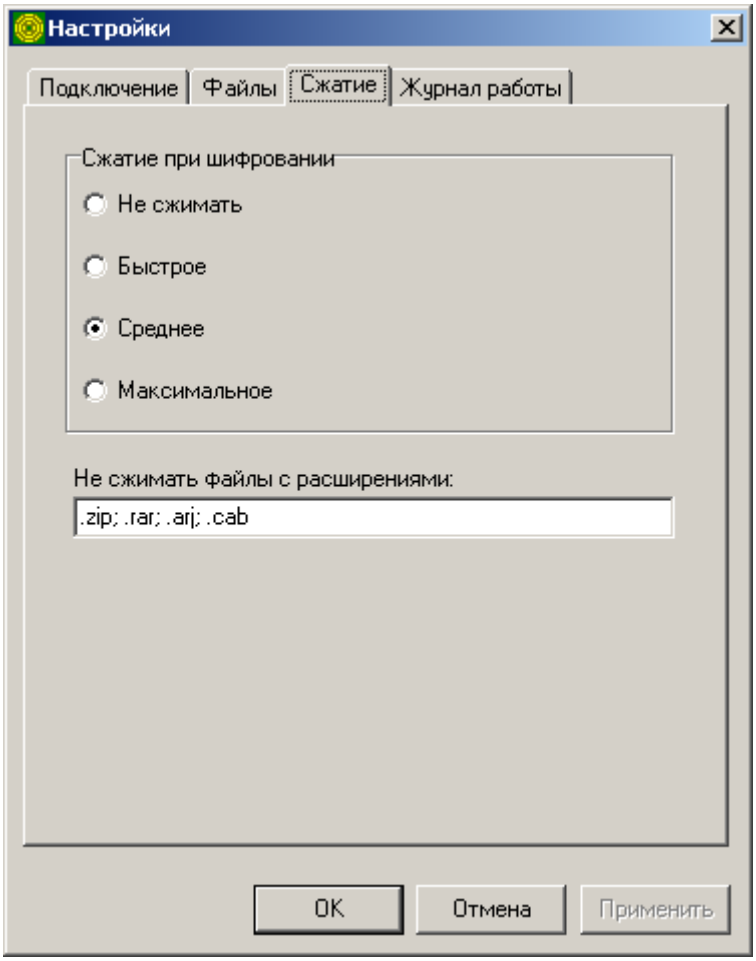

Рисунок 12 Вкладка Сжатие

После указания желаемых настроек нужно нажать кнопку «Применить».

5.4 Вкладка «Журнал работы»

На вкладке Журнал работы (см. Рисунок 13) существует возможность регулировать общие настройки файла журнала, как метод ведения журнала: дописывать в конец существующего файла, создавать каждый раз новый журнал (как с созданием резервной копии существующего, так и без), либо не использовать вовсе. Кроме того, можно указать название и размещение файла журнала (по умолчанию журнал называется AvPCK.log и помещается в папку, куда была установлена программа).

Нажав на кнопку Просмотр журнала можно ознакомится с содержимым журнала работы (если он был включен).

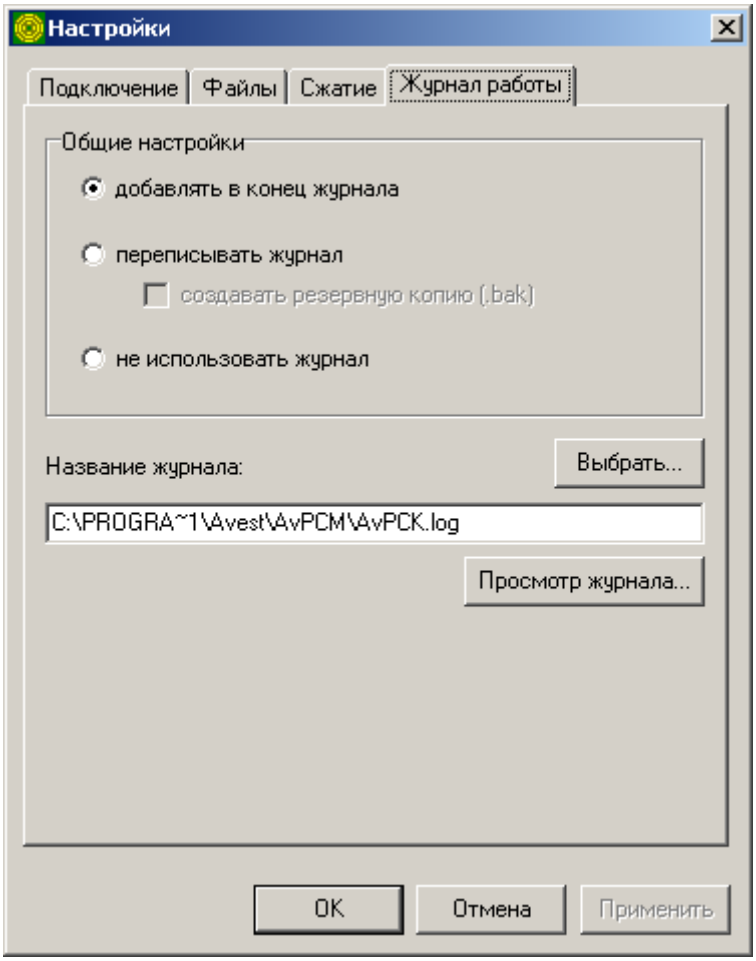

Рисунок 13 Вкладка Журнала работы

Нажав на кнопку Просмотр журнала можно ознакомится с содержимым журнала работы (если он был включен).

После указания желаемых настроек нужно нажать кнопку «Применить».

6. КРИПТОГРАФИЧЕСКИЕ ОПЕРАЦИИ

Перед тем как производить над файлами какие-либо криптографические операции следует учесть, что на диске должно быть достаточное количество свободного места, как минимум равное объёму обрабатываемых файлов. При нехватке места для создаваемого файла, будет выдаваться сообщение об ошибке.

При проведении процедур выработки/проверки ЭЦП, шифрования для файлов больших размеров необходимо учитытывать технические параметры ПЭВМ, на которой проводятся вычисления. В общем случае, чем больше размер файла, тем более длительное время потребуется на выполнение криптографической операции.

Avest Personal CryptoKit может проводить следующие операции:

- Подпись файлов (максимальный размер подписываемого файла зависит от режима, см. ниже ***6.1 Выработка ЭЦП***).

- Проверка подписи;

- Зашифрование файлов (максимальный размер зашифровываемого файла теоретически ограничен размером 2 в степени 63 байт ($9.22337204 \times 10^{18}$);

- Расшифрование ранее зашифрованных файлов.

Также есть возможность комбинировать проводимые операции. К примеру провести операцию подписи, а затем подписанный файл зашифровать.

6.1 Выработка ЭЦП

Существует два режима выработки ЭЦП:

detach - с отделением подписи файла в файл sgn (максимальный размер подписываемого файла теоретически ограничен размером 2 в степени 63 байт ($9.22337204 \times 10^{18}$).

attach - с добавлением к имени файла расширения sgn, когда и файл и его ф (максимальный размер подписываемого файла составляет 700 Mb).

Для того, чтобы произвести операцию подписи файла, нужно вызвать контекстное меню этого файла и выбрать команду Подписать (см. Рисунок 8).

В появившемся окне мастера выработки ЭЦП необходимо указать в разделе Входные файлы все файлы, которые нужно подписать (см.Рисунок 14). При необходимости, их количество можно регулировать кнопками «Добавить файл» и «Удалить файл», которые находятся в нижней части окна. Также в этом окне можно увидеть общее количество файлов подготовленных для подписи. Эта информация отображается в строке Всего файлов.

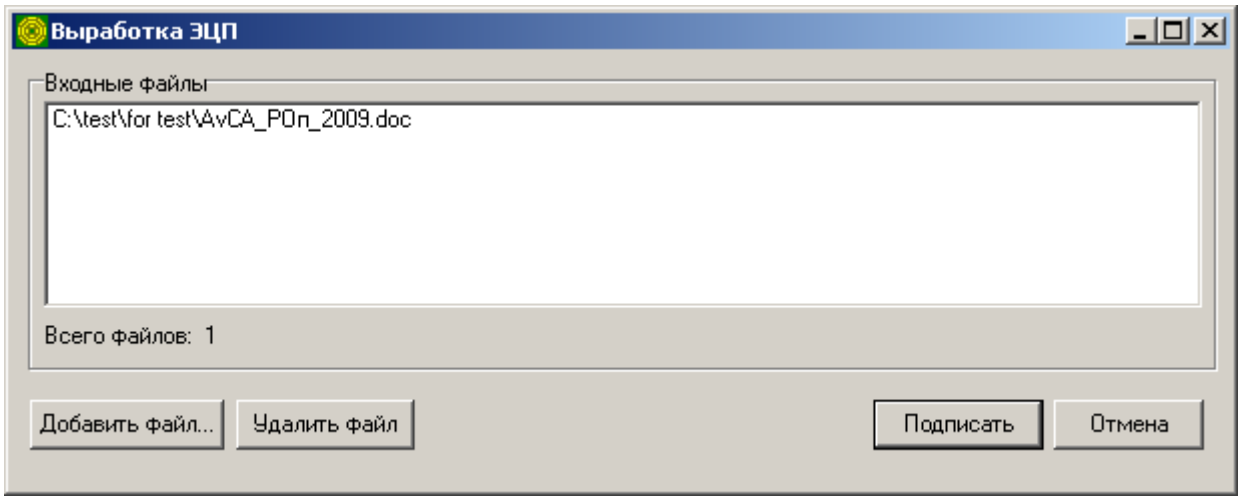

Рисунок 14 Выработка ЭЦП

Сверив количество и имена файлов, под которыми вы хотите выработать электронно-цифровую подпись, нужно нажать кнопку «Подписать».

Если это первое подключения личного сертификата, или истекло время кэширования пароля с момента проведения последней операции с помощью программы AvPCK, то CryptoTray выдаст окно авторизации пользователя (см. Рисунок 15). В окне нужно выбрать личный сертификат для авторизации и нажать кнопку «ОК».

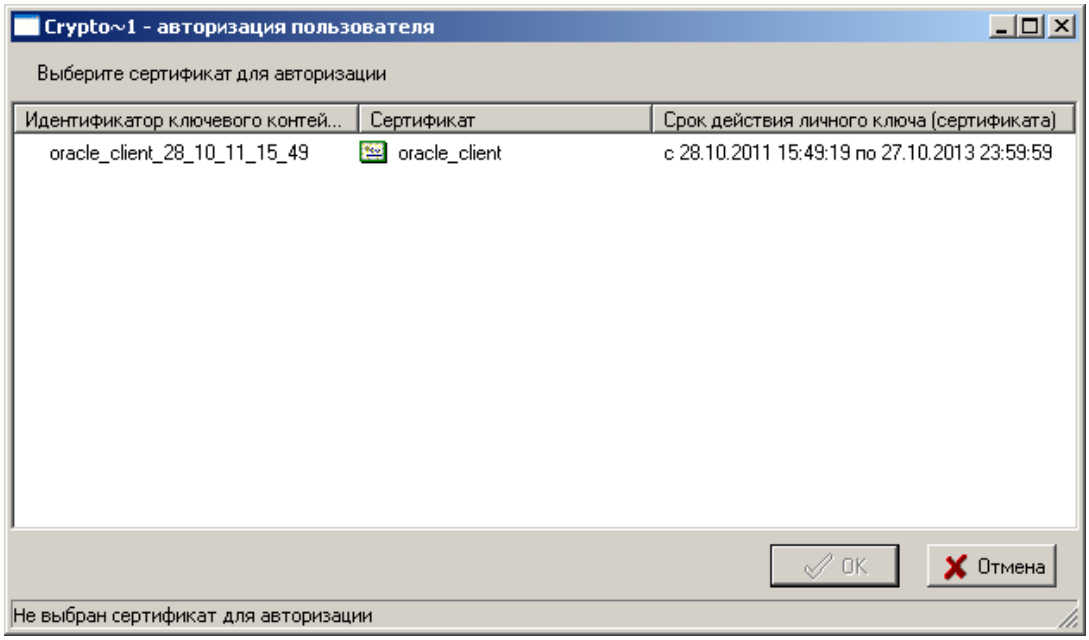

Рисунок 15 Авторизация пользователя

Затем появится окно доступа к контейнеру личных ключей, в котором нужно будет выбрать тип носителя и ввести пароль доступа к контейнеру личных ключей. Пароль сохранится в системе на время, соответствующее времени кэширования логина, которое указано в настройках Avest Personal CryptoKit на Вкладке Подключение.

В результате операции выработки подписи, в зависимости от того, какие опции были выбраны, мы получим либо подписанный файл с расширением *.sgn, либо исходный файл и подпись в виде отдельного файла с расширением *.sgn.

После процедуры подписи файла на экран будет выведено окно журнала работы (см. Рисунок 16). После ознакомления с результатом выработки ЭЦП необходимо нажать кнопку «Завершить».

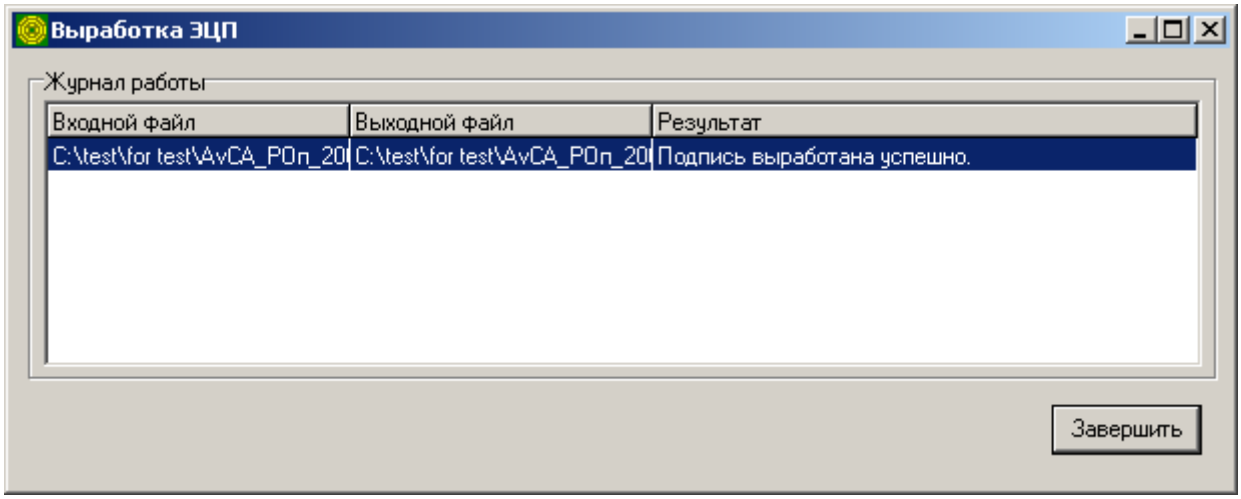

Рисунок 16 Результат выработки ЭЦП

6.2 Проверка ЭЦП

Внимание! Проверять ЭЦП можно только у тех файлов, которые ранее были подписаны кем либо, обычно, такие файлы имеют расширение *.sgn. Если же будет произведена попытка проверить файл, который не содержит подписи, то программа выдаст сообщение Неверный формат.

Для того, чтобы произвести операцию проверки ЭЦП, нужно вызвать контекстное меню этого файла и выбрать команду Проверить (см. Рисунок 8), после чего появится окно мастера проверки ЭЦП (см. Рисунок 17).

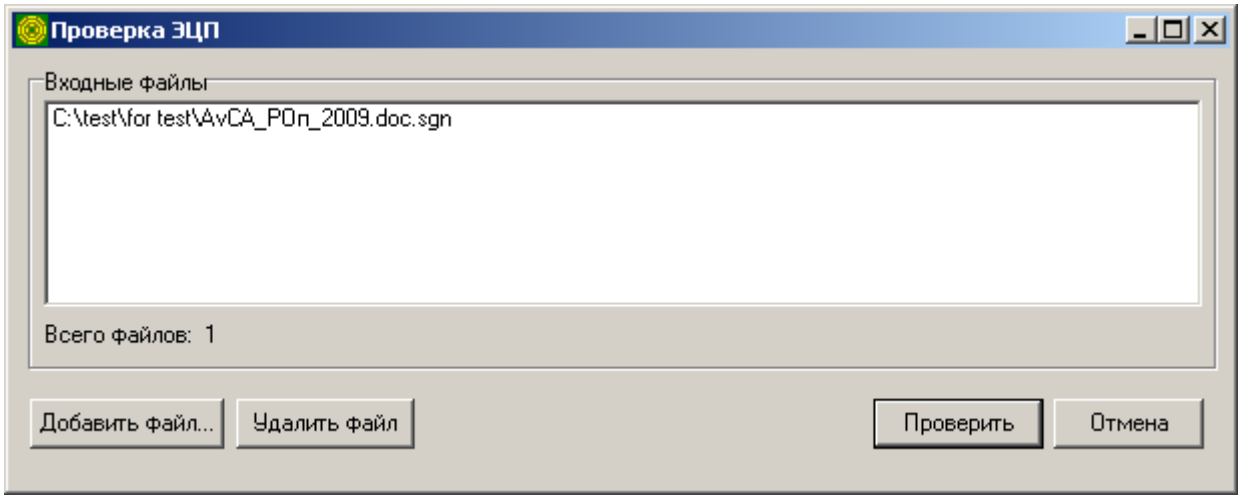

Рисунок 17 Проверка ЭЦП

В разделе Входные файлы нужно указать все файлы, подпись под которыми нужно проверить. При необходимости, их количество можно регулировать кнопками «Добавить файл» и «Удалить файл», которые находятся в нижней части окна. Также в этом окне можно увидеть общее количество файлов подготовленных для проверки подписи. Эта информация отображается в строке Всего файлов.

Сверив количество и имена файлов, у которых вы хотите проверить электронно-цифровую подпись, нужно нажать кнопку «Проверить» (см. Рисунок 17).

Если это первое подключения личного сертификата, или истекло время кэширования пароля с момента проведения последней операции с помощью программы AvPCK, то CryptoTray выдаст окно авторизации пользователя (см. Рисунок 15). В окне нужно выбрать личный сертификат для авторизации и нажать кнопку «ОК».

Затем появится окно доступа к контейнеру личных ключей, в котором нужно будет выбрать тип носителя и ввести пароль доступа к контейнеру личных ключей. Пароль сохранится в системе на время, соответствующее времени кэширования логина, которое указано в настройках Avest Personal CryptoKit на вкладке Подключение.

После процедуры проверки подписи файла на экран будет выведено окно журнала работы (см. Рисунок 18). После ознакомления с результатом выработки ЭЦП необходимо нажать кнопку «Завершить».

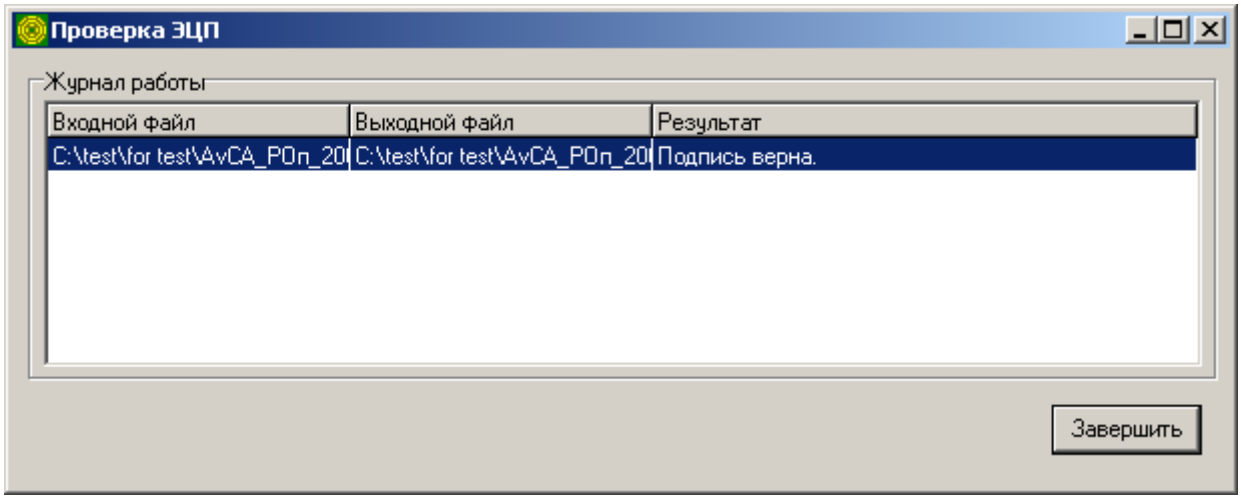

Рисунок 18 Результат проверки ЭЦП

6.3 Зашифрование

При зашифровании файлов, по размеру превышающих 700 мегабайт, необходимо отключать сжатие (выставлять в настройках уровень «Не сжимать»). Если этого не сделать, то будет выдаваться ошибка «Файл имеет слишком большой размер».

Для того, чтобы произвести операцию зашифрования, нужно вызвать контекстное меню этого файла и выбрать команду Зашифровать(см. Рисунок 8), после чего появится окно мастера зашифрования (см. Рисунок 19).

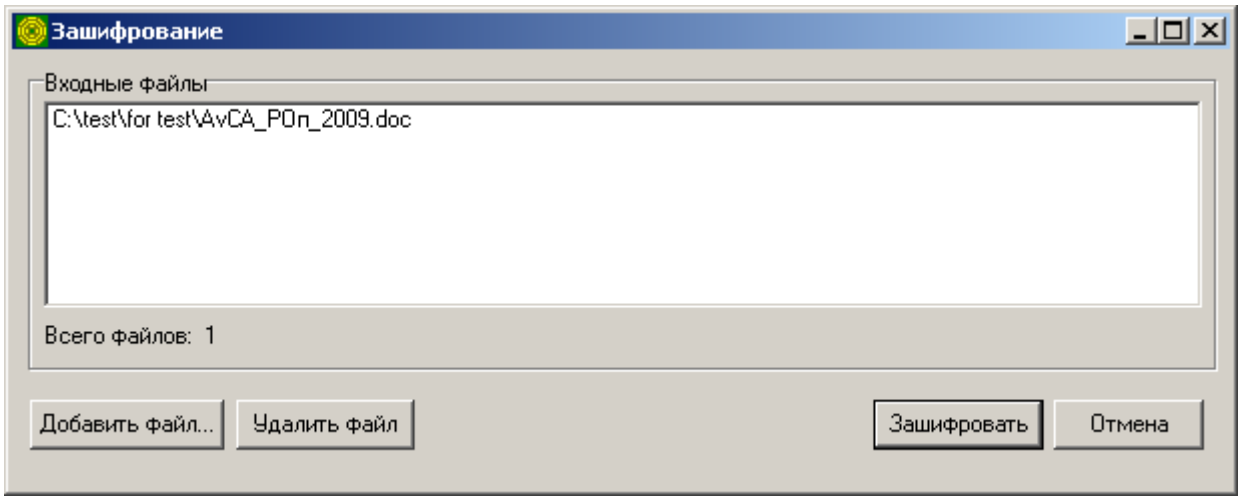

Рисунок 19 Зашифрование файла

В разделе Входные файлы нужно указать все файлы, которые требуется зашифровать. При необходимости, их количество можно регулировать кнопками «Добавить файл» и «Удалить файл», которые находятся в нижней части окна. Также в этом окне можно увидеть общее количество файлов подготовленных для зашифрования. Эта информация отображается в строке Всего файлов.

Сверив количество и имена файлов, у которых вы хотите зашифровать, нужно нажать кнопку «Зашифровать» (см. Рисунок 19).

Если это первое подключения личного сертификата, или истекло время кэширования пароля с момента проведения последней операции с помощью программы AvPCK, то CryptoTray выдаст окно авторизации пользователя (см. Рисунок 15). В окне нужно выбрать личный сертификат для авторизации и нажать кнопку «ОК». Затем появится окно доступа к контейнеру личных ключей, в котором нужно будет выбрать тип носителя и ввести пароль доступа к контейнеру личных ключей. Пароль сохранится в системе на время,

соответствующее времени кэширования логина, которое указано в настройках Avest Personal CryptoKit на Вкладке Подключение.

Перед вами появится окно выбора сертификатов для зашифрования (см. Рисунок 20). Выбор сертификата абонента, который находится в списке сертификатов в верхней половине окна, происходит двойным щелчком по нему. После этого сертификат перемещается в нижнюю половину окна, в которой формируется список абонентов, которые будут иметь возможность расшифровать файл. Количество абонентов может быть любым.

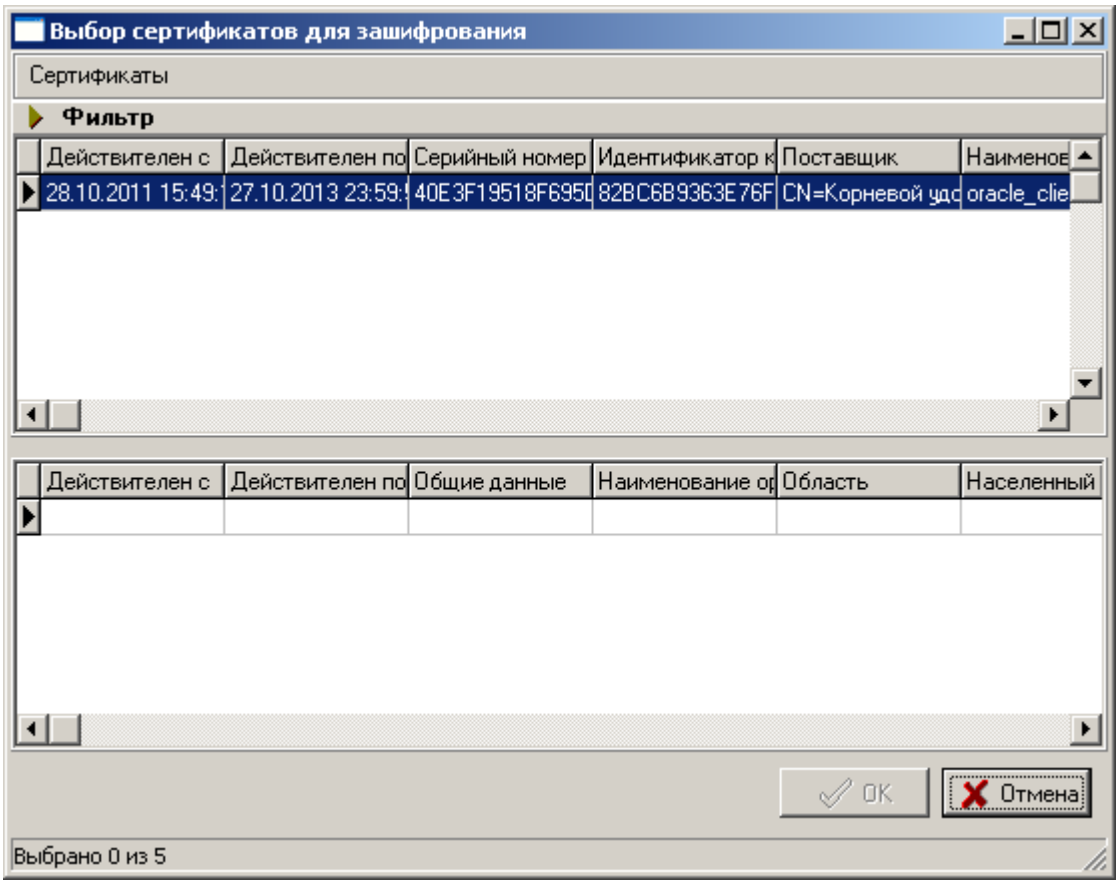

Рисунок 20 Выбор сертификата для зашифрования

Удаление из списка абонентов происходит с помощью двойного щелчка по «ненужному» сертификату в нижней половине окна.

В строке состояния отображается, сколько сертификатов из общего количества выбрано в качестве абонентов.

После того, как список абонентов сформирован, нужно нажать «ОК» для зашифрования.

После процедуры зашифрования на экран будет выведено окно журнала работы (см. Рисунок 21). После ознакомления с результатом зашифрования необходимо нажать кнопку «Завершить».

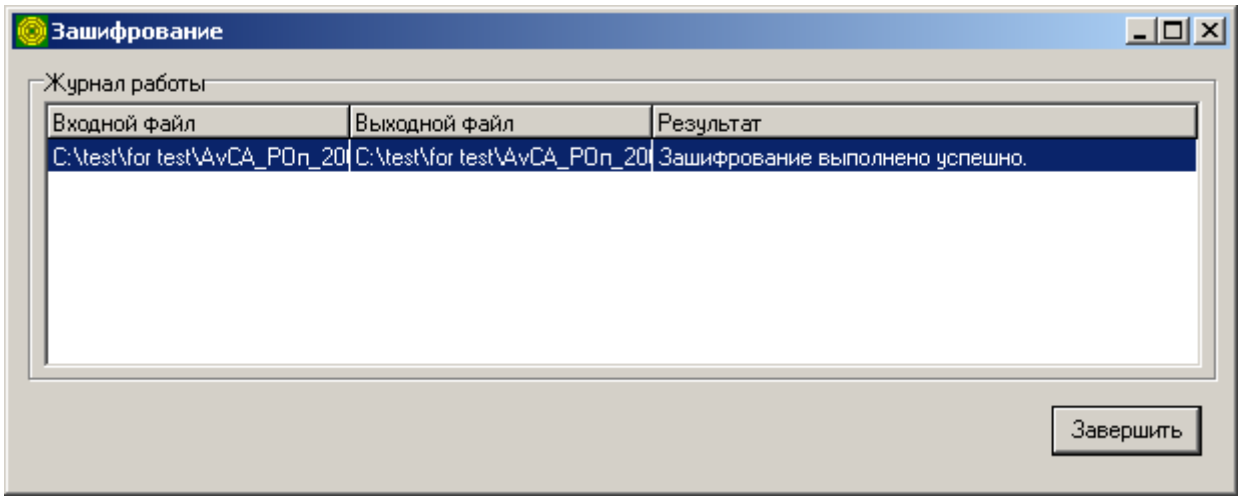

Рисунок 21 Результат зашифрования

Обратите внимание на то, что если в настройках программы был выбрана опция Сжатие при шифровании, то расширение зашифрованного файла будет *.enp вместо *.enc.

6.4 Расшифрование

Внимание! Расшифровывать можно только те файлы, которые ранее были зашифрованы кем-либо, используя в качестве сертификата получателя ваш личный сертификат. Обычно, такие файлы имеют расширение *.enc или *.enp. Если же будет произведена попытка расшифровать файл, который адресован не вам, либо не зашифрован, то программа выдаст сообщение об ошибке «Среди сертификатов получателей сообщения отсутствует личный сертификат аутентифицированного пользователя» или «Внутренняя ошибка библиотеки», соответственно.

Для того, чтобы произвести расшифрование, нужно вызвать контекстное меню этого файла и выбрать команду Расшифровать (см. Рисунок 8), после чего появится окно мастера расшифрования (см. Рисунок 22)

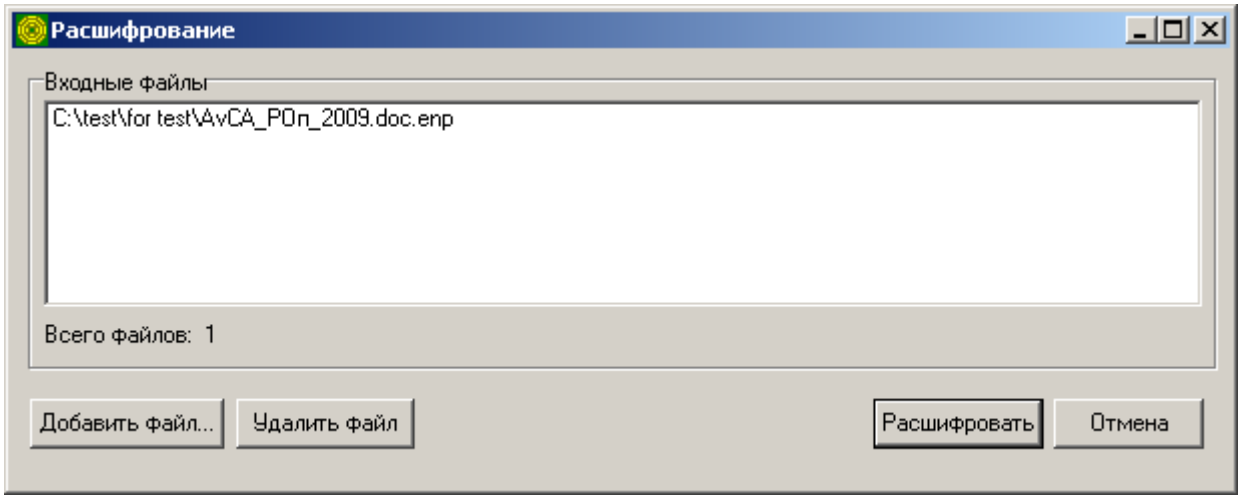

Рисунок 22 Расшифрование файла

В разделе Входные файлы нужно указать файлы, которые требуется расшифровать. При необходимости, их количество можно регулировать кнопками «Добавить файл» и «Удалить файл», которые находятся в нижней части окна. Также в этом окне можно увидеть общее количество файлов подготовленных для расшифрования. Эта информация отображается в строке Всего файлов.

Сверив количество и имена файлов, которые вы хотите расшифровать, нужно нажать кнопку «Расшифровать».

Если это первое подключения личного сертификата, или истекло время кэширования пароля с момента проведения последней операции с помощью программы AvPCK, то CryptoTray выдаст окно авторизации пользователя (см. Рисунок 15). В окне нужно выбрать личный сертификат для авторизации и нажать кнопку «ОК». Затем появится окно доступа к контейнеру личных ключей, в котором нужно будет выбрать тип носителя и ввести пароль доступа к контейнеру личных ключей. Пароль сохранится в системе на время, соответствующее времени кэширования логина, которое указано в настройках Avest Personal CryptoKit на Вкладке Подключение.

После процедуры подписи файла на экран будет выведено окно журнала работы (см. Рисунок 23). После ознакомления с результатом выработки ЭЦП необходимо нажать кнопку «Завершить».

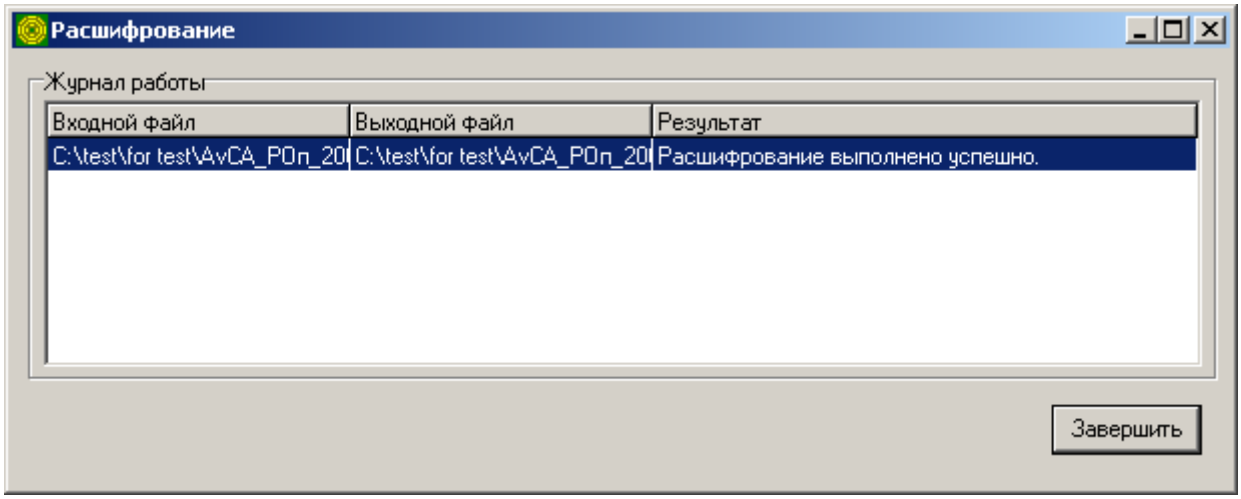

Рисунок 23 Результат расшифрования

7. ДЕИНСТАЛЛЯЦИЯ AVPCK

Деинсталлировать программу Avest Personal CryptoKit можно двумя способами:

Способ 1: Открыть папку Установка и удаление программ: Пуск →Настройка →Панель управления (см. Рисунок 24).

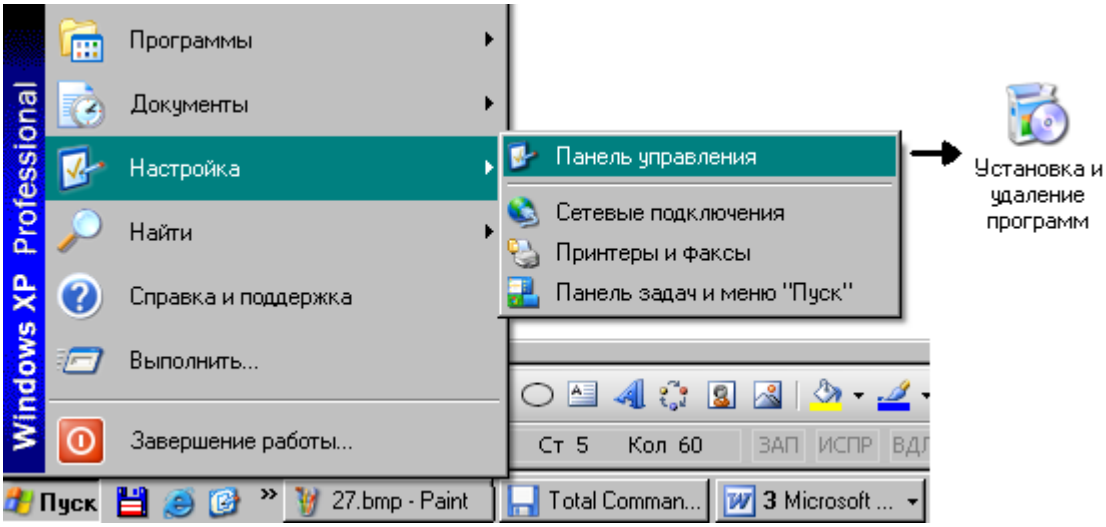

Рисунок 24 Открытие папки «Установка и удаление программ»

Выбрать из списка программ Avest Personal CryptoKit и нажать на кнопку «Удалить». Появится сообщение о деинсталляции (см. Рисунок 25), нужно нажать кнопку «Да».

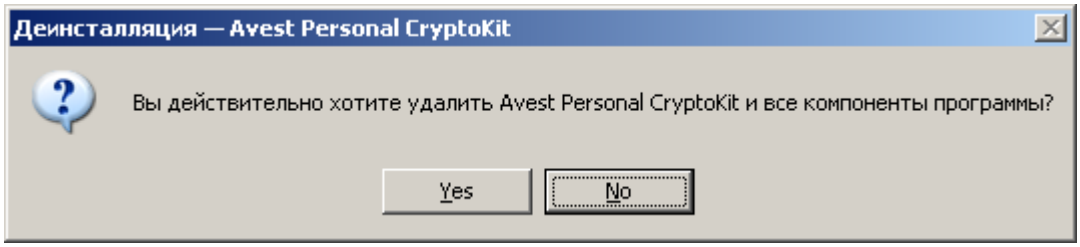

Рисунок 25 Подтверждение о деинсталляции

После удаления программы системе потребуется перезагрузка, выполните её.

Способ 2: Открыть папку, в которую была проинсталлирована программа Avest Personal CryptoKit. Так как программа инсталлируется в ту же папку, куда предварительно был установлен Персональный Менеджер Сертификатов, то, при установке менеджера по умолчанию, путь к папке будет такой: c:\Program Files\Avest\AvPCM. В этой папке есть деинсталляционный файл unins001.exe. Его нужно запустить для деинсталляции. Появится сообщение о деинсталляции (см. Рисунок 25), нужно нажать кнопку «Да». После удаления программы системе потребуется перезагрузка, выполните её.

Лист регистрации изменений									
Номер листов (страниц)					Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	І одп.	ата
И зм	з-ме-нен-ных	За менен-ных	Но вых	А нну-лиро-ванных					