Инструкция по установке

Установка комплекта абонента с сертификатом ГосСУОК с помощью объединённого инсталлятора AvPKIsetup

2017 г.

Оглавление

[Аннотация 2](#_Toc491941349)

[Системные требования 3](#_Toc491941350)

[Установка 3](#_Toc491941351)

[Установка на компьютер, на котором уже присутствуют более ранние версии криптографического ПО ЗАО Авест 8](#_Toc491941352)

[Удаление криптографического программного обеспечения с помощью объединенного инсталлятора 9](#_Toc491941353)

[Приложение 1. Установка сертификатов 12](#_Toc491941354)

[Приложение 2. Способы получения/обновления списков отзыва сертификатов СОС: 19](#_Toc491941355)

[Приложение 3. Только для абонентов системы MAILGOV (Почта госорганов). Настройка криптографических параметров в программе Microsoft Outlook после обновления (на примере Microsoft Outlook 2007) 20](#_Toc491941356)

[Приложение 4. Только для абонентов системы MAILGOV (Почта госорганов). Отправка сообщений программой Microsoft Outlook (на примере Microsoft Outlook 2007) 25](#_Toc491941357)

[1. Первоначальная отправка сообщения 25](#_Toc491941358)

[2. Получение сообщения 26](#_Toc491941359)

[3. Получение подписанного и зашифрованного сообщения 28](#_Toc491941360)

# Аннотация

В настоящей инструкции описан порядок установки криптографического программного обеспечения «Комплект абонента AvUCK» с сертификатом ГосСУОК с помощью объединенного инсталлятора AvPKISetup.

# Системные требования

Работа инсталлятора AvPKISetup рассчитана на выполнение под управлением 32-х и 64-х битных операционных систем:

* **Windows Server 2003** с установленным Service Pack 2 c обновлением **KB2836198,**
* **Windows XP** с установленным Service Pack 3 c обновлением **KB2836198**,
* **Windows Server 2008 R1,**
* **Windows Server 2008 R2,**
* **Windows Server 2012,**
* **Windows Server 2012 R2,**
* **Windows Server 2016,**
* **Windows 7**,
* **Windows 8**,
* **Windows 8.1,**
* **Windows 10**.

Требуется наличие **Microsoft Internet Explorer 6.0** или выше.

Пользователь для установки и запуска должен иметь права в операционной системе **Windows** не ниже «**PowerUser**».

Файлы, содержащие личный ключ подписи/шифрования, а также другие необходимые параметры, должны находиться на электронных устройствах **AvToken, AvPass** в защищенном виде.

**ВНИМАНИЕ!** На время установки антивирусное программное обеспечение (в том числе встроенное в ОС, например, Windows Defender) рекомендуется отключать, т.к. некоторые антивирусные программы могут создавать препятствие записи значений в реестр Windows и установке компонентов программ в системные папки.

**Только для абонентов системы MAILGOV (Почта госорганов):**

Программа электронной почты Microsoft Outlook (версии Microsoft Outlook 2003 или более поздней) или Outlook Express не ниже 6-й версии.

# Установка

Комплект абонента AvUCK совместно с сертификатом, сконфигурированный для установки с помощью AvPKISetup, передается пользователям на диске, флеш-носителе или иным способом (порядок определяется Удостоверяющим центром, выдающим ПО).

Каждое окно объединенного инсталлятора AvPKISetup снабжено пояснительными надписями, которые следует внимательно читать.

В любой момент установку можно прервать, нажав кнопку «**Отмена**».

Для начала обновления ПО необходимо запустить файл **AvPKISetup2.exe**.

В окне мастера установки следует нажать кнопку «**Далее**», чтобы начать установку ПО на компьютер (Рисунок 1).

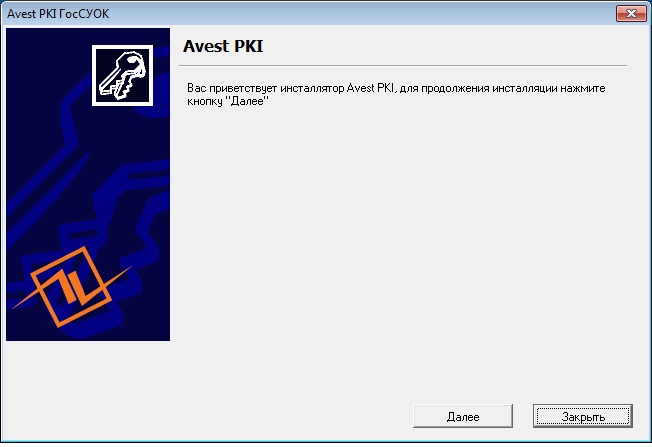


Рисунок 1.  Окно мастера установки Avest PKI

В следующем окне следует выбрать режим **Установка** и нажать кнопку «**Далее**».

В появившемся окне представлен список устанавливаемых на компьютер компонентов, отмеченный флажками. В колонке «**Инсталлируемая версия**» отображается версия устанавливаемого продукта. В списке устанавливаемых компонентов будет указана версия устанавливаемого криптопровайдера Avest CSP Bel и Avest CSP 6.3.0.791 (или выше), версия устанавливаемого Персонального менеджера сертификатов, AvJCEProv, плагина AvCMXWebP (Рисунок 2. Выбор компонентов).

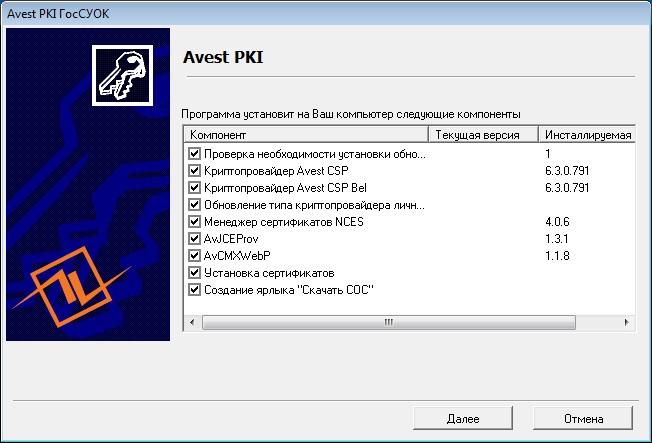


Рисунок 2. Выбор компонентов

Для корректной работы криптопровайдера на операционных системах **Windows XP** **Service Pack 3** и **Windows Server 2003** обязательно должно быть установлено обновление **KB2836198**. Эта процедура обязательно требует перезагрузки компьютера (Рисунок 3 Предупреждение о перезагрузке).

Если мастер установки AvPKISetup обнаруживает, что это обновление отсутствует, выдаёт собщение об этом и предлагает нажать «Далее».

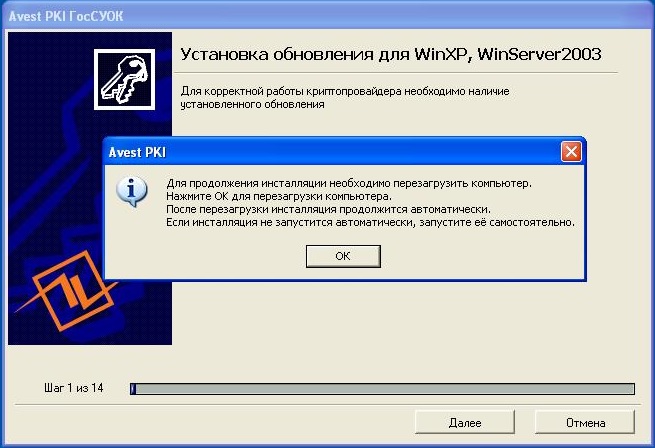


Рисунок 3 Предупреждение о перезагрузке

Если по каким-то причинам AvPKISetup после перезагрузки не запустится сам, то его нужно снова запустить, открыв появившийся на рабочем столе ярлык «Продолжение установки AvPKISetup», как это показано на Рисунок *4* Ярлык «Продолжение установки AvPKISetup (ярлык после успешной установки удалится с рабочего стола самостоятельно).

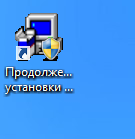


Рисунок 4 Ярлык «Продолжение установки AvPKISetup»

Следующий шаг мастера установки – сбор случайных данных. Для их сбора нужно подвигать мышью в окне установки, пока индикатор сбора случайных данных не достигнет отметки 100%.

Далее произойдет установка:

* криптопровайдера Avest CSP Bel,
* криптопровайдера Avest CSP,
* веб плагина AvCMXWebP,
* программного комплекса AvJCEProv,
* персонального менеджера сертификатов AvPCM,
* импорт сертификата в Личный справочник,
* импорт атрибутного сертификата,
* установка доверия сертификатам Корневых удостоверяющих центров (**см. Приложение 1. Установка сертификатов),**
* обновление типа криптопровайдера личных сертификатов в справочниках Microsoft, если в системе есть сертификаты MailGov.

Мастер установки произведет все действия автоматически.

Для получения/обновления списков отзыва сертификатов (СОС) на рабочем столе во время установки криптографического программного обеспечения будет создан ярлык «Скачать СОС». 

Перед завершением инсталляции программа выведет окно о результате работы. В графе «**Состояние**» можно увидеть, произошла ли установка того или иного компонента.

Более подробная информация находится в «**Журнале работы**», который доступен при нажатии соответствующей кнопки.

Для завершения работы AvPKISetup нужно нажать кнопку «**Закрыть**»(Рисунок 5. Завершение установки).

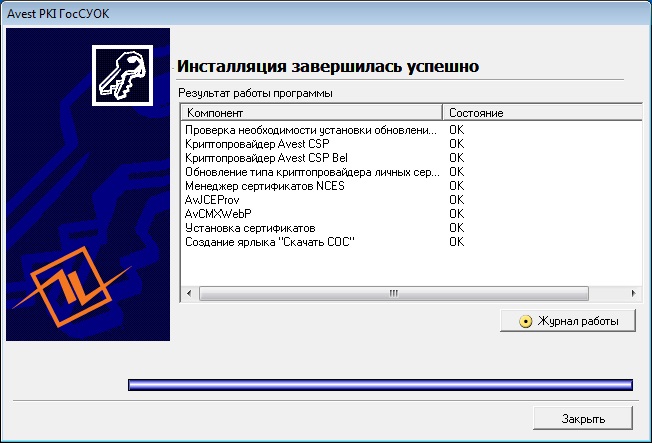


Рисунок 5. Завершение установки

Установка комплекта абонента завершена.

Сертификат ГосСУОК может быть использован различных информационных системах, например:

* подписание электронных деклараций, работа на сайте portal.nalog.gov.by;
* подписание ЭСЧФ, работа на сайте vat.gov.by;
* работа на сайте portal.gov.by;
* и в прочих государственных сервисах, уточняйте, пожалуйста, есть ли такая возможность, у владельца сервиса.

# Установка на компьютер, на котором уже присутствуют более ранние версии криптографического ПО ЗАО Авест

Вариантов и комбинаций предустановленного криптографического ПО может быть несколько, поэтому версии ПО, указанные в этом разделе, могут не совпадать с установленными на компьютере.

Обновление программного обеспечения с помощью объединенного инсталлятора AvPKISetup будет происходить аналогично установке без обновления, описанной выше, с небольшими отличиями, о которых рассказано ниже:

В списке устанавливаемых компонентов будет указана версия текущего криптопровайдера, которая будет заменена на версию 6.3.0.791 (или выше), версия установленного менеджера сертификатов, которая будет заменена на 4.0.6 (или выше) (см. Рисунок 6 Обновление компонентов*)*

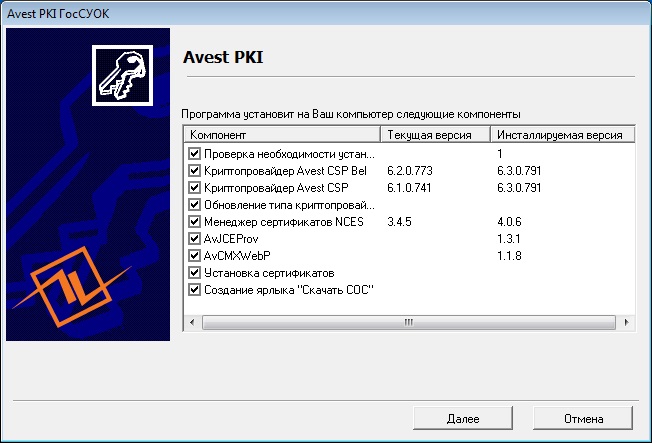


Рисунок 6 Обновление компонентов

После того, как кнопка **«**Далее**»** будет нажата, мастер установки **AvPKISetup** выдаст сообщение о том, что он удалит текущую версию криптопровайдера и проинсталлирует новую версию. Эта процедура обязательно требует перезагрузки компьютера (см. Рисунок 3 Предупреждение о перезагрузке). Если по каким-то причинам **AvPKISetup** после перезагрузки не запустится сам, то его нужно снова запустить, открыв появившийся на рабочем столе ярлык «Продолжение установки AvPKISetup», как это показано на Рисунок 4 Ярлык «Продолжение установки AvPKISetup». Ярлык после успешной установки удалится с рабочего стола самостоятельно.

Далее установка проходит аналогичным способом, описанным выше в данном руководстве.

# Удаление криптографического программного обеспечения с помощью объединенного инсталлятора

Для того, чтобы корректно удалить криптографическое программное обеспечение, необходимо использовать объединенный инсталлятор AvPKISetup. Для начала удаления ПО необходимо запустить файл **AvPKISetup2.exe**.

В окне мастера установки следует нажать кнопку «Далее», В следующем окне следует выбрать режим «**Удаление»** и нажать кнопку «Далее» (см. Рисунок 7 Выбор типа инсталляции).

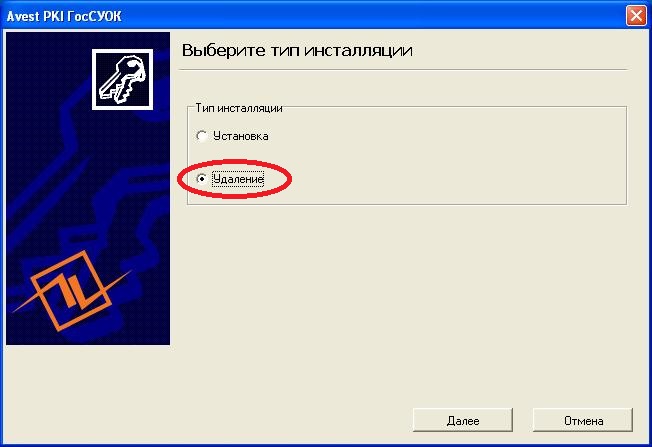


Рисунок 7 Выбор типа инсталляции

В следующем окне программа выводит список удаляемых компонентов. Необходимо выбрать те компоненты, которые надо удалить, и нажать кнопку «Далее» (см. Рисунок *8* Список удаляемых компонентов).

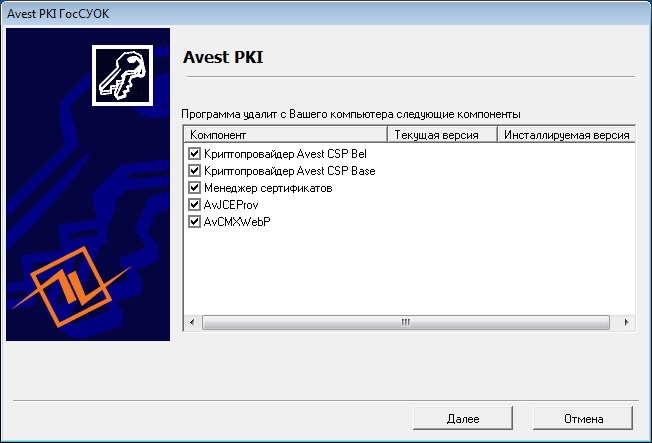


Рисунок 8 Список удаляемых компонентов

В следующем окне отображается результат работы мастера установки «AvPKISetup». В столбце «Компонент» отображается что именно было удалено, в столбце «Состояние» отображается статус удаления компонентов (см. Рисунок *9* Результат работы программы).

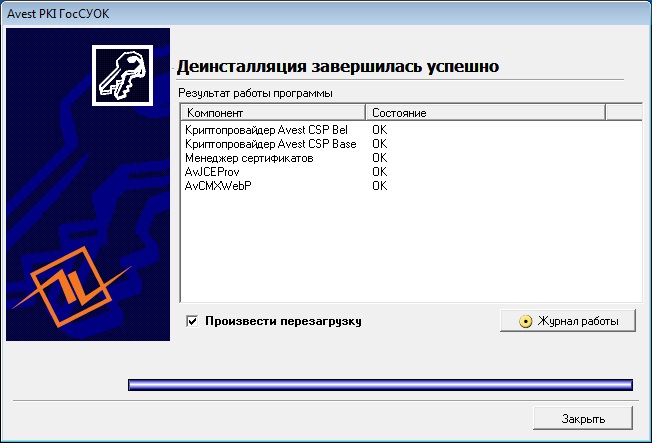


Рисунок 9 Результат работы программы

В этом же окне возможно отказаться от перезагрузки путем снятия галочки. Если отметка о перезагрузке была снята, появится окно с предупреждением о необходимости перезагрузки (см. Рисунок *10* Предупреждение о необходимости перезагрузки*)*.

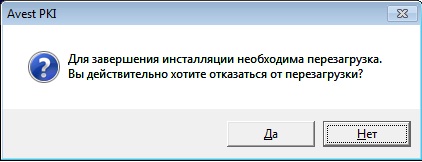


Рисунок 10 Предупреждение о необходимости перезагрузки

Также можно более подробно просмотреть результат работы мастера установки AvPKISetup, нажав кнопку «Журнал работы» (см. Рисунок *11* Журнал работы).

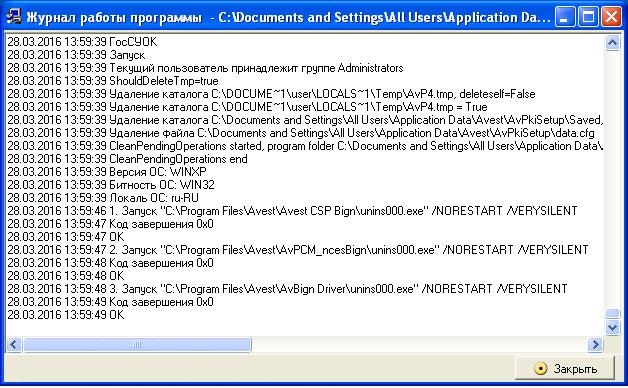


Рисунок 11 Журнал работы

# Приложение 1. Установка сертификатов

На шаге «Установка сертификатов» открывается окно Мастера импорта и происходит установка сертификатов в системные справочники Windows (см. Рисунок *12* Импортируемые сертификаты). Галочками отмечены сертификаты, которые будут проимпортированы и которые отсутствуют в системном справочнике. Необходимо нажать кнопку «Далее». Если в списке импортируемых объектов сертификаты повторяются, оставьте галочки по умолчанию, как предлагает Мастер импорта.

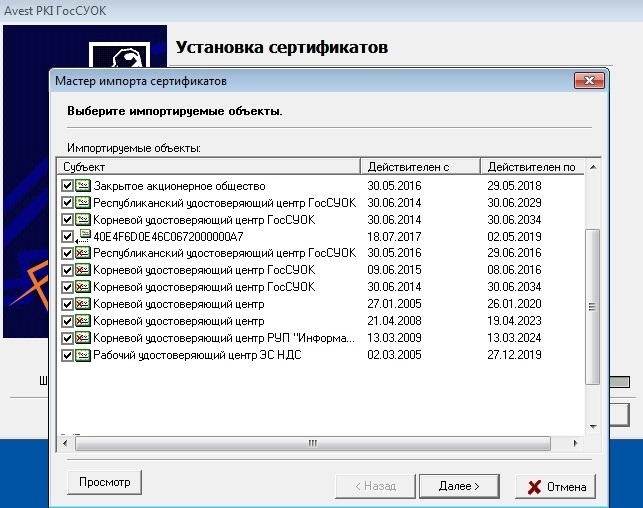


Рисунок 12 Импортируемые сертификаты

Мастер импорта уведомит о количестве импортированных сертификатов (см. Рисунок *13*Уведомление о количестве импортируемых сертификатов).

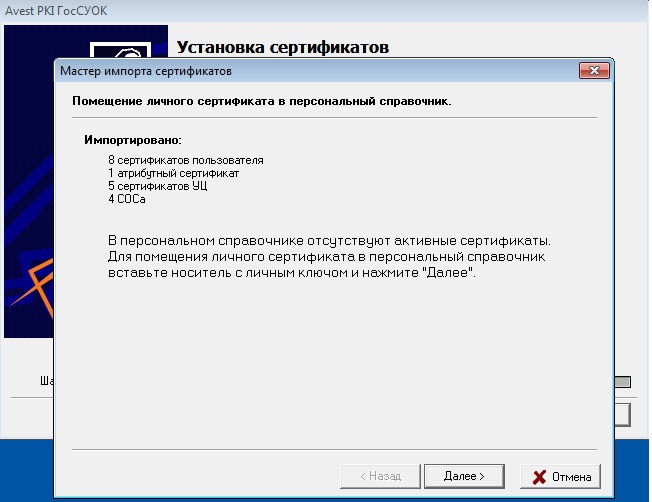


Рисунок 13Уведомление о количестве импортируемых сертификатов

Для установки личного сертификата надо вставить носитель **AvToken** (**AvPass**), на котором записан личный ключ, в USB-разъем компьютера и нажать кнопку «Далее». В окне выбора контейнера отобразятся все контейнеры с личными ключами, записанные на носителе **AvToken** (**AvPass**). Если на носителе записано более одного контейнера, то в списке нужно выбрать тот, который соответствует Вашему личному сертификату. Определить это можно, например, по дате регистрации в УЦ предприятия. После того, как соответствующий контейнер выбран, нужно нажать на кнопку «Далее» (см. Рисунок *14* Выбор контейнера).

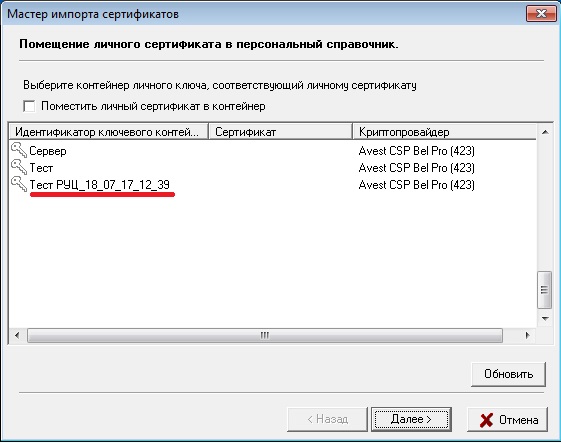


Рисунок 14 Выбор контейнера

.

В появившемся окне криптопровайдера нужно ввести пароль, который был задан при создании личных ключей, и нажать кнопку «ОК».

На следующем шаге будет установлено доверие сертификатам Корневых удостоверяющих центров (см. Рисунок *15* Сертификаты корневых удостоверяющих центров).

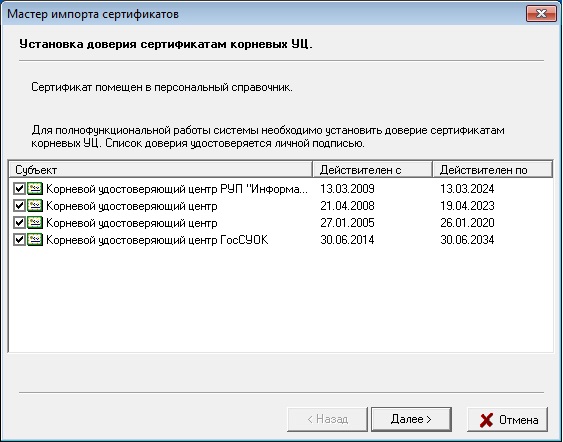


Рисунок 15 Сертификаты корневых удостоверяющих центров

Перед установкой сертификатов корневых удостоверяющих центров на экране возникает «Предупреждение системы безопасности» Windows о добавлении сертификата в список доверенных УЦ, в этом сообщении всегда указываются атрибуты помещаемого сертификата. Нужно сравнить имя сертификата корневого УЦ с именем, указанным в бумажной карточке открытого ключа, а значения поля «Отпечаток» со значениями, изображенными на рисунке. Если всё соответствует, то нажать кнопку «Да» (см. Рисунок *16* Предупреждение системы безопасности).

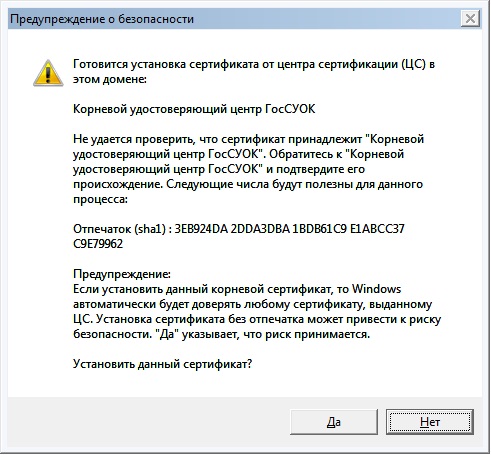


Рисунок 16 Предупреждение системы безопасности

На следующем шаге Мастер импорта уведомит о сертификатах, которым было установлено доверие. Нажмите кнопку «Закрыть». (См. Рисунок *17* Завершение работы мастера импорта сертификатов)

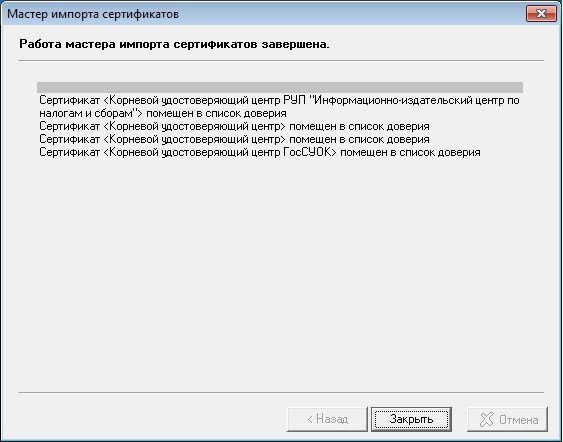


Рисунок 17 Завершение работы мастера импорта сертификатов

# 

# Приложение 2. Способы получения/обновления списков отзыва сертификатов СОС:

Для того, чтобы запустить обновление СОС, в персональном менеджере сертификатов нужно выбрать меню «Сервис» – «Контроль точек распределения СОС» или «Обновление СОС и сертификатов УЦ», если установлена версия менеджера 3.6.0 и выше. Интернет при этом должен быть включён.

Если у вас интернет через прокси или если требуется автоматизировать процесс получения СОС, можно воспользоваться заранее сконфигурированным файлом-«батником» **get\_crl.bat**, который поставляется вместе с ПО на диске:

Для получения/обновления списков отзыва сертификатов (СОС) с помощью **get\_crl.bat** на рабочем столе при установке криптографического программного обеспечения создается ярлык «Скачать СОС», нажав на который можно получить актуальные СОС.

\* **Внимание!** Если выход в интернет осуществляется через прокси, необходимо:

1. в файле **get\_crl.bat**

который находится в c:\Program Files (x86)\Avest\AvPCM\_nces\ - ОС 64-разрядная или

c:\Program Files \Avest\AvPCM\_nces\ - ОС 32-разрядная)

раскомментировать строки (удалить слово «rem»):

set PX\_USER, set PX\_PASS, set http\_proxy

и указать данные пользователя и адрес прокси.

1. Зайти по пути c:\Program Files (x86)\Avest\AvPCM\_nces или c:\Program Files \Avest\AvPCM\_nces\ и запустить файл **get\_crl.bat**

(при использовании прокси предварительно надо внести необходимые данные, как описано выше).

# Приложение 3. Только для абонентов системы MAILGOV (Почта госорганов). Настройка криптографических параметров в программе Microsoft Outlook после обновления (на примере Microsoft Outlook 2007)

**Внимание! Этот пункт нужно выполнять Только абонентам системы MAILGOV (Почта госорганов).**

Чтобы убедиться в том, что сертификат можно использовать для подписи и шифрования писем, его можно открыть в менеджере сертификатов, вкладка Состав, в поле Улучшенный ключ должно быть указано «Защищенная электронная почта» ( Рисунок *18* Применение ключа), также выделив поле Субъект можно проверить адрес электронной почты (Рисунок *19* Адрес электронной почты).

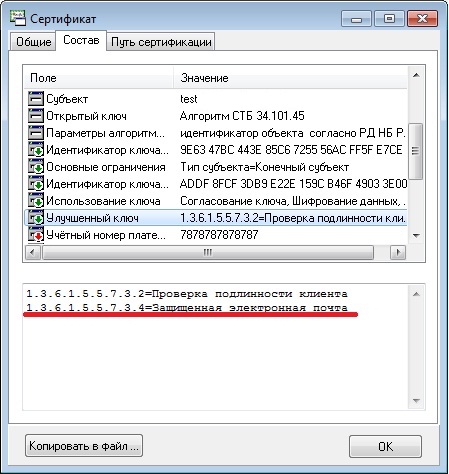


Рисунок 18 Применение ключа

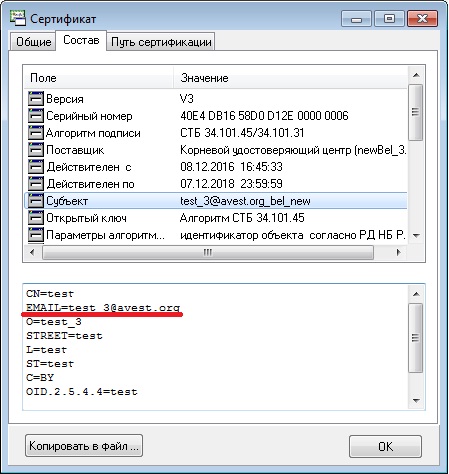


Рисунок 19 Адрес электронной почты

Список рекомендуемой версии почтового клиента для определенной ОС

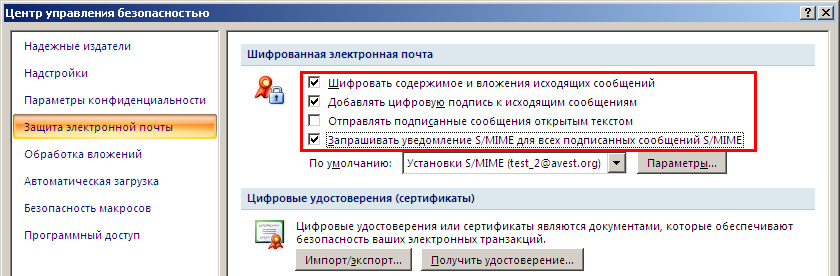
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Outlook **(x86)** / OC | Windows XP | Windows 7 | Windows 8 | Windows 8.1 | Windows 10 | Windows Server 2003 | Windows Server 2008 R2 | Windows Server 2012 R2 |
| Outlook  Express | + |  |  |  |  |  |  |  |
| Outlook  2003 | + | + |  |  |  | + |  |  |
| Outlook  2007 | + | + | + |  |  | + | + |  |
| Outlook  2010 | + | + | + | + |  | + | + | + |
| Outlook  2013 |  | + | + | + |  |  | + | + |
| Outlook  2016 |  |  |  |  | + |  |  |  |
| Windows Live Mail 2011 |  | + |  |  |  |  | + |  |
| Windows Live Mail 2012 |  | + |  | + |  |  |  |  |

1. Запустить программу Microsoft Outlook.
2. Выбрать в пункте меню «Сервис» → «Центр управления безопасностью» закладку «Защита электронной почты».

В закладке «Защита электронной почты» нужно отметить галочками следующие пункты:

* **шифровать** содержимое и вложения исходящих сообщений;
* **добавлять** цифровую подпись к исходящим сообщениям;

Для получения уведомлений от получателей сообщений о криптографической обработке сообщений с указанием даты и времени обработки, необходимо в данной закладке отметить галочкой пункт «**Запрашивать уведомления S/MIME для всех подписанных сообщений S/MIME**» (Рисунок *20* Защита электронной почты).

Рисунок 20 Защита электронной почты

1. Нажать кнопку «Параметры», откроется окно «Изменение настройки безопасности». В разделе «Сертификаты и алгоритмы» следует выбрать «Сертификат подписи», нажать кнопку «Выбрать» (Рисунок 21 Изменение настройки безопасности)

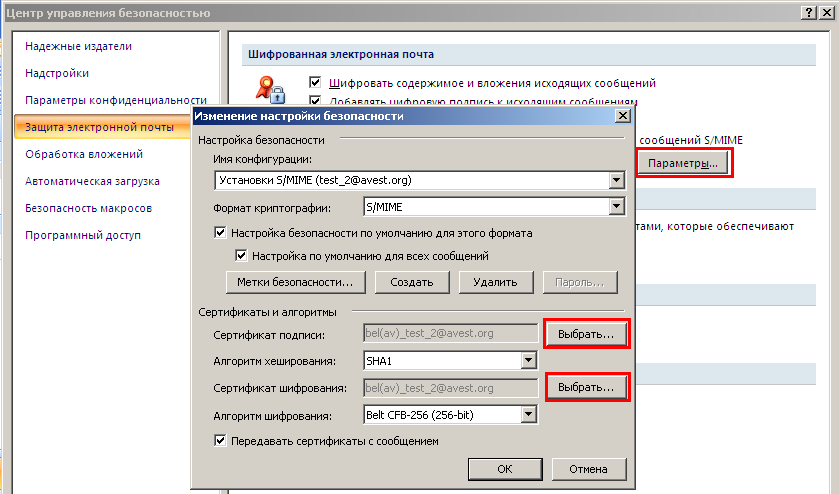
****

Рисунок 21 Изменение настройки безопасности

В окне «Выбор сертификата» выбрать действующий сертификат и нажать «ОК». Появится окно «Avest CSP Bel Pro – контейнер личных ключей», в котором нужно ввести пароль и нажать «ОК».

**ВНИМАНИЕ!** Необходимо убедиться, что окно ввода пароля называется правильно: **«Avest CSP Bel Pro – контейнер личных ключей»**, т. е. произошло обновление типа сертификата (Рисунок 22 Окно ввода пароля «Avest CSP Bel Pro – контейнер личных ключей»*).*

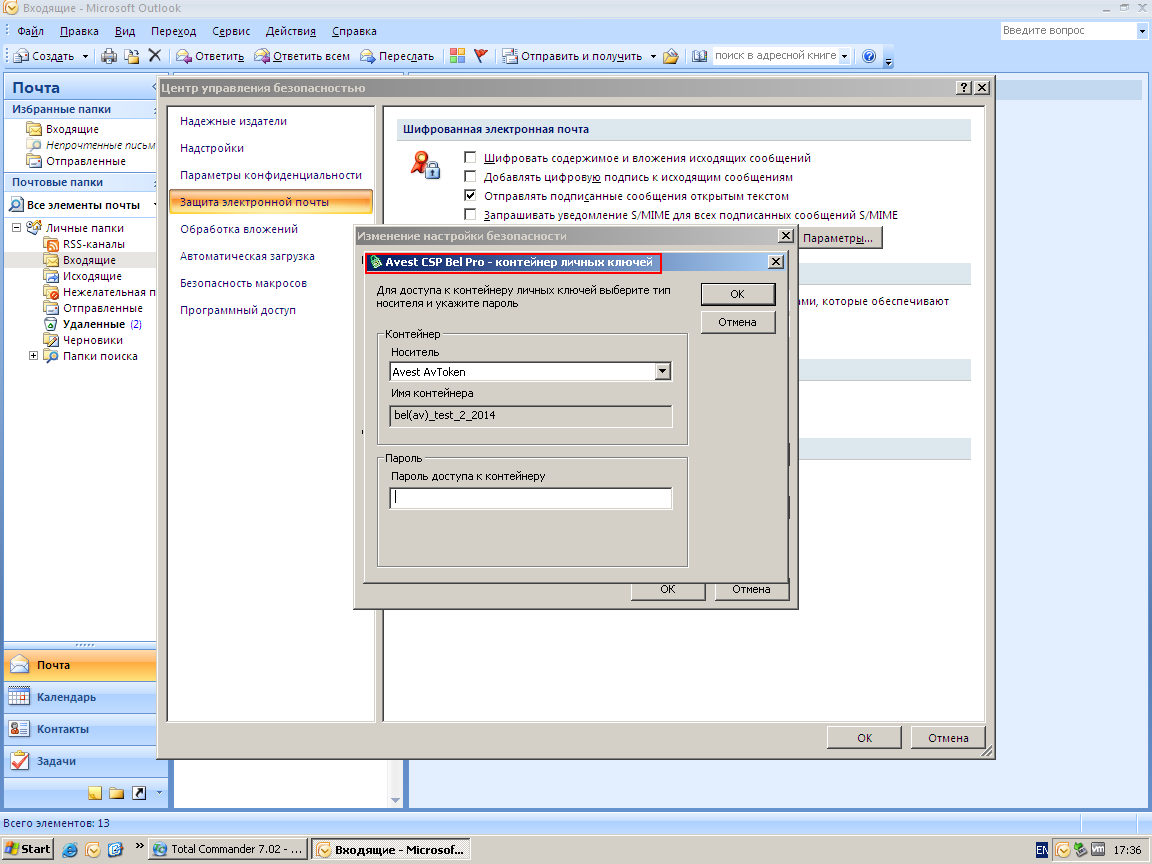


Рисунок 22 Окно ввода пароля «Avest CSP Bel Pro – контейнер личных ключей»

1. Сменить алгоритм хеширования на СТБ 34.101.31 (Рисунок 23 Изменение алгоритма хеширования).

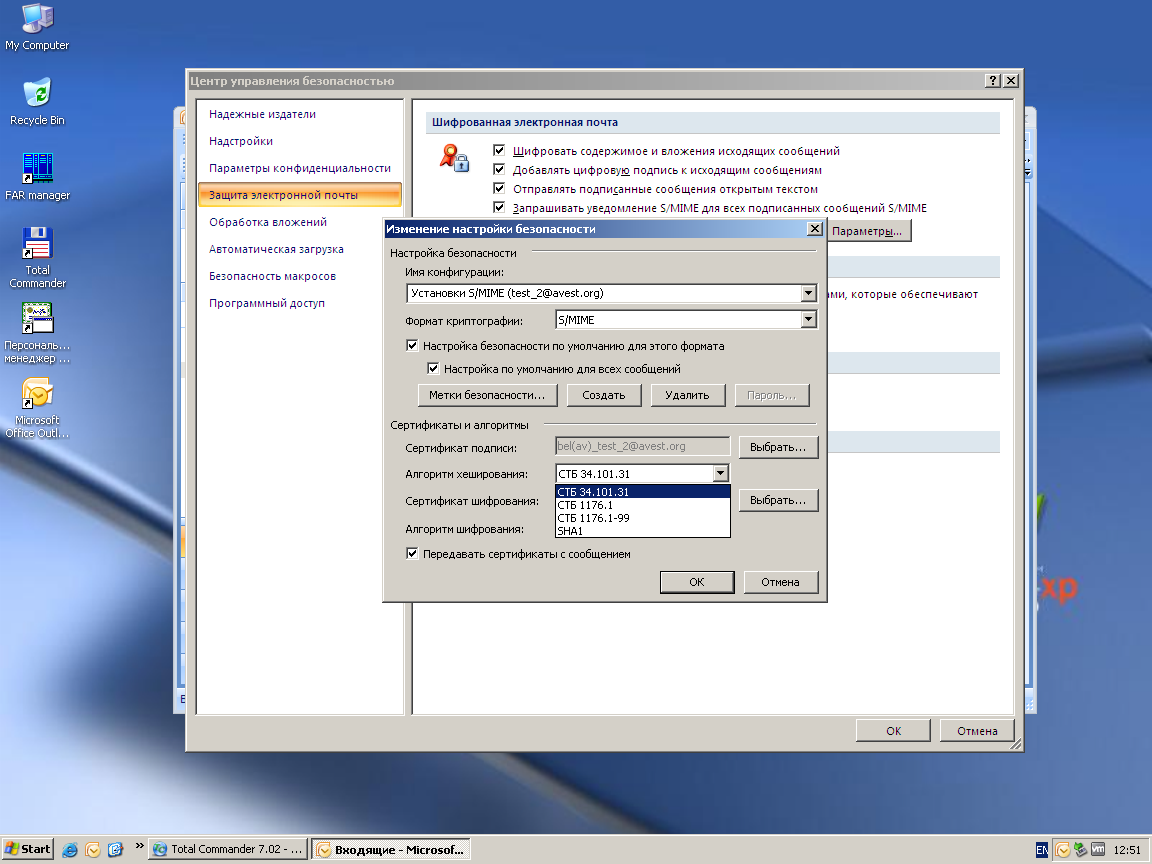


Рисунок 23 Изменение алгоритма хеширования

1. Нажать кнопку «Выбрать» в разделе «Сертификат шифрования» и, выбрав сертификат для электронной почты, ввести пароль.
2. В выпадающем меню в качестве алгоритма шифрования нужно выбрать Belt CFB-256 (256-bit).
3. На последнем шаге следует установить галочку на опции «Передавать сертификаты вместе с сообщением»
4. Нажать кнопку «OK» для сохранения изменений.

# Приложение 4. Только для абонентов системы MAILGOV (Почта госорганов). Отправка сообщений программой Microsoft Outlook (на примере Microsoft Outlook 2007)

**Внимание! Этот пункт нужно выполнять Только абонентам системы MAILGOV (Почта госорганов):**

Для возможности обмениваться защищенными сообщениями по новым алгоритмам шифрования с другими абонентами в системе «MailGov» необходимо отправить подписанное электронно-цифровой подписью сообщение другому пользователю, работающему на обновленном почтовом аккаунте, передав ему свой личный сертификат нового типа. Получатель сообщения должен добавить аккаунт отправителя в адресную книгу «Outlook» и отправить в ответ зашифрованное и подписанное сообщение вместе со своим личным сертификатом. При получении ответа необходимо добавить аккаунт данного абонента в свою адресную книгу.

В результате у пользователей появится возможность обмениваться подписанными и зашифрованными сообщения по новым алгоритмам шифрования.

## Первоначальная отправка сообщения

Запустить программу Microsoft Outlook.

На панели инструментов выбрать «Действия» → «Создать сообщение»

В окне Сообщение надо набрать текст сообщение, выбрать получателя, нажав на кнопку «Кому» или набрав адрес получателя вручную. Перед тем, как нажать кнопку «Отправить», необходимо убедиться, что кнопка «Сообщение с цифровой подписью» активна, как это показано на Рисунок *24* Первоначальная отправка подписанного сообщения:

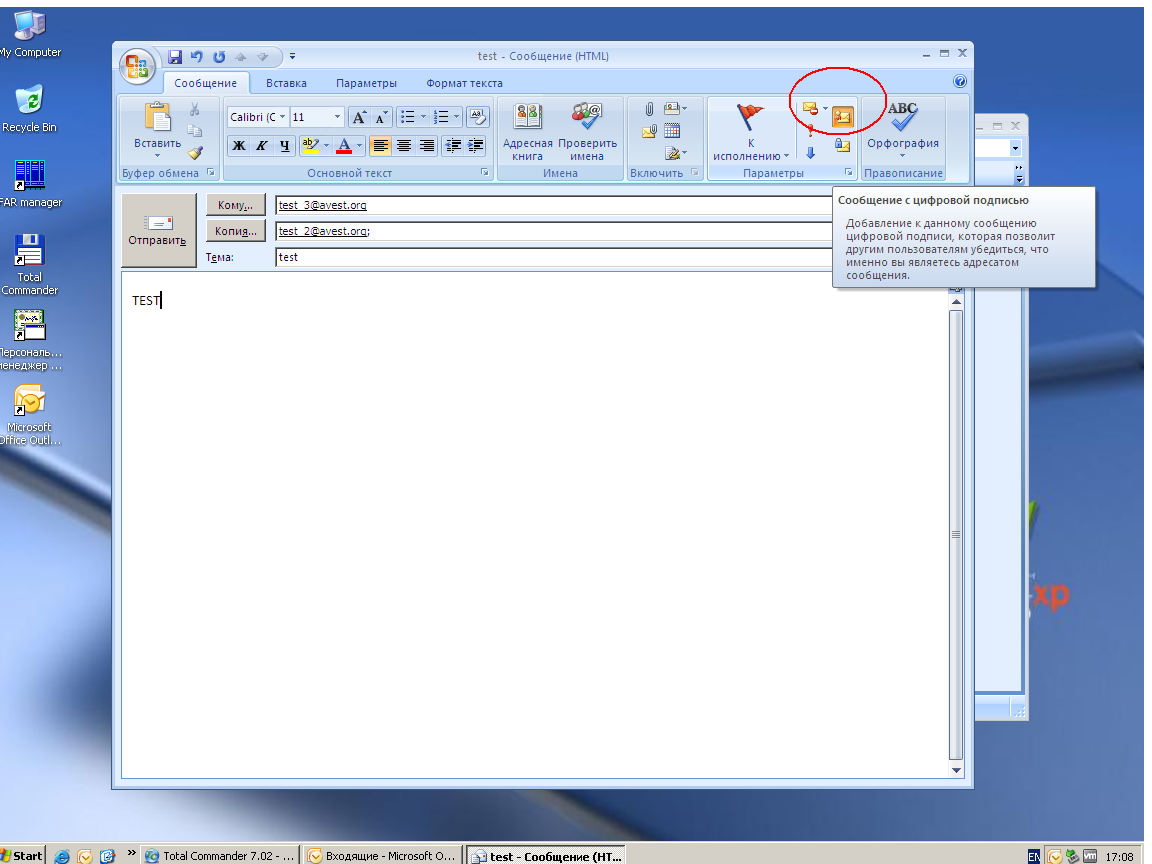


Рисунок 24 Первоначальная отправка подписанного сообщения

Таким образом будет отправлено подписанное сообщение с прикрепленным сертификатом.

## Получение сообщения

Получение первого сообщения от пользователя, перешедшего на новый тип шифрования

1. Запустить программу Microsoft Outlook. На панели инструментов выбрать «Сервис» → «Отправить/получить» → «Доставить почту» или нажать кнопку «F9».
2. Подписанное сообщение в папке Входящие будет помечено красной иконкой, при нажатии на которую появится информация о проверке цифровой подписи (Рисунок 25 Просмотр подписанного сообщения)

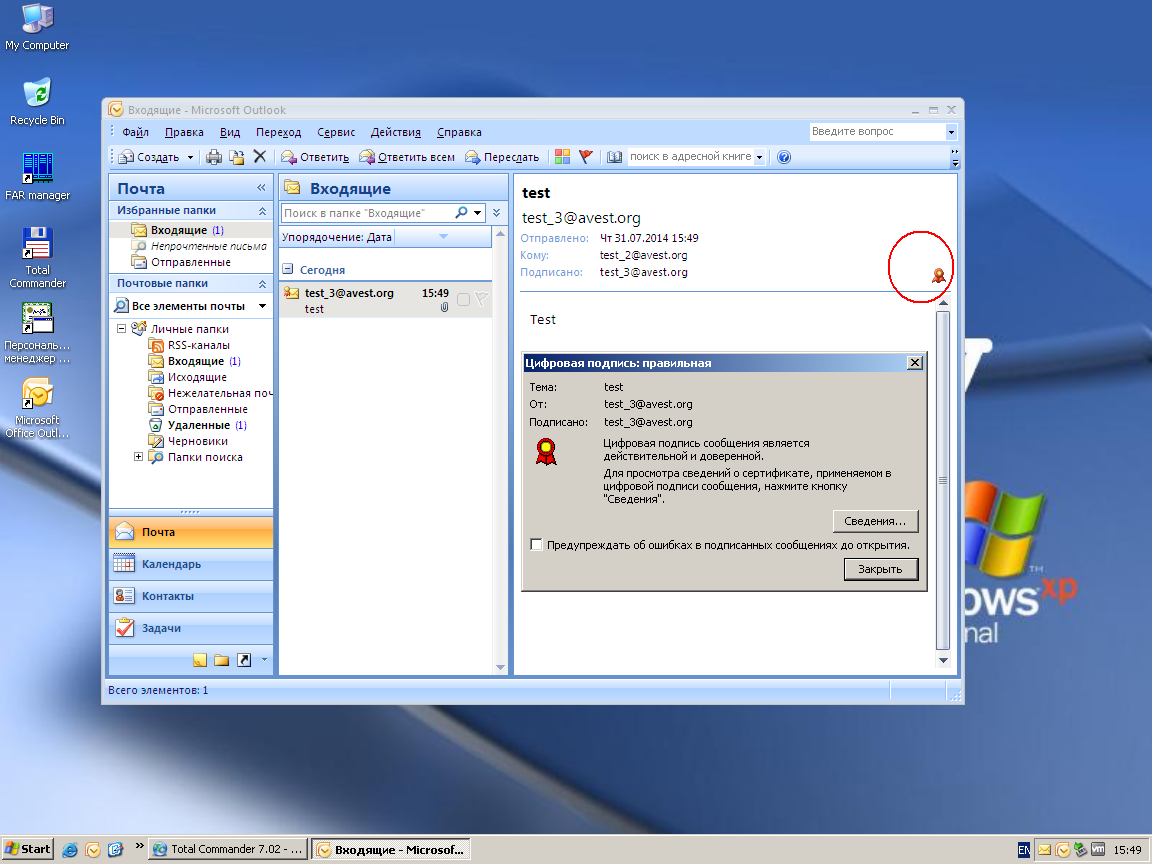


Рисунок 25 Просмотр подписанного сообщения

1. Далее необходимо добавить отправителя в контакты Outlook, для чего в окне просмотра сообщения необходимо кликнуть правой клавишей мыши по имени отправителя и выбрать в меню пункт «Добавить в контакты Outlook» (Рисунок 26 Добавление аккаунта в контакты).

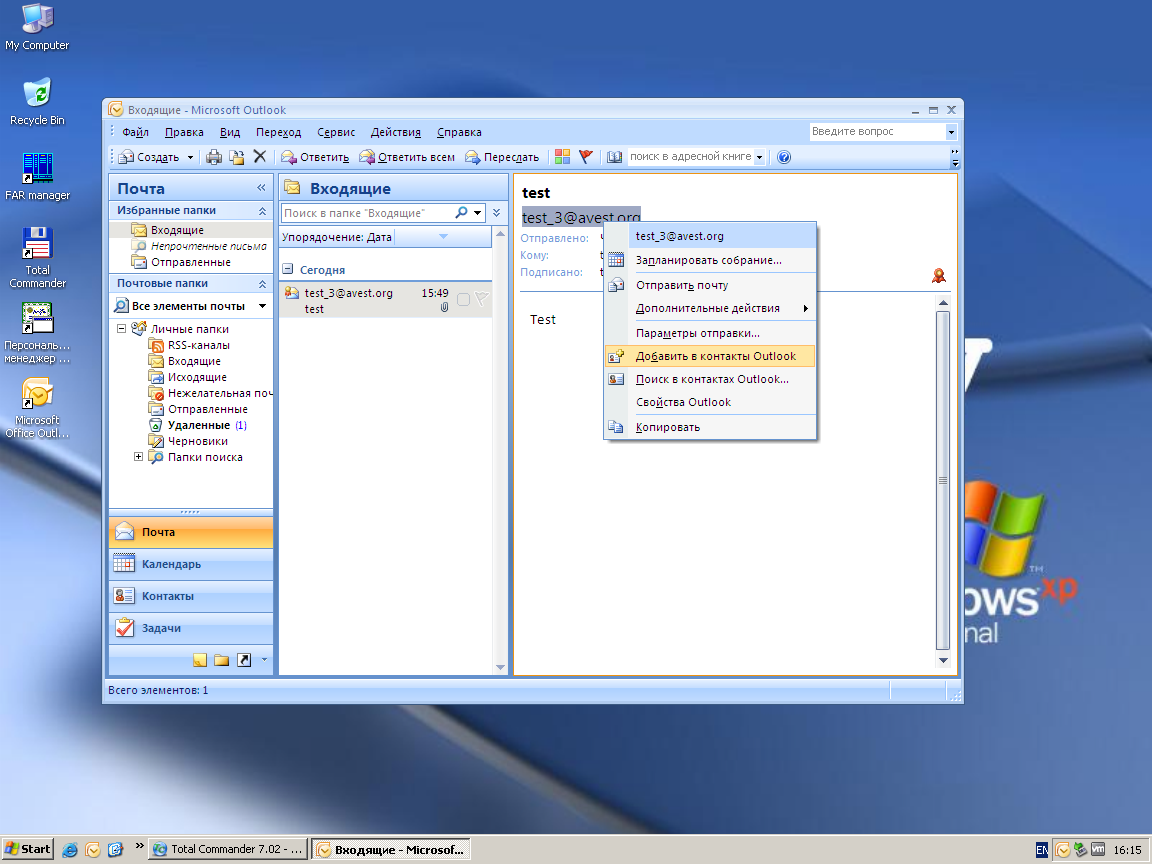


Рисунок 26 Добавление аккаунта в контакты

1. Заполнив сведения о контакте и убедившись в наличии сертификата получателя электронной почты (просмотреть сертификат аккаунта можно нажав кнопку «Сертификаты»), сохранить контакт, нажав кнопку «Сохранить и закрыть» (Рисунок 27 Заполнение сведений о контакте).

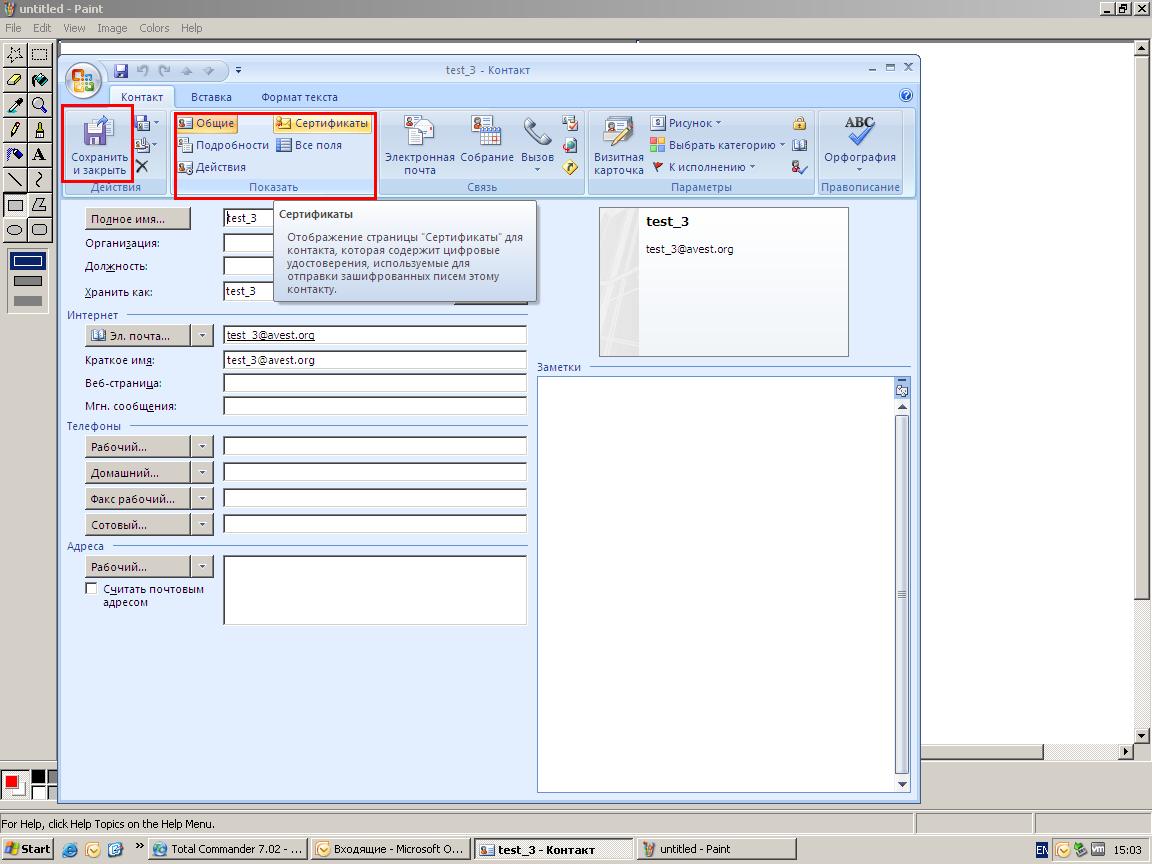


Рисунок 27 Заполнение сведений о контакте

В случае Outlook 2013 сертификата получателя будет отсутствовать (особенность работы в Outlook 2013), его необходимо проимпортировать. Для этого нужно нажать кнопку «Сертификаты» → «Импорт». Сертификат должен быть в файле с расширением \*.cer.

Далее необходимо отправить ответное сообщение, зашифрованное на данного абонента. Действия по созданию данного сообщения аналогичны описанным в пункте «**Первоначальная отправка сообщения**».

При отправке сообщения должны быть нажаты две кнопки: кнопка «Подписать сообщение» и кнопка «Шифровать сообщение», а при нажатии кнопки «Отправить» должно появиться окно ввода пароля «Avest CSP Bel Pro» (Рисунок 28 Отправка зашифрованного и подписанного сообщения).

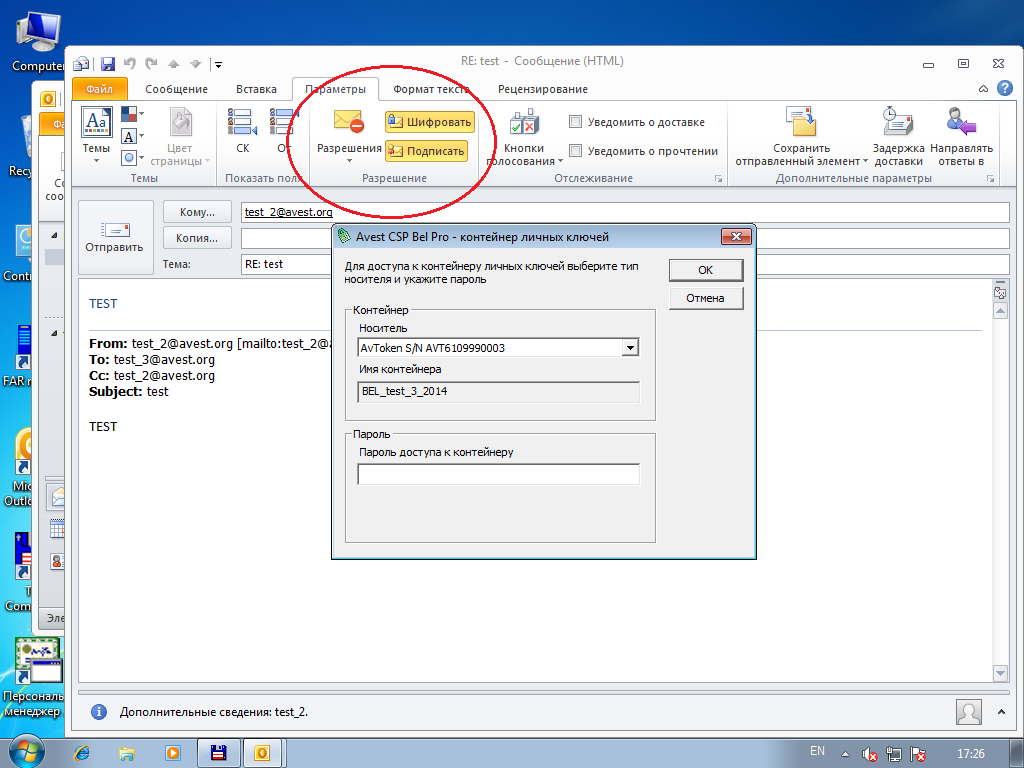
****

Рисунок 28 Отправка зашифрованного и подписанного сообщения

## Получение подписанного и зашифрованного сообщения

При получении зашифрованное сообщение будет скрыто от быстрого просмотра (Рисунок 29 Получение зашифрованного сообщения).

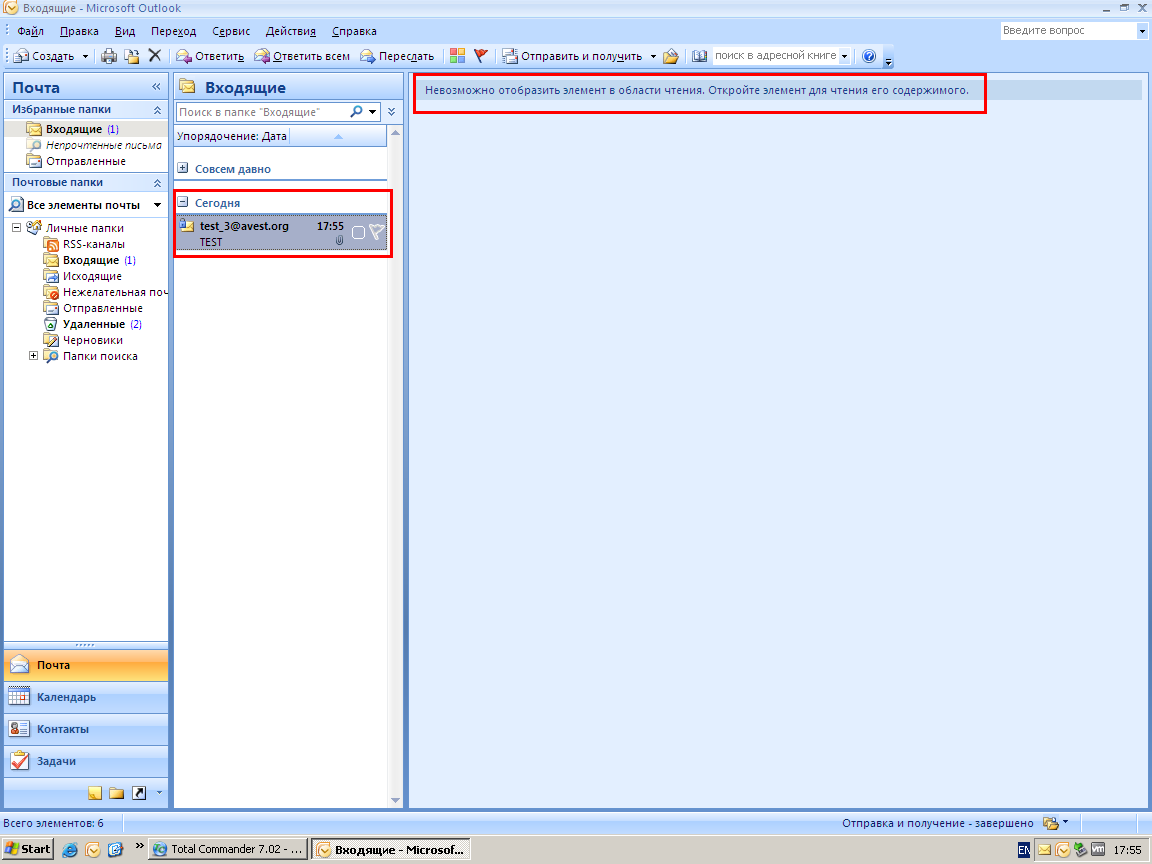


Рисунок 29 Получение зашифрованного сообщения

Для криптографической обработки входящего сообщения необходимо предъявить пароль для носителя ключей получателя сообщения, который вводится в окне криптопровайдера Avest CSP Bel Pro.

Сохранение аккаунта отправителя в контактах Outlook даст возможность в дальнейшем составлять и отправлять для этого абонента зашифрованные сообщения.