

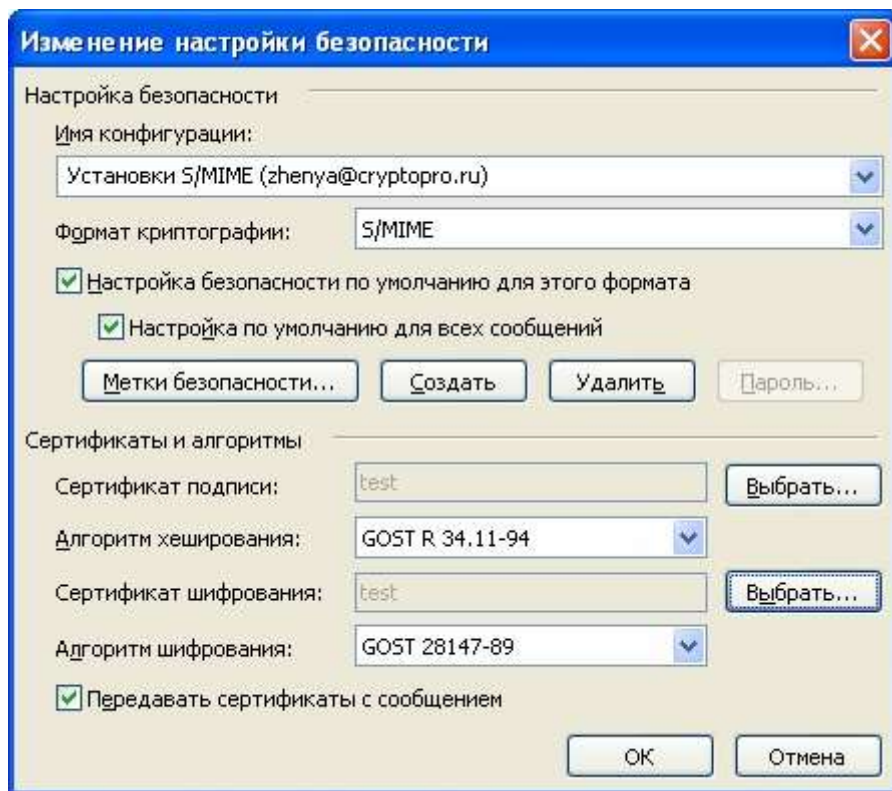
Использование КриптоПро CSP в Outlook 2007

Использование средств криптографической защиты в Outlook 2007 во многом совпадает с использованием в Outlook ранних версий. Однако стоит отметить следующие особенности:

1. Почтовая программа Outlook 2007 поддерживается только криптопровайдером КриптоПро CSP версии 3.0 (с установленным пакетом обновления SP2) и выше.
2. Криптопровайдер КриптоПро CSP поддерживает только формат S/MIME защищенных почтовых сообщений, и поэтому в настройках сервера Exchange должна стоять опция использования формата MIME и разрешения маршрутизации защищенных сообщений S/MIME.
3. Криптопровайдер КриптоПро CSP не поддерживает работу KMS сервера Exchange и хранения сертификатов открытых ключей в глобальной адресной книге. Поэтому для создания сертификатов открытых ключей должен использоваться внешний центр сертификации.
4. Для хранения сертификатов открытых ключей абонентов используйте локальную или общую (корпоративную) папку **Контакты**.

Настройка Outlook 2007

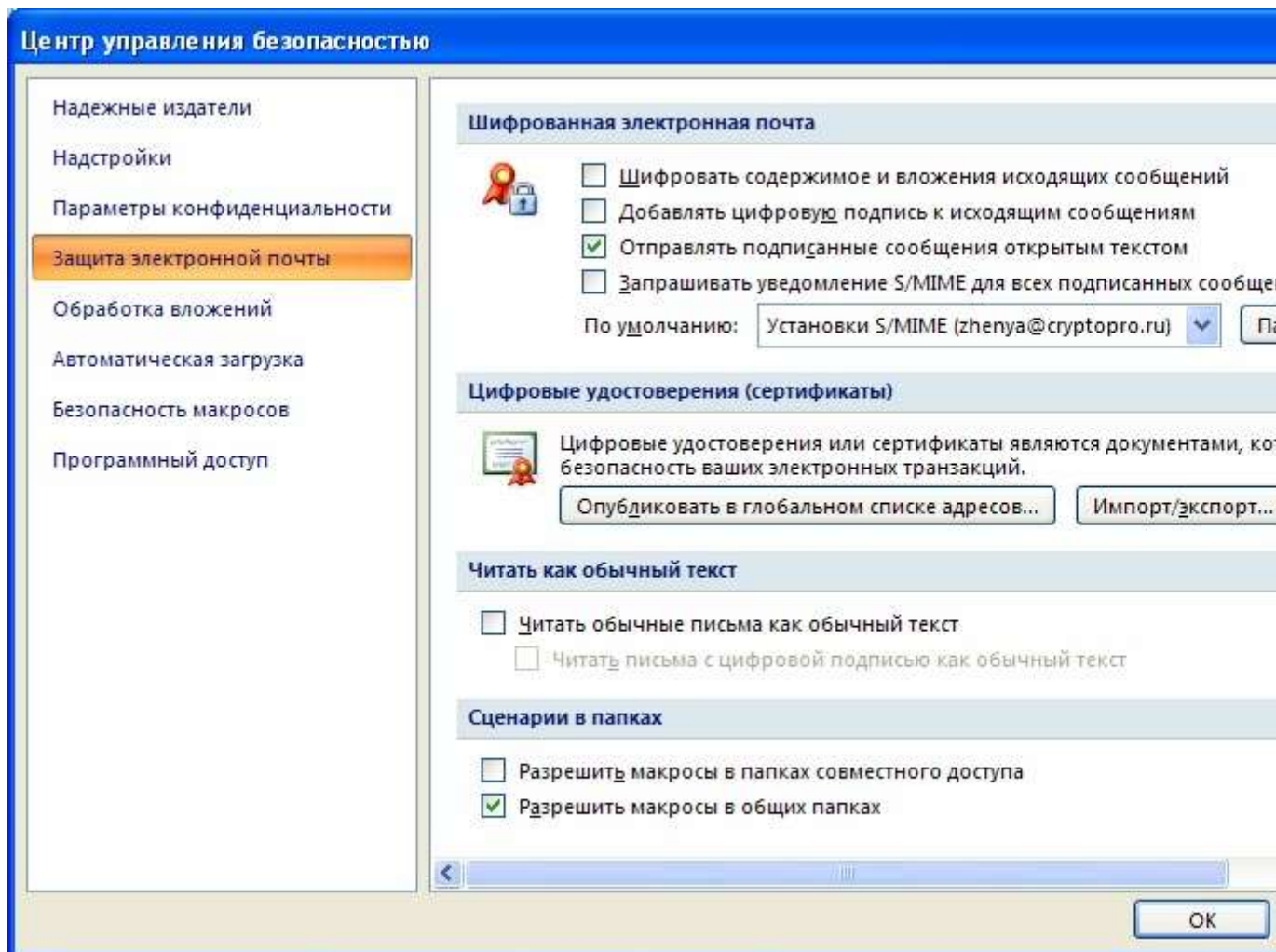
Выберите пункт меню **Сервис, Центр управления безопасностью** и нажмите на закладку **Защита электронной почты**. Нажмите кнопку **Параметры**.



Выберите личные сертификаты, соответствующие ключам подписи и шифрования, используя кнопку **Выбрать**. Отображаемый диалог позволяет пользователю указать свои личные сертификаты, которые будут использоваться при выборе личных ключей пользователя для

формирования электронной цифровой подписи и расшифрования входящих сообщений. Как уже было отмечено ранее, в диалоге выбора сертификата отображаются только сертификаты, имеющие совпадающий адрес электронной почты и разрешенные для защиты электронной почты.

Выберите пункт меню **Сервис, Центр управления безопасностью** и нажмите на закладку **Защита электронной почты**.



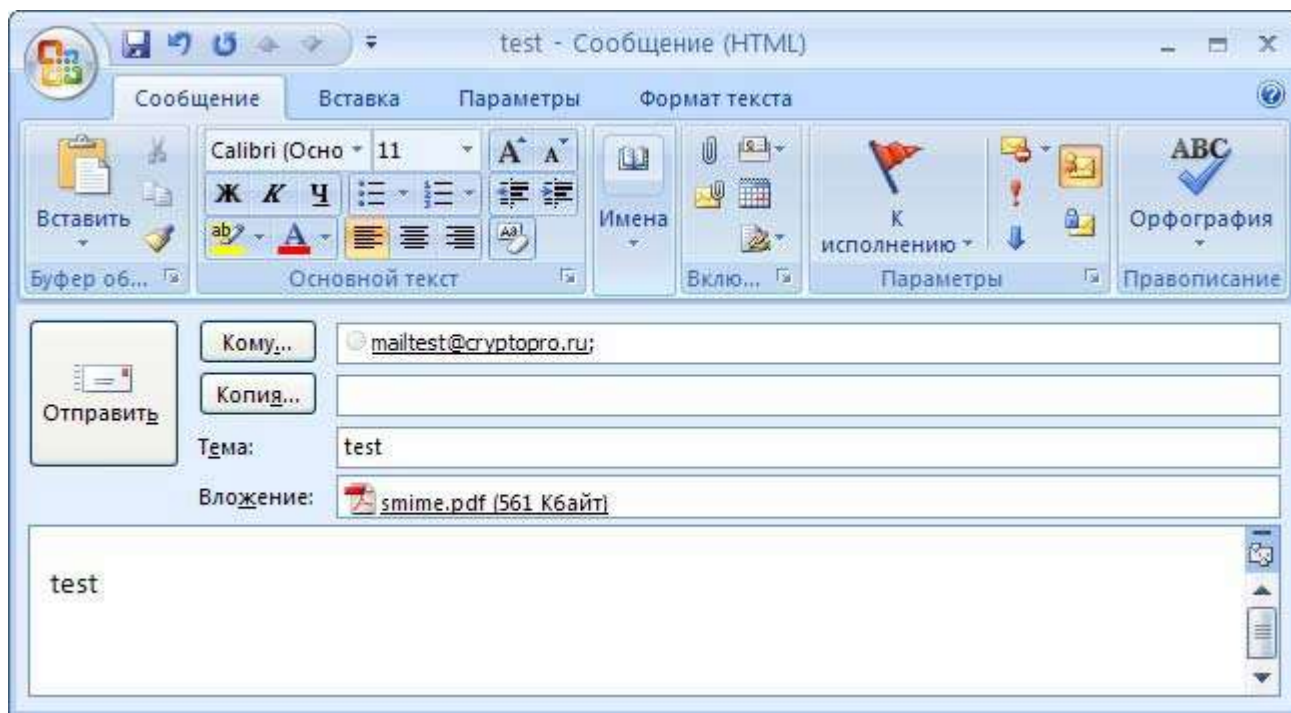
В отображаемом диалоге можно включить режимы **Шифровать содержимое и вложения исходящих сообщений** и **Добавлять цифровую подпись к исходящим сообщениям** для того, чтобы шифрование и электронная цифровая подпись выполнялись автоматически для каждого сообщения. Если эти режимы не включены, опции шифрования и подписи нужно будет включать для каждого отправляемого сообщения. В этом же диалоге дополнительно можно установить опцию **Отправлять подписанные сообщения открытым текстом**. При включенном режиме подпись формируется в виде одного отдельного вложения для всех вложений. Если режим выключен - сообщения и все вложения будут объединены в единое вложение с включенной в него цифровой подписью.

Отправка подписанных сообщений

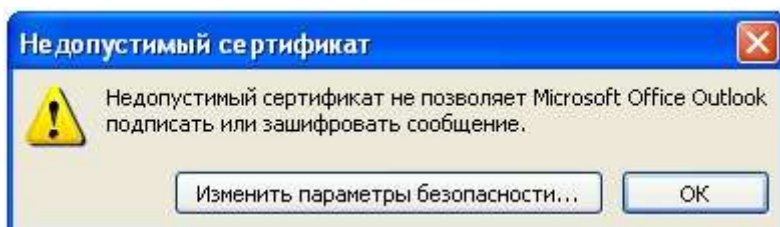
Для создания и отправки подписанного сообщения нажмите кнопку **Создать** или выберите пункт меню **Файл, Создать, Сообщение**.

Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить файл**. Для отправки сообщения в подписанном виде нажмите кнопку **Письмо**.

После того, как сообщение подготовлено к отправке, нажмите кнопку **Отправить**.



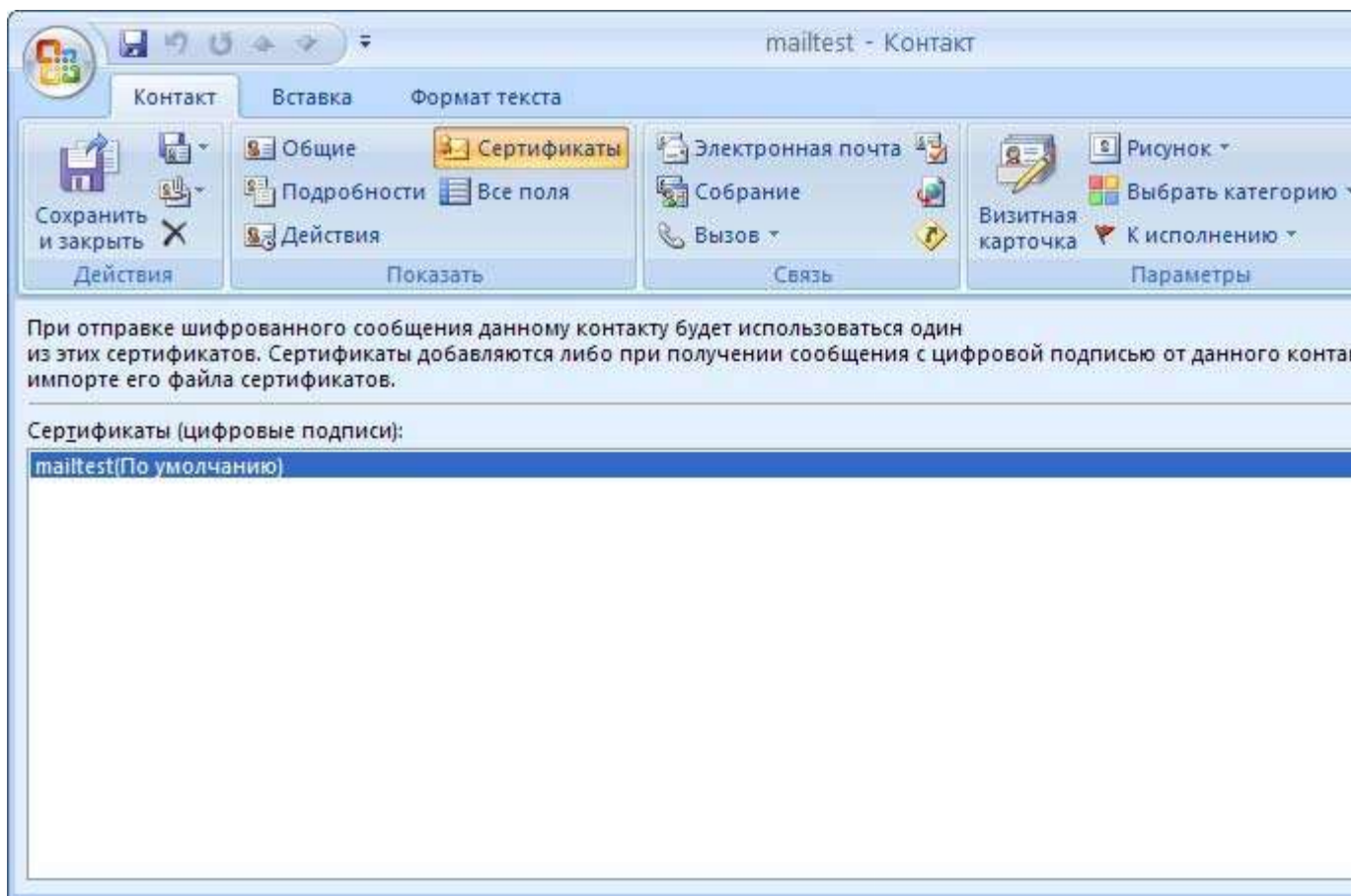
Если сертификат, с помощью которого подписано сообщение, был отозван, то появится следующее предупреждение, а само сообщение не будет отправлено.



Получение сертификата открытого ключа абонента для шифрования сообщений

Для шифрования сообщений в адрес других пользователей необходимо предварительно произвести обмен сертификатами. Для этого обычно достаточно переслать подписанное сообщение в адрес требуемого абонента (сообщение посылается вместе с сертификатом отправителя). После получения сообщения и проверки электронной цифровой подписи производится автоматическое добавление адреса отправителя и его сертификата в адресную книгу.

Для контроля добавления выполните следующие действия. Откройте полученное подписанное письмо. Установите курсор на адрес отправителя и, нажав правую кнопку мыши, выберите пункт **Добавить в контакты Outlook**. В отображаемом диалоге нажмите на закладку **Сертификаты** и убедитесь в наличии сертификата отправителя.



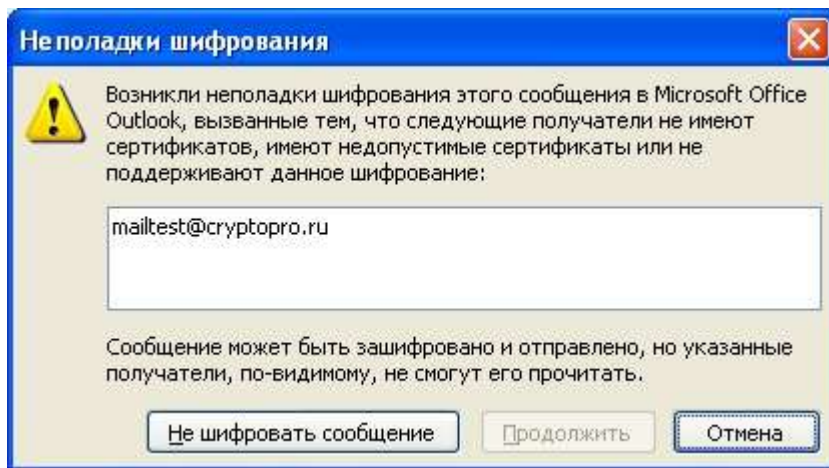
После этого нажмите на кнопку **Сохранить и закрыть**. Если абонент с таким адресом уже существует, программа предложит, либо **добавить новый контакт**, либо **обновить сведения о выделенном контакте**. Выберите второй пункт. При этом в существующий контакт будет добавлен полученный сертификат. Если контакт до этого содержал сертификат, новый сертификат станет использоваться по умолчанию.

Отправка зашифрованных сообщений

Для создания и отправки зашифрованного сообщения нажмите кнопку **Создать** или выберите пункт меню **Файл, Создать, Сообщение**.

Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить файл**. Для отправки сообщения в зашифрованном виде нажмите кнопку. После того, как сообщение подготовлено к отправке, нажмите кнопку **Отправить**.

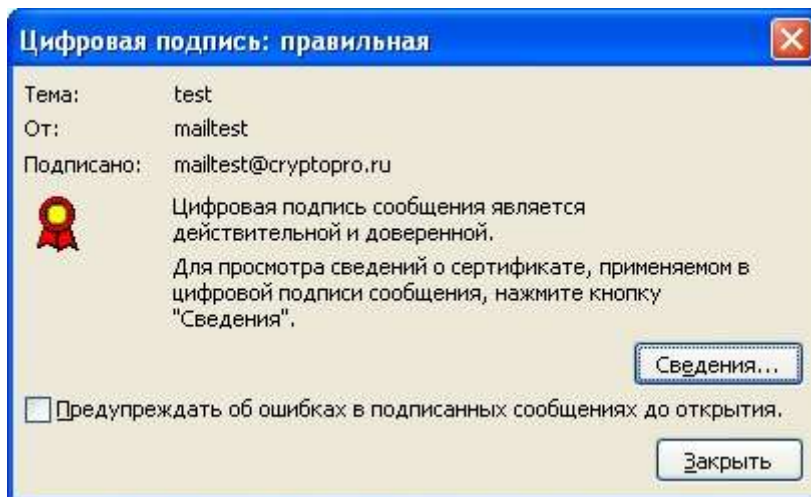
При попытке зашифровать письмо на открытом ключе владельца отозванного сертификата, появится следующее предупреждение.



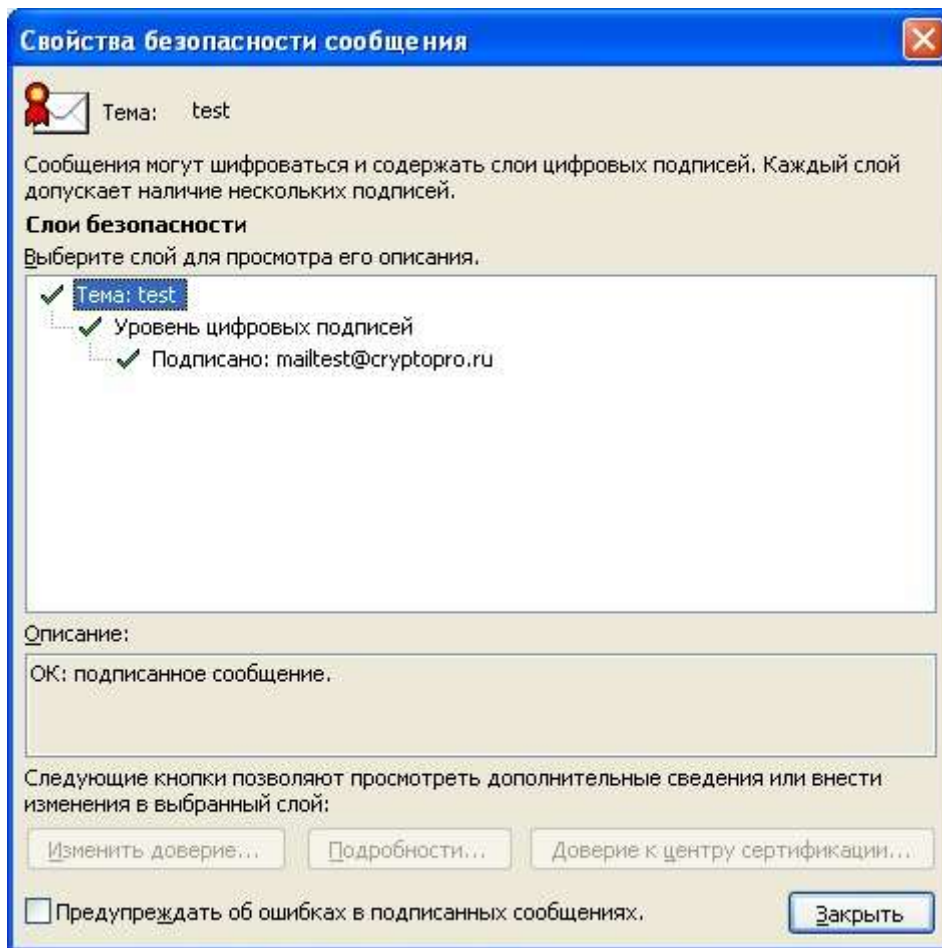
Проверка сертификата на отзыв

Для контроля проверки сертификатов на отзыв выполните следующие действия.

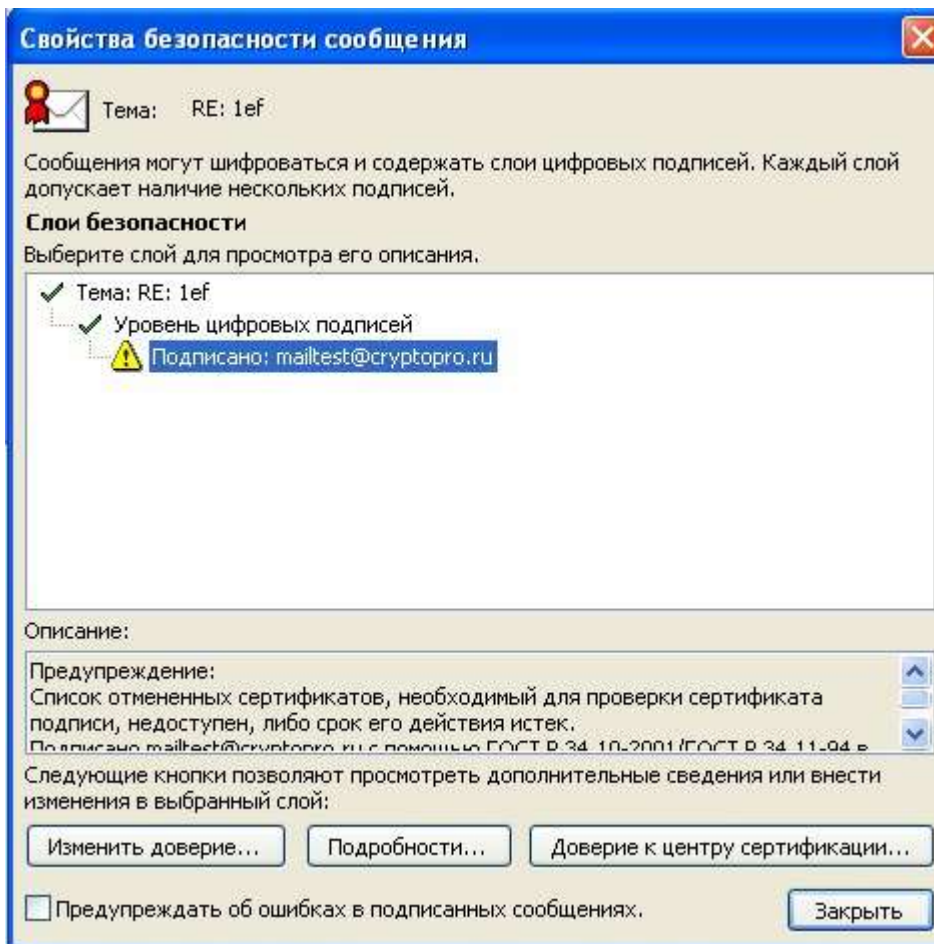
Откройте полученное подписанное письмо. Нажмите кнопку – признак подписанного сообщения.



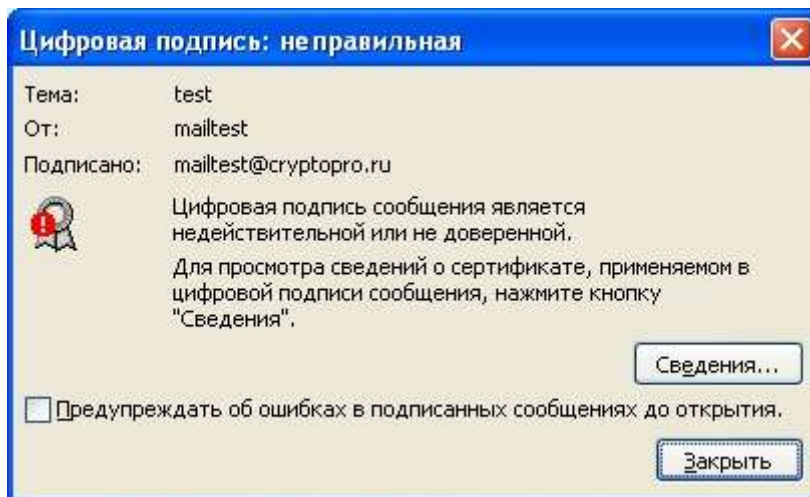
Нажмите кнопку **Сведения**. Если сертификат действительный и не был отозван, то откроется окно, подобное этому:



А если открывшееся окно подобно следующему, то СОС не установлен либо срок его действия истек. Обновите СОС, хранящийся в локальном справочнике сертификатов, с использованием доступных средств.



Если же СОС обновлен, а письмо подписано отозванным сертификатом, то при нажатии кнопки появится следующее предупреждение:



Нажмите кнопку Сведения для просмотра сведений о сертификате:

Свойства безопасности сообщения



Тема: test

Сообщения могут шифроваться и содержать слои цифровых подписей. Каждый слой допускает наличие нескольких подписей.

Слои безопасности

Выберите слой для просмотра его описания.

- Тема: test
- Уровень цифровых подписей
- Подписано: mailtest@cryptopro.ru

Описание:

Ошибка:

Использованный для создания данной подписи сертификат находится в допустимом списке отмененных сертификатов.
Подписано mailtest@cryptopro.ru с помощью ГОСТ Р 34.10.2001/ГОСТ Р 34.11.94 в

Следующие кнопки позволяют просмотреть дополнительные сведения или внести изменения в выбранный слой:

Изменить доверие...

Подробности...

Доверие к центру сертификации...

Предупреждать об ошибках в подписанных сообщениях.

Закреть