Использование КриптоПро CSP в Outlook 2002/2003

Особенностями использования почтовой программы Outlook 2002/2003 и сервера Exchange являются:

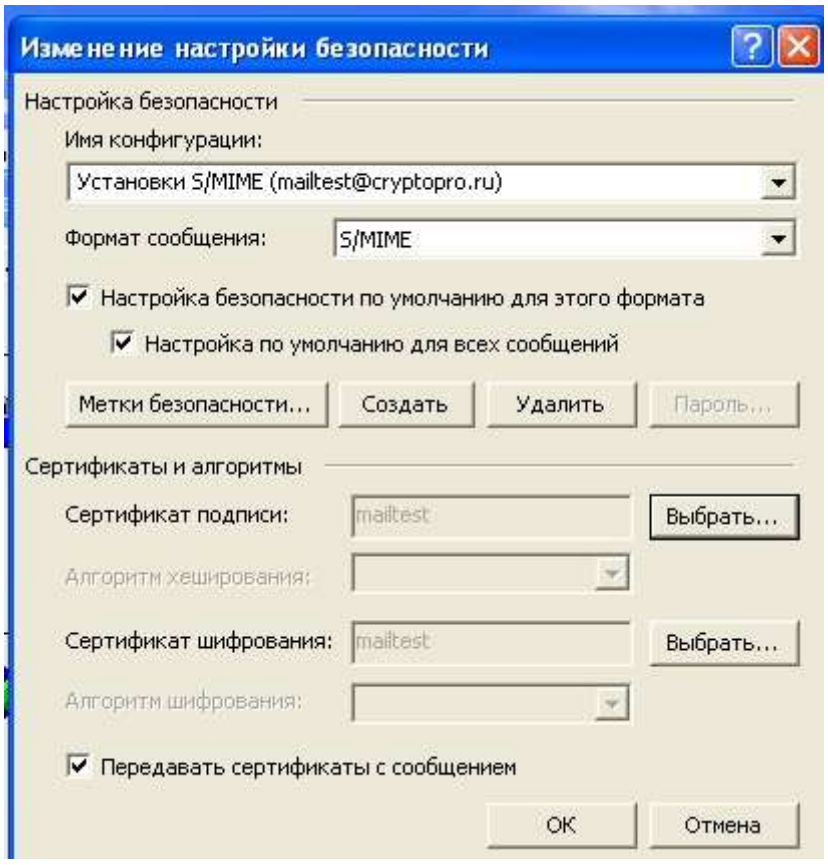
1. Криптопровайдер КриптоПро CSP поддерживает только формат S/MIME защищенных почтовых сообщений, и поэтому в настройках сервера Exchange должна стоять опция использования формата MIME и разрешения маршрутизации защищенных сообщений S/MIME.

2. 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.

3. Для хранения сертификатов открытых ключей абонентов используйте локальную или общую (корпоративную) папку**Контакты**.

Настройка Outlook 2002/2003

Выберите пункт меню **Сервис, Параметры**… и нажмите на закладку **Безопасность**. Нажмите кнопку **Параметры**.



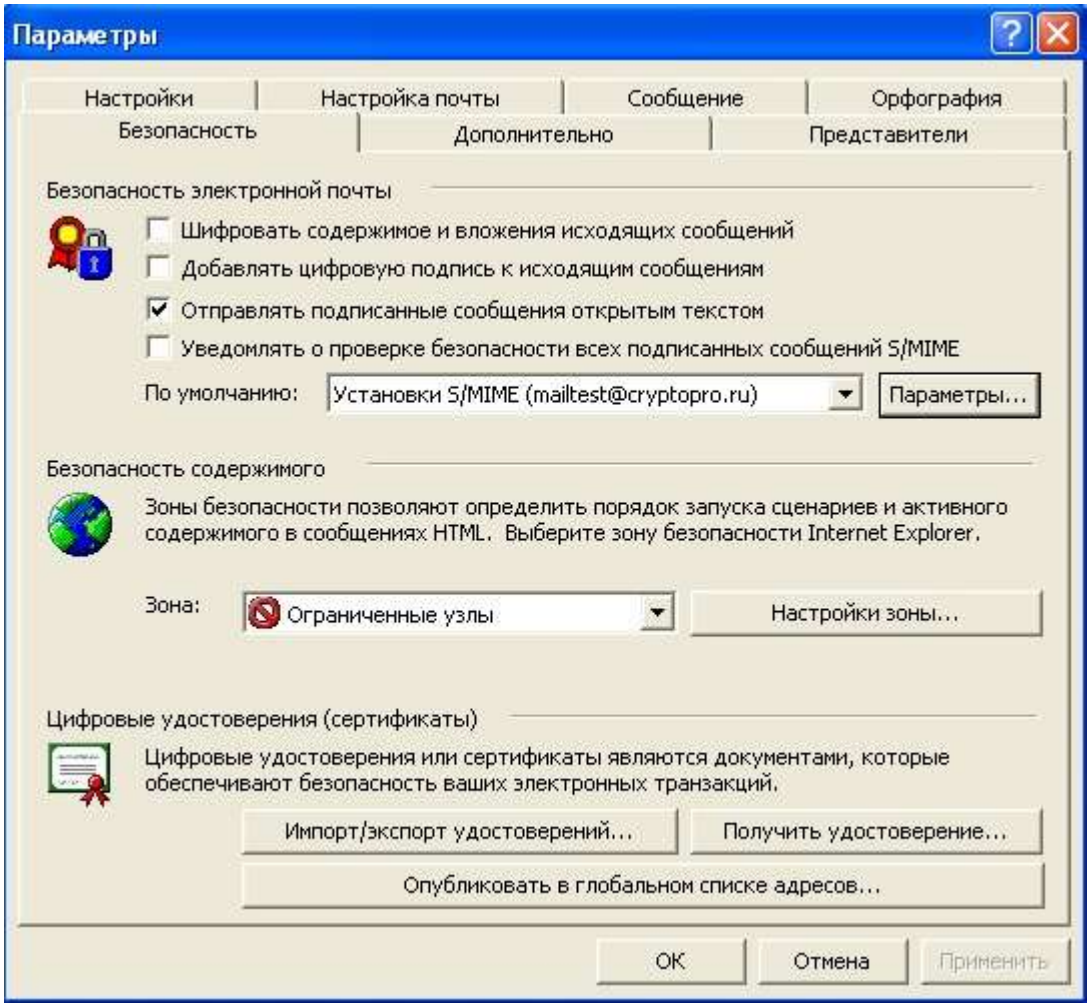
Выберите личные сертификаты, соответствующие ключам подписи и шифрования, используя кнопку **Выбрать**. Отображаемый диалог позволяет пользователю указать свои личные сертификаты, которые будут использоваться при выборе личных ключей

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, Параметры**... и нажмите на закладку**Безопасность**. 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.

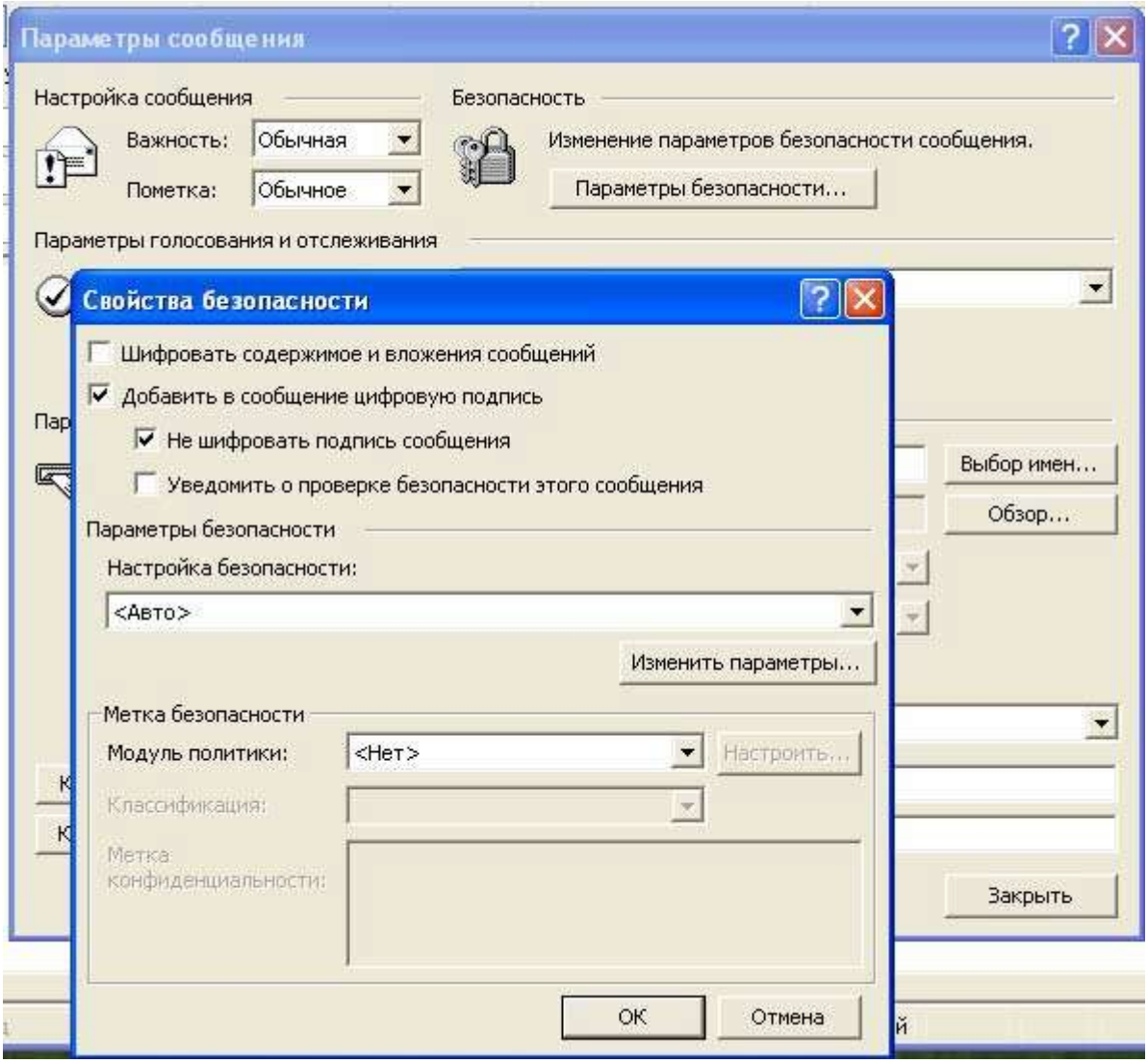
Если режим выключен - сообщения и все вложения будут объединены в единое вложение с включенной в него цифровой подписью.

Отправка подписанных сообщений

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

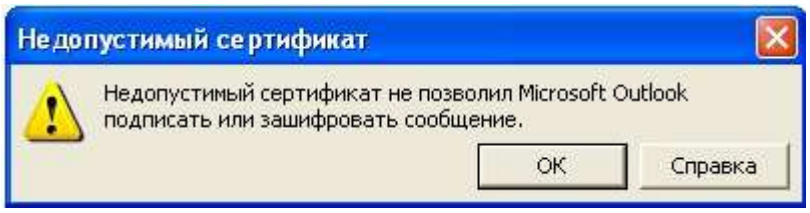
Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить**.

Для отправки сообщения в подписанном виде нажмите кнопку , затем кнопку **Параметры безопасности**, и в отображаемом диалоге установите флаг **Добавить в сообщение цифровую подпись.**



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

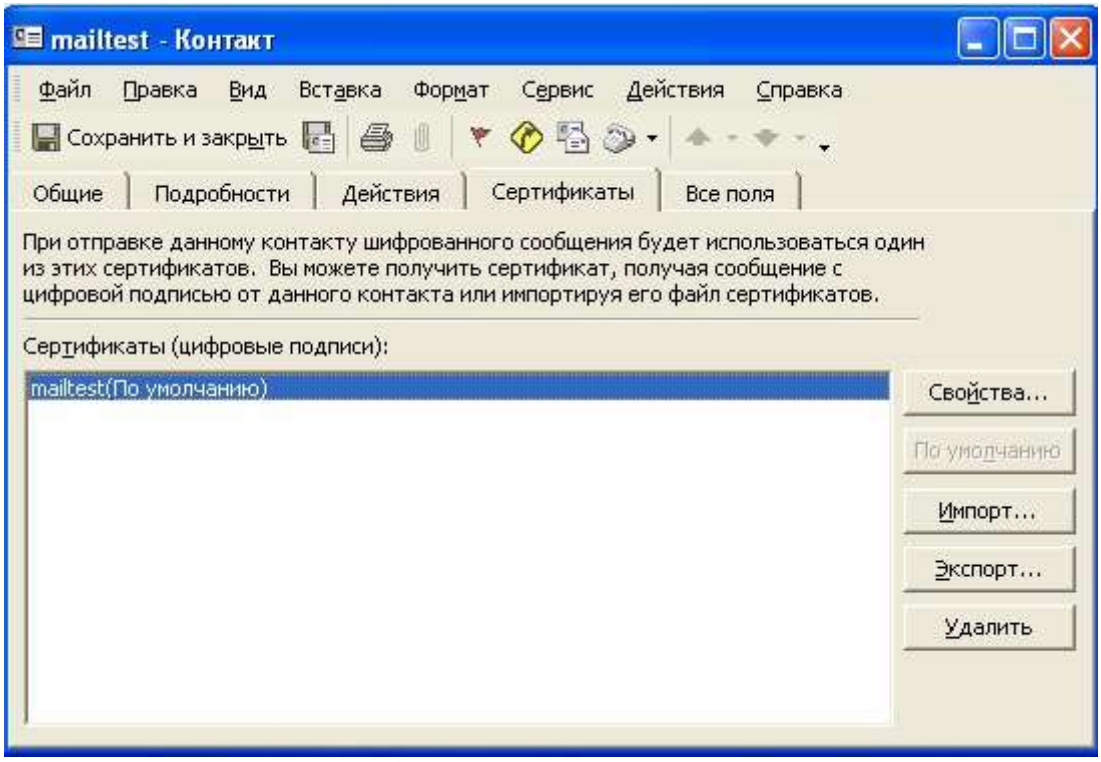
Если сертификат, с помощью которого подписано сообщение, был отозван, то появится следующее предупреждение, а само сообщение не будет отправлено.



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 к контактам.** 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 данный контакт как новый**, либо **обновить существующий контакт.** Выберите пункт обновить существующий контакт. При этом в существующий контакт будет добавлен полученный сертификат. Если контакт до этого содержал сертификат, новый сертификат станет использоваться по умолчанию.

Отправка шифрованных сообщений

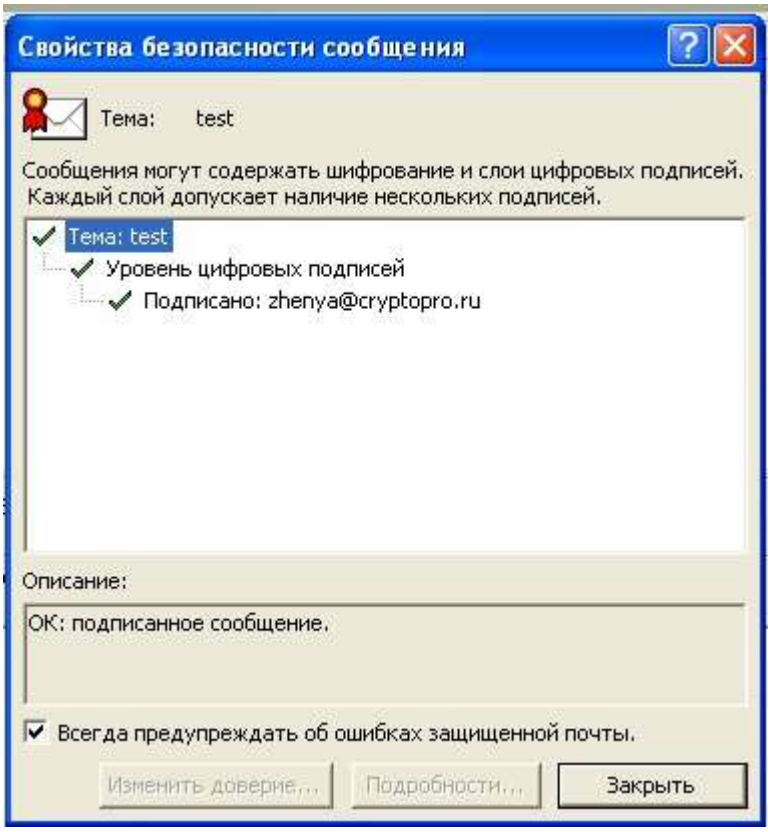
Для создания и отправки шифрованного сообщения нажмите кнопку **Создать** или выберите пункт меню **Файл, Создать, Сообщение.**

Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить**. Для отправки сообщения в зашифрованном виде нажмите кнопку , затем кнопку **Параметры безопасности**, и в отображаемом диалоге установите флаг **Шифровать содержимое и вложения сообщений.** После того, как сообщение подготовлено к отправке, нажмите кнопку**Отправить**. При попытке зашифровать письмо на открытом ключе владельца отозванного сертификата возникнет та же ситуация, что и при отправке сообщения, подписанного с помощью отозванного сертификата.

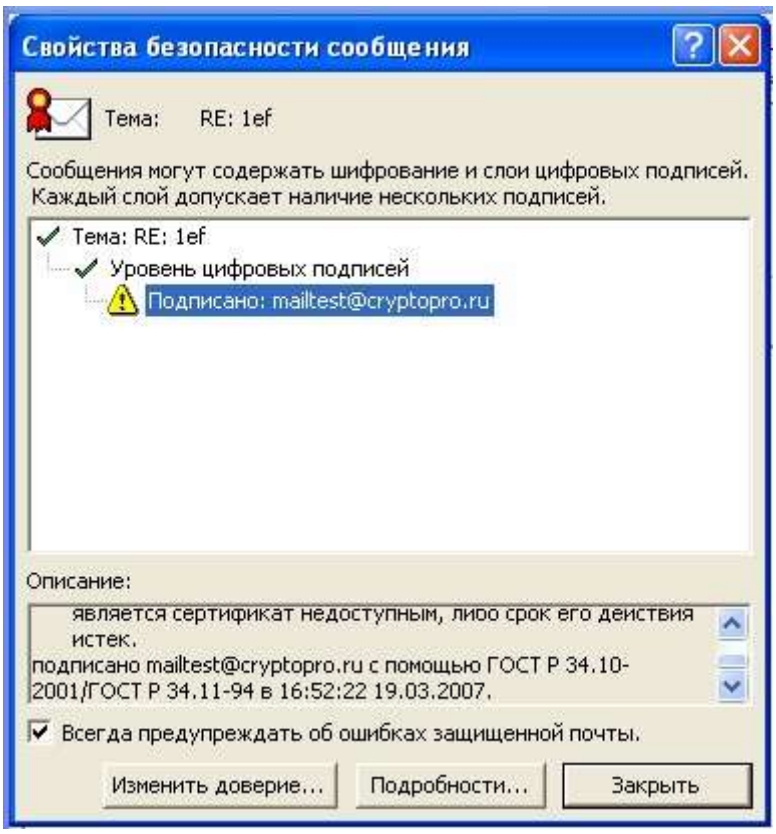
Проверка сертификата на отзыв

Для контроля проверки сертификатов на отзыв выполните следующие действия.

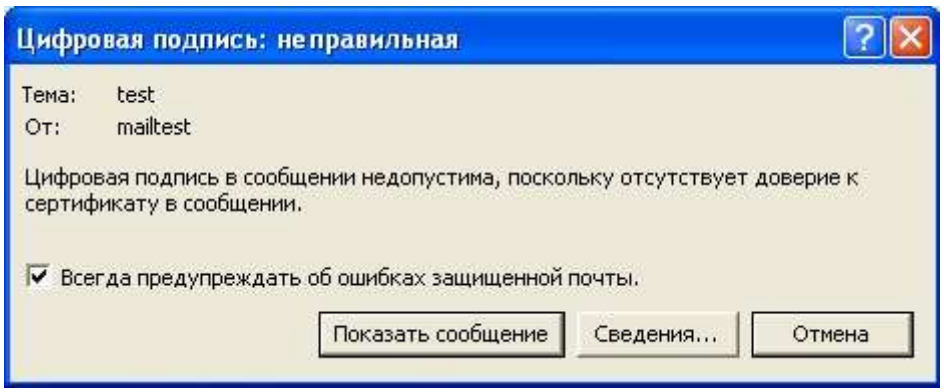
Откройте полученное подписанное письмо. Нажмите кнопку – признак подписанного сообщения. Если сертификат действительный и не был отозван, то откроется окно, подобное этому:



Следующее предупреждение означает, что СОС не установлен либо срок его действия истек. Обновите СОС, хранящийся в локальном справочнике сертификатов, с использованием доступных средств.



Если же СОС обновлен, то при открытии письма, подписанного отозванным сертификатом, появится следующее предупреждение:



Нажмите кнопку **Сведения** для просмотра сведений о сертификате: