

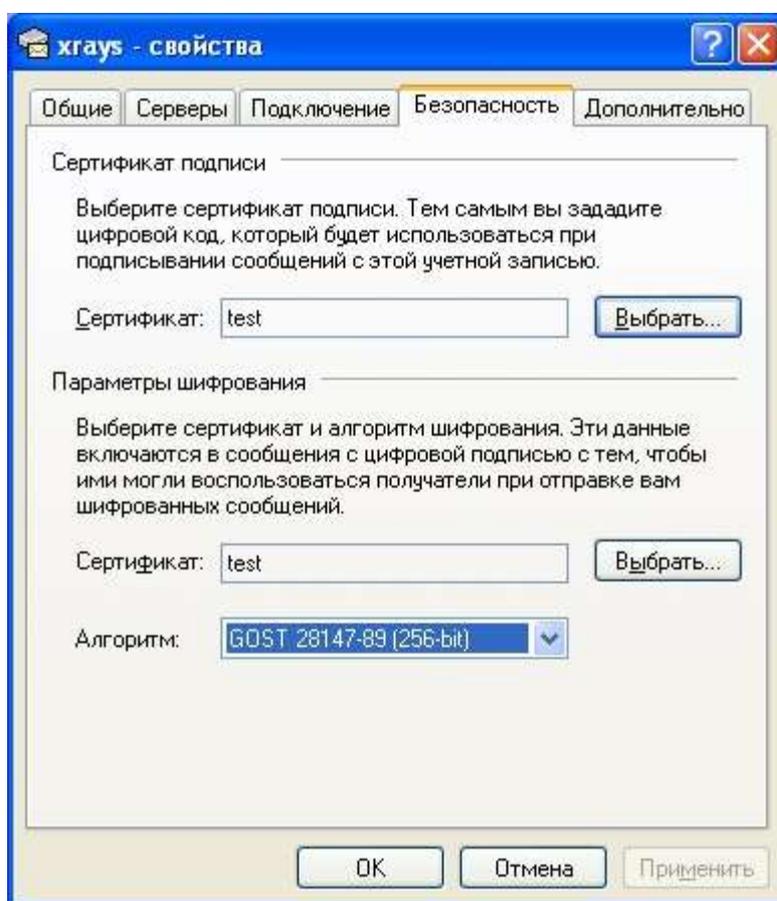
Использование КриптоПро CSP в Outlook Express

Настройка Outlook Express

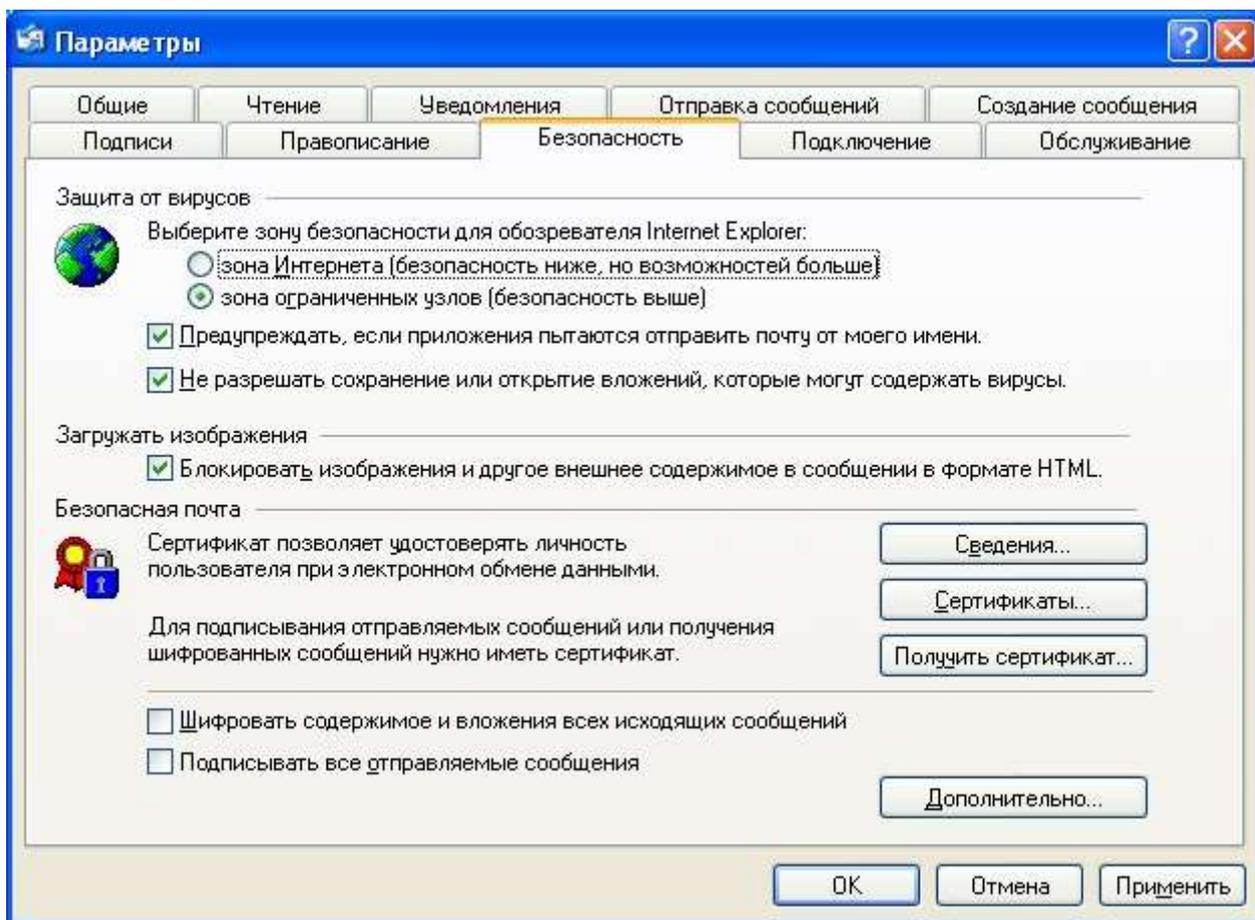
Выберите пункт меню **Сервис, Учетные записи...** и нажмите на закладку **Почта**. В отображаемом списке учетных записей выберите ту, которую необходимо настроить, и нажмите кнопку **Свойства**. В отображаемом диалоге выберите закладку **Безопасность**.

Отображаемый диалог позволяет пользователю указать свои личные сертификаты, которые будут использоваться при выборе личных ключей пользователя для формирования электронной цифровой подписи и расшифровки 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 **Включить цифровую подпись во все отправляемые сообщения** 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.

Нажмите кнопку **Дополнительно**. В отображаемом диалоге установите следующие режимы:

Шифровать при отправке зашифрованной почты самому себе. Установка режима включения дает возможность отправителю расшифровывать отправленные им сообщения.

Добавлять мой сертификат при отправлении сообщений с подписью.

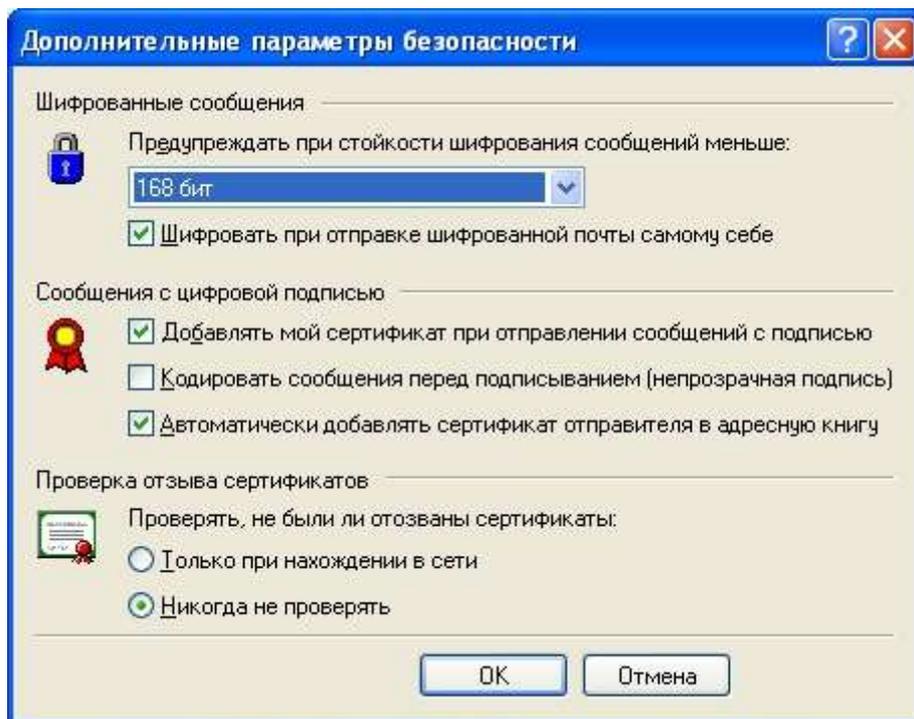
Установка этого режима автоматически будет добавлять сертификат отправителя ко всем сообщениям. Этот режим позволяет производить обмен сертификатами с использованием подписанного сообщения, а затем использовать полученные сертификаты для

последующего шифрования сообщений между адресатами.

Кодировать сообщения перед подписыванием (непрозрачная подпись). При включенном режиме сообщения и все вложения будут объединены в единое вложение с включенной в него цифровой подписью. Если режим выключен – подпись формируется в

виде одного отдельного вложения для всех вложений.

Автоматически добавлять сертификат отправителя в адресную книгу. При включенном режиме сертификаты, передаваемые в составе подписанного сообщения, будут автоматически добавляться в адресную книгу.



Проверять, не были ли отозваны сертификаты:

только при нахождении в сети – установка флага проверки приводит к тому, что каждая операция формирования или проверки электронной цифровой подписи будет сопровождаться проверкой на отзыв сертификата.

Для проверки на отзыв используется **список отозванных сертификатов (CRL)**, информация о нахождении которого, записывается в виде дополнения в сертификате каждого пользователя. По умолчанию данная опция не включена, и Outlook Express

не отслеживает факта компрометации ключей пользователей.

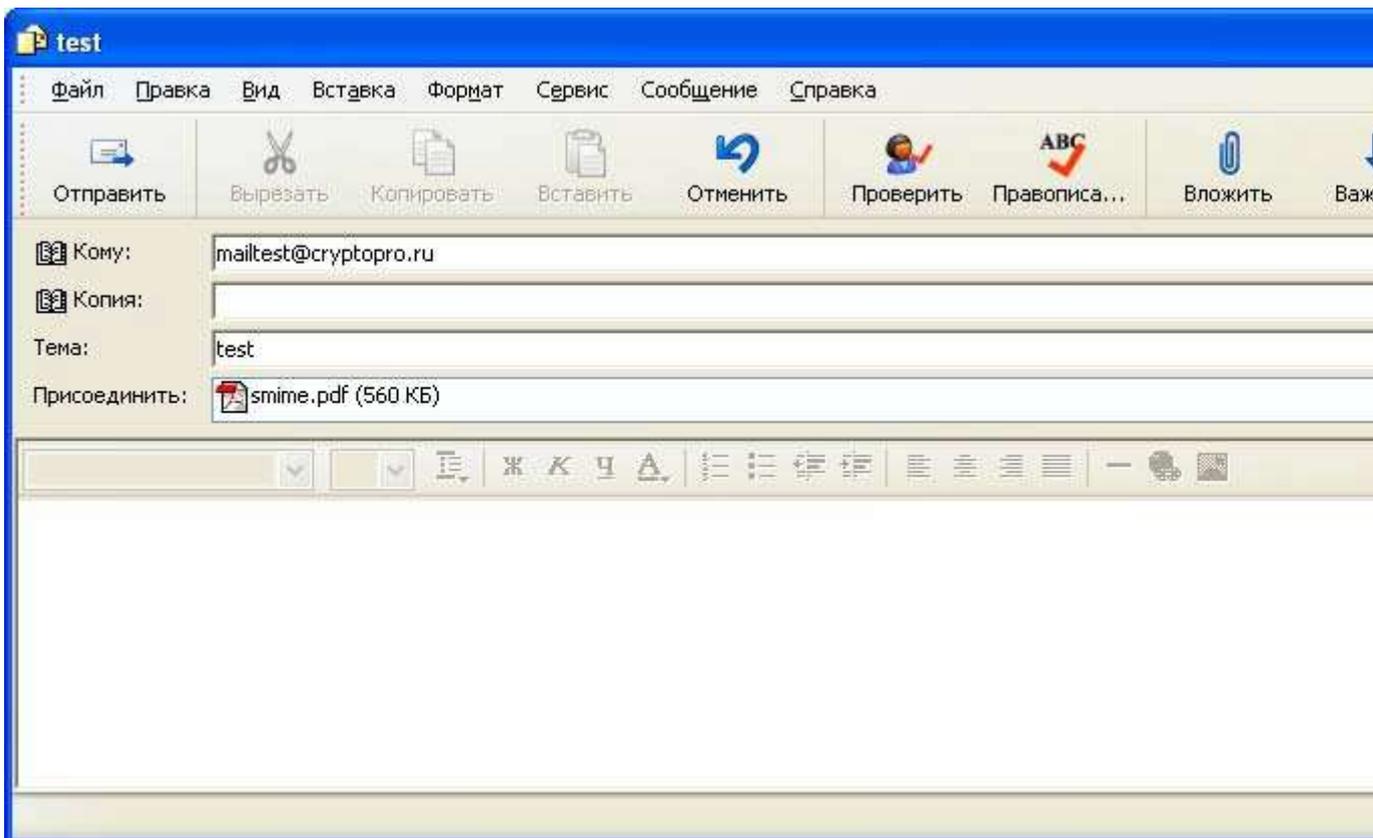
никогда не проверять – проверка на отзыв не выполняется.

Отправка подписанных сообщений

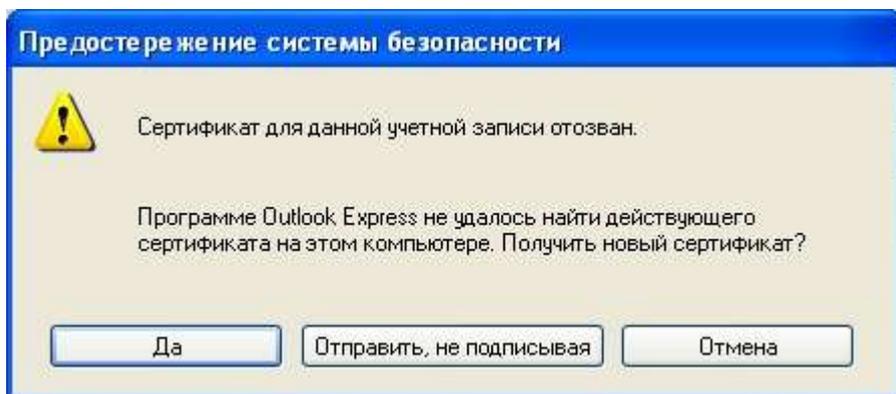
Для создания и отправки подписанного сообщения нажмите кнопку **Создать сообщение** или выберите пункт меню **Файл, Создать, Сообщение**.

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 проверьте состояние кнопки **Подписать**.

Она должна быть нажата и должен быть виден признак подписанного сообщения в правой части экрана.



После того, как сообщение подготовлено к отправке, нажмите кнопку **Отправить**. Если в ответ появится следующее предупреждение, то это означает, что сертификат был отозван.

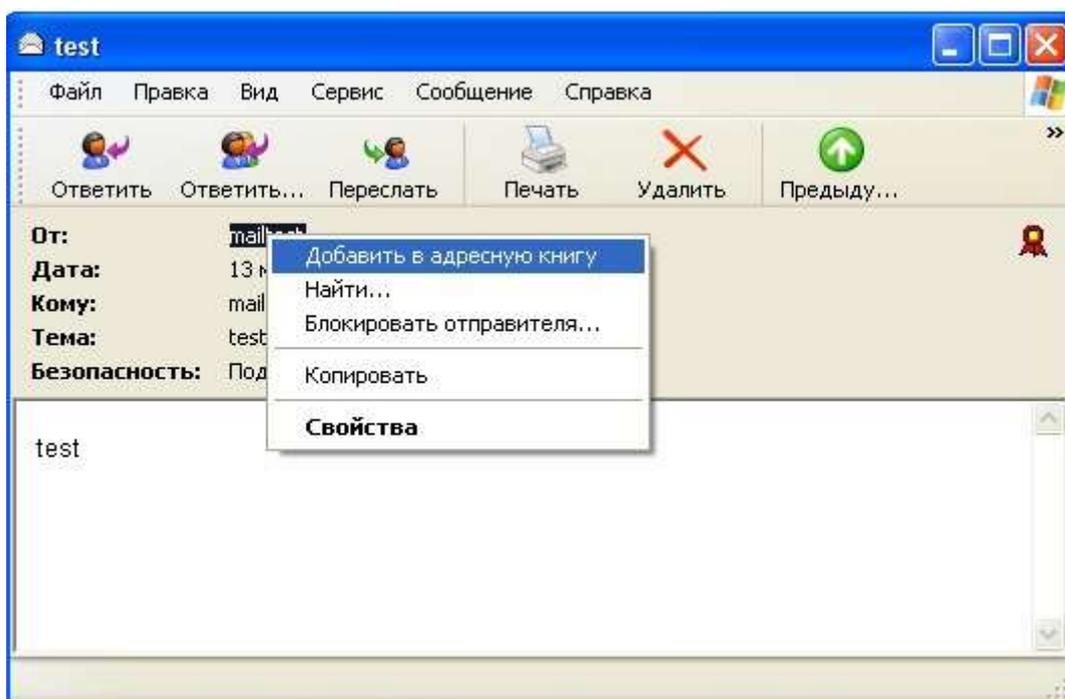


Получение сертификата открытого ключа абонента для шифрования сообщений

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 адресную книгу**.



Для того, чтобы проверить наличие сертификата абонента в адресной книге, нажмите на кнопку **Адреса** в основном меню и выберите запись с требуемым абонентом (см. Рисунок 2). Если в записи абонента отсутствует сертификат или сертификат не обновился

(у абонента был старый сертификат), удалите полностью запись абонента из адресной книги и получите от него подписанное сообщение еще раз. При этом должно произойти автоматическое создание записи с сертификатом.

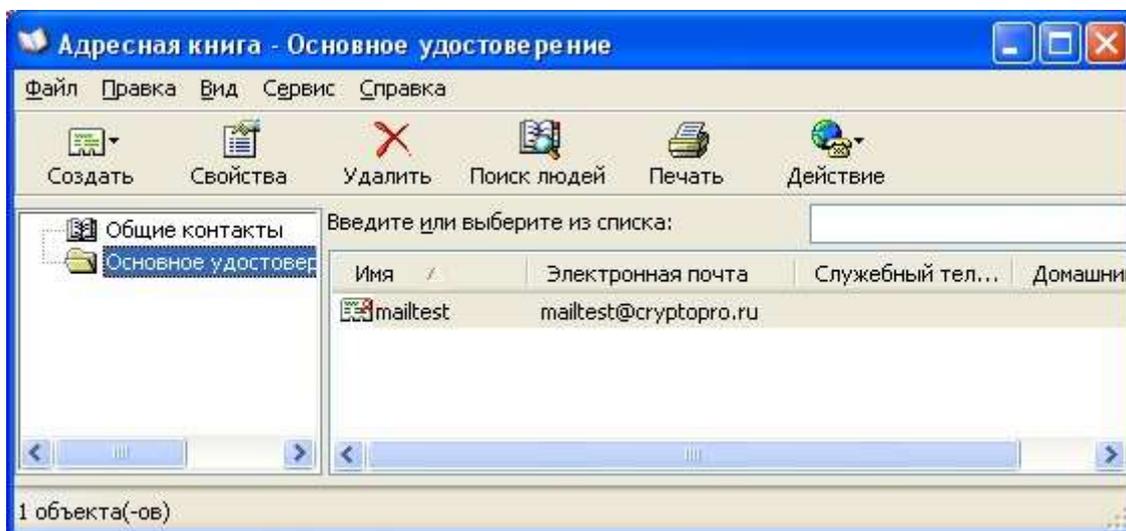


Рисунок 2. Адресная книга

Отправка шифрованных сообщений

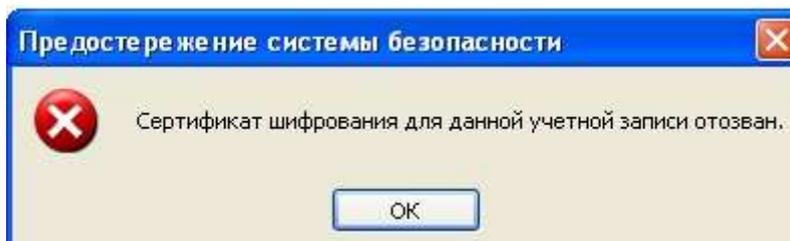
Для создания и отправки подписанного сообщения нажмите кнопку **Создать сообщение** или выберите пункт меню **Файл, Создать, Сообщение**.

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 проверьте состояние кнопки **Зашифровать**.

Она должна быть нажата и должен быть виден признак шифрованного сообщения в правой части экрана. 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. А предупреждающее окно будет выглядеть так:



Проверка сертификата на отзыв

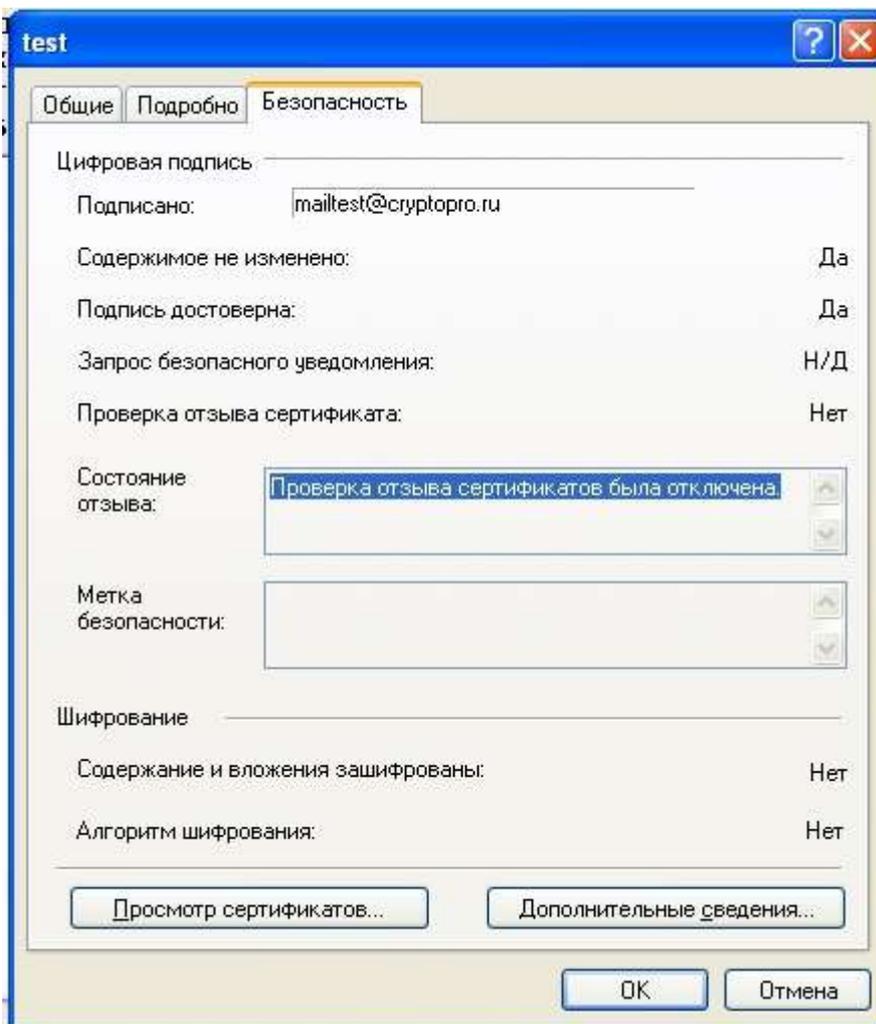
Периодичность издания списков отозванных сертификатов (СОС) определяется Удостоверяющим центром. Центр Сертификации издает СОС и публикует его в сетевом справочнике (при его наличии).

Пользователи должны регулярно обновлять СОС, хранящийся в локальном справочнике сертификатов, с использованием доступных средств.

Для контроля проверки сертификатов на отзыв выполните следующие действия.

Откройте полученное подписанное письмо. Нажмите кнопку – признак подписанного сообщения. Как уже было отмечено ранее, для автоматической проверки подписи на отзыв необходимо установить флаг **Проверить, не были ли отозваны сертификаты:**

только при нахождении в сети. В противном случае, в открывшемся диалоге в закладке **Безопасность** увидите следующее:



При установленном флаге проверки, если сертификат не отозван, в графе **Состояние отзыва** получите **Сертификат не был отозван, или не удалось получить информацию об отзыве этого сертификата.**

Если же сертификат отозвали, то при открытии письма появится предупреждение: «Этот сертификат был отозван»

А при нажатии кнопки, в открывшемся окне во вкладке Безопасность будет значиться: **Этот сертификат был отозван.**