Использование КриптоПро CSP в Outlook 2000

Использование средств криптографической защиты в Outlook 2000 для клиента во многом совпадает с использованием в Outlook Express.

Особенностями использования почтовой программы Outlook 2000 и сервера Exchange являются:

1. При использовании Outlook 2000 рекомендуется установить набор исправлений Office 2000 SR-1a, (http://office.microsoft.com/ru-ru/officeupdate/CD010225951049.aspx) который позволяет корректно:

- обрабатывать кодировки KOI8, Win1251 в подписанных сообщениях (без этого кодировка должна быть UTF-8);
- обрабатывать ошибку невозможности шифрования сообщения с использованием получателя из глобального списка адресов сервера Exchange.

2. Версия Outlook, входящая в состав Office 2000, устанавливаемая дистрибутивом, не обрабатывает списки отозванных сертификатов.

Для устранения этой ошибки необходимо добавить следующий ключ в реестре Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\{7801ebd0-cf4b-11d0-851f-0060979387ea} и в этом ключе добавить значение PolicyFlags со значением 0x00010000.

3. Криптопровайдер КриптоПро CSP поддерживает только формат S/MIME

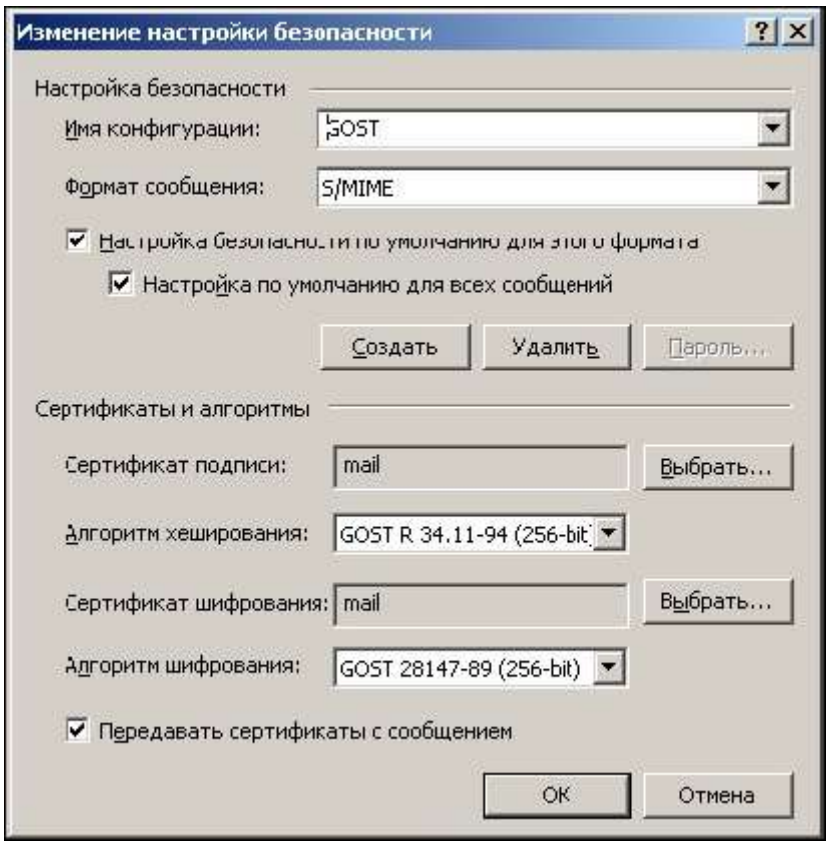
защищенных почтовых сообщений, и поэтому в настройках сервера Exchange должна стоять опция использования формата MIME и разрешения маршрутизации защищенных сообщений S/MIME.

4. 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.

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

Настройка Outlook 2000

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

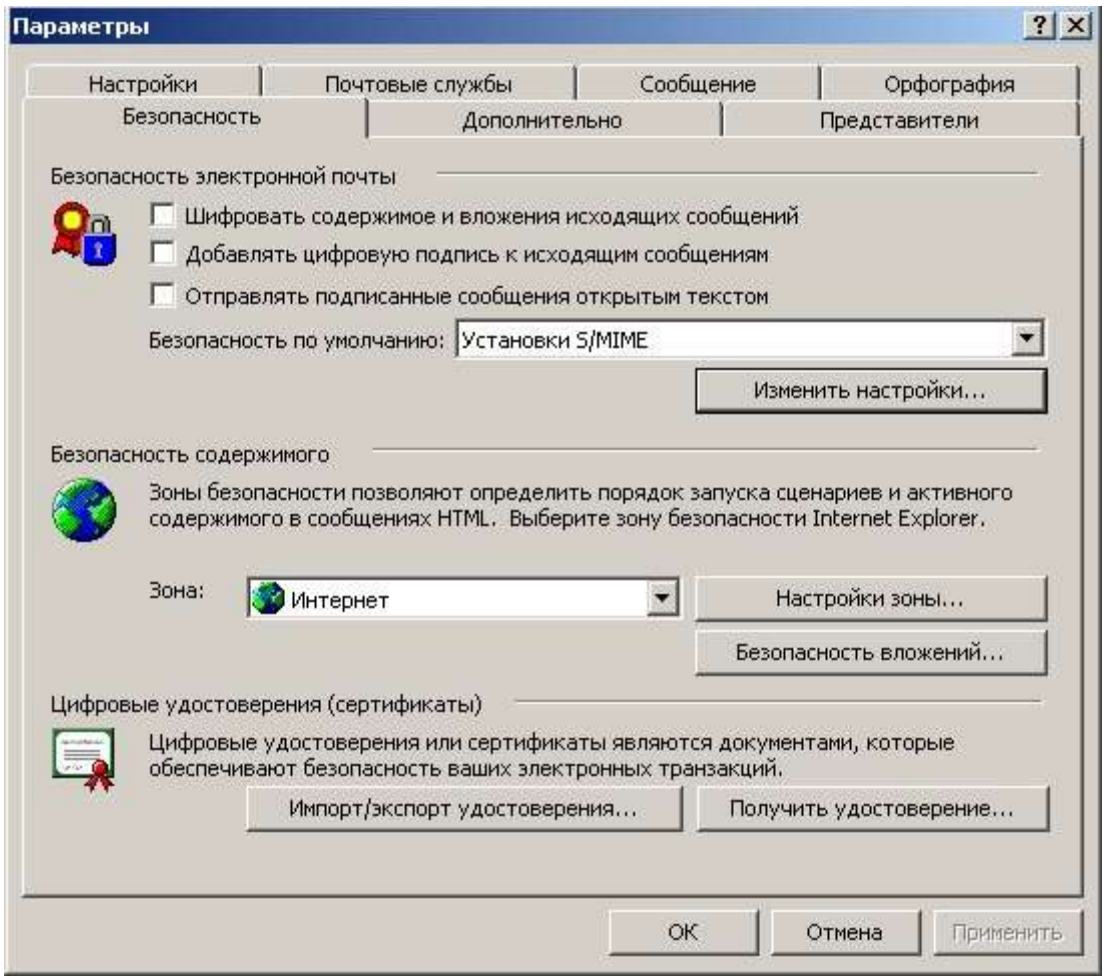


Выберите личные сертификаты, соответствующие ключам подписи и шифрования, используя кнопку **Выбрать**.

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.

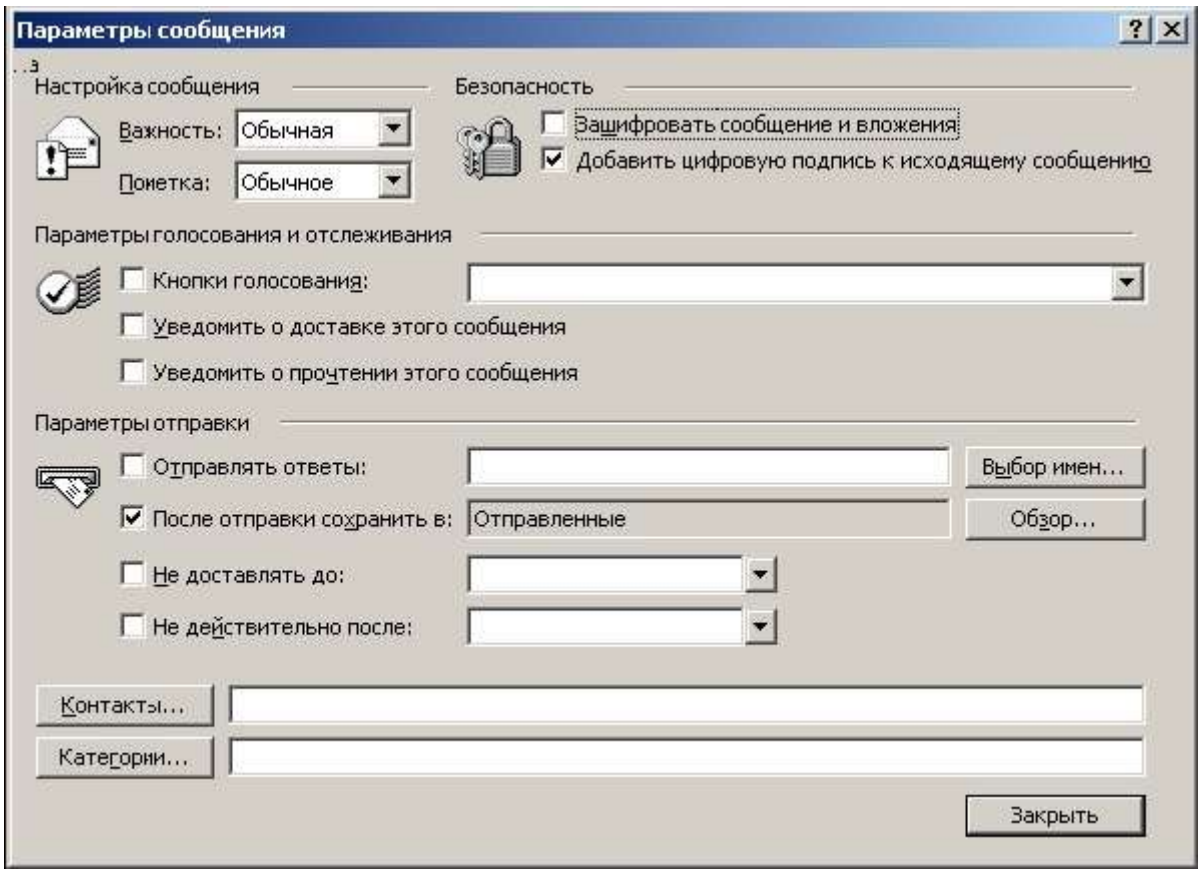
Если режим выключен - сообщения и все вложения будут объединены в единое вложение с включенной в него цифровой подписью.

Отправка подписанных сообщений

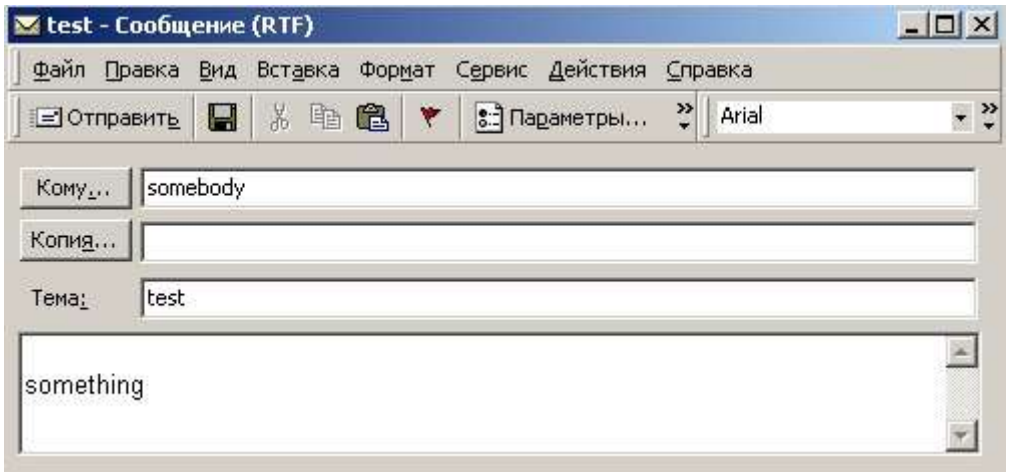
Для создания и отправки подписанного сообщения нажмите кнопку **Создать** или выберите пункт меню **Файл, Создать, Сообщение.**

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

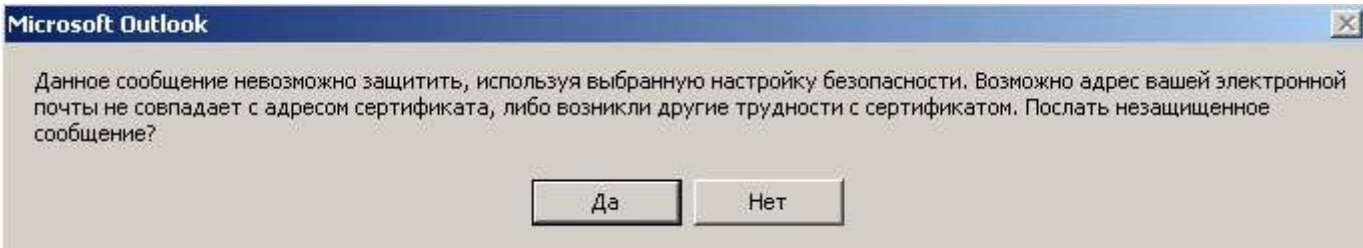
Для отправки сообщения в подписанном виде нажмите кнопку и в отображаемом диалоге установите флаг **Добавить цифровую подпись к исходящему сообщению.**



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



Если сертификат, с помощью которого Вы подписываете сообщение, был отозван, то в ответ появится следующее предупреждение:



Получение сертификата открытого ключа абонента для шифрования сообщений

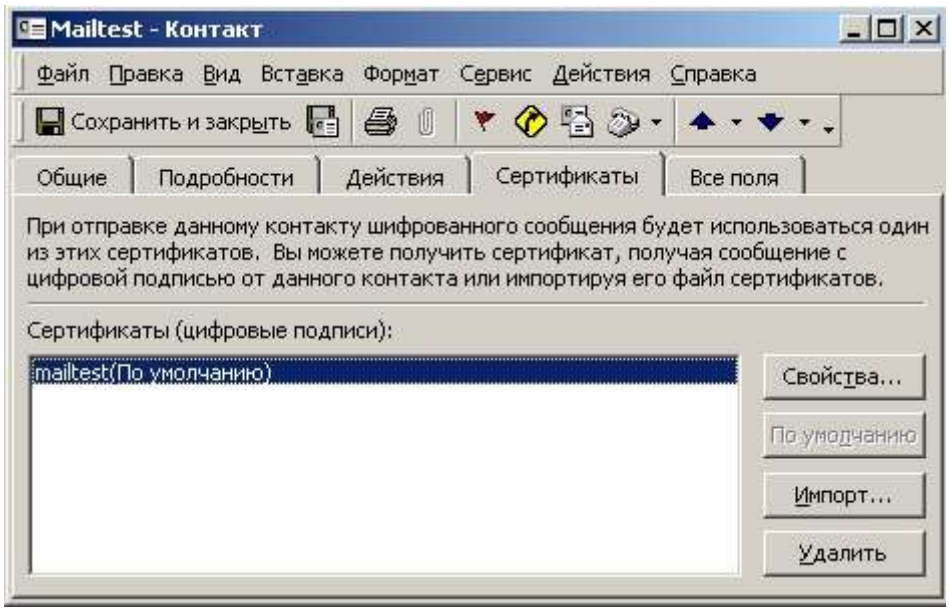
Для шифрования сообщений в адрес других пользователей необходимо предварительно произвести обмен сертификатами.

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**.

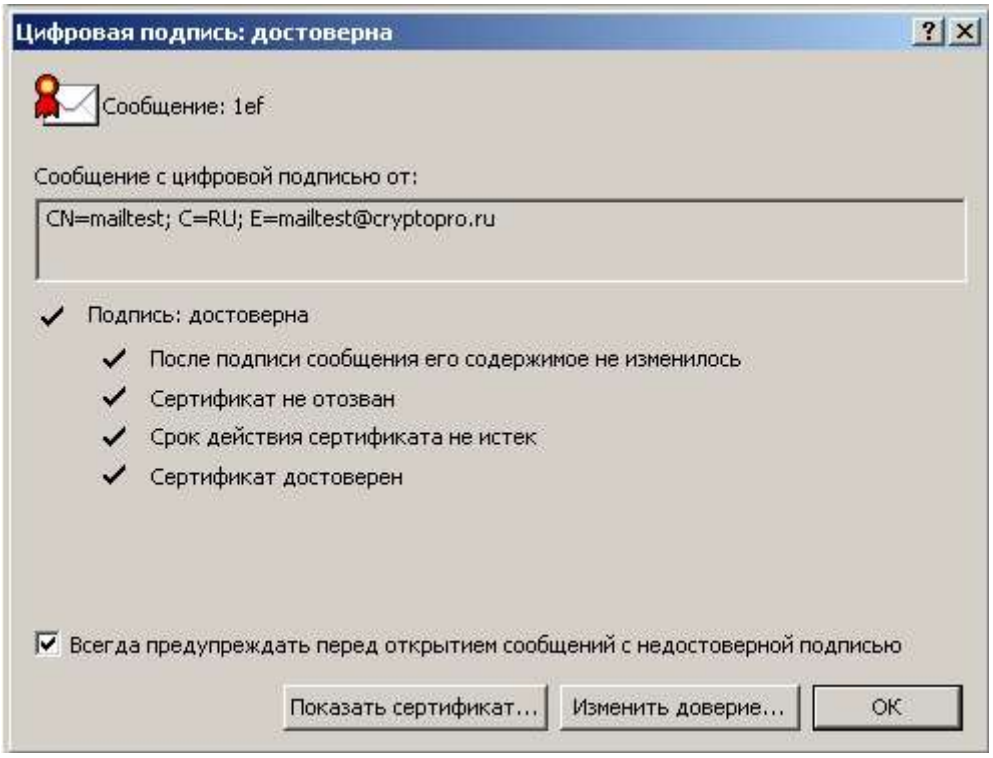
Для отправки сообщения в зашифрованном виде нажмите кнопку и в отображаемом диалоге установите флаг**Зашифровать сообщение и вложение.** После того, как сообщение подготовлено к отправке, нажмите кнопку**Отправить**.

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:



При открытии письма, подписанного отозванным сертификатом, появится следующее предупреждение: **«Цифровая подпись в сообщение недопустима, поскольку отсутствует доверие к сертификату в сообщении»**