Научно-производственное предприятие
“ИЖИНФОРМПРОЕКТ”

Инструкция
по работе с защищенной электронной почтой «КриптоСвязь»

Ижевск 2005

Содержание

1 Общие сведения о защищенной электронной почте «КриптоСвязь»

Защищенная электронная почта является одним из приложений Инфраструктуры открытых ключей (ИОК) / Public Key Infrastructure (PKI) — технологическая инфраструктура и сервисы, гарантирующие безопасность информационных и коммуникационных систем, использующих криптографические алгоритмы с открытыми ключами.

Электронная почта с цифровой подписью позволяет получателю убедиться в подлинности и целостности сообщения. Шифрование сообщений электронной почты препятствует его прочтению другими людьми в процессе доставки.

Шифрованные сообщения или сообщения с цифровой подписью можно читать так же, как и любые другие сообщения.

Если защищенное сообщение с ошибками (например, сообщение подделано или истек срок действия сертификата ключа подписи отправителя), перед тем, как можно будет просмотреть содержимое сообщения будет отображается предупреждение обеспечения безопасности, в котором излагается подробное описание неполадки. На основе содержащихся в предупреждении сведений пользователь может принять решение относительно возможности просмотра данного сообщения и уровня доверия к нему.

В рамках системы защищенной электронной почты «КриптоСвязь» используются почтовые клиенты Outlook Express (рекомендуется версия 6 и выше) и MicroSoft Outlook (рекомендуется версия MicroSoft Outlook 2003 из пакета MicroSoft Office 2003 и выше).

Указанные программы совместимы со спецификациями протокола защищенной электронной почты S/MIME (Secure/Multipurpose Internet Mail Extensions) версии 2 и 3.

Для защиты сообщений используются сертифицированные средства криптографической защиты информации (СКЗИ) «КриптоПро CSP» и совместимые с ним.

Применение сертифицированных СКЗИ обеспечивает использование российских криптографических алгоритмов:

— Алгоритм зашифрования/расшифрования данных и вычисление имитовставки в соответствии с ГОСТ 28147 89 «Системы обработки информации. Защита криптографическая»;

— Алгоритм формирования и проверки ЭЦП в соответствии с ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», а также (до 01.01.2008) ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Система электронной цифровой подписи на базе асимметричного криптографического алгоритма»;

— Алгоритм выработки значения хэш-функции в соответствии с ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

Для возможности работы с защищенной электронной почтой «КриптоСвязь» пользователь должен получить сертификат ключа подписи в Удостоверяющем центре InfoTrust ООО НПП «Ижинформпроект» в соответствии с требованиями Федерального закона от 10 января 2002 № 1-ФЗ «Об электронной цифровой подписи».

После обмена абонентами их сертификатами (сертификат направляется вместе с подписанным сообщением) и помещением этих сертификатов в адресные книги можно направлять сообщения в зашифрованном виде. Когда принимается сообщение с цифровой подписью, сертификат ключа подписи отправителя будет автоматически добавлен адресную книгу, если он там отсутствует.

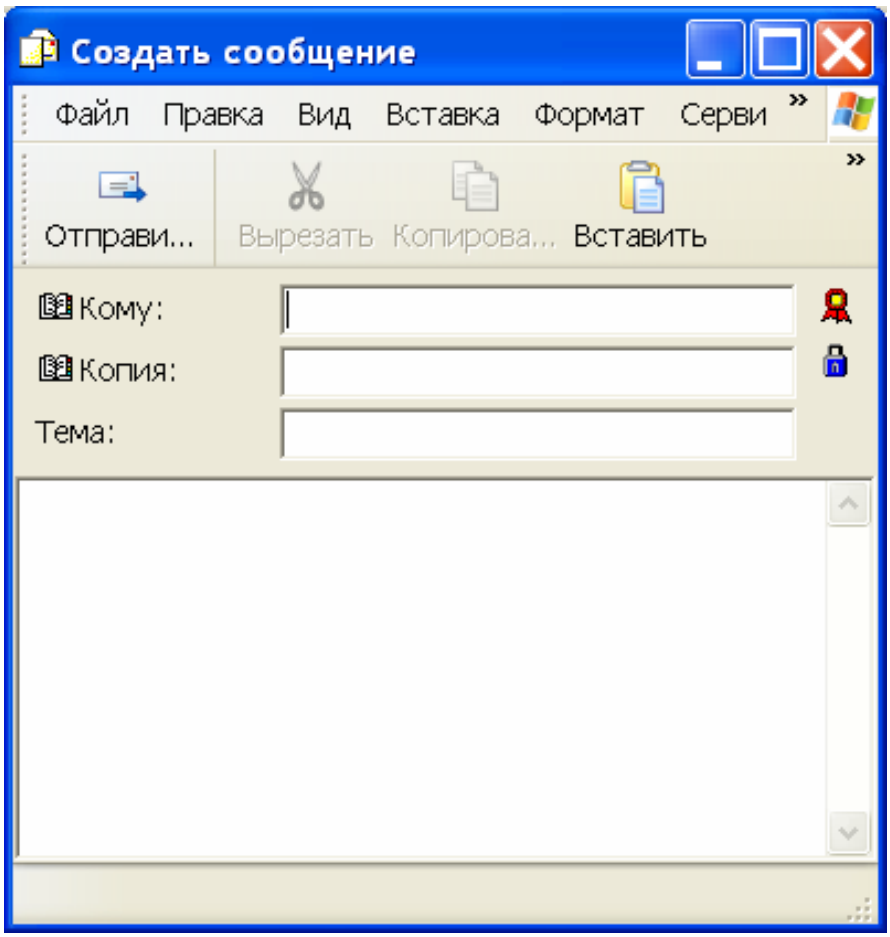
Если проверка отзыва сертификатов ключей подписи включена, статус сертификатов проверяется при открытии сообщения, если установлено подключение через Интернет к серверу Удостоверяющего центра.

2 Создание и отправление сообщений в Outlook Express

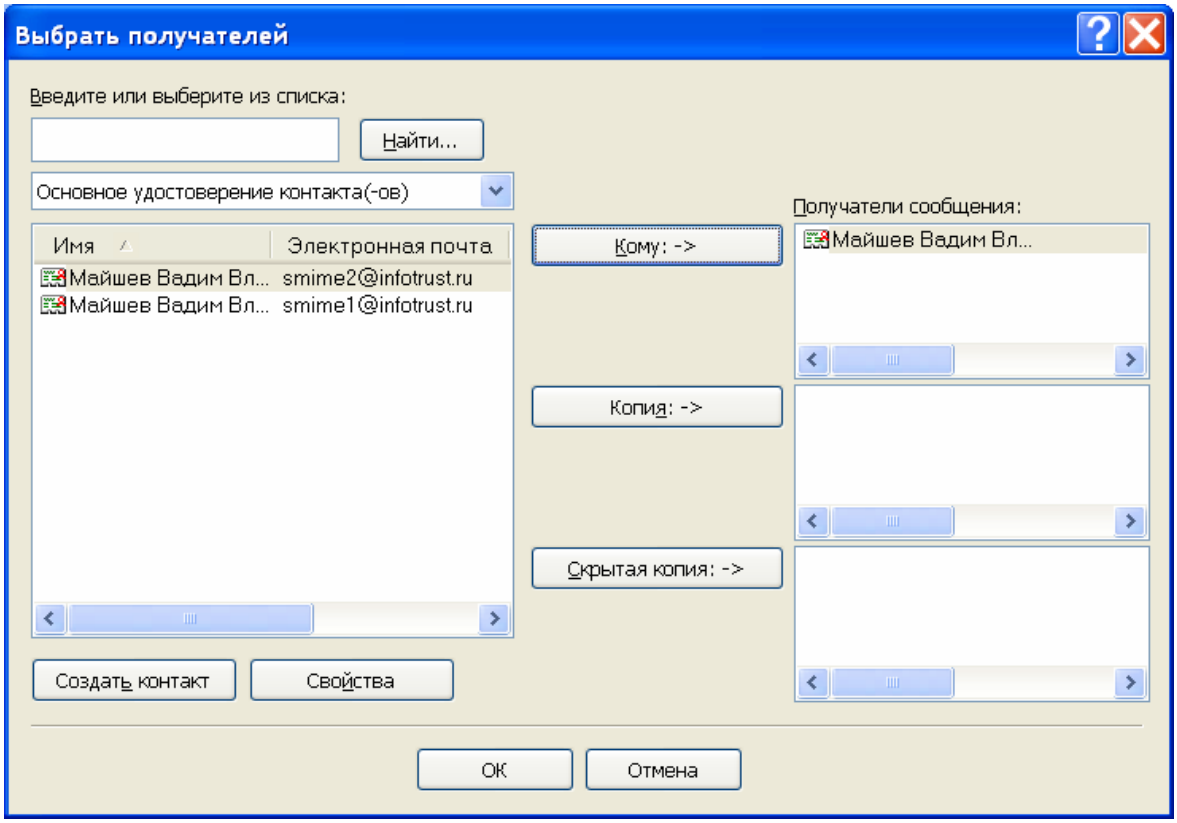
Программное обеспечение Outlook Express версии 6 и выше полностью поддерживает Инфраструктуру открытых ключей, обеспечивающую конфиденциальность информации, целостность и подлинность почтовых сообщений, передаваемых по протоколам SMTP-POP3. В качестве формата защищенных сообщений используется формат, описанный в рекомендациях Secure Multipurpose Internet Mail Extensions (S/MIME).

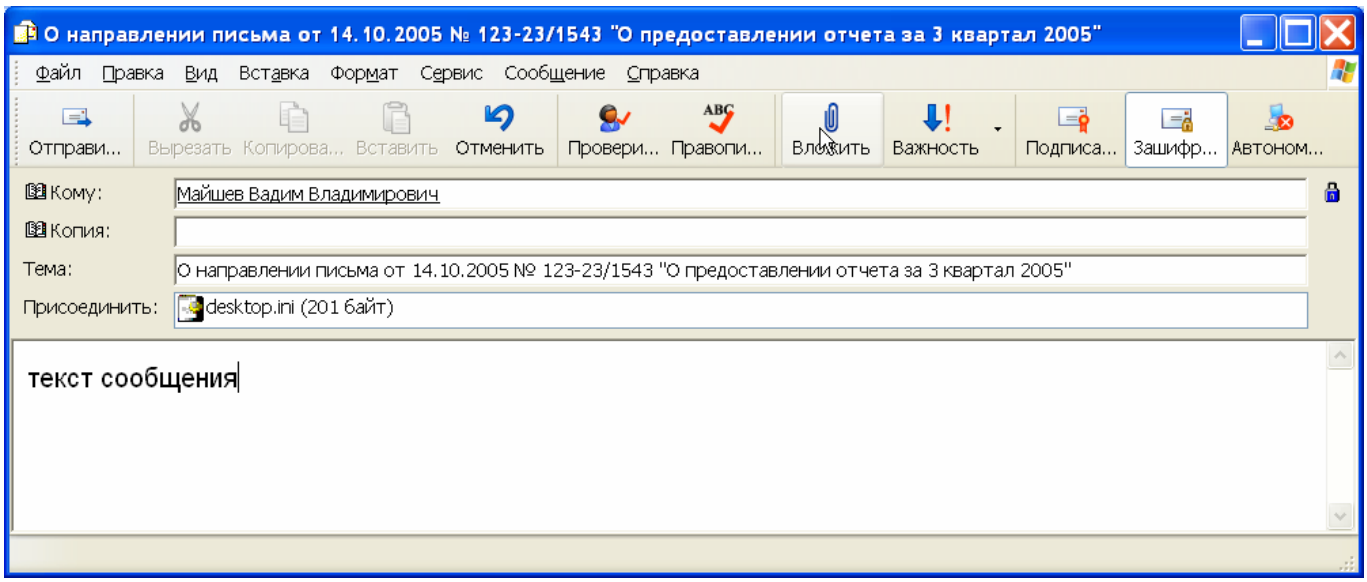
Для создания и отправки защищенного сообщения:

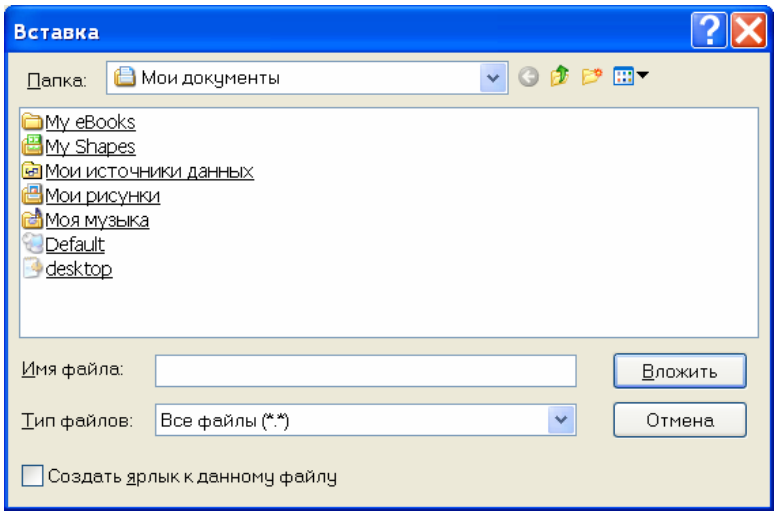
1 Нажмите на кнопку Создать сообщение или выберите пункт меню Файл → Создать → Почтовое Сообщение.



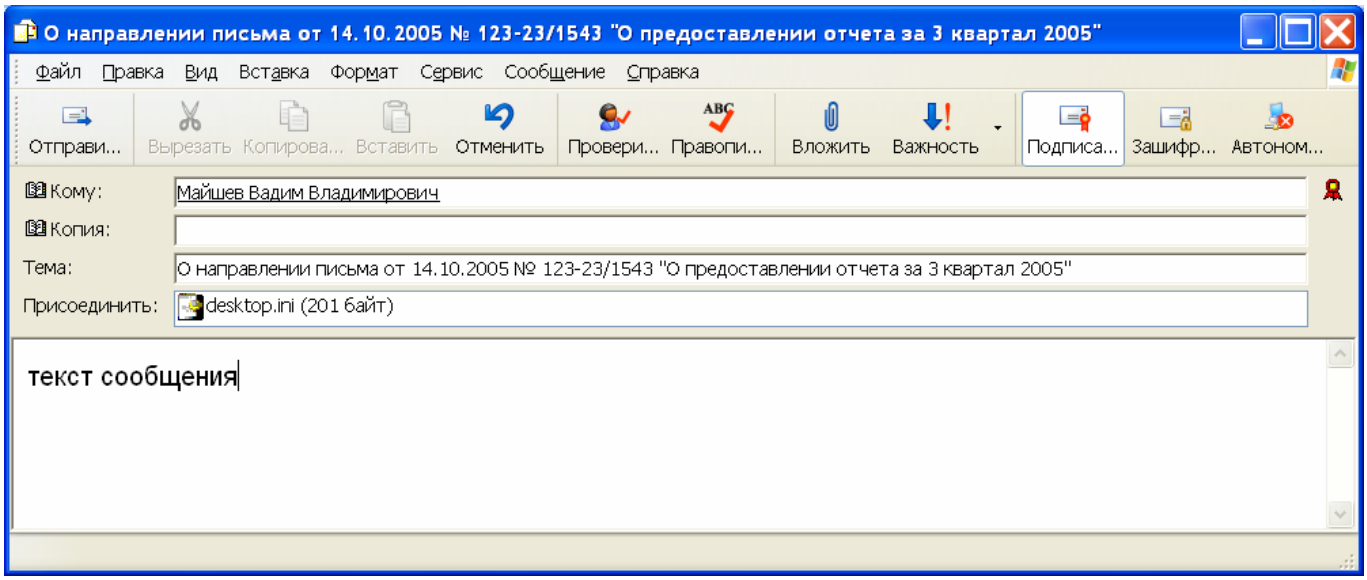
2 Далее выберите получателя сообщения (поле Кому) и введите тему сообщения. Если письмо дополнительно будет содержать файлы, добавьте их в письмо, используя кнопку Вложить.


Выбрать получателей
Введите или выберите из списка:
Найти...
Основное удостоверение контакта(-ов)
Имя
Электронная почта
Майшев Вадим Вл... smime2@infotrust.ru
Майшев Вадим Вл... smime1@infotrust.ru
Кому: ->
Копия: ->
Скрытая копия: ->
Получатели сообщения:
Майшев Вадим Вл...
Создать контакт
Свойства
ОК
Отмена

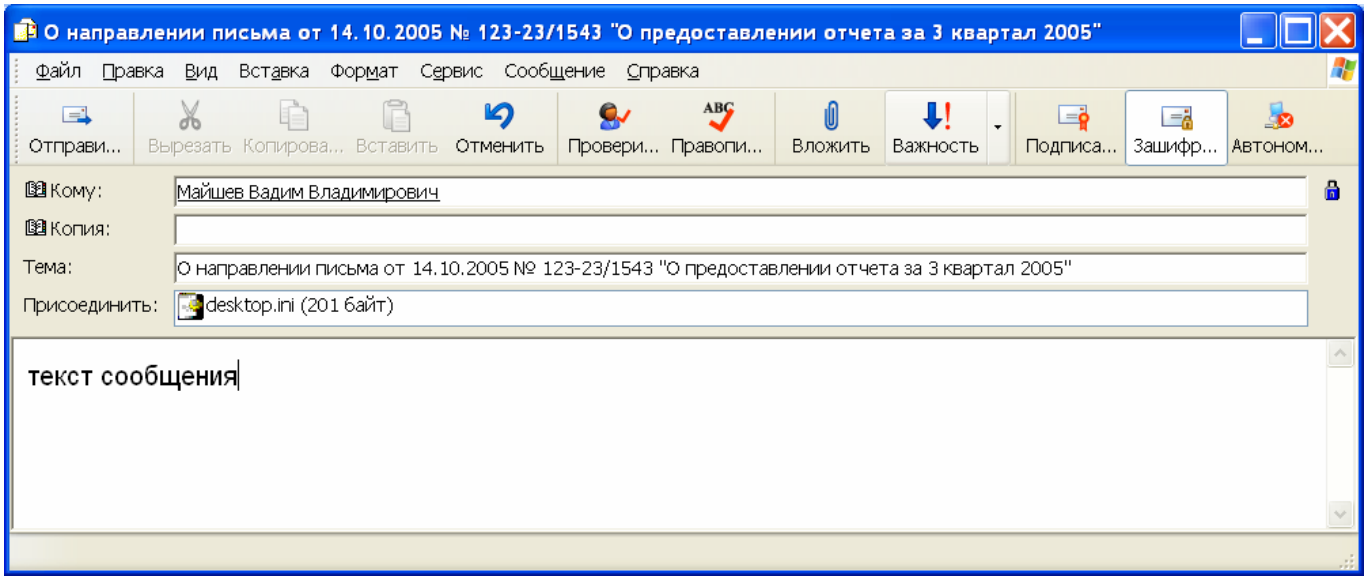

О направлении письма от 14.10.2005 № 123-23/1543 "О предоставлении отчета за 3 квартал 2005"
Файл Правка Вид Вставка Формат Сервис Сообщение Справка
Отправи... Вырезать Копирова... Вставить Отменить Провери... Правопи... Вложить Важность Подписа... Зашифр... Автоном...
Кому: Майшев Вадим Владимирович
Копия:
Тема: О направлении письма от 14.10.2005 № 123-23/1543 "О предоставлении отчета за 3 квартал 2005"
Присоединить: desktop.ini (201 байт)
текст сообщения


Вставка
Папка: Мои документы
My eBooks
My Shapes
Мои источники данных
Мои рисунки
Моя музыка
Default
desktop
Имя файла:
Вложить
Тип файлов: Все файлы (*.*)
Отмена
Создать ярлык к данному файлу

3 Для отправки сообщения в подписанном виде проверьте состояние кнопки Подписать. Она должна быть нажата, и должен быть виден знак подписанного сообщения в правой части экрана.



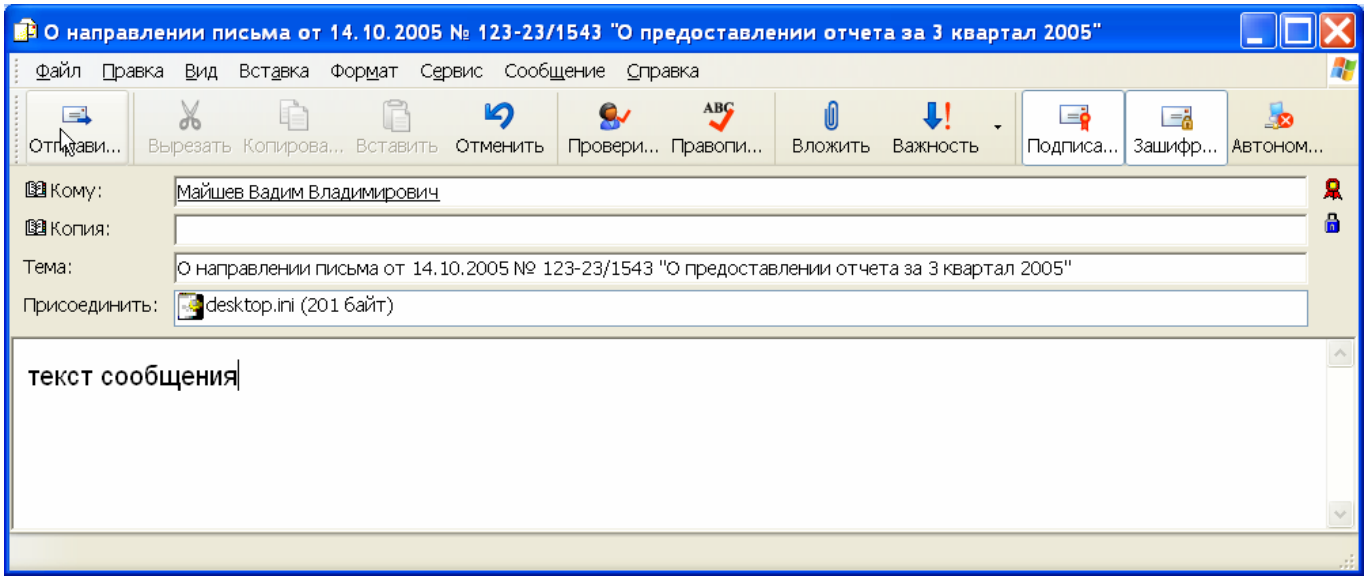
4 Для отправки сообщения в зашифрованном виде проверьте состояние кнопки Зашифровать. Она должна быть нажата, и должен быть виден знак зашифрованного сообщения в правой части экрана. Зашифрованные сообщения можно отправлять только в адрес абонентов, сертификаты ключей подписи которых соответствуют адресам электронной почты этих абонентов и имеются в адресной книге.



Примечание: кнопки Подписать и Зашифровать при настройке программы на автоматическое подписание и зашифрование сообщений являются

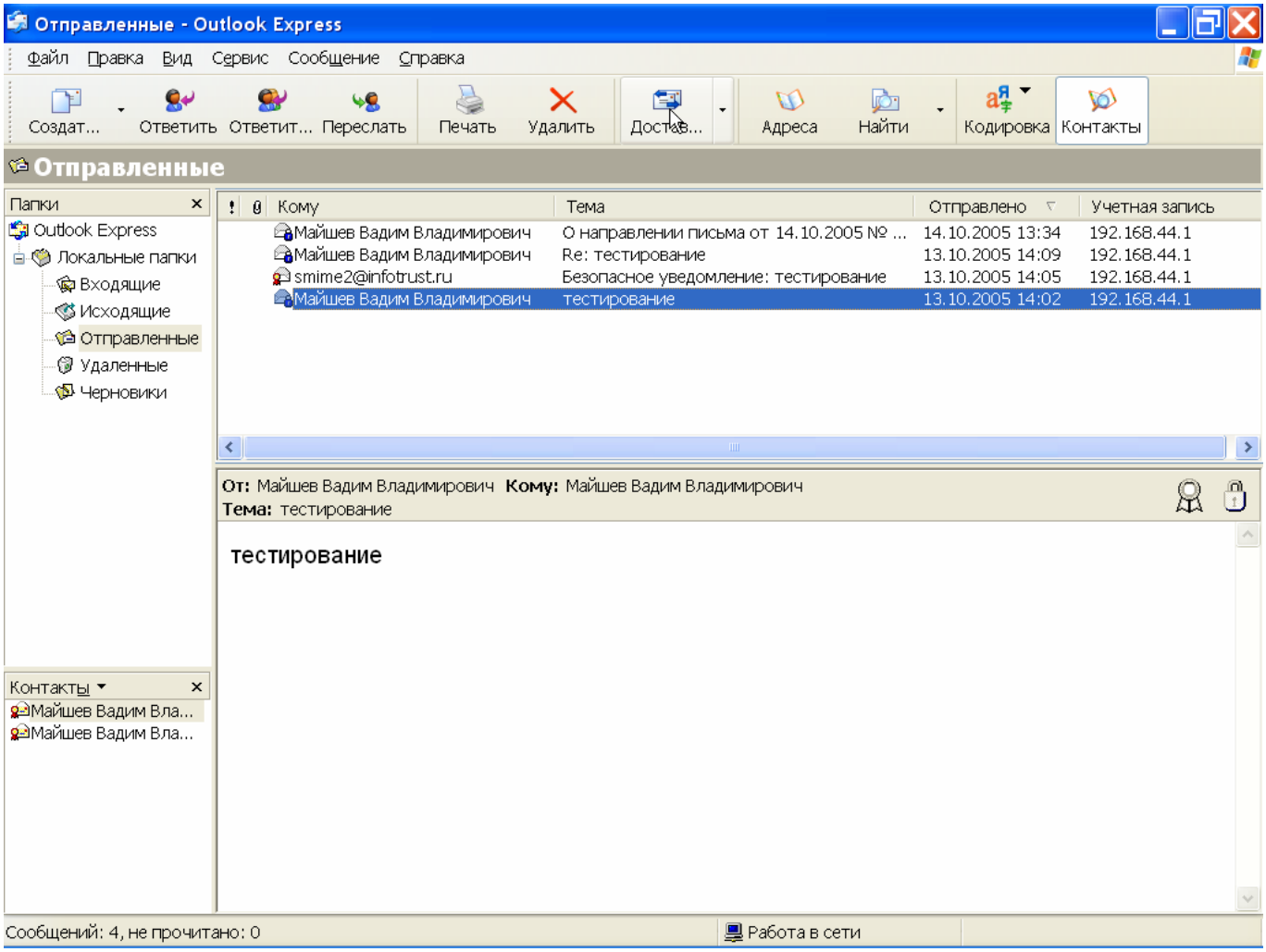
включенными. При необходимости отправки адресату сообщения без функций защиты их можно выключить.

5 После того как сообщение подготовлено к отправке, нажмите на кнопку Отправить:

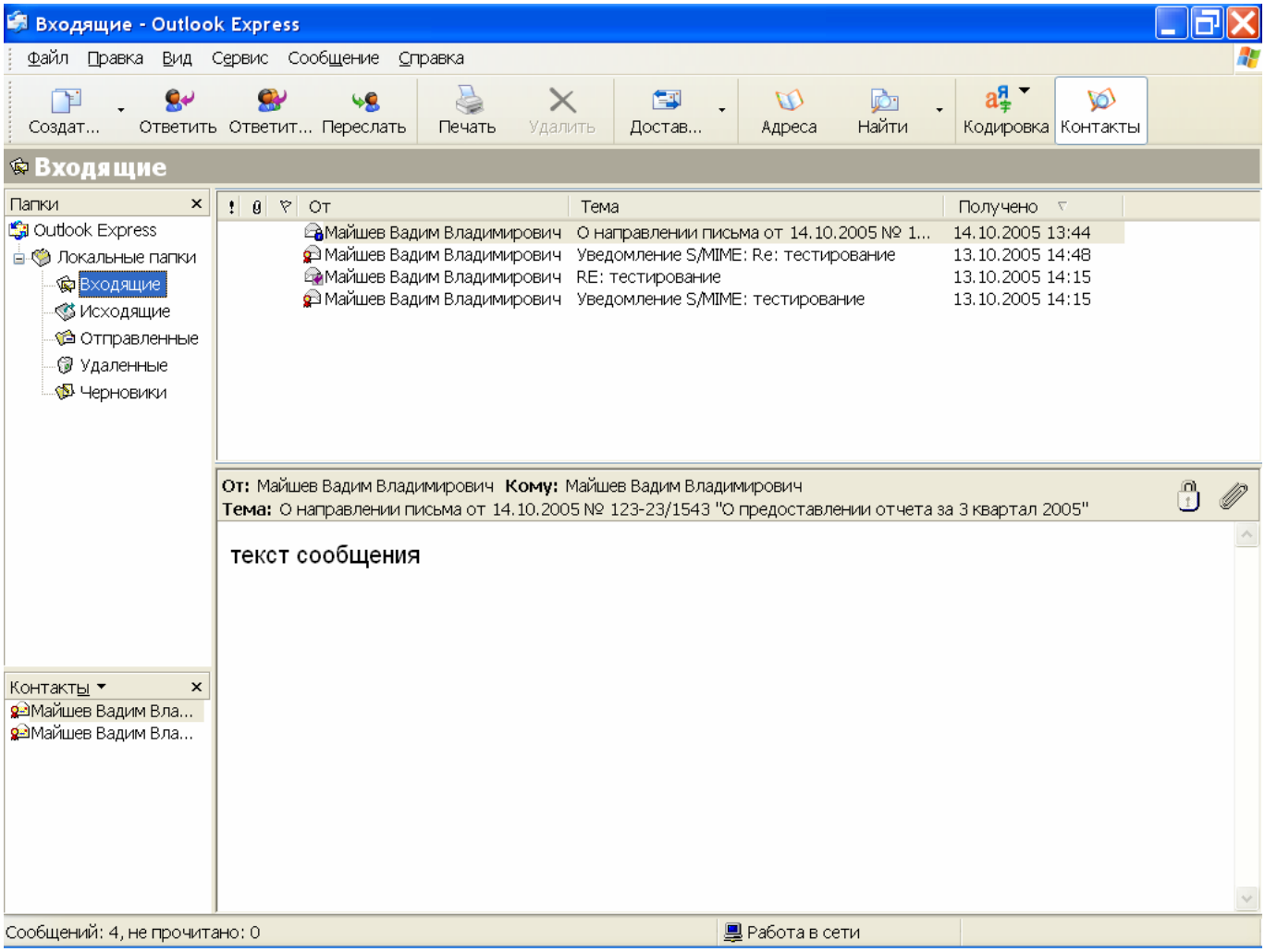


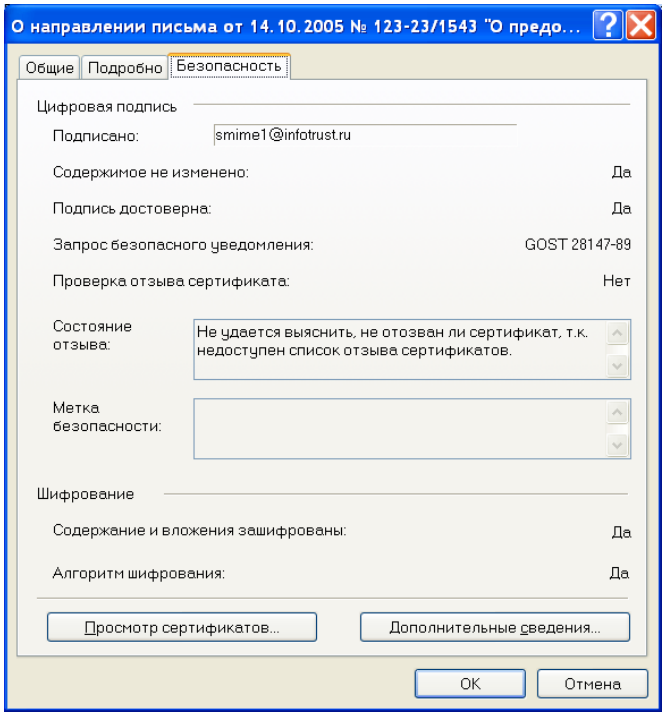
3 Получение сообщений в Outlook Express

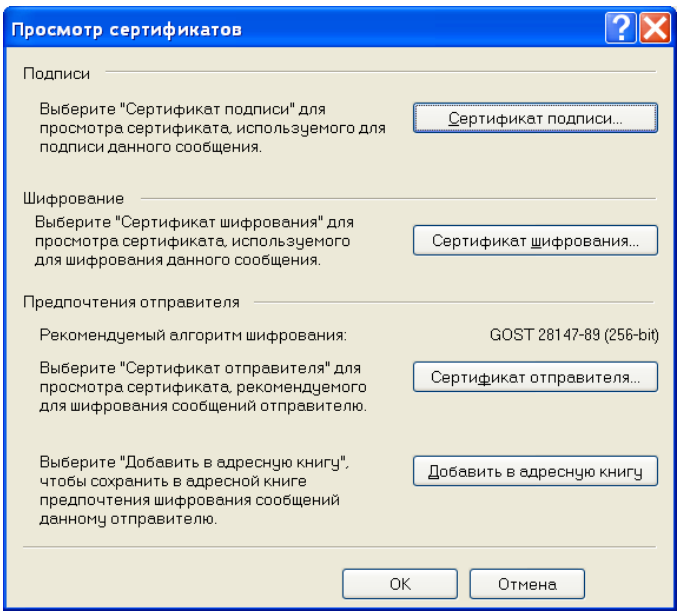
1 Нажмите на кнопку Доставить почту или выберите пункт меню Сервис → Доставить почту.



2 При получении нового письма, его расшифровании и проверке подписи запрашивается ключевой носитель получателя. О защите сообщения сообщает соответствующий значок в правой части экрана — подписанное или зашифрованное. При нажатии на один из этих значков выводится окно о характеристиках безопасности данного сообщения. При этом пользователь имеет возможность посмотреть сертификаты отправителя, которые использовались для подписи и шифрования сообщения.

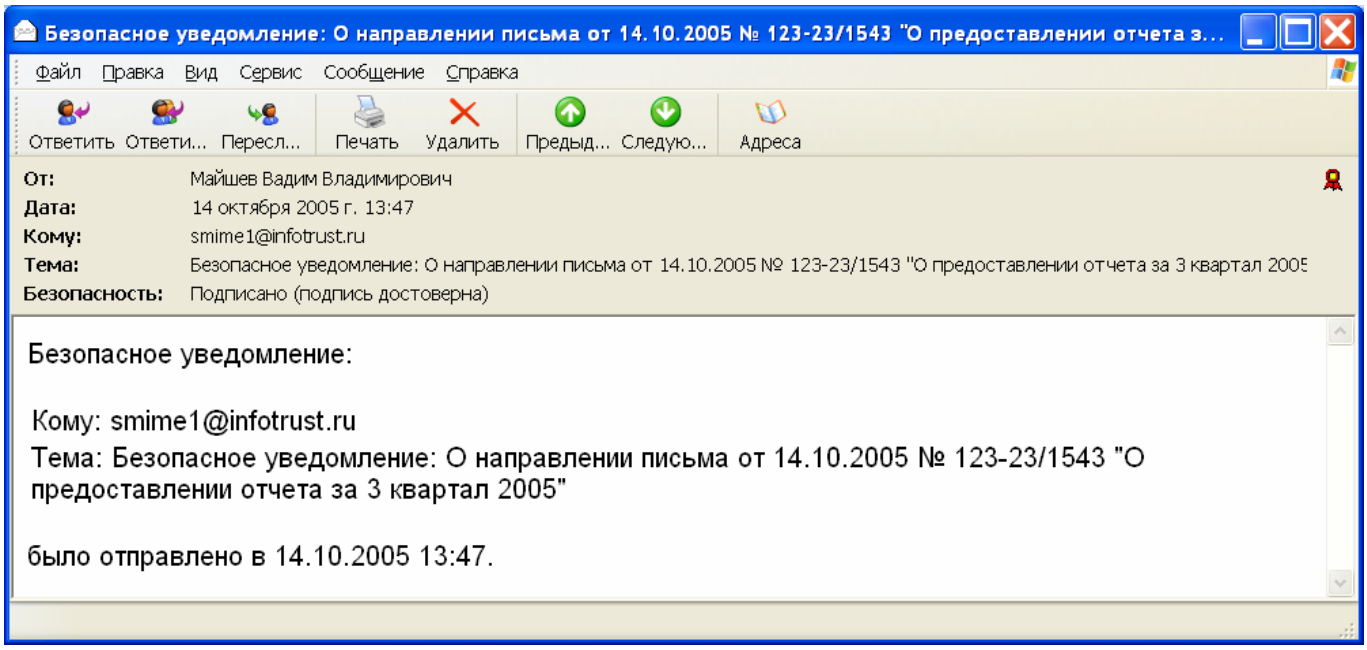






3 При прочтении защищенного письма получателем автоматически (если это настроено в системе) по соответствующему запросу отправителя формируется и

отправляется безопасное уведомление (уведомление S/MIME) — уведомление о прочтении сообщения, подписанное получателем.

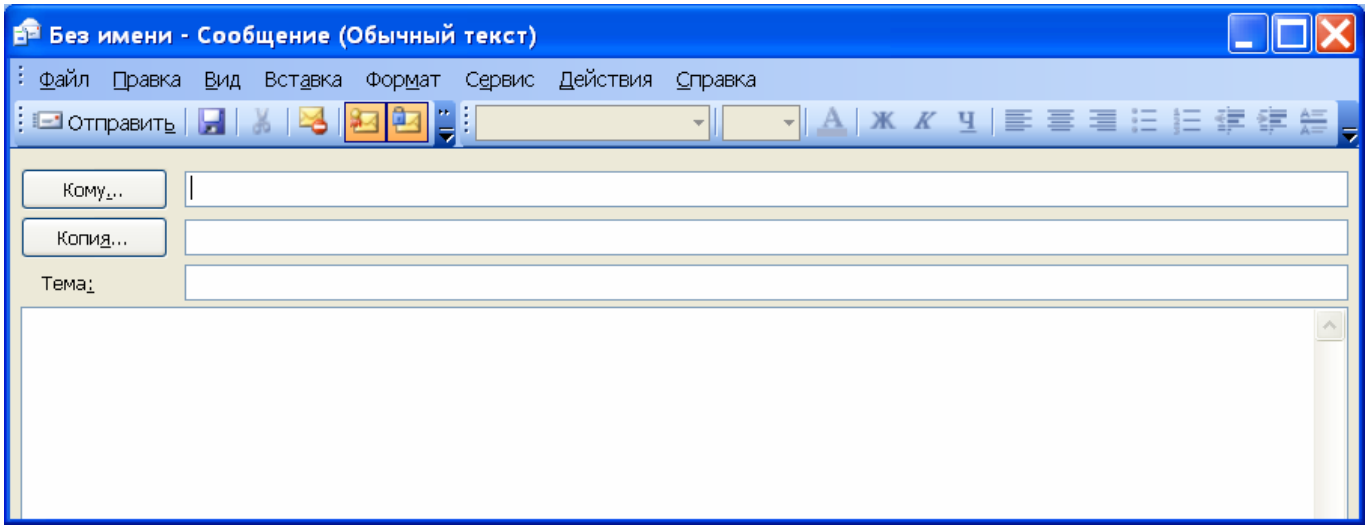


4 Создание и отправление сообщений в MicroSoft Outlook

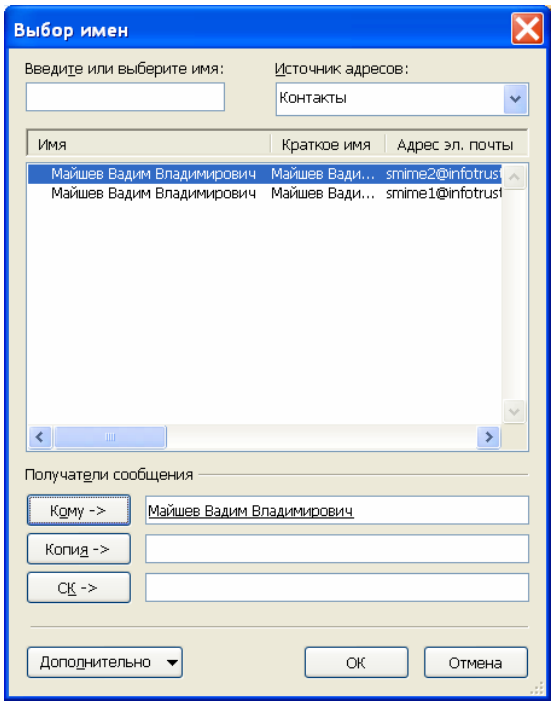
Применение средств криптографической защиты информации для создания защищенных электронных сообщений в MicroSoft Outlook для клиента во многом совпадает с работой в Outlook Express.

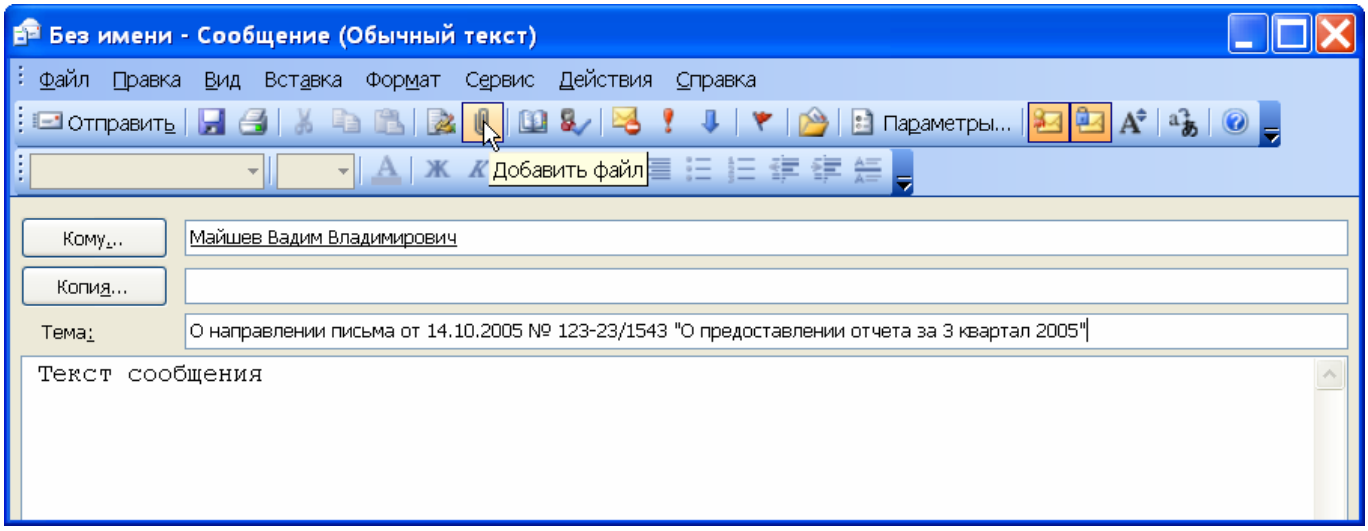
Для создания и отправления сообщения:

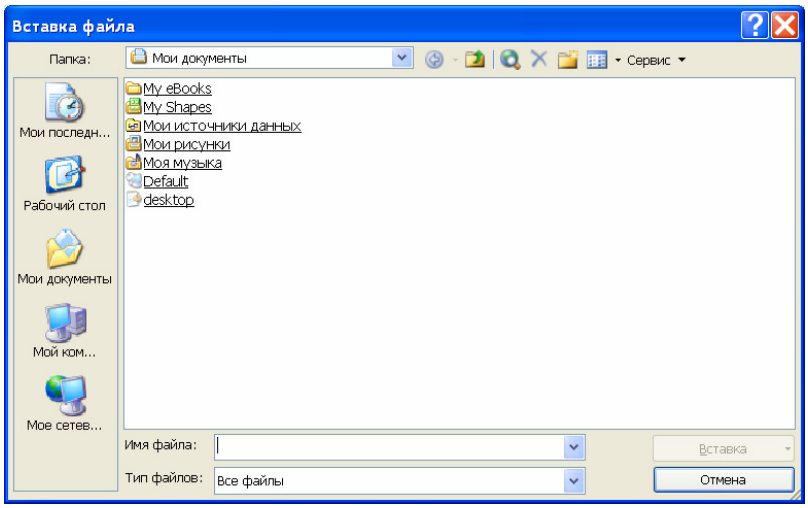
1 Нажмите на кнопку Создать сообщение или выберите пункт меню Файл → Создать → Сообщение.



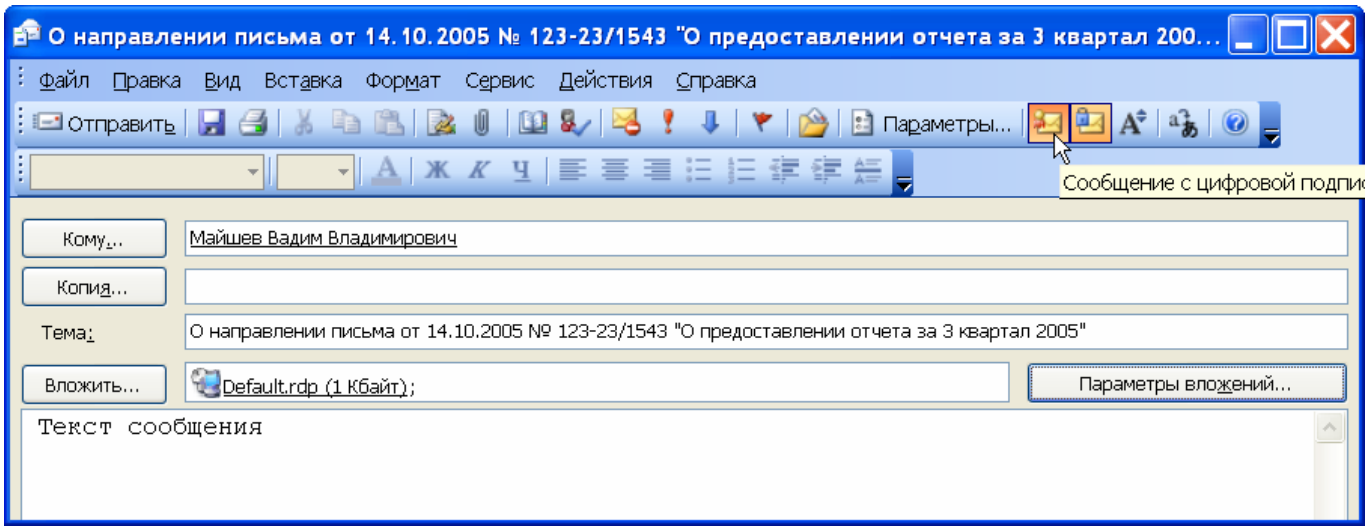
2 Далее выберите получателя сообщения (поле Кому) и введите тему сообщения. Если письмо дополнительно будет содержать файлы, добавьте их в письмо, используя кнопку Вложить.





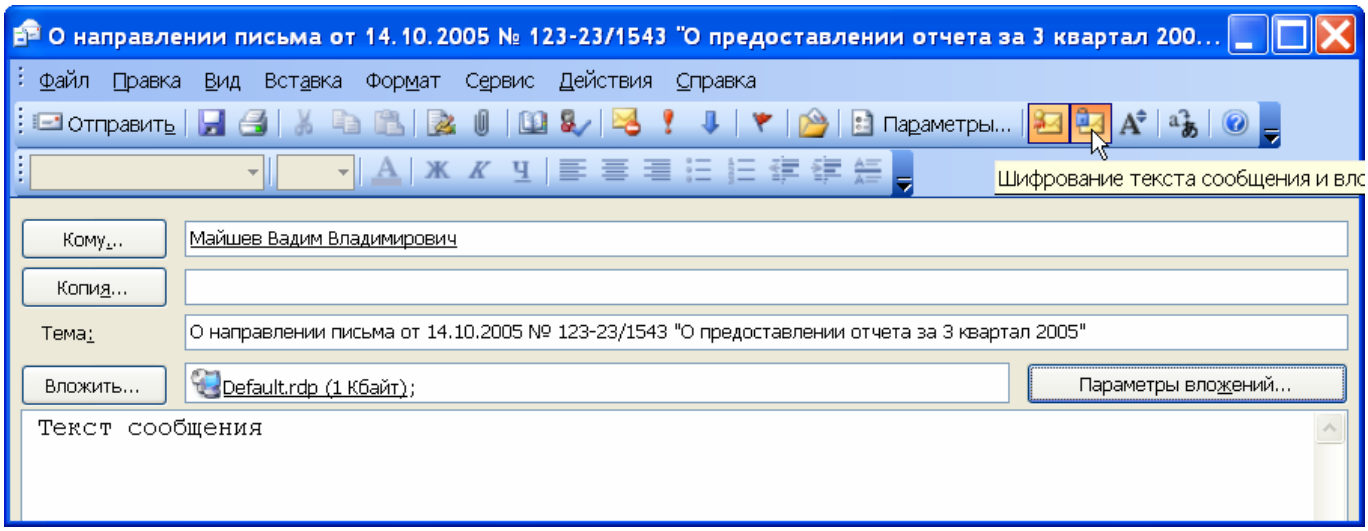


3 Для отправки сообщения в подписанном виде проверьте состояние кнопки Сообщение с цифровой подписью.



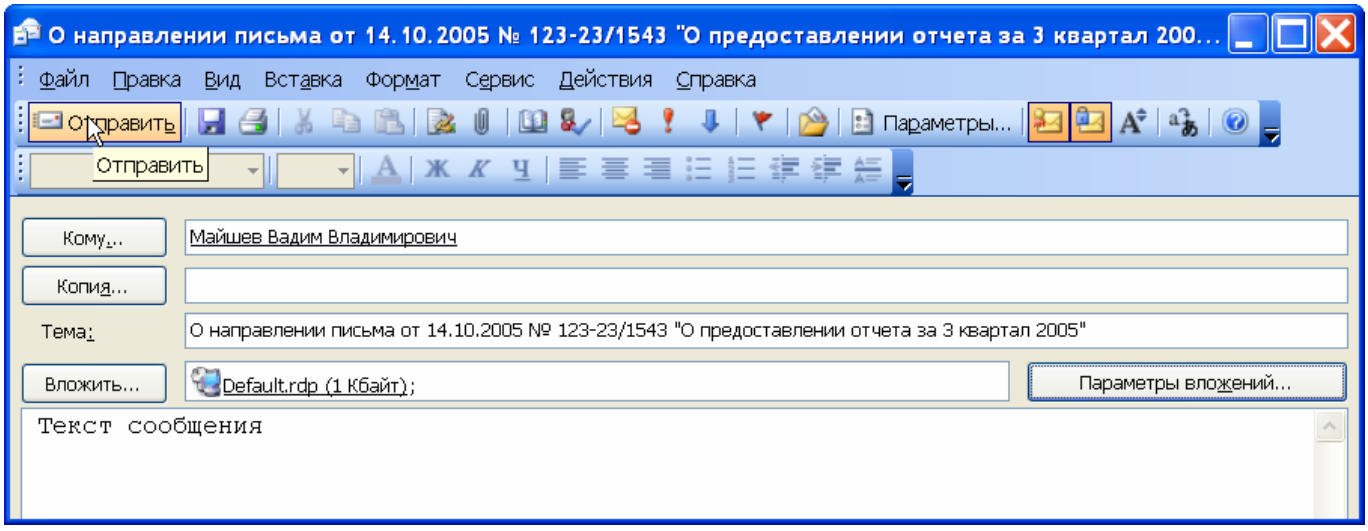
4 Для отправки сообщения в зашифрованном виде проверьте состояние кнопки Шифрование текста сообщений и вложений. Зашифрованные сообщения можно отправлять только в адрес абонентов, сертификаты ключей подписи которых

соответствуют адресам электронной почты этих абонентов и имеются в адресной книге.



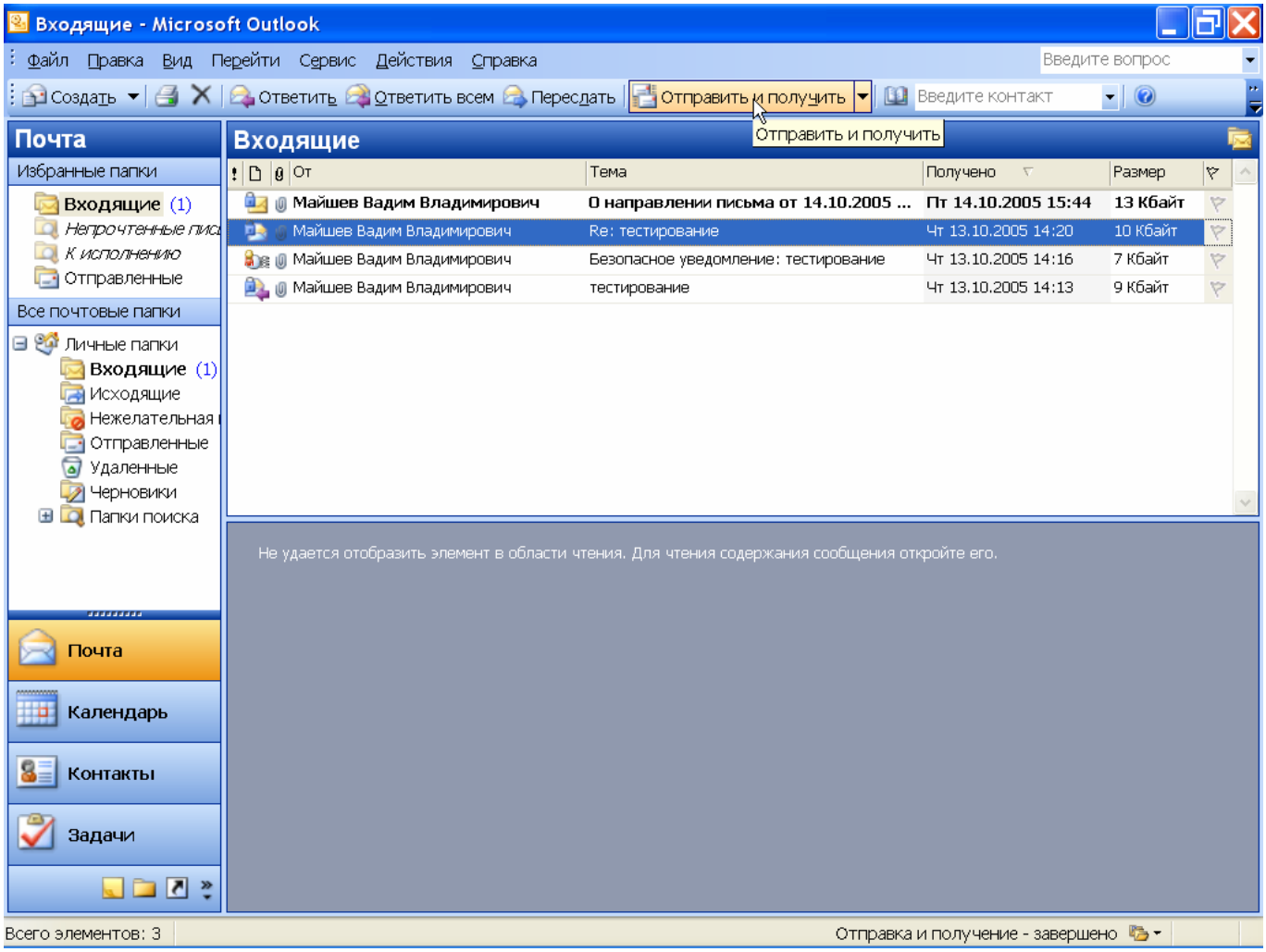
Примечание: кнопки ***Сообщение с цифровой подписью*** *и* ***Шифрование текста сообщений и вложений*** *при настройке программы на автоматическое подписание и зашифрование сообщений являются включенными. При необходимости отправки адресату сообщения без функций защиты их можно выключить.*

5 После того как сообщение подготовлено к отправке, нажмите на кнопку Отправить:

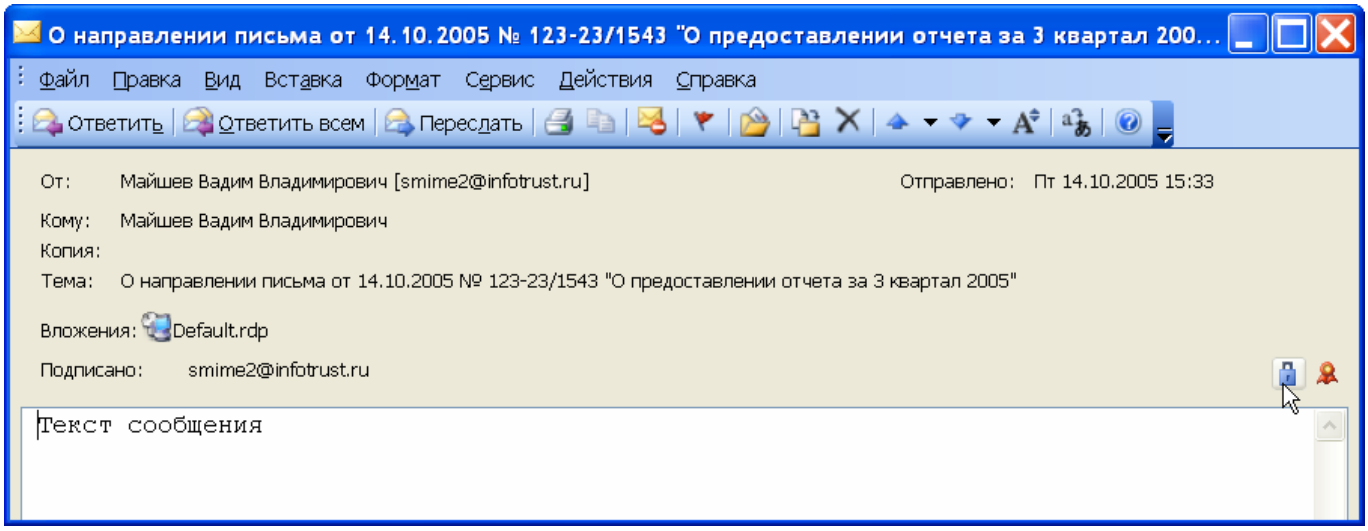


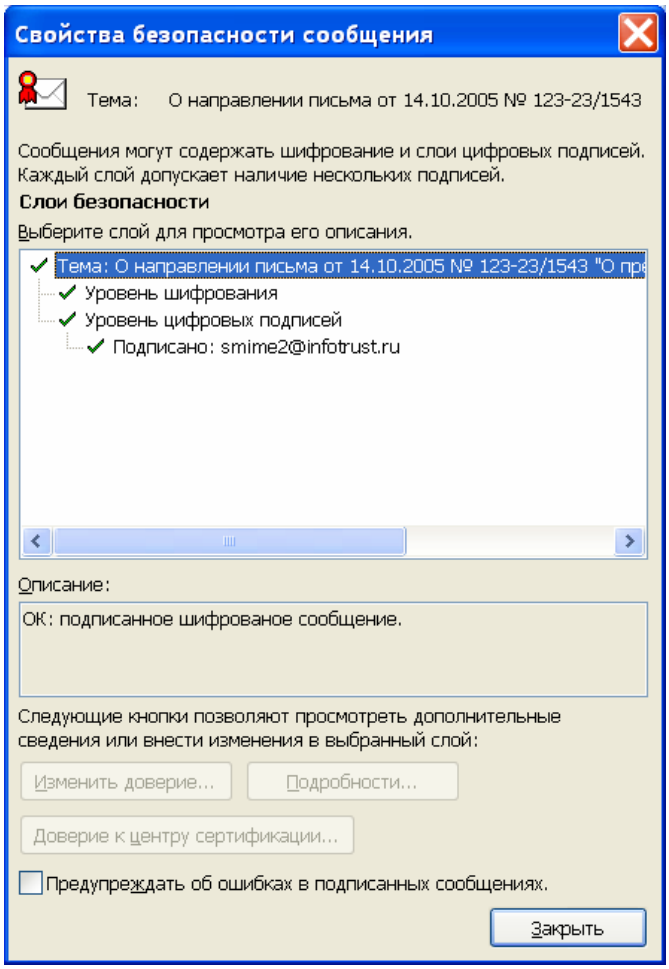
5 Получение сообщений в MicroSoft Outlook

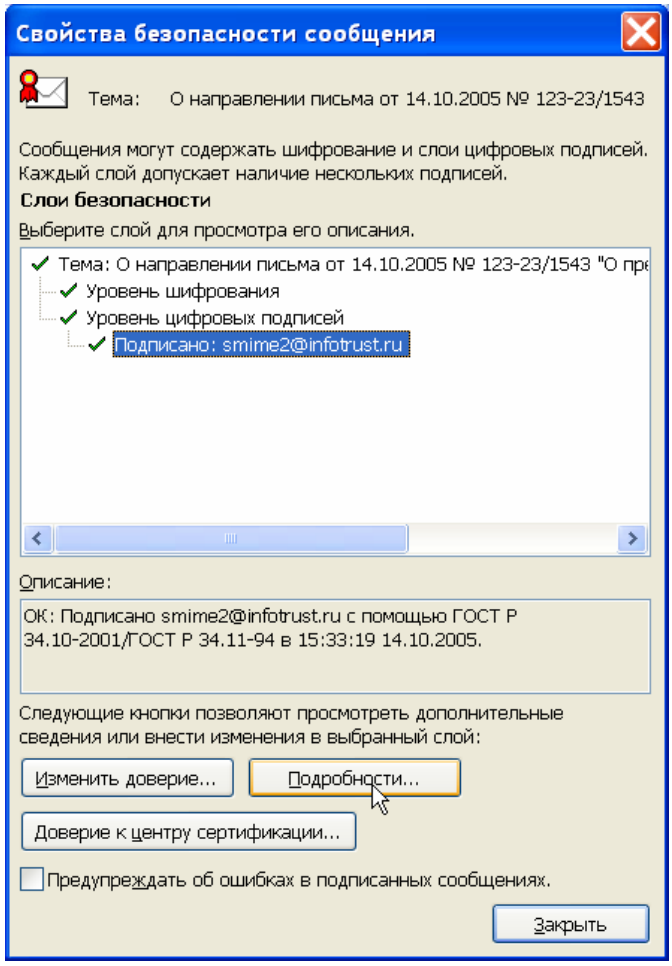
1 Нажмите на кнопку Отправить и получить или выберите пункт меню Сервис → Отправить и получить → Доставить почту.

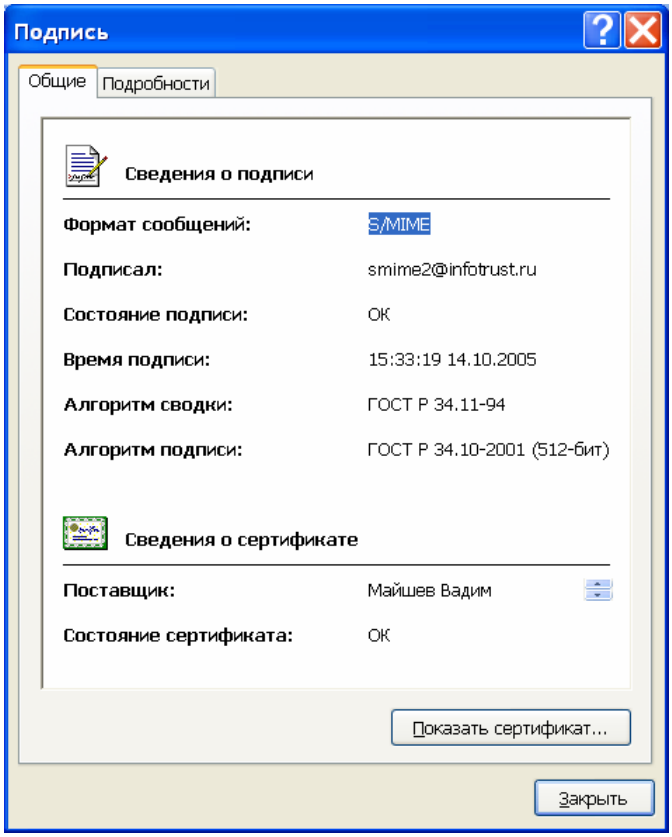


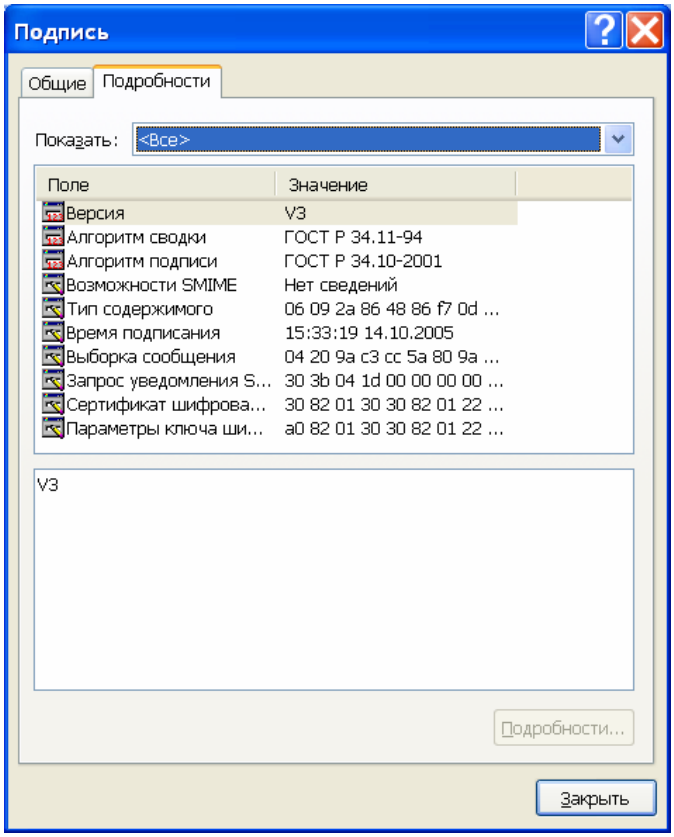
2 При получении нового письма, его расшифровании и проверке подписи запрашивается ключевой носитель получателя. О защите сообщения сообщает соответствующий значок в правой части экрана — подписанное или зашифрованное. При нажатии на один из этих значков выводится окно о свойствах безопасности данного сообщения и их подробности. При этом пользователь имеет возможность посмотреть сертификаты отправителя, которые использовались для подписи и шифрования сообщения.


О направлении письма от 14.10.2005 № 123-23/1543 "О предоставлении отчета за 3 квартал 200...
Файл Правка Вид Вставка Формат Сервис Действия Справка
Ответить Ответить всем Переслать
От: Майшев Вадим Владимирович [smime2@infotrust.ru]
Отправлено: Пт 14.10.2005 15:33
Кому: Майшев Вадим Владимирович
Копия:
Тема: О направлении письма от 14.10.2005 № 123-23/1543 "О предоставлении отчета за 3 квартал 2005"
Вложения: Default.rdp
Подписано: smime2@infotrust.ru
Текст сообщения


Свойства безопасности сообщения
Тема: О направлении письма от 14.10.2005 № 123-23/1543
Сообщения могут содержать шифрование и слои цифровых подписей. Каждый слой допускает наличие нескольких подписей.
Слои безопасности
Выберите слой для просмотра его описания.
Тема: О направлении письма от 14.10.2005 № 123-23/1543 "О пр
Уровень шифрования
Уровень цифровых подписей
Подписано: smime2@infotrust.ru
Описание:
ОК: подписанное шифрованое сообщение.
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.
Закрыть


Свойства безопасности сообщения
Тема: О направлении письма от 14.10.2005 № 123-23/1543
Сообщения могут содержать шифрование и слои цифровых подписей. Каждый слой допускает наличие нескольких подписей.
Слои безопасности
Выберите слой для просмотра его описания.
Тема: О направлении письма от 14.10.2005 № 123-23/1543 "О пр
Уровень шифрования
Уровень цифровых подписей
Подписано: smime2@infotrust.ru
Описание:
ОК: Подписано smime2@infotrust.ru с помощью ГОСТ Р 34.10-2001/ГОСТ Р 34.11-94 в 15:33:19 14.10.2005.
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.
Закрыть





3 При прочтении защищенного письма получателем автоматически (если это настроено в системе) по соответствующему запросу отправителя формируется и отправляется безопасное уведомление (уведомление S/MIME) — уведомление о прочтении сообщения, подписанное получателем.