127 018, Москва, Сущевский Вал, д.18
Телефон: (495) 780 4820
Факс: (495) 780 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Защита информации

в корпоративной электронной почте

Аннотация

В операционных системах Microsoft® Windows® 2000/XP/2003/Vista/2008/7/2008R2 /8/2012/8.1/2012R2 в полном объеме реализована инфраструктура открытых ключей (PKI – Public Key Infrastructure). Эта инфраструктура представляет собой интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих криптографию с открытыми ключами, а также для управления ими. Она позволяет корпоративным клиентам использовать криптографические средства для защиты информации, передаваемой с использованием электронной почты Microsoft. Реализованное по стандарту Microsoft CSP сертифицированное средство криптографической защиты информации – КриптоПро CSP позволяет теперь использовать инфраструктуру открытых ключей и стандартные продукты Microsoft со стойкими российскими криптографическими алгоритмами.

СОДЕРЖАНИЕ

ЗАЩИТА ИНФОРМАЦИИ *4*

КРИПТОГРАФИЯ С ОТКРЫТЫМИ КЛЮЧАМИ *5*

Возможности криптографии с открытыми ключами **5**

Электронные цифровые подписи **6**

Проверка подлинности **6**

Согласование общего секретного ключа сессии **7**

Шифрование без предварительного обмена симметричным секретным ключом **7**

Защита и проверка подлинности криптографических ключей **7**

Сертификаты **8**

Центры сертификации **8**

Подтверждение доверия **8**

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ *10*

Иерархии центров сертификации **10**

ОТЗЫВ СЕРТИФИКАТОВ *13*

Доверие **13**

ИСПОЛЬЗОВАНИЕ РОССИЙСКИХ КРИПТОАЛГОРИТМОВ В WINDOWS *15*

ЦЕНТР СЕРТИФИКАЦИИ В КОРПОРАТИВНОЙ ПОЧТОВОЙ СИСТЕМЕ *18*

Задачи Центра Регистрации **18**

ГЕНЕРАЦИЯ КЛЮЧА И ПОЛУЧЕНИЕ СЕРТИФИКАТА ДЛЯ РАБОТЫ В ЭЛЕКТРОННОЙ ПОЧТЕ *21*

ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В OUTLOOK EXPRESS *22*

Конфигурация Outlook Express **22**

Отправка подписанных сообщений **24**

Получение сертификата открытого ключа абонента для шифрования сообщений **25**

Отправка шифрованных сообщений **26**

Проверка сертификата на отзыв **27**

ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В ПРОГРАММЕ "ПОЧТА WINDOWS" *29*

Конфигурация программы "Почта Windows" **29**

Отправка подписанных сообщений **31**

Получение сертификата открытого ключа абонента для шифрования сообщений **32**

Отправка шифрованных сообщений **32**
Проверка сертификата на отзыв **33**
ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В WINDOWS LIVE MAIL ***35***
Конфигурация Windows Live Mail **35**
Отправка подписанных сообщений **37**
Получение сертификата открытого ключа абонента для шифрования сообщений **38**
Отправка шифрованных сообщений **39**
Проверка сертификата на отзыв **40**
ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В OUTLOOK 2000 ..... ***43***
Конфигурация Outlook 2000 ..... **43**
Отправка подписанных сообщений **45**
Получение сертификата открытого ключа абонента для шифрования сообщений **46**
Отправка шифрованных сообщений **47**
Проверка сертификата на отзыв **47**
ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В OUTLOOK 2002/2003 ..... ***49***
Конфигурация Outlook 2002/2003 ..... **49**
Отправка подписанных сообщений **50**
Получение сертификата открытого ключа абонента для шифрования сообщений **52**
Отправка шифрованных сообщений **52**
Проверка сертификата на отзыв **53**
ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В OUTLOOK 2007 ..... ***55***
Конфигурация Outlook 2007 ..... **55**
Отправка подписанных сообщений **56**
Получение сертификата открытого ключа абонента для шифрования сообщений **57**
Отправка шифрованных сообщений **58**
Проверка сертификата на отзыв **59**
ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В OUTLOOK 2010 ..... ***62***
Конфигурация Outlook 2010 ..... **62**
Отправка подписанных сообщений **65**
Получение сертификата открытого ключа абонента для шифрования сообщений **66**
Отправка шифрованных сообщений **67**

Проверка сертификата на отзыв 67

ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В OUTLOOK 2013 70

Конфигурация Outlook 2013 70

Отправка подписанных сообщений 73

Получение сертификата открытого ключа абонента для шифрования сообщений 74

Отправка шифрованных сообщений 76

Проверка сертификата на отзыв 77

© ООО "Крипто-Про", *2001-2015.* Все права защищены.

Информация, содержащаяся в настоящем документе, представляет текущую точку зрения "Крипто-Про" по обсуждаемым вопросам на момент публикации. В условиях меняющейся рыночной конъюнктуры, требующей соответствующей корректировки ведущихся разработок, данную информацию не следует рассматривать в качестве какого бы то ни было обязательства со стороны "Крипто-Про". "Крипто-Про" не может гарантировать точность информации, представленной после даты публикации.

Данный документ имеет информативный характер. "Крипто-Про" не предоставляет никаких гарантий, ни явно выраженных, ни подразумеваемых, в связи с данным документом.

КриптоПро CSP является охраняемым товарным знаком ООО "Крипто-Про". Microsoft, ActiveX, Authenticode, Outlook, Windows, Windows NT и эмблема BackOffice являются охраняемыми товарными знаками корпорации Microsoft. Названия других продуктов или предприятий, указанные здесь, могут быть товарными знаками соответствующих владельцев.

ООО "Крипто-Про", Россия, 127 018, Москва, Сущевский Вал, д.18

ЗАЩИТА ИНФОРМАЦИИ

Происходящее сейчас бурное развитие компьютерных сетей и коммуникаций значительно расширяет возможности применения информационных технологий для обмена информацией между различными категориями пользователей. Вместе с внедрением в повседневную работу различных средств обмена информацией в электронном виде, все актуальнее становится проблема обеспечения ее безопасности: конфиденциальности, целостности и авторства.

Пользователь все больше хочет быть уверен, что отправленные им сообщения никто не прочитает, кроме указанного адресата. Получатель же хочет быть уверен, что информация получена именно из того источника, от которого он их ожидал. Для обеспечения безопасности передаваемой информации во всем мире все активнее применяются технологии криптографической защиты с использованием открытых ключей.

По мере расширения использования систем электронной почты в российском деловом мире стремительно растет и количество конфиденциальных данных, передаваемых по сети Интернет. В результате становится актуальной проблема автоматизации и защиты документооборота, осуществляемого с помощью средств электронной почты: хочется быть уверенным, что отправленные сообщения никто не прочитает, кроме указанного адресата. Важно также быть уверенным, что отправляемые электронные документы в процессе пересылки и хранения не будут подделаны.

Наличие защищенных модификаций таких программных продуктов как, например, клиентское окончание системы электронной почты - MS Outlook, выполненных в строгом соответствии с отечественными криптографическими стандартами, позволило бы российским потребителям строить на их основе собственные защищенные корпоративные системы электронного документооборота любого уровня сложности: от бухгалтерии небольшой частной компании до расчетной системы крупного коммерческого банка. С помощью этих средств возможна также организация взаимодействия торговых предприятий с дилерами и предоставление им коммерческой информации через Интернет. Крупные промышленные предприятия могут строить на их основе собственный конфиденциальный документооборот. Предприятия добывающей и перерабатывающей промышленности могут создавать системы взаимодействия Центральных офисов с удаленными филиалами и многое другое. Круг задач, решаемых такими прикладными системами, практически неограничен.

КРИПТОГРАФИЯ С ОТКРЫТЫМИ КЛЮЧАМИ

Криптография – это комплексная наука о защите данных. Криптографические алгоритмы используются для шифрования открытого текста (plaintext) с использованием ключа шифрования (encryption key), в результате чего получаются зашифрованные данные (ciphertext). Зашифрованный по надежному криптографическому алгоритму текст практически невозможно расшифровать без дополнительных данных, которые называются ключом расшифрования (decryption key).

В криптографии с симметричными ключами (symmetric key) для шифрования и расшифрования используется один и тот же секретный ключ (secret key), то есть ключ шифрования совпадает ключом расшифрования. Стороны могут передавать друг другу данные, зашифрованные секретным ключом, только после того, как они обменяются этим общим ключом.

В отличие от шифрования с секретным ключом, фундаментальным свойством шифрования с открытым ключом является различие между ключом шифрования и ключом расшифрования. Открытый ключ позволяет зашифровать открытый текст, но не позволяет расшифровать его. В этом смысле открытый ключ можно назвать односторонним (one-way). Чтобы расшифровать текст, нужен ключ расшифрования, который отличается от ключа шифрования, хотя и связан с ним. Таким образом, при шифровании с открытым ключом у каждого пользователя должно быть два ключа – открытый (public) и личный (private) – секретный ключ. Если открытый ключ сделать общедоступным, пользователи смогут отправлять вам зашифрованные с ним данные, которые только вы будете способны расшифровать с помощью своего личного секретного ключа. С помощью личного ключа вы также можете преобразовать отправляемые данные таким образом, что пользователи смогут удостовериться в том, что эти данные были отправлены именно вами, а не кем-то другим. Эта возможность служит основой цифровых подписей, которые подробнее обсуждаются далее.

Возможности криптографии с открытыми ключами

Различие ключей – открытого и личного – в криптографии с открытыми ключами позволило создать следующие технологии: электронные цифровые подписи, распределенная проверка подлинности, согласование общего секретного ключа сессии, шифрование больших объемов данных без предварительного обмена общим секретным ключом.

В настоящее время хорошо известен целый ряд алгоритмов шифрования с открытым ключом. Некоторые алгоритмы, например RSA (Rivest-Shamir-Adleman) и ECC (Elliptic Curve Cryptography), универсальны, они поддерживают все перечисленные выше операции. Другие алгоритмы более специализированы и поддерживают не все возможности. К их числу относятся:

- российский алгоритм электронной цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.102001;
- алгоритм электронной цифровой подписи DSA (Digital Signature Algorithm входящий в принятый в США государственный стандарт цифровой подписи Digital Signature Standard, FIPS 186);

- алгоритм DH (Diffie-Hellman), применяемый для выработки общего секретного ключа сессии.

Далее кратко описываются принципы использования криптографии с открытыми ключами. Традиционно для иллюстрации криптографических алгоритмов используются условные пользователи: Алиса и Боб. Подразумевается, что они могут обмениваться информацией, но не имеют предварительно распределенных общих секретных ключей.

Электронные цифровые подписи

Создание и проверка электронных цифровых подписей (digital signature) – это, вероятно, самый интересный аспект криптографии с открытыми ключами. Основой электронной цифровой подписи является математическое преобразование подписываемых (signed) данных с использованием личного секретного ключа и выполнением следующих условий.

- Создать электронную цифровую подпись можно только с использованием личного секретного ключа.
- Проверить действительность электронной цифровой подписи может любой, имеющий доступ к соответствующему открытому ключу.
- Любое изменение подписанных данных (даже изменение всего одного бита в большом файле) делает электронную цифровую подпись недействительной.

Электронную цифровую подпись, как и любые другие данные, можно передавать вместе с подписанными, то есть защищенными ею, данными. Например, Боб может создать подписанное сообщение электронной почты и отправить текст сообщения вместе с подписью Алисе, предоставив ей возможность удостовериться в подлинности отправителя этого сообщения. Кроме того, цифровая подпись позволяет убедиться в том, что данные при передаче адресату не были изменены (случайно или преднамеренно).

Проверка подлинности

Криптография с открытыми ключами обеспечивает надежные службы распределенной аутентификации. Если Алиса получила от Боба данные и отправила ему зашифрованный с его открытым ключом запрос на подтверждение подлинности, то Боб сможет расшифровать его и вернуть Алисе расшифрованный запрос, подтвердив, что он воспользовался личным секретным ключом, связанным именно с тем открытым ключом, с помощью которого Алиса зашифровала свой запрос. Алиса также может отправить Бобу запрос открытым текстом. В этом случает, Боб отвечает на ее запрос, подписав свое сообщение электронной цифровой подписью. Затем Алиса проверяет подпись Боба с помощью его открытого ключа и удостоверяется в том, что Боб действительно имеет соответствующий личный секретный ключ. Такой запрос делает полученное Алисой сообщение уникальным и исключает возможность злоупотреблений со стороны посторонних лиц. Описанная схема называется протоколом доказательства владения (proof-of-possession), поскольку

отправитель доказывает, что он владеет требуемым для расшифрования и создания электронной цифровой подписи личным секретным ключом.

Согласование общего секретного ключа сессии

Криптография с открытыми ключами также позволяет двум сторонам согласовать общий секретный ключ сессии при обмене информацией через незащищенные каналы связи. Схема выработки общего ключа сессии выглядит следующим образом. Сначала Алиса и Боб генерируют по одному случайному числу, которые используются как половины их общего секретного ключа. Затем Боб отправляет Алисе свою половину секретного ключа, зашифрованную с ее открытым ключом. Алиса отправляет Бобу свою половину, зашифрованную с его открытым ключом. Каждая из сторон расшифровывает полученное сообщение с недостающей половиной секретного ключа, и создает из этих двух половин общий секретный ключ. Выполнив такой протокол, стороны могут пользоваться общим секретным ключом для шифрования последующих сообщений.

Шифрование без предварительного обмена симметричным секретным ключом

Технология шифрования с открытым ключом позволяет шифровать большие объемы данных в том случае, если у обменивающихся информацией сторон нет общего ключа. Существующие алгоритмы шифрования с открытым ключом требуют значительно больше вычислительных ресурсов, чем симметричные алгоритмы, поэтому они неудобны для шифрования больших объемов данных. Однако можно реализовать комбинированный подход с использованием, как симметричного шифрования, так и шифрования с открытым ключом.

Сначала выбирается алгоритм шифрования с секретным ключом (ГОСТ 28147-89, DES и т. п.) затем создается случайный сеансовый ключ (random session key), который будет использоваться для шифрования данных. Боб шифрует этот ключ сеанса, используя открытый ключ Алисы. Затем он отправляет Алисе зашифрованный ключ и зашифрованные данные. Своим личным ключом Алиса расшифровывает ключ сеанса и использует его для расшифрования данных.

Защита и проверка подлинности криптографических ключей

Обмениваясь сообщениями, зашифрованными симметричным секретным ключом, Алиса и Боб доверяют своему общему секретному ключу, потому что они создали его или обменялись им безопасным способом, а также условились надежно хранить этот ключ, чтобы исключить доступ к нему посторонних лиц. При использовании шифрования с открытым ключом Алисе и Бобу нужно защищать только свои личные секретные ключи. А открытые ключи им нужно использовать совместно. Хранить их в секрете нет необходимости, нужна лишь возможность идентифицировать открытый ключ другой стороны. Поэтому для применения шифрования с открытым ключом критическое значение имеет доверие к соответствию между известным субъектом и его открытым ключом.

Алиса может доверять открытому ключу Боба, если Боб передал ей ключ безопасным способом. Но безопасность передачи обеспечивается только защищенными средствами связи. Более вероятно, что Алиса получила открытый ключ Боба с помощью незащищенного средства связи (например, из общего каталога), поэтому нужен механизм, который может обеспечить Алисе уверенность в том, что имеющийся у нее открытый ключ действительно принадлежит Бобу, а не кому-либо другому. Один их таких механизмов основан на сертификатах (certificate), выдаваемых центром сертификации (certification authority).

Сертификаты

Сертификаты обеспечивают механизм надежной связи между открытым ключом и субъектом, которому принадлежит соответствующий личный ключ. Сертификат – это цифровой документ, который содержит открытый ключ субъекта (subject public key) и подписан электронной цифровой подписью его издателя (issuer). Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом субъекта и информацией, его идентифицирующей.

В настоящее время наиболее часто используются сертификаты на основе стандарта Международного союза телекоммуникаций ITU-T X.509 версии 3 и рекомендаций IETF (Internet Engineering Task Force) RFC 2459. Эта базовая технология, используемая в инфраструктуре открытых ключей операционных систем Windows 2000/XP/2003/Vista/2008/7/2008R2/8/2012/8.1/2012R2. Это не единственный вид сертификатов. Например, система защиты сообщений электронной почты PGP (Pretty Good Privacy) использует свою специфическую форму сертификатов.

Центры сертификации

Центр сертификации (ЦС) – это служба, которая выдает сертификаты. Центр сертификации является гарантом связи между открытым ключом субъекта и содержащейся в сертификате информацией по идентификации этого субъекта. Различные ЦС устанавливают и гарантируют эту связь различными способами, поэтому прежде чем доверять сертификатам того или иного ЦС, следует ознакомиться с его политикой и регламентом.

Подтверждение доверия

Когда Алиса получает подписанное сообщение, у нее возникает важный вопрос – можно ли этой подписи доверять? Иными словами – действительно ли эта подпись принадлежит отправителю сообщения? Алиса может проверить целостность подписи с помощью известного ей открытого ключа отправителя и криптографических алгоритмов. Однако при этом Алиса должна быть уверена в том, что использованный ею для проверки открытый ключ действительно принадлежит тому субъекту, именем которого подписано сообщение. Если у Алисы нет прямого доказательства, что

открытый ключ принадлежит Бобу, то ей надо получить хотя бы достаточно веское подтверждение этого.

Если Алиса сможет найти сертификат открытого ключа Боба, выданный тем центром сертификации, которому она доверяет, то она получит убедительное подтверждение того, что открытый ключ Боба действительно принадлежит Бобу. Итак, у Алисы появится веское основание полагать, что открытый ключ принадлежит именно Бобу, если она найдет сертификат, который:

- имеет действительную с криптографической точки зрения подпись его издателя;
- подтверждает связь между именем Боб и открытым ключом Боба;
- выдан центром сертификации, которому Алиса доверяет.

Если Алиса найдет такой сертификат открытого ключа Боба, то она сможет проверить подлинность этого сертификата с помощью открытого ключа центра сертификации. Однако теперь у Алисы возникает следующий вопрос. Как убедиться в том, что этот открытый ключ действительно принадлежит данному центру сертификации? Алисе нужно найти сертификат, удостоверяющий подлинность этого центра сертификации.

Таким образом, в процессе проверки сертификата Алиса продвигается по цепочке сертификатов (certification path). В конце цепочки сертификатов, ведущей от сертификата открытого ключа Боба через ряд центров сертификации, находится сертификат, выданный тем ЦС, которому Алиса полностью доверяет. Такой сертификат называется доверенным корневым сертификатом (trusted root certificate), поскольку он образует в иерархии связей «открытые ключи – личность» корень (самый верхний узел), который Алиса считает надежным (см. раздел «Иерархии центров сертификации»). Если Алиса явно решит доверять этому доверенному корневому сертификату, то она неявно будет доверять всем сертификатам, выданным доверенным корневым сертификатом и всеми сертифицированными им ЦС.

Набор доверенных корневых сертификатов, которым Алиса доверяет явно – это единственная информация, которую Алиса должна получить надежным способом. На этом наборе сертификатов базируется ее система доверия и обоснование надежности инфраструктуры открытых ключей.

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

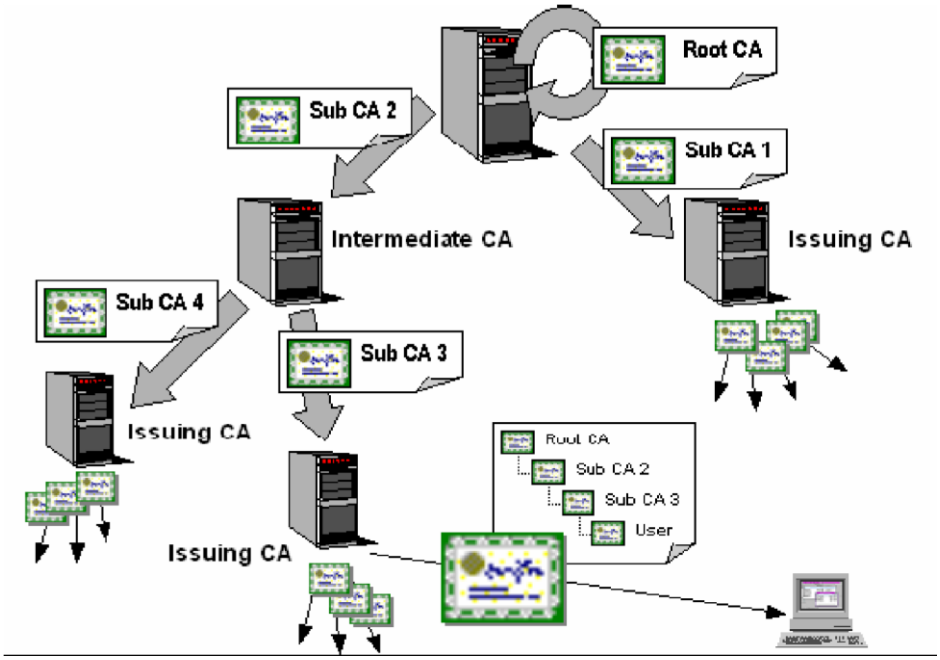
Включенные в серверные операционные системы Windows 2000/2003/2008/2008R2/8/2012 /8.1/2012R2 службы сертификации предоставляют предприятию средства для организации центров сертификации. Службы сертификации содержат применяемый по умолчанию модуль политики, который можно использовать для выдачи сертификатов пользователям, компьютерам и службам. При этом выполняется идентификация объекта, отправившего запрос на сертификат, и проверка допустимости запрошенного сертификата в соответствии с политикой безопасности домена. Разработчики могут изменить этот модуль таким образом, чтобы он соответствовал другой политике, а также расширить поддержку ЦС для различных сценариев Интранета и Интернета.

В рамках инфраструктуры открытых ключей можно поддерживать как ЦС предприятия, так и внешние ЦС, связанные с другими организациями и коммерческими поставщиками услуг. Эта возможность позволяет предприятию подстраивать свою среду под конкретные условия деятельности.

Иерархии центров сертификации

Инфраструктура открытых ключей предполагает иерархическую модель построения центров сертификации. Такая модель обеспечивает масштабируемость, удобство администрирования и согласованность с растущим числом коммерческих продуктов и ЦС различных поставщиков. Простейшая форма иерархии ЦС состоит из одного ЦС, а в общем случае – из множества ЦС с явно определенными отношениями «родительский-дочерний», как показано на рисунке 1. Как видно из этого рисунка, допускается существование не связанных между собой иерархий. Другими словами, центры сертификации не обязательно должны иметь общий родительский (корневой) ЦС на самом верхнем уровне.

В этой модели дочерние ЦС сертифицируются родительским ЦС. ЦС, находящийся на самом верхнем уровне иерархии, обычно называется корневым (root) ЦС. Подчиненные ЦС являются промежуточными (intermediate) или выдающими (issuing) ЦС. В данном документе выдающим ЦС называется тот центр сертификации, который выдает сертификаты конечным пользователям. Промежуточным ЦС здесь называется тот ЦС, который не является корневым и выдает сертификаты только другим ЦС, а не конечным пользователям.



Фундаментальное преимущество этой модели состоит в том, что проверка сертификатов требует доверия только относительно малому числу корневых ЦС. В то же время эта модель позволяет иметь различное число ЦС, выдающих сертификаты. Поддержка нескольких выдающих ЦС применяется по ряду причин практического свойства. К ним относятся следующие:

- **Использование**. Сертификаты могут выдаваться для различных целей (например, для защиты электронной почты, сетевой аутентификации и так далее). Политика выдачи сертификатов для этих целей может быть различной, а существование нескольких ЦС позволяет реализовать различные политики.
- **Структура подразделений организации**. Политики выдачи сертификатов могут различаться в зависимости от роли субъекта в организации. Для разделения этих политик и управления ими можно создать несколько выдающих ЦС.
- **Территориальное деление**. Организации могут иметь территориально отдаленные подразделения. Из-за условий сетевой связи между этими подразделениями может потребоваться несколько выдающих ЦС.

Иерархия центров сертификации имеет также административные преимущества, в том числе следующие.

- Гибкая настройка среды безопасности ЦС (степень защиты ключа, физическая защищенность, защита от сетевых атак и так далее) для достижения компромисса между степенью защиты и удобством применения. Например, для корневого ЦС можно использовать специализированное криптографическое оборудование, эксплуатируемое в физически защищенном месте и не подключенное к сети. Такой ЦС нецелесообразно использовать для выдачи сертификатов конечным объектам, поскольку это было бы слишком сложно с практической точки зрения.

- Возможность часто обновлять ключи и сертификаты, выдаваемые выдающими ЦС, которые находятся в условиях риска компрометации, и при этом не изменять установленные отношения доверия с корневым ЦС.
- Возможность отключить часть иерархии ЦС, не затрагивая установленные отношения доверия. Например, можно закрыть выдающий ЦС какого-либо отдельно расположенного подразделения и отозвать его сертификаты без отрицательных последствий для остальной части организации.

В общем случае желательно, чтобы иерархия ЦС не менялась, но это не является обязательным условием. Добавление и удаление подчиненных ЦС выполняется без особых затруднений. Можно также объединить существующие иерархии ЦС, сделав один из корневых ЦС промежуточным – он будет сертифицироваться другим корневым ЦС. Перед этим, однако, следует тщательно рассмотреть вопрос о том, не вызовет ли это противоречие политик и не нарушит ли ограничение на глубину вложенности, которое может быть заложено в существующие сертификаты.

ОТЗЫВ СЕРТИФИКАТОВ

Существует целый ряд причин, по которым доверие к сертификату может быть подорвано до истечения срока его действия. Примеры:

- Потеря ключевых носителей.
- Потеря ключевых носителей с их последующим обнаружением.
- Увольнение сотрудников, имевших доступ к ключевой информации.
- Нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа.
- Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
- Нарушение правил хранения ключевых носителей.
- Получение сертификата незаконным путем.
- Изменение статуса субъекта.
- Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Инфраструктура открытых ключей допускает распределенную проверку сертификата, которая не требует прямого обмена данными с центральным доверенным объектом, выпустившим этот сертификат. Для этого необходима информация об отзыве сертификатов, распределяемая лицам, которым требуется проверить сертификат.

В инфраструктуре открытых ключей предусмотрены специальные списки отозванных сертификатов (CRL – Certificate Revocation List). ЦС предприятия поддерживает отзыв сертификатов и публикацию списков отозванных сертификатов в Active Directory под контролем администратора. Клиенты домена могут получить эту информацию и записать ее в локальный кэш, чтобы использовать для проверки сертификатов. Этот же механизм поддерживает публикацию списков CRL коммерческими ЦС и сертификационными серверами других поставщиков, если опубликованные ими списки доступны клиентам через сеть.

Доверие

При использовании криптографии с открытыми ключами важнейшее значение для пользователя имеет доверие к проверке сертификата. Обычно проверка основывается на доверии к ЦС, выдавшему данный сертификат. Выше уже объяснялось, что инфраструктура открытых ключей предполагает иерархию ЦС, в которой управление доверием основано на решении о доверии корневому ЦС. Если проверка показывает, что данный сертификат конечного пользователя является конечным звеном цепочки, ведущей к доверенному корневому ЦС, и если сертификат

используется с целью, соответствующей контексту приложения, то такой сертификат считается действительным. Если какое-либо из указанных условий не соблюдено, то сертификат считается недействительным.

Пользователи имеют возможность принимать решения о доверии, затрагивающие только их самих. Они могут делать это путем установки или удаления сертификатов доверенных корневых ЦС в хранилища на своих рабочих станциях. Однако это должно быть исключением, а не правилом. Такие доверительные отношения следует устанавливать как часть политики предприятия. Установленные политикой доверительные отношения автоматически распространяются на клиентские компьютеры, работающие под управлением операционных систем Windows 2000/XP/2003/Vista/2008/7/2008R2/8/2012/8.1/2012R2.

ИСПОЛЬЗОВАНИЕ РОССИЙСКИХ КРИПТОАЛГОРИТМОВ В WINDOWS

Пользователям Windows теперь стала доступна возможность использовать сертифицированные средства криптографической защиты информации в составе операционной системы Windows.

Средство криптографической защиты информации КриптоПро CSP, разработанное компанией "Крипто-Про" (http://www.cryptopro.ru), реализовано в соответствии с криптографическим интерфейсом корпорации Microsoft — CSP (Cryptographic Service Provider) и российскими криптографическими алгоритмами:

- ГОСТ Р 34.10-94 "Информационная технология. Криптографическая защита информации. Система электронной цифровой подписи на базе асимметричного криптографического алгоритма" (КриптоПро CSP версии 1.1 (ЖТЯИ.00001-01 30 01);
- ГОСТ Р 34.10-94 и ГОСТ Р34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи" (КриптоПро CSP версии 2.0 ЖТЯИ.00005-01 30 01);
- хэширования ("ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.");
- шифрования и имитозащиты данных ("ГОСТ 28147-89. Системы обработки информации. Защита криптографическая").

Важно: С 1 января 2008 года не допускается применение алгоритма ГОСТ Р 34.10-94, реализованного СКЗИ «КриптоПро CSP» (версия 2.0) и СКЗИ «КриптоПро CSP» (версия 3.0), для формирования электронной цифровой подписи электронных документов. Применение данного алгоритма допустимо для подтверждения подлинности электронной цифровой подписи (проверки ЭЦП).

Использование СКЗИ КриптоПро CSP позволяет решить сразу несколько задач:

- корпоративные пользователи получают возможность использовать стандартные и повсеместно используемые приложения корпорации Microsoft с надежной российской криптографией (256 бит).
- системные интеграторы получают возможность создавать новые, надежно защищенные приложения, используя проверенный временем инструментарий разработки корпорации Microsoft.

К стандартным приложениям, которые теперь могут использовать российские алгоритмы электронной цифровой подписи и шифрования, относятся:

- Центр Сертификации сертификатов открытых ключей X.509 — Microsoft Certification Authority.

- Электронная почта — Microsoft Outlook, входящая в состав Microsoft Office 2000/XP/2003/2007/2010/2012.
- Электронная почта — Microsoft Outlook Express, входящая в состав Internet Explorer версии 5.0 и выше.
- Электронная почта — Почта Windows (Windows Mail), входящая в состав в ОС Windows Vista и ОС Windows Server 2008.
- Электронная почта — Windows Live Mail.
- Защита соединений в Интернете с использованием протокола TLS/SSL. СКЗИ КриптоПро CSP (разных версий) имеют сертификаты соответствия ФСБ РФ:

  http://www.cryptopro.ru/CryptoPro/products/csp/conformance.htm

ЗАЩИТА ИНФОРМАЦИИ В КОРПОРАТИВНОЙ ЭЛЕКТРОННОЙ ПОЧТЕ

Клиентское программное обеспечение Microsoft Outlook, входящее в состав пакетов Office 2000, Office XP, Office 2003, Office 2007 и Office 2010, а также Microsoft Outlook Express, поставляемый вместе с Internet Explorer, Почта Windows (Windows Mail), Windows Live Mail используют функции CryptoAPI 2.0 для обеспечения конфиденциальности, целостности и подтверждения авторства почтовых сообщений, передаваемых в формате S/MIME (Secure MIME). Стандартная поставка этих продуктов содержит ограничения на область применения криптографических функций: либо длиной ключа 40 или 56 бит, либо возможными используемыми алгоритмами.

Установка сертифицированного средства криптографической защиты информации КриптоПро CSP позволяет использовать эти клиентские средства электронной почты Microsoft с российскими криптографическими алгоритмами и ключами 256 бит.

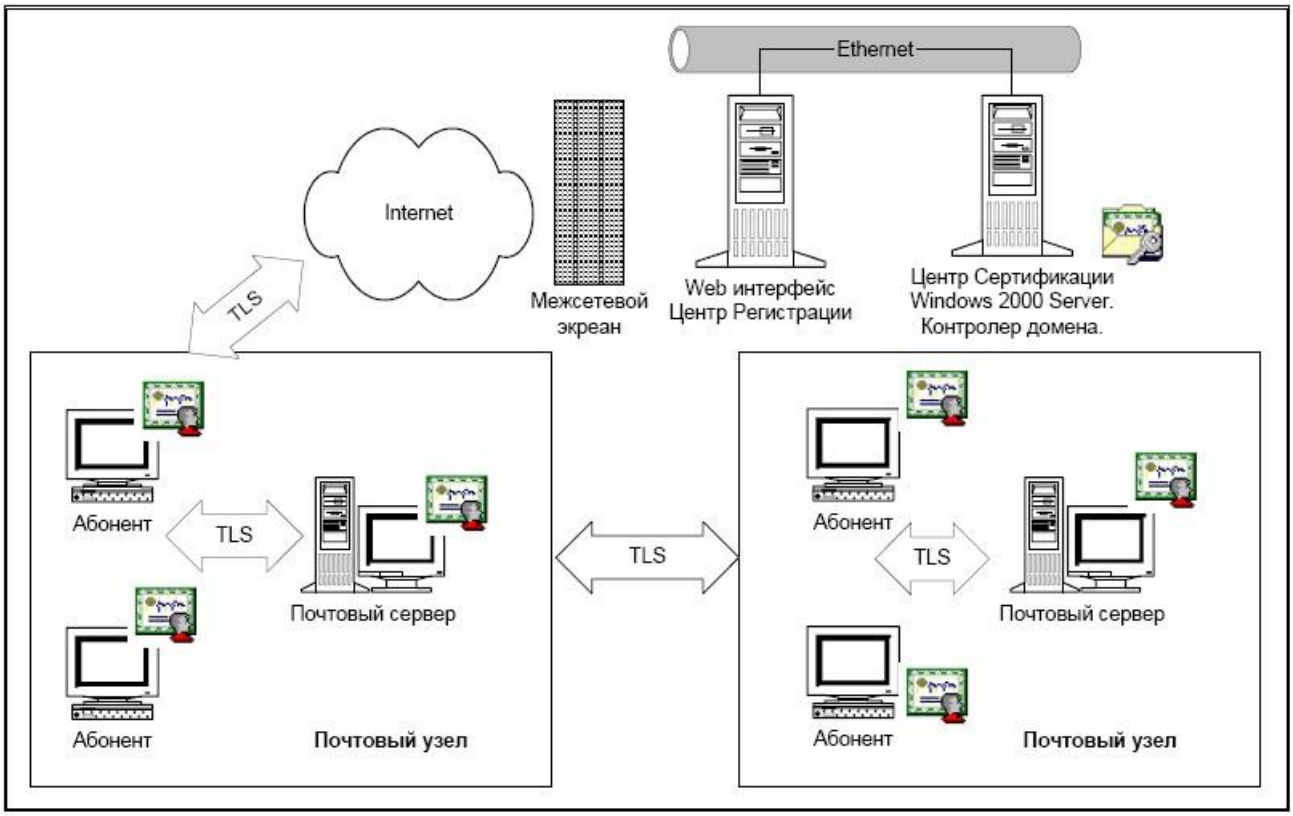
ЦЕНТР СЕРТИФИКАЦИИ В КОРПОРАТИВНОЙ ПОЧТОВОЙ СИСТЕМЕ

Использование Центра Сертификации в корпоративной системе имеет отличия от принятой схемы предоставления услуг по заверению сертификатов открытых ключей, предоставляемых такими организациями как VeriSign, Thawte или GTE. Для корпоративного использования услуги Центра Сертификации должны удовлетворять следующим требованиям:

- минимальный интерфейс взаимодействия пользователя;
- автоматизация процесса регистрации пользователя и получения сертификата, за счет использования данных о пользователе в домене Windows.

Построение Центра Регистрации (ЦР) относительно несложно, но требует некоторого дополнительного знания, так как использование этой службы почти не освещается в документации Microsoft. В Microsoft Windows 2000/2003/2008/2008R2 Центр Регистрации — это тот же Центр Сертификации, имеющий дополнительную настройку. Чтобы построить ЦР, у Центра Сертификации необходимо отключить способность подписывать сертификаты, но сохранить его функцию обслуживания запросов на сертификаты через Web интерфейс.

Общая схема построения корпоративной системы, использующий Центр Регистрации и Центр Сертификации, приведена на следующем рисунке.



Задачи Центра Регистрации

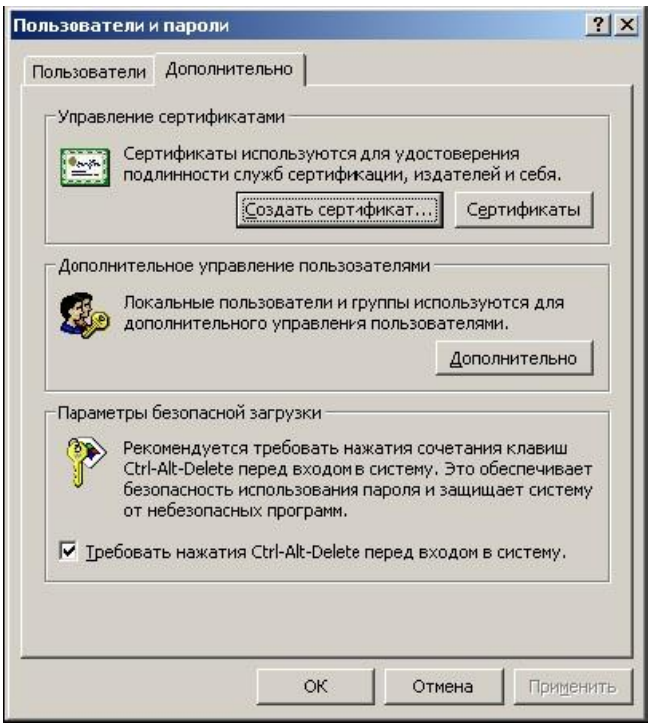
Центр Регистрации в корпоративной системе должен обеспечить выполнение следующих функций:

- конфиденциальность данных, передаваемых пользователем в процессе регистрации;
- аутентификацию пользователя при обработке запроса на сертификат;
- защищенную доставку сертификата Центра Сертификации;
- обновление списка отозванных сертификатов для пользователей корпоративной системы.

Конфиденциальность передаваемых данных регистрации и доверенную доставку сертификата Центра Сертификации можно обеспечить, используя протокол SSL (TLS), реализованный с помощью криптопровайдера КриптоПро CSP. Аутентификация в данном случае должна быть односторонняя, так как в момент регистрации пользователь не имеет своего личного секретного ключа и сертификата.

Идентификацию пользователя и определение его прав и учетной информации можно производить по результату парольного входа в домен Windows. Предварительная регистрация пользователя в домене (там, где он не был зарегистрирован) с одной стороны потребует дополнительных усилий, но с другой стороны позволит достоверно определить информацию о пользователе, включая его адрес электронной почты, и автоматически внести эту информацию в формируемый запрос на сертификат. Такая схема позволяет автоматизировать процесс выпуска сертификата в корпоративной сети и отказаться от личного присутствия пользователя в Центре Сертификации.

Пользователи, работающие в операционной системе Windows 2000 или Windows NT, имеют возможность автоматической генерации сертификата, на основе данных, зарегистрированных в домене. Для этого они должны воспользоваться меню "Пуск", "Настройка", "Панель управления", "Пользователи и пароли" и в диалоге выбрать закладку "Дополнительно". Используя кнопку "Создать сертификат", пользователи домена с помощью мастера диалогов проходят цепочку генерации ключей и получения сертификата (см. рисунок).


Пользователи и пароли
Пользователи
Дополнительно
Управление сертификатами
Сертификаты используются для удостоверения подлинности служб сертификации, издателей и себя.
Создать сертификат...
Сертификаты
Дополнительное управление пользователями
Локальные пользователи и группы используются для дополнительного управления пользователями.
Дополнительно
Параметры безопасной загрузки
Рекомендуется требовать нажатия сочетания клавиш Ctrl-Alt-Delete перед входом в систему. Это обеспечивает безопасность использования пароля и защищает систему от небезопасных программ.
Требовать нажатия Ctrl-Alt-Delete перед входом в систему.
OK
Отмена
Применить

ГЕНЕРАЦИЯ КЛЮЧА И ПОЛУЧЕНИЕ СЕРТИФИКАТА ДЛЯ РАБОТЫ В ЭЛЕКТРОННОЙ ПОЧТЕ

Как было описано в предыдущем разделе корпоративный пользователь, используя Internet Explorer и Web интерфейс Центра Регистрации (Центра Сертификации), должен:

- установить защищенное соединение с ЦР;
- по результатам аутентификации и на основе данных, подготовленных автоматически ЦР, сформировать личный секретный ключ и запрос на сертификат;
- передать запрос на сертификат в ЦР;
- в случае корректной криптографической проверки запроса на сертификат получить свой личный сертификат и установить его в справочник сертификатов.

Функции генерации секретных ключей, формирования запроса на сертификат и установки сертификата пользователя обычно реализуются через COM интерфейс Certificate Enrollment Control (https://msdn.microsoft.com/en-us/library/windows/desktop/aa376517.aspx). Примеры использования этого интерфейса приведены в ASP страницах, устанавливаемых Web интерфейсом Центра Сертификации Microsoft.

Следует обратить особое внимание на две следующие особенности при формировании сертификатов пользователей, используемых в электронной почте:

- сертификат пользователя должен содержать дополнение **расширенная область применения ключа** (extendedKeyUsage) со значением 1.3.6.1.5.5.7.3.4 (защита электронной почты);
- сертификат пользователя должен содержать адрес электронной почты Владельца сертификата в формате RFC 822 (name@domain.country).

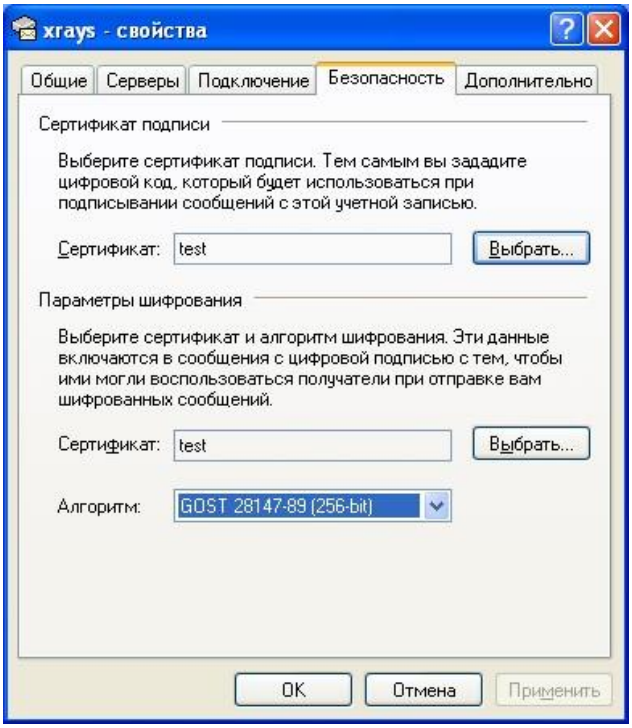
ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В OUTLOOK EXPRESS

Программное обеспечение Outlook Express версии 5.0 и выше полностью поддерживает Инфраструктуру Открытых Ключей для обеспечения конфиденциальности, целостности, авторства почтовых сообщений, передаваемых по протоколам SMTP, IMAP, POP3. Для этих целей Outlook Express использует функции CryptoAPI 2.0 и сертификаты открытых ключей X.509. В качестве формата защищенных сообщений используется формат, описанный в рекомендациях Secure Multipurpose Internet Mail Extensions (S/MIME).

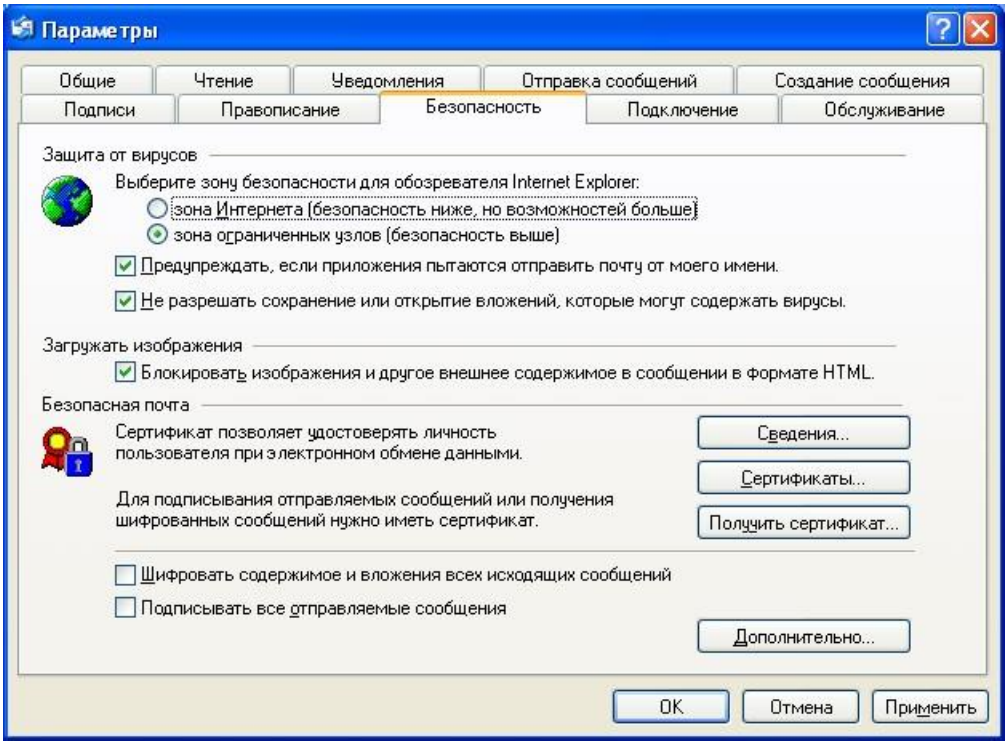
Приведенная ниже информация описывает действия по конфигурации в Outlook Express, необходимые для обеспечения защиты почтовых сообщений.

Конфигурация 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 расшифрования входящих сообщений. Как уже было отмечено раннее, 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.

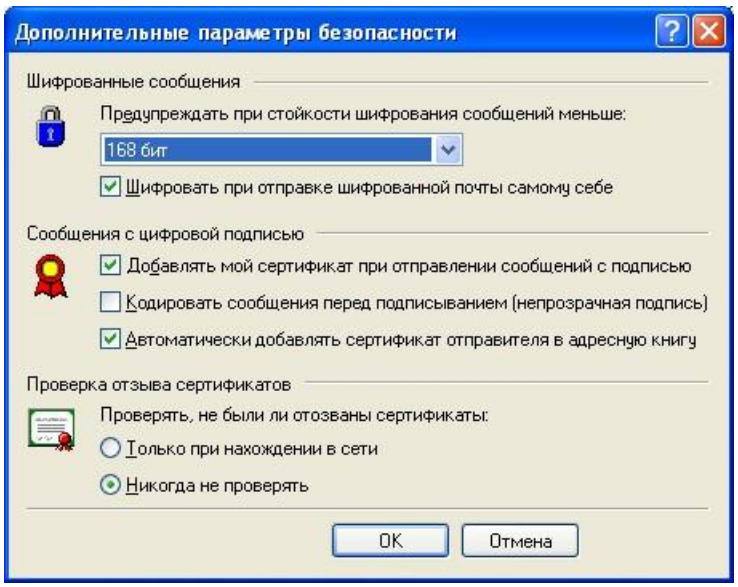
Нажмите кнопку **Дополнительно**. В отображаемом диалоге установите следующие режимы:

Шифровать при отправке шифрованной 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 подпись формируется в виде одного отдельного вложения для сообщения. Если режим выключен - текст сообщения и все вложения объединяются в единое целое и кодируются в соответствии с правилами кодирования BASE64, после чего результат кодирования подписывается.

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;

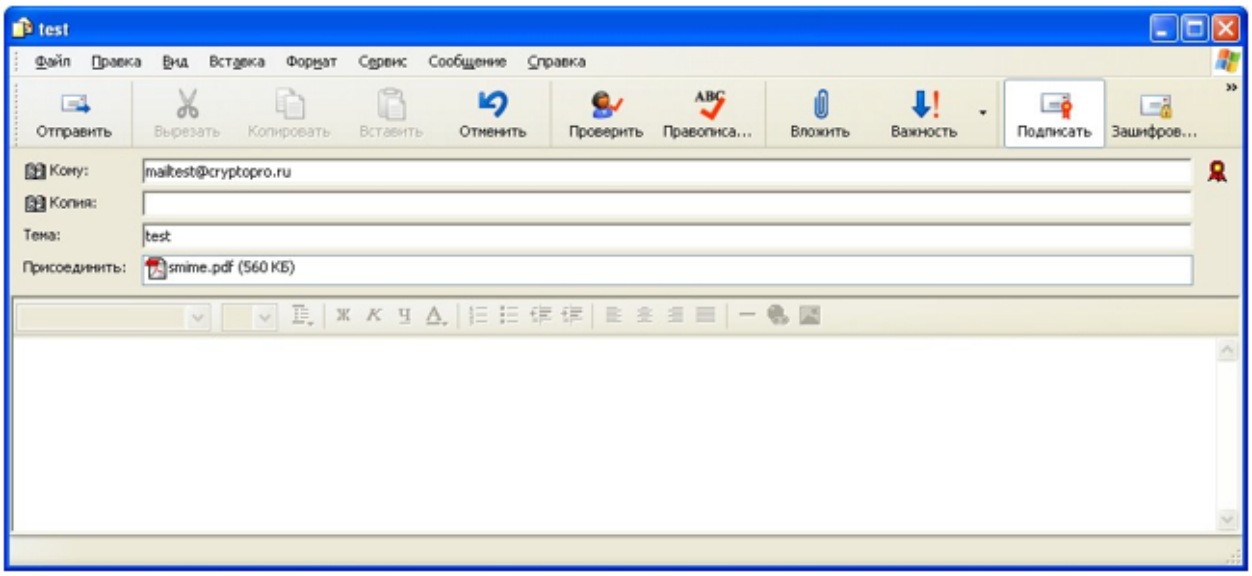
никогда не проверять – проверка на отзыв не выполняется.

Отправка подписанных сообщений

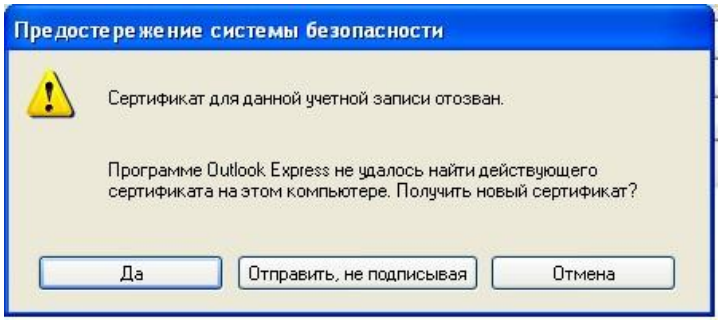
Для создания и отправки подписанного сообщения нажмите кнопку **Создать сообщение** или выберите пункт меню **Файл, Создать, Сообщение**.

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**.



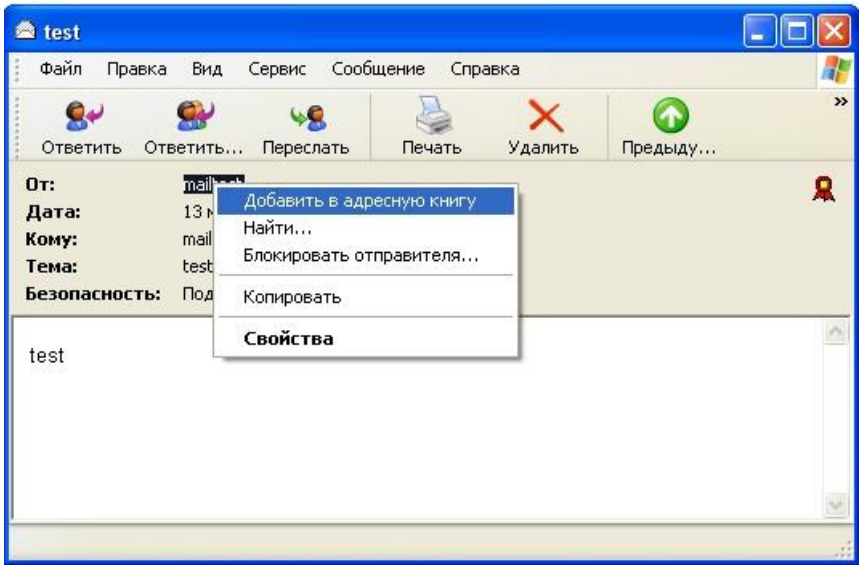
Если в ответ появится следующее предупреждение, то это означает, что сертификат был отозван.



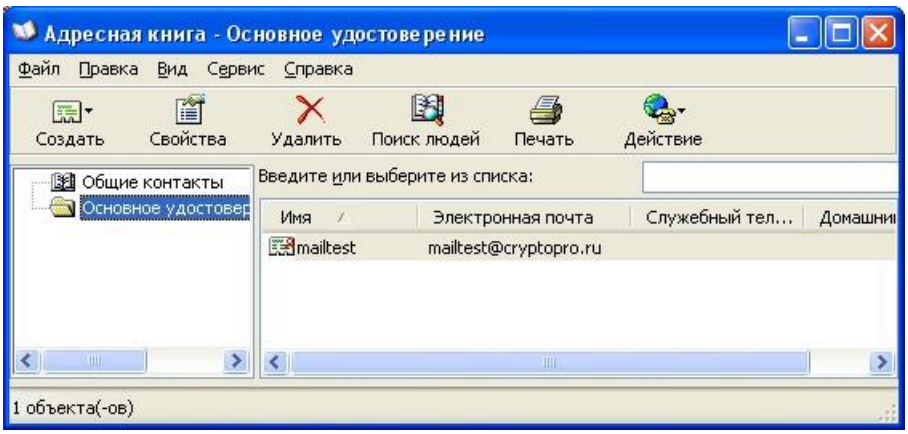
Получение сертификата открытого ключа абонента для шифрования сообщений

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). 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.



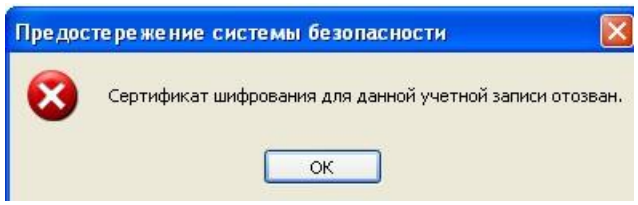
Отправка шифрованных сообщений

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**.

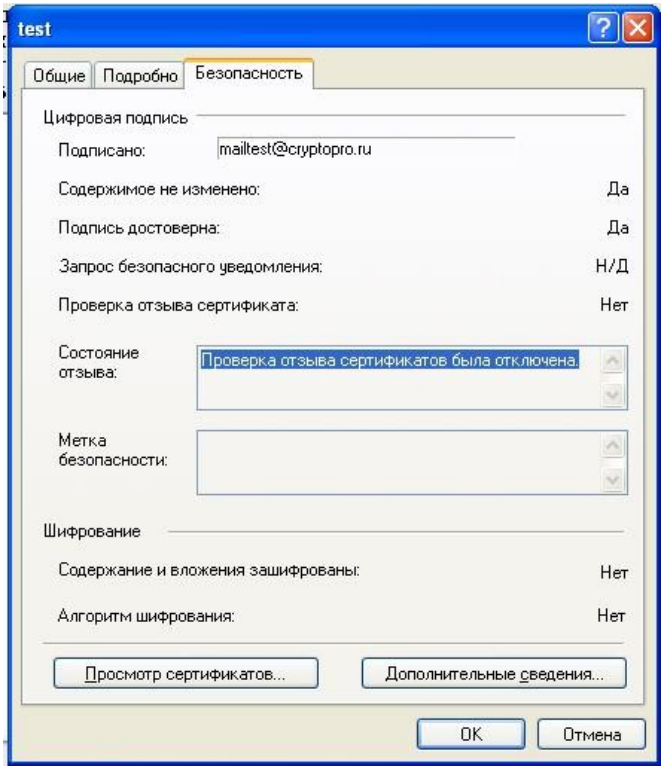
При попытке зашифровать письмо на открытом ключе владельца отозванного сертификата возникнет та же ситуация, что и при отправке сообщения, подписанного с помощью отозванного сертификата. А предупреждающее окно будет выглядеть так:



Проверка сертификата на отзыв

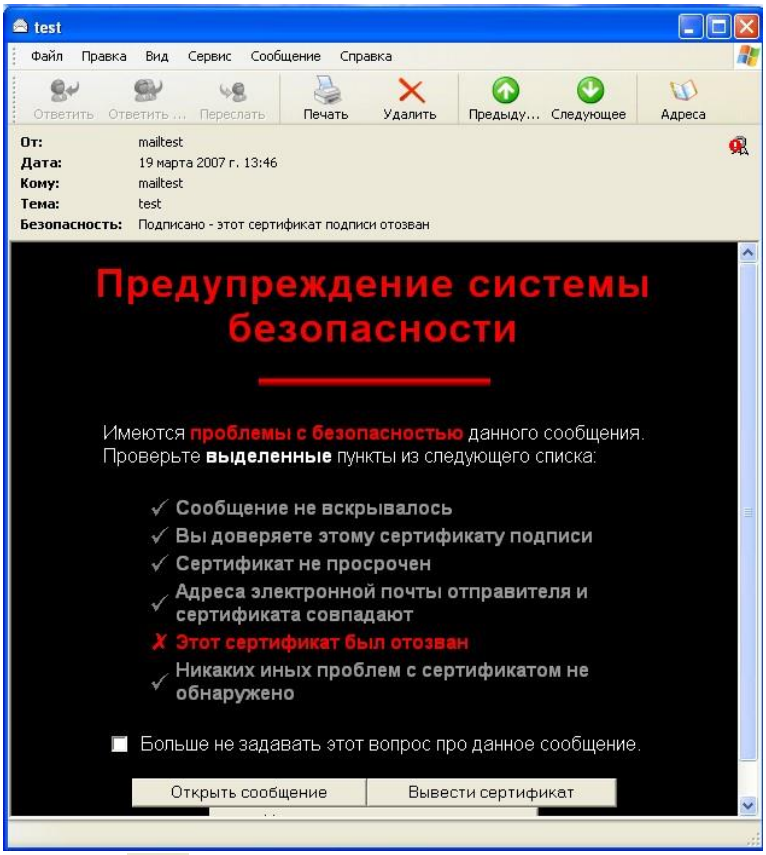
Периодичность издания списков отозванных сертификатов (СОС) определяется Удостоверяющим центром. Центр Сертификации издает СОС и публикует его в сетевом справочнике (при его наличии). Пользователи должны регулярно обновлять СОС, хранящийся в локальном справочнике сертификатов с использованием доступных средств.

Для контроля проверки сертификатов на отзыв выполните следующие действия. Откройте полученное подписанное письмо. Нажмите кнопку  – признак подписанного сообщения. Как уже было отмечено раннее, для автоматической проверки подписи на отзыв необходимо установить флаг **Проверять, 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:



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

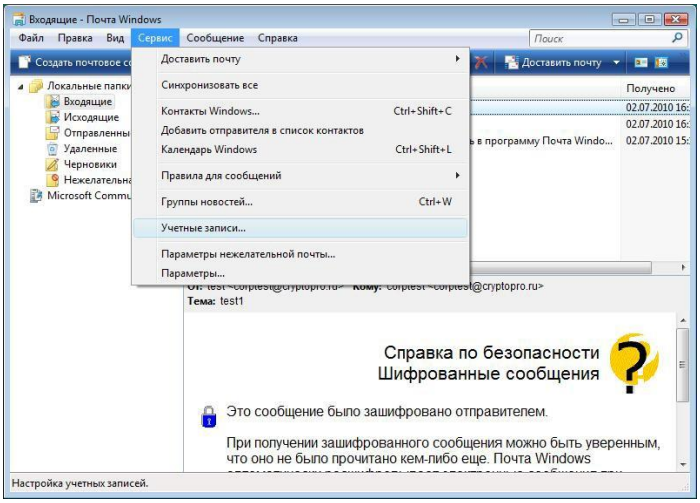
ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В ПРОГРАММЕ "ПОЧТА WINDOWS"

Программа "Почта Windows" (Windows Mail) является компонентом только ОС Windows Vista и Windows 2008 Server.

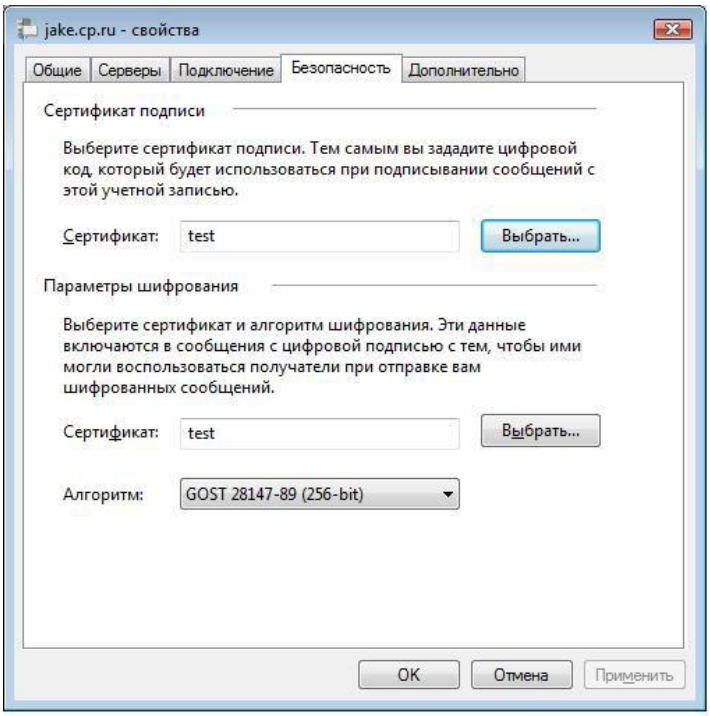
Использование средств криптографической защиты в программе "Почта Windows" для клиента во многом совпадает с использованием в других почтовых программах.

Конфигурация программы "Почта Windows"

Выберите пункт **меню Сервис**, **Учетные записи**.



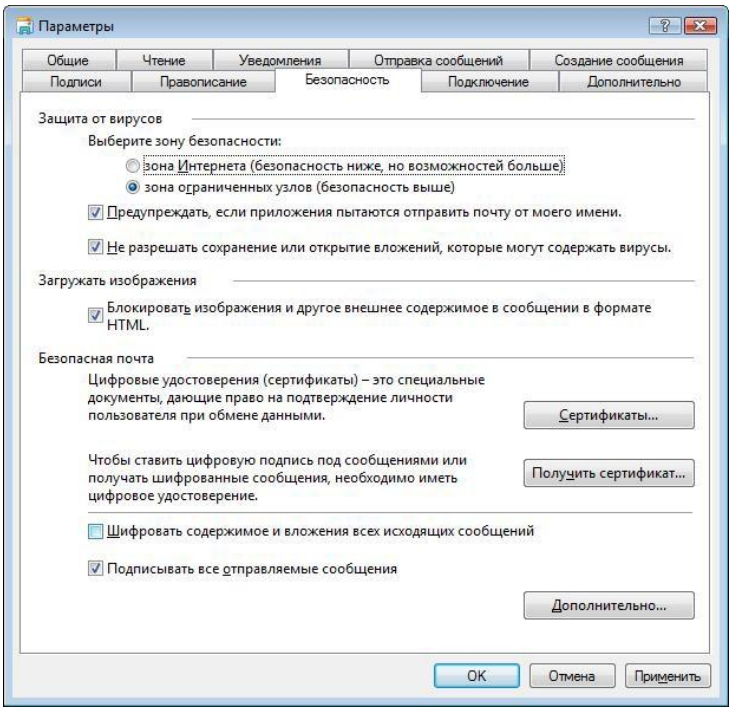
Выберите свою учетную запись, нажмите на **Свойства**. Нажмите на закладку **Безопасность**.



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 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**, нажмите на закладку **Безопасность.** В отображаемом диалоге можно включить режимы **Шифровать содержимое и вложения исходящих сообщений** и **Подписывать 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 **Дополнительно**.

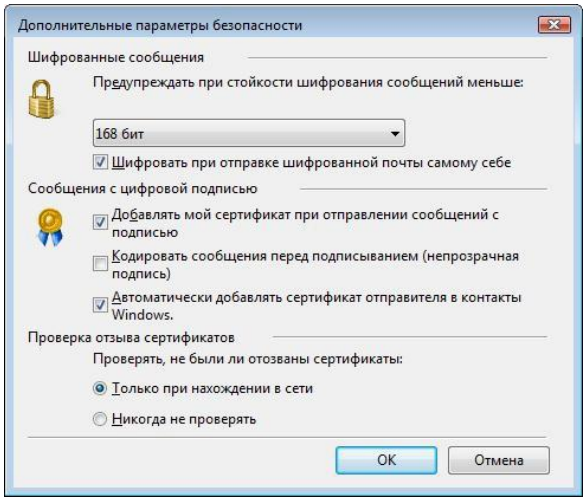
Шифровать при отправке шифрованной почты самому себе. Установка режима включения дает возможность отправителю расшифровывать отправленные им сообщения.

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 подпись формируется в виде одного отдельного вложения для сообщения. Если режим

выключен - текст сообщения и все вложения объединяются в единое целое и кодируются в соответствии с правилами кодирования BASE64, после чего результат кодирования подписывается.

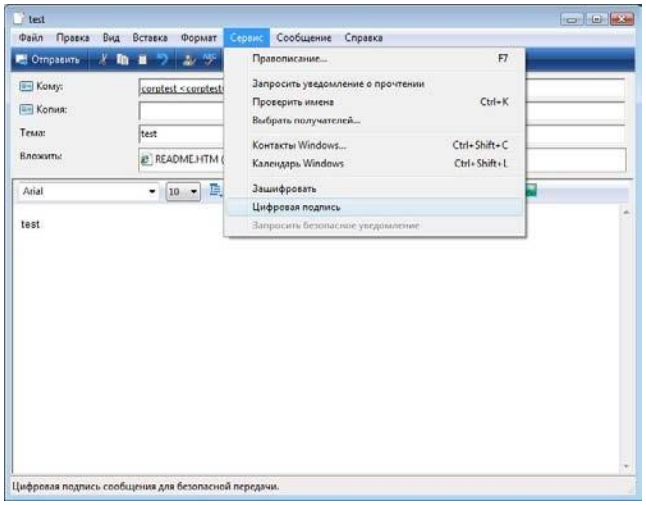
Автоматически добавлять сертификаты отправителей в контакты Windows. При включенном режиме сертификаты, передаваемые в составе подписанного сообщения, будут автоматически добавляться в контакты.



Отправка подписанных сообщений

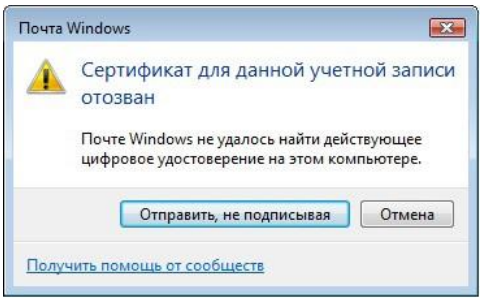
Для создания и отправки подписанного сообщения нажмите кнопку **Создать почтовое сообщение.** 

Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Прикрепить**.  Для отправки сообщения в подписанном виде нажмите кнопку меню **Сервис**, отметьте **Цифровая подпись.** Или выделите пункт меню **Подписать**  **.**



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

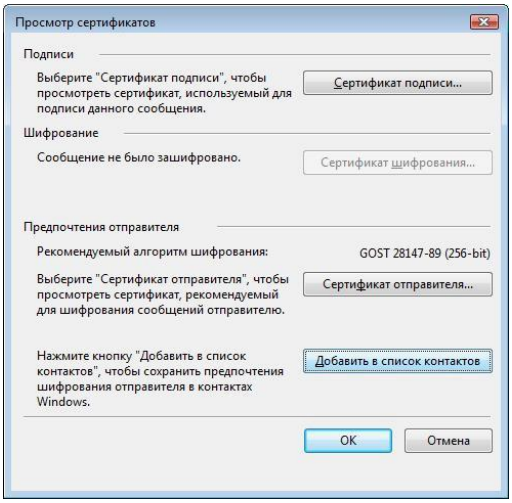
Если сертификат, с помощью которого подписано сообщение, был отозван, то появится следующее предупреждение, а само сообщение не будет отправлено.



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 список контактов.

Для контроля добавления выполните следующие действия. Откройте полученное подписанное письмо. Нажмите кнопку  - признак подписанного сообщения. Нажмите **Просмотреть сертификаты, Добавить в список контактов.**

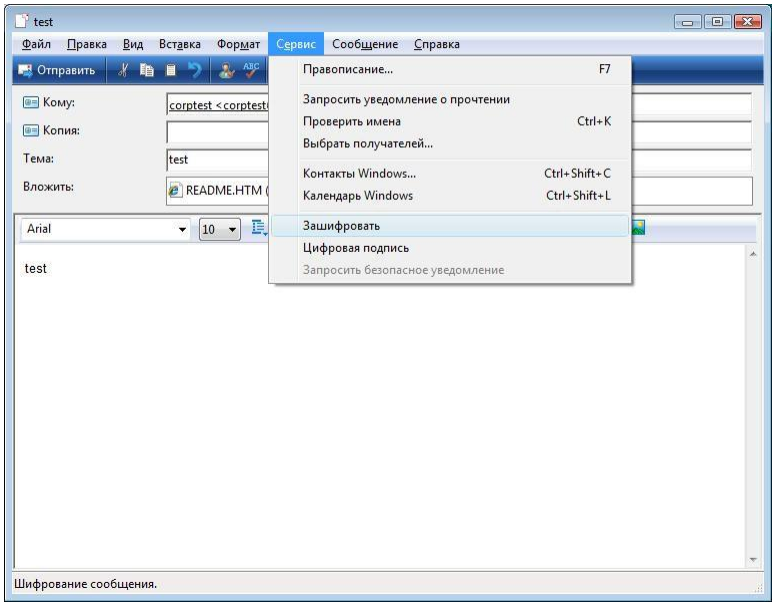


После чего появится сообщение: «Сертификат отправителя был добавлен во все контакты, в которых был встречен его электронный адрес. (Если таких контактов не было, был создан новый)»

Отправка шифрованных сообщений

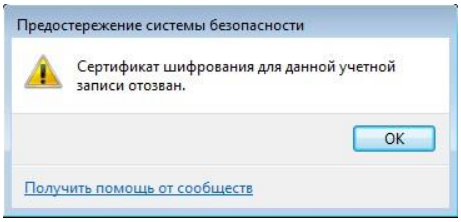
Для создания и отправки подписанного сообщения нажмите кнопку **Создать почтовое сообщение.** 

Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Прикрепить**. Для отправки сообщения в зашифрованном виде нажмите кнопку меню **Сервис**, отметьте **Зашифровать.** Или выделите пункт меню **Зашифровать.**



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

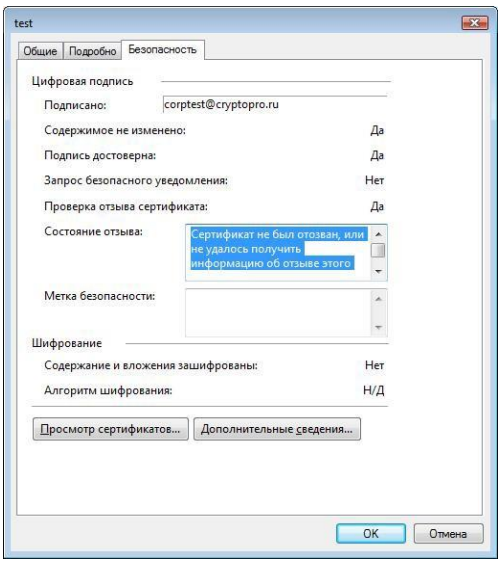
При попытке зашифровать письмо на открытом ключе владельца отозванного сертификата, появится следующее предупреждение.



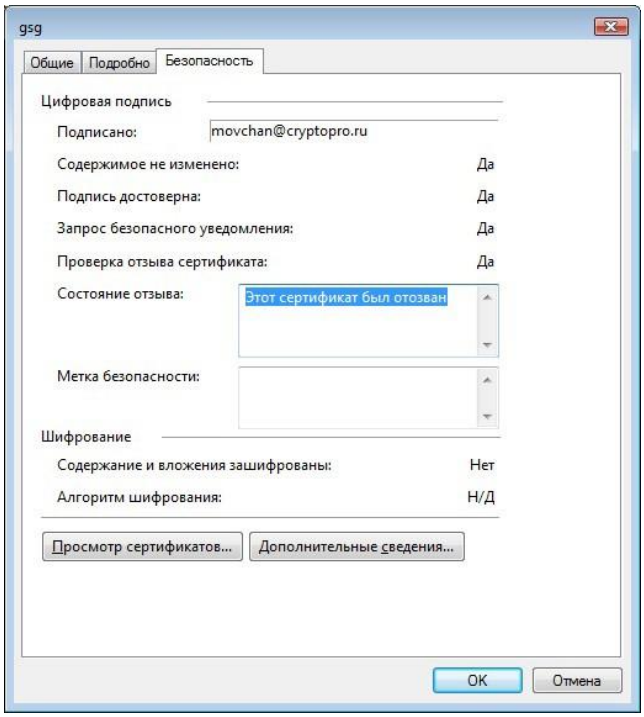
Проверка сертификата на отзыв

Для контроля проверки сертификатов на отзыв выполните следующие действия. Откройте полученное подписанное письмо. Нажмите кнопку – признак подписанного сообщения.

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 окно осталось прежним, то сертификат не был отозван.



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

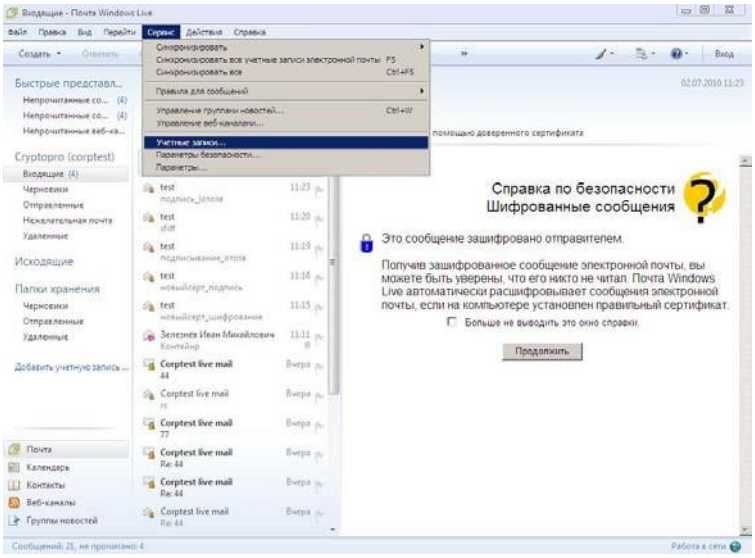


ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В WINDOWS LIVE MAIL

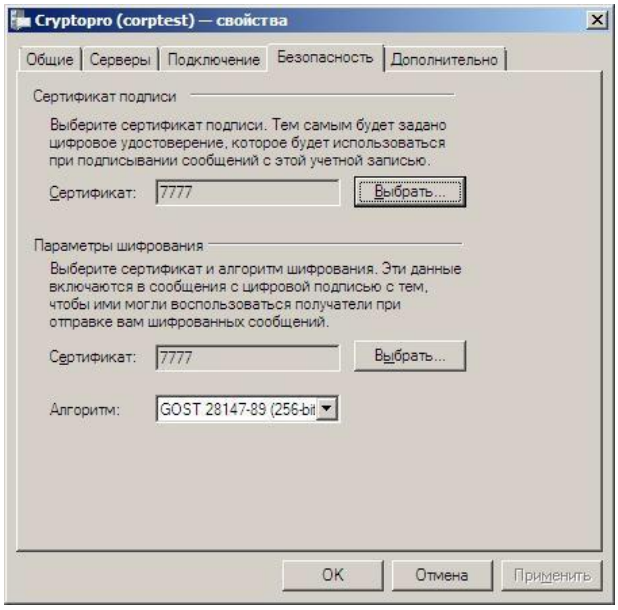
Использование средств криптографической защиты в Windows Live Mail для клиента во многом совпадает с использованием в других почтовых программах.

Конфигурация Windows Live Mail

Выберите пункт **меню Сервис**, **Учетные записи**.



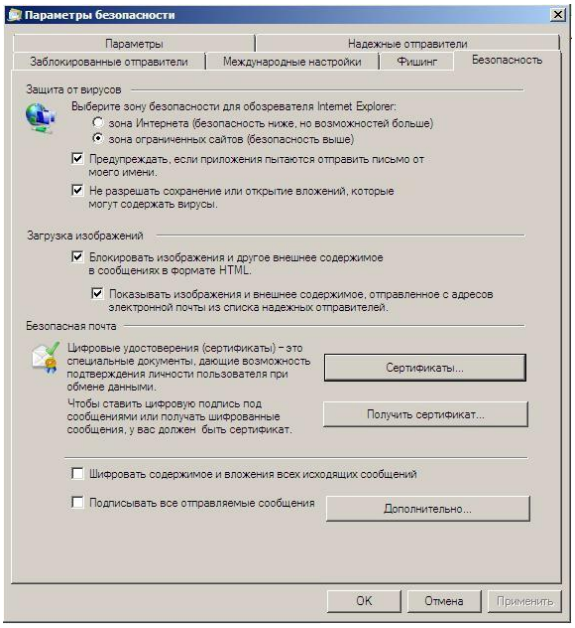
Выберите свою учетную запись, нажмите на **Свойства**. Нажмите на закладку **Безопасность**.



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 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 **Параметры безопасности**, нажмите на закладку **Безопасность.** В отображаемом диалоге можно включить режимы **Шифровать содержимое и вложения исходящих сообщений** и **Подписывать 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.



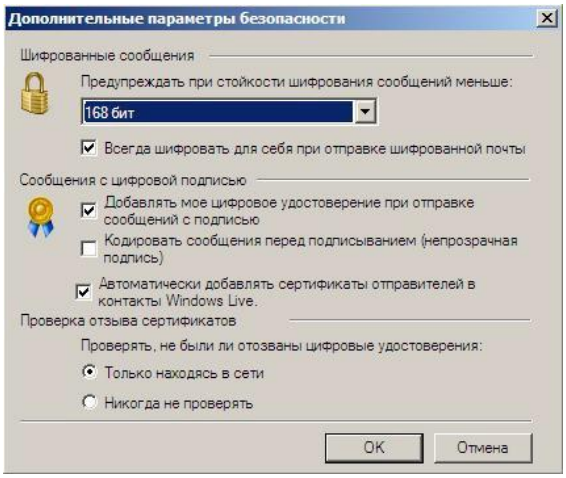
Нажмите **Дополнительно**.

Всегда шифровать для себя при отправке шифрованной почты. Установка режима включения дает возможность отправителю расшифровывать отправленные им сообщения.

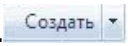
Добавлять мое цифровое удостоверение при отправке сообщений с подписью. Установка этого режима автоматически будет добавлять сертификат отправителя ко всем сообщениям. Этот режим позволяет производить обмен сертификатами с использованием подписанного сообщения, а затем использовать полученные сертификаты для последующего шифрования сообщений между адресатами.

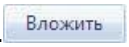
Кодировать сообщения перед подписыванием (непрозрачная подпись). При включенном режиме подпись формируется в виде одного отдельного вложения для сообщения. Если режим выключен - текст сообщения и все вложения объединяются в единое целое и кодируются в соответствии с правилами кодирования BASE64, после чего результат кодирования подписывается.

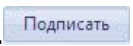
Автоматически добавлять сертификаты отправителей в контакты Windows Live. При включенном режиме сертификаты, передаваемые в составе подписанного сообщения, будут автоматически добавляться в контакты.

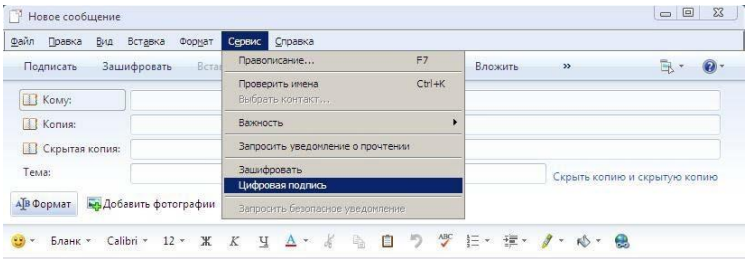


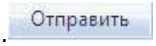
Отправка подписанных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку **Создать.** 

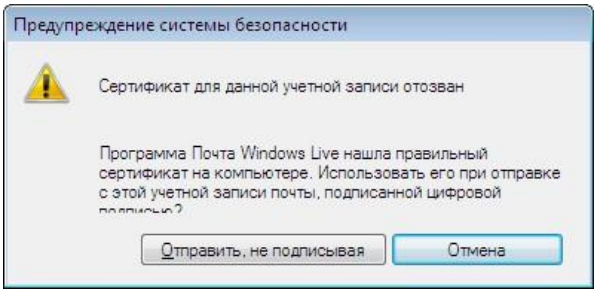
Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить**. 

Для отправки сообщения в подписанном виде нажмите кнопку меню **Сервис**, отметьте **Цифровая подпись.** Или выделите пункт меню **Подписать.** 



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

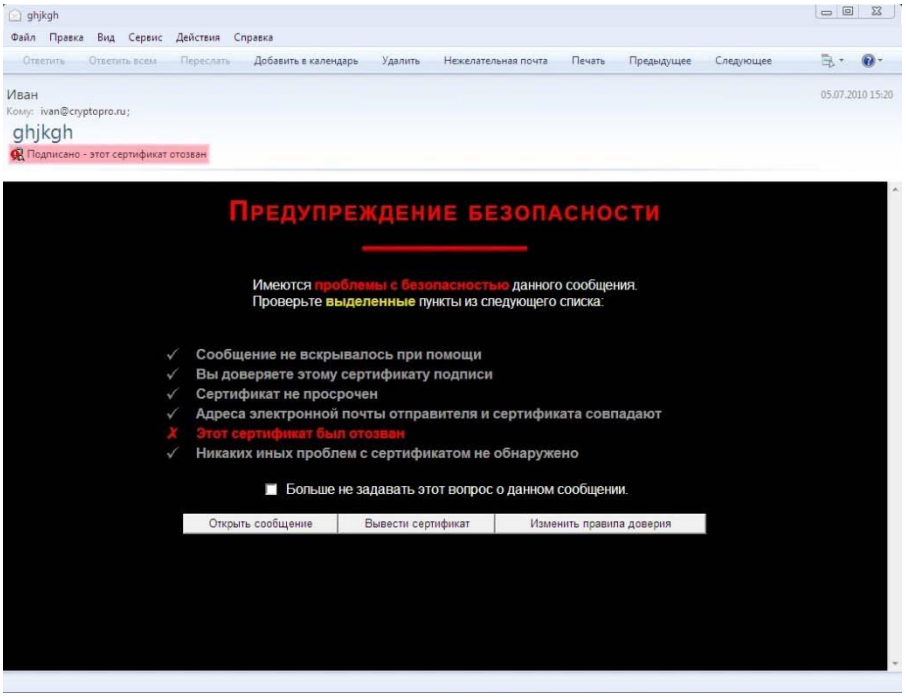
Если сертификат, с помощью которого подписано сообщение, был отозван, то появится следующее предупреждение, а само сообщение не будет отправлено.



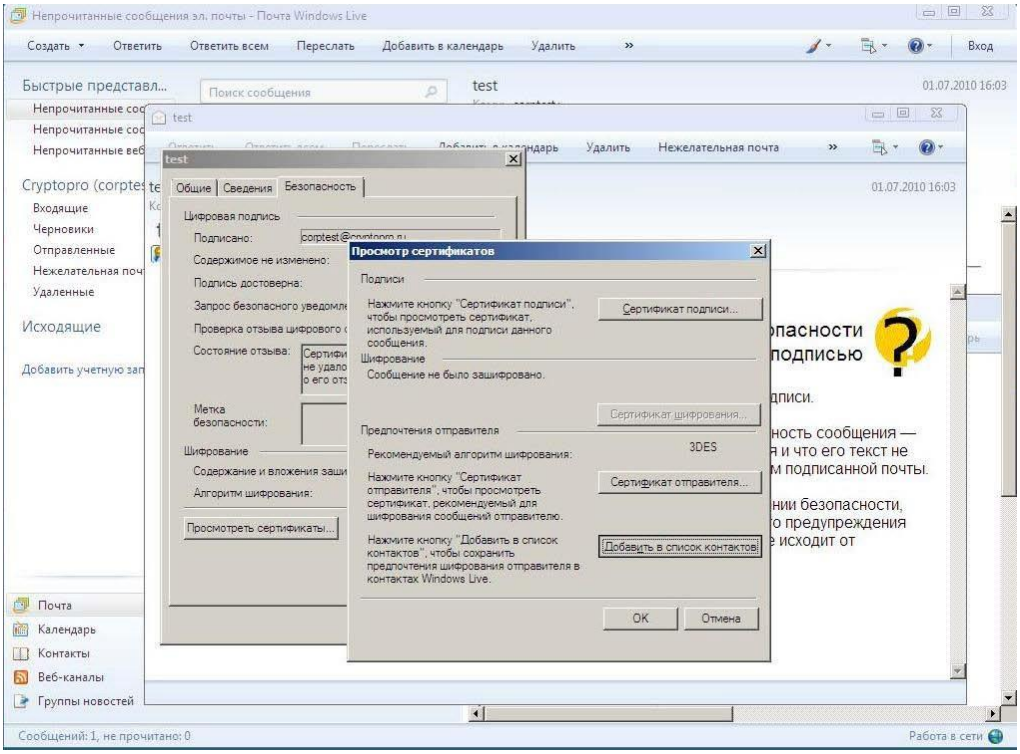
Получение сертификата открытого ключа абонента для шифрования сообщений

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.

Если сертификат, с помощью которого подписано сообщение, был отозван, то появится следующее предупреждение:

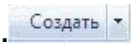


Для контроля добавления выполните следующие действия. Откройте полученное подписанное письмо. Нажмите кнопку - признак подписанного сообщения. Нажмите **Просмотреть сертификаты, Добавить в список контактов.**



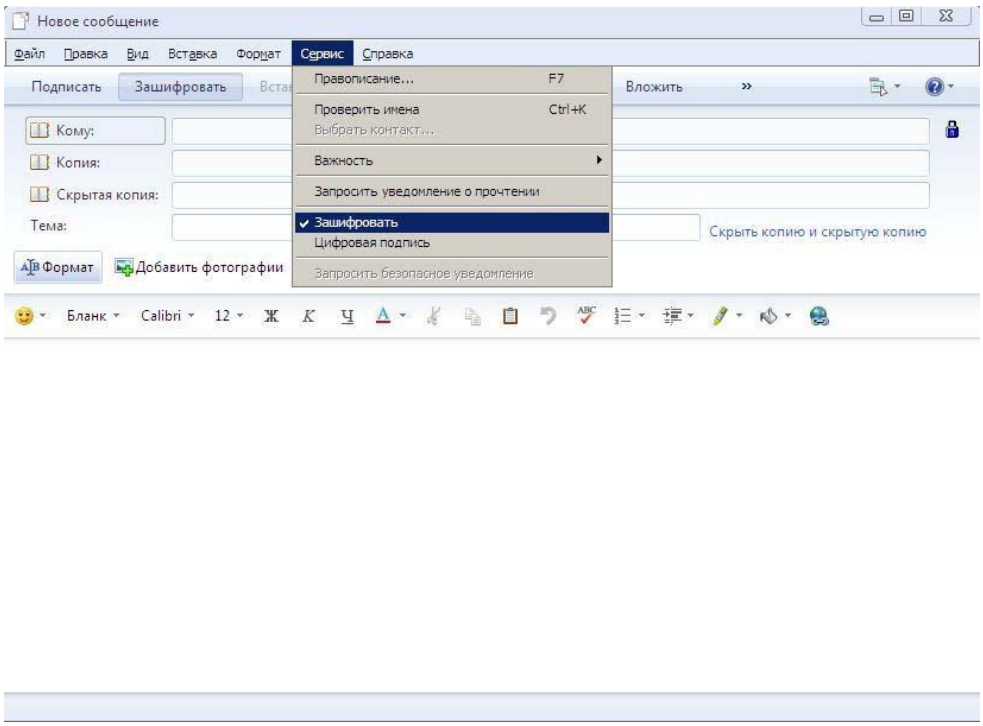
После чего появится сообщение: «Сертификат отправителя был добавлен во все контакты, в которых был встречен его электронный адрес. (Если таких контактов не было, был создан новый)»

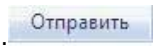
Отправка шифрованных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку **Создать.** 

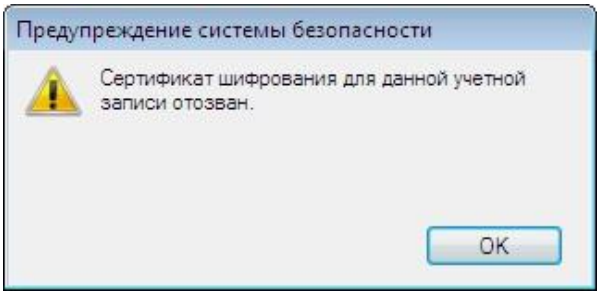
Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить**. 

Для отправки сообщения в зашифрованном виде нажмите кнопку меню **Сервис**, отметьте **Зашифровать.** Или выделите пункт меню **Зашифровать.** 



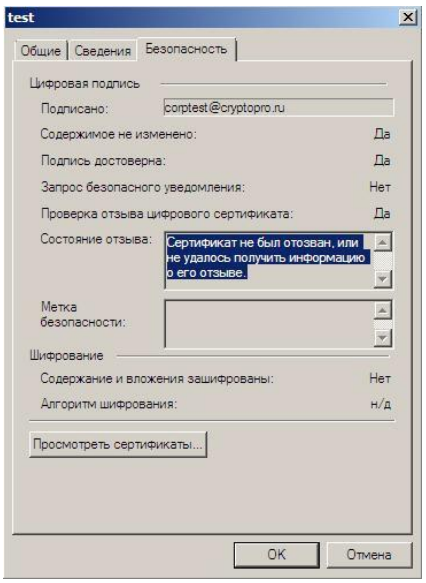
После того, как сообщение подготовлено к отправке, нажмите кнопку **Отправить**. 

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

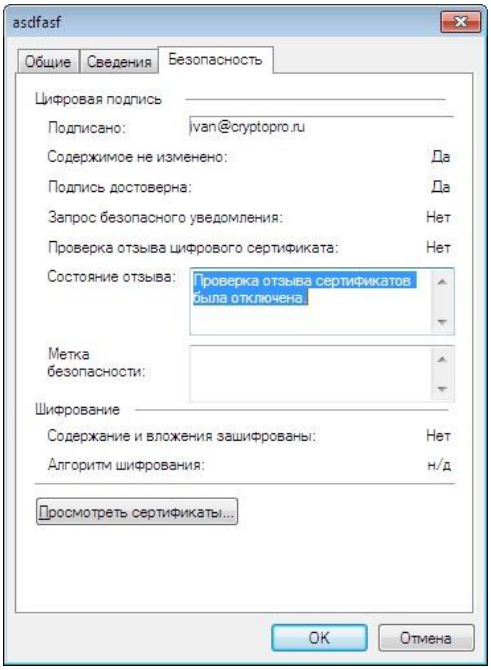


Проверка сертификата на отзыв

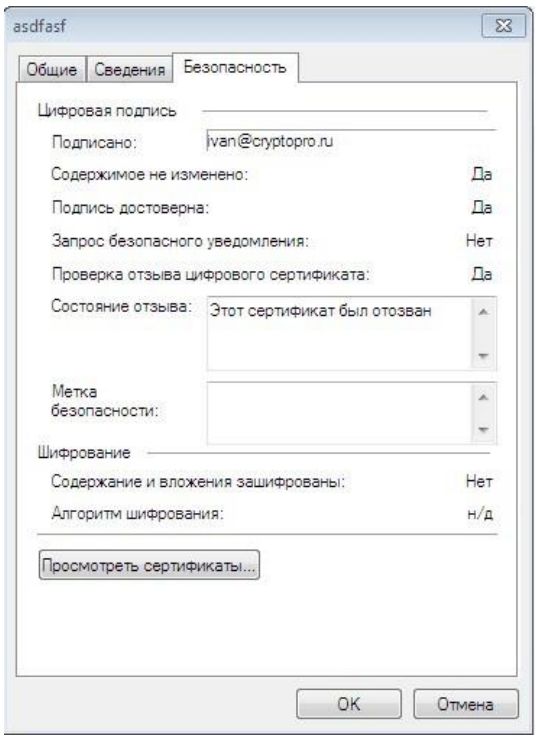
Для контроля проверки сертификатов на отзыв выполните следующие действия. Откройте полученное подписанное письмо. Нажмите кнопку – признак подписанного сообщения. Если открывшееся окно подобно следующему, то СОС не установлен либо срок его действия истек. Обновите СОС, хранящийся в локальном справочнике сертификатов, с использованием доступных средств. Если после обновления СОС окно осталось прежним, то сертификат не был отозван.



Если проверка сертификатов не была включена, то окно будет следующим:



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


asdfasf
Общие
Сведения
Безопасность
Цифровая подпись
Подписано:
ivan@cryptopro.ru
Содержимое не изменено:
Да
Подпись достоверна:
Да
Запрос безопасного уведомления:
Нет
Проверка отзыва цифрового сертификата:
Да
Состояние отзыва:
Этот сертификат был отозван
Метка безопасности:
Шифрование
Содержание и вложения зашифрованы:
Нет
Алгоритм шифрования:
н/д
Просмотреть сертификаты...
OK
Отмена

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**.

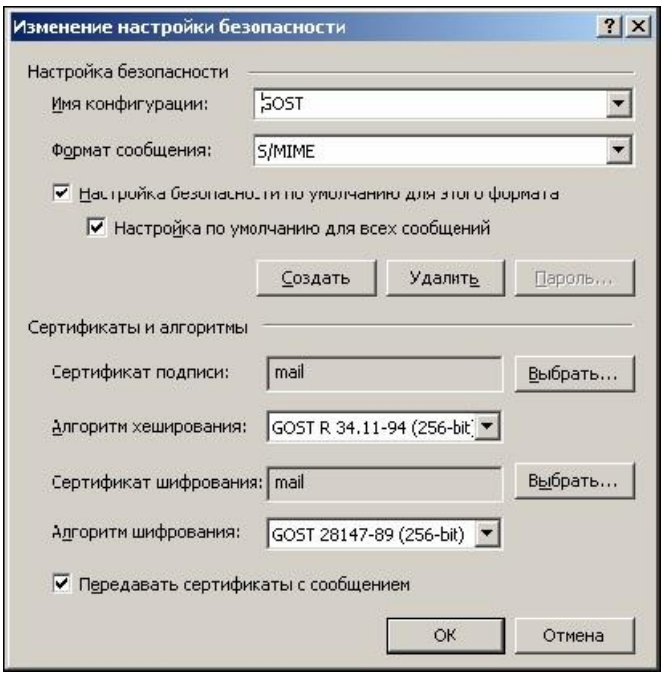
3. Криптопровайдер КриптоПро CSP поддерживает только формат S/MIME защищенных почтовых сообщений, и поэтому в настройках сервера Exchange должна стоять опция использования формата MIME и разрешения маршрутизации защищенных сообщений S/MIME.

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**.

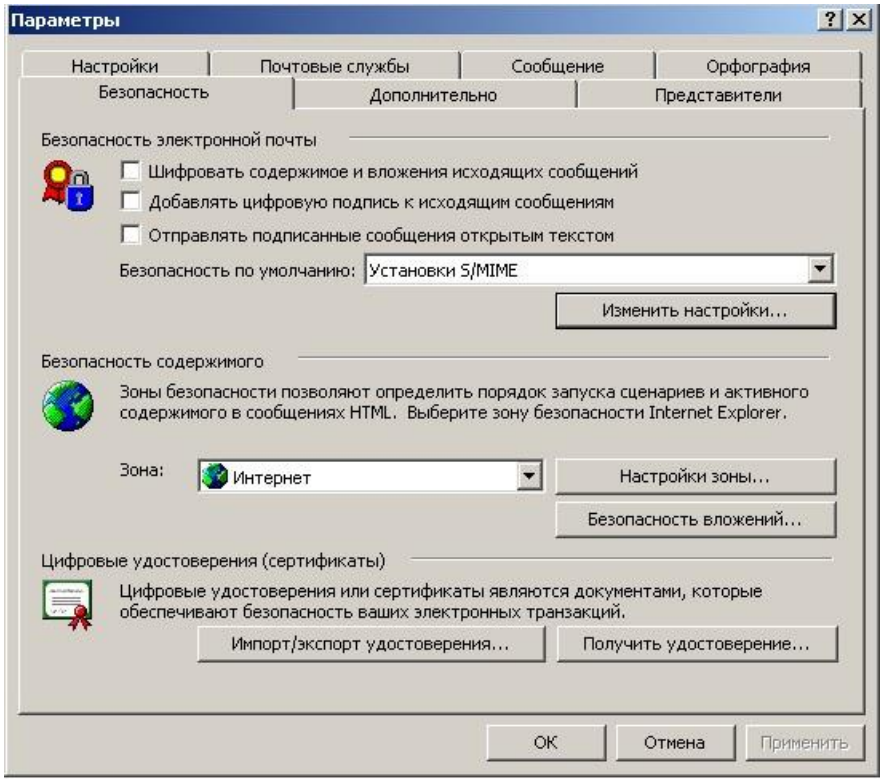
Конфигурация Outlook 2000

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**.



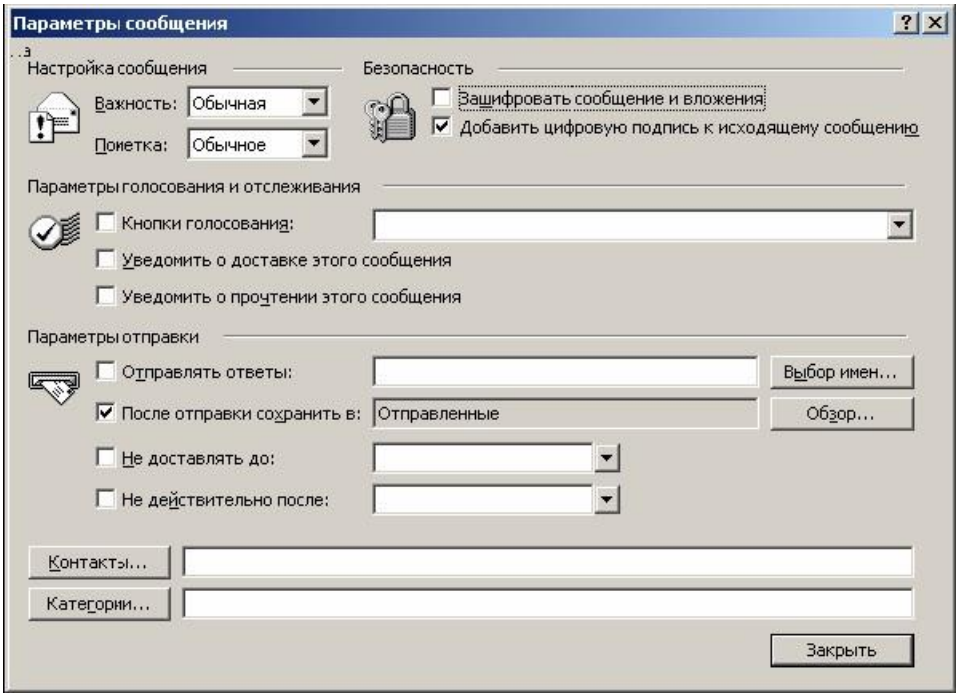
В отображаемом диалоге можно включить режимы **Шифровать содержимое и вложения исходящих сообщений** и **Добавлять цифровую подпись к исходящим сообщениям** для того, чтобы шифрование и электронная цифровая подпись выполнялись автоматически для каждого сообщения. Если эти режимы не включены, опции шифрования 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 сообщения. Если режим выключен - текст сообщения и все вложения объединяются в единое целое и кодируются в соответствии с правилами кодирования BASE64, после чего результат кодирования подписывается.

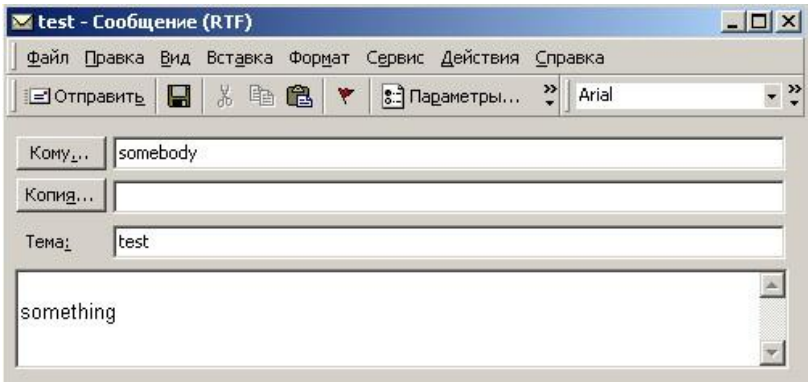
Отправка подписанных сообщений

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

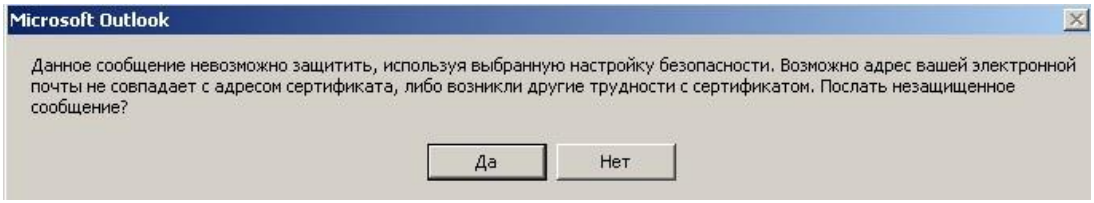
Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить**. Для отправки сообщения в подписанном виде нажмите кнопку и в отображаемом диалоге установите флаг **Добавить цифровую подпись к исходящему сообщению**.



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



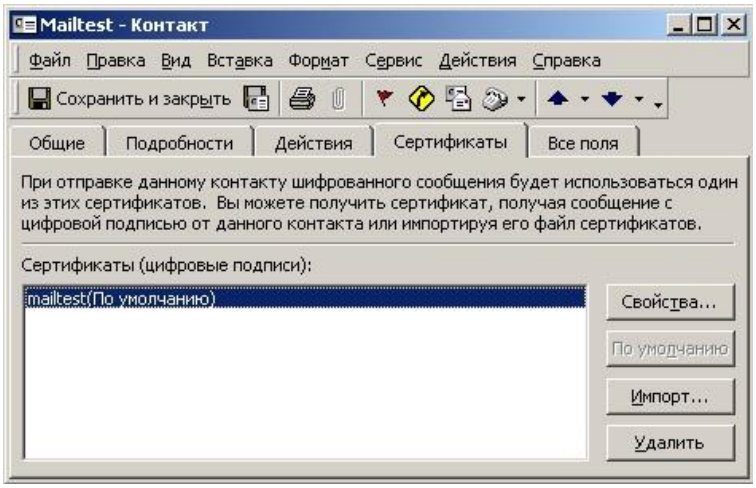
Если сертификат, с помощью которого подписываете сообщение, был отозван, то в ответ появится следующее предупреждение:



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

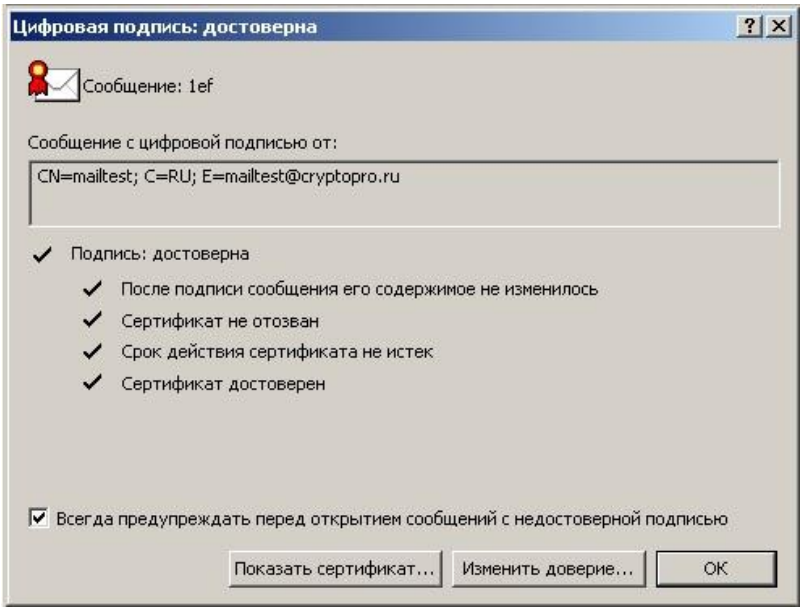
Для создания и отправки шифрованного сообщения нажмите кнопку **Создать** или выберите пункт меню **Файл, Создать, Сообщение**.

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 **Параметры** и в отображаемом диалоге установите флаг **Зашифровать сообщение и вложение**. После того, как сообщение подготовлено к отправке, нажмите кнопку **Отправить**.

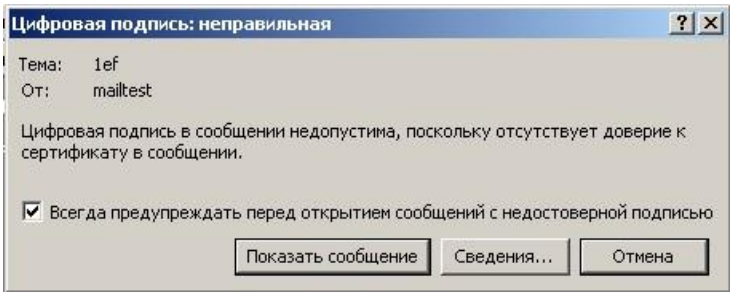
При попытке зашифровать письмо на открытом ключе владельца отозванного сертификата возникнет та же ситуация, что и при отправке сообщения, подписанного с помощью отозванного сертификата.

Проверка сертификата на отзыв

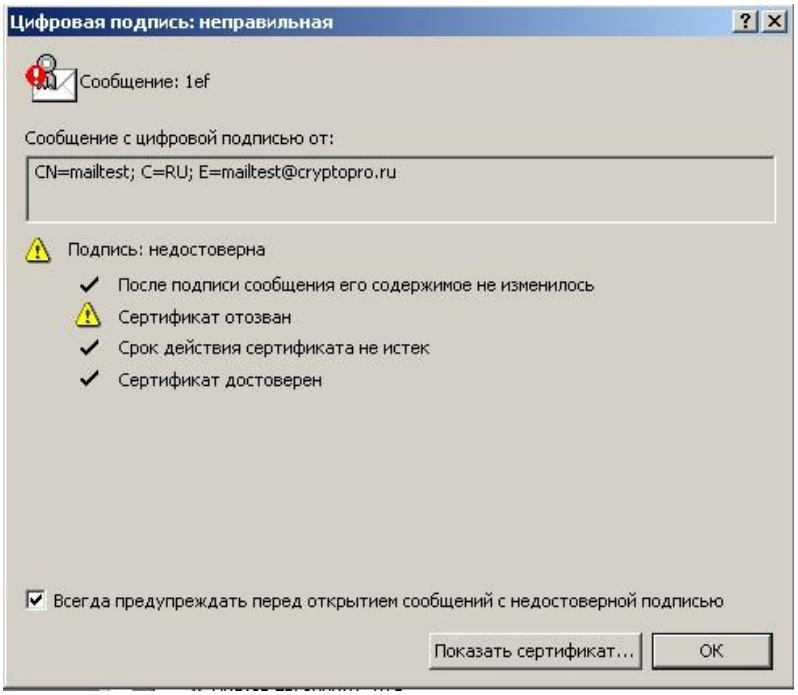
Для контроля проверки сертификатов на отзыв выполните следующие действия. Откройте полученное подписанное письмо. Нажмите кнопку  – признак подписанного сообщения. Если сертификат действительный и не был отозван, то откроется окно, подобное этому:



При открытии письма, подписанного отозванным сертификатом, появится следующее предупреждение:



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



ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В OUTLOOK 2002/2003

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

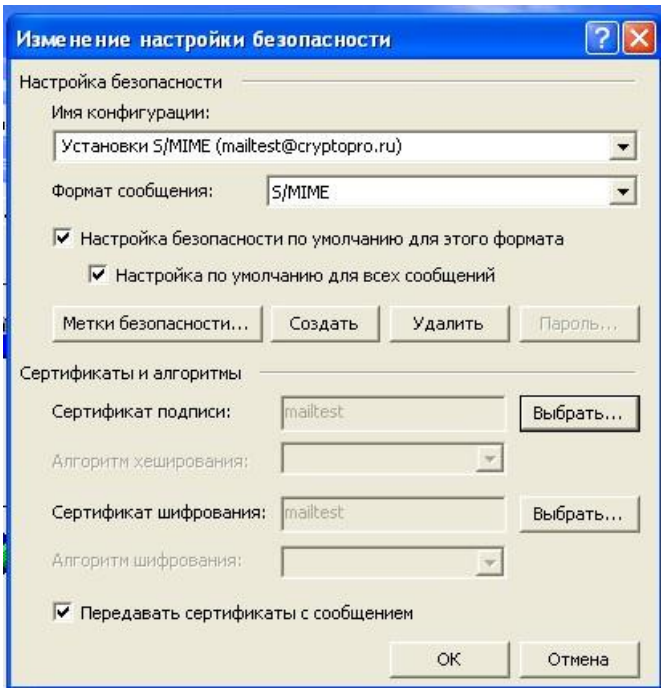
1. Криптопровайдер КриптоПро CSP поддерживает только формат S/MIME защищенных почтовых сообщений, и поэтому в настройках сервера Exchange должна стоять опция использования формата MIME и разрешения маршрутизации защищенных сообщений S/MIME.

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**.

Конфигурация Outlook 2002/2003

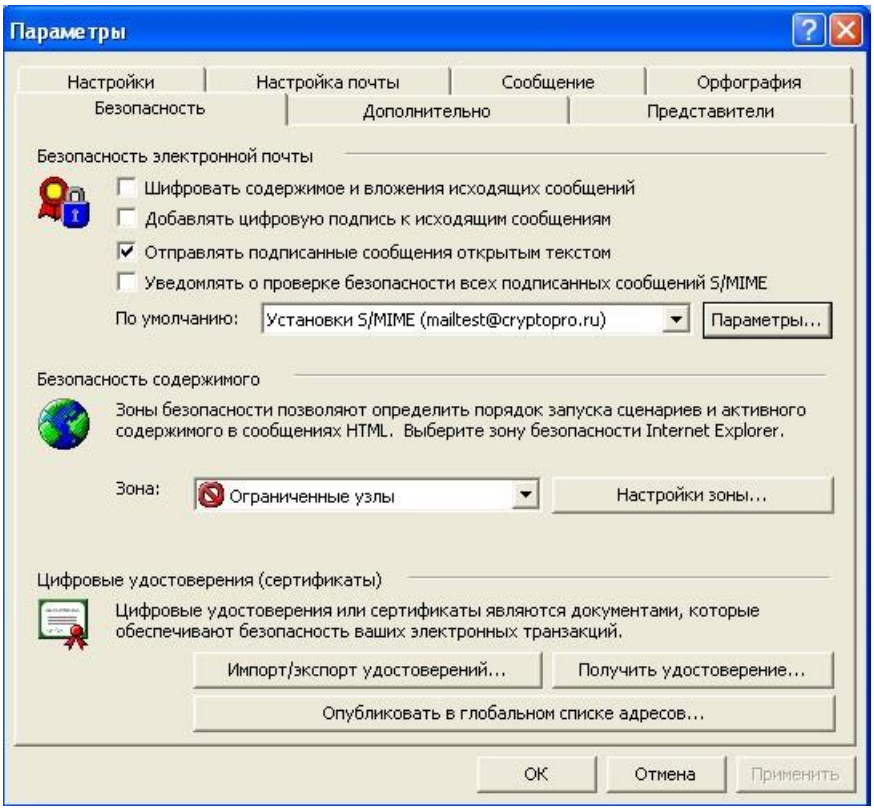
Выберите пункт меню **Сервис**, **Параметры…** и нажмите на закладку **Безопасность**. Нажмите кнопку **Параметры**.



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.

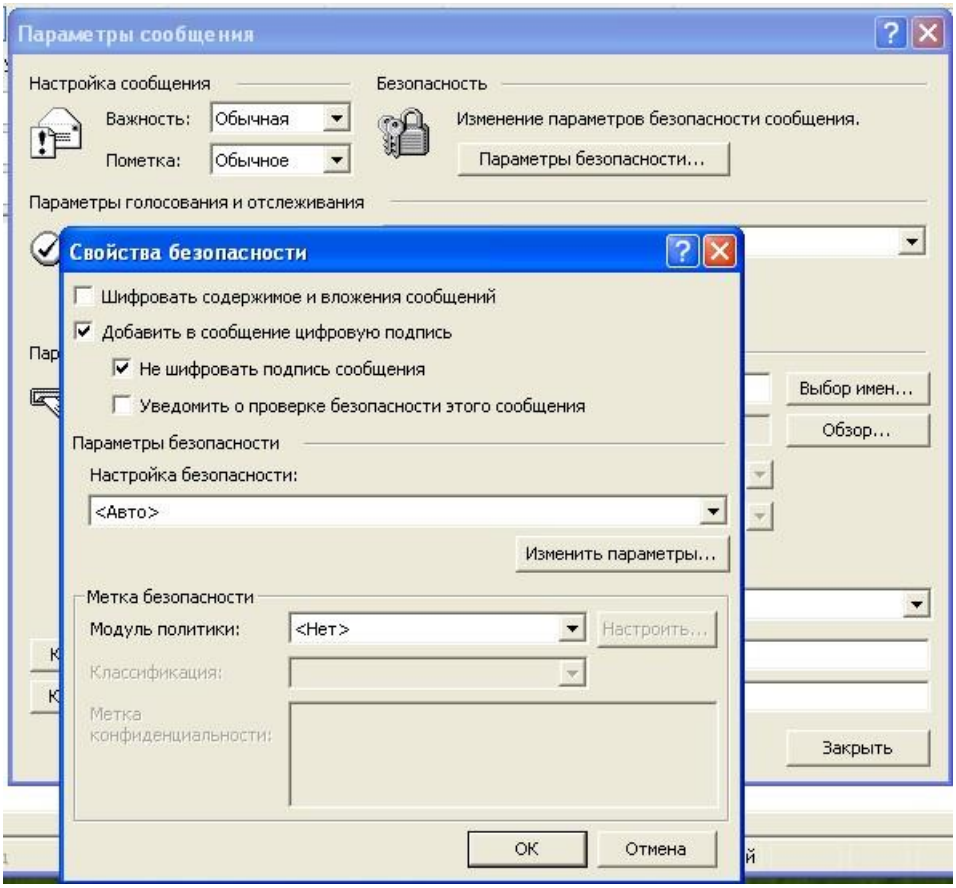


В этом же диалоге дополнительно можно установить опцию **Отправлять подписанные сообщения открытым текстом**. При включенном режиме подпись формируется в виде одного отдельного вложения для сообщения. Если режим выключен - текст сообщения и все вложения объединяются в единое целое и кодируются в соответствии с правилами кодирования BASE64, после чего результат кодирования подписывается.

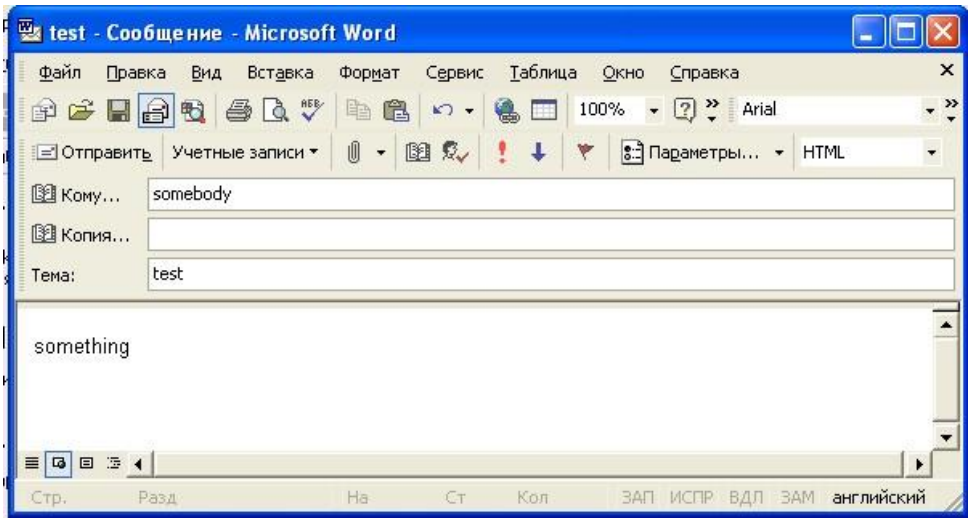
Отправка подписанных сообщений

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

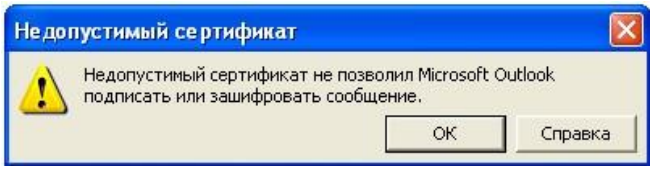
Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить**. Для отправки сообщения в подписанном виде нажмите кнопку **Параметры…**, затем кнопку **Параметры безопасности,** и в отображаемом диалоге установите флаг **Добавить в сообщение цифровую подпись**.



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



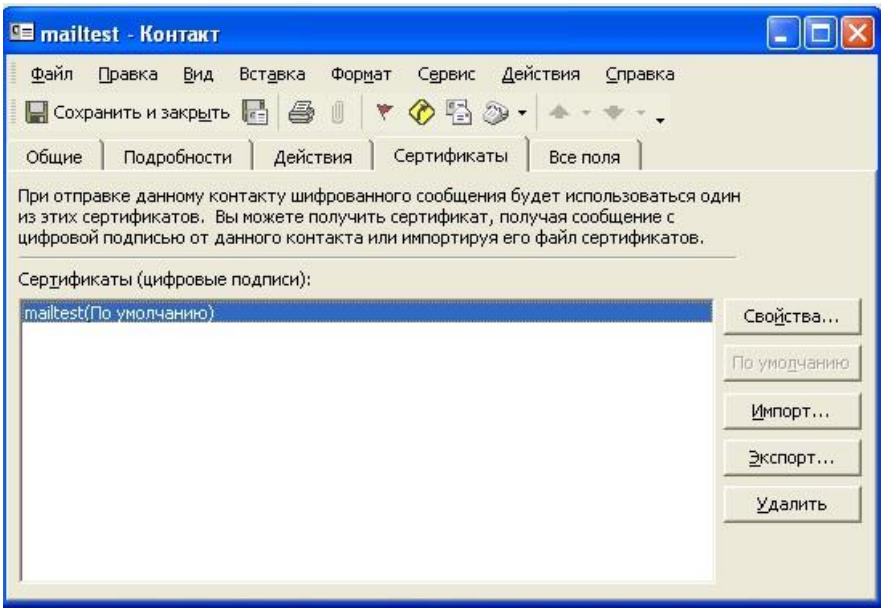
Если сертификат, с помощью которого подписано сообщение, был отозван, то появится следующее предупреждение, а само сообщение не будет отправлено.



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

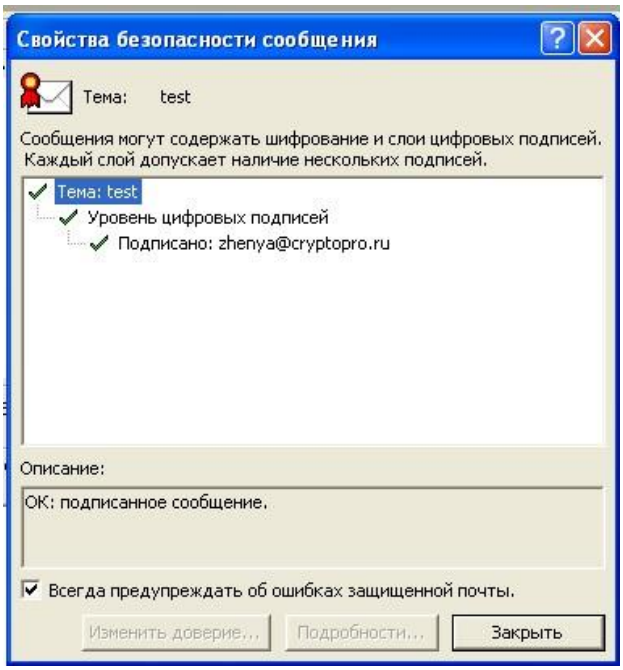
Для создания и отправки шифрованного сообщения нажмите кнопку **Создать** или выберите пункт меню **Файл, Создать, Сообщение**.

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 **Параметры…**, затем кнопку **Параметры безопасности,** и в отображаемом диалоге установите флаг Ш**ифровать содержимое и вложения сообщений**. После того, как сообщение подготовлено к отправке, нажмите кнопку **Отправить**. При

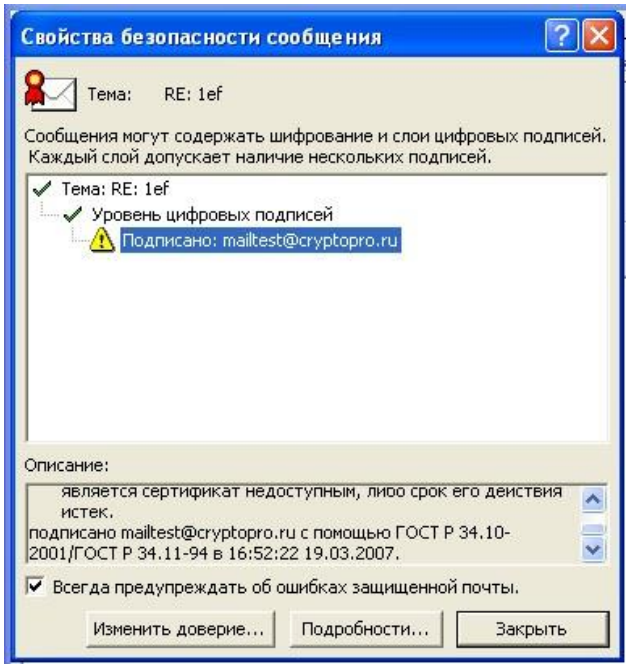
попытке зашифровать письмо на открытом ключе владельца отозванного сертификата возникнет та же ситуация, что и при отправке сообщения, подписанного с помощью отозванного сертификата.

Проверка сертификата на отзыв

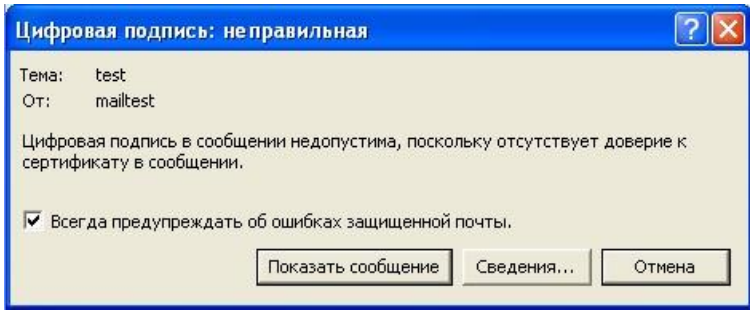
Для контроля проверки сертификатов на отзыв выполните следующие действия. Откройте полученное подписанное письмо. Нажмите кнопку  – признак подписанного сообщения. Если сертификат действительный и не был отозван, то откроется окно, подобное этому:



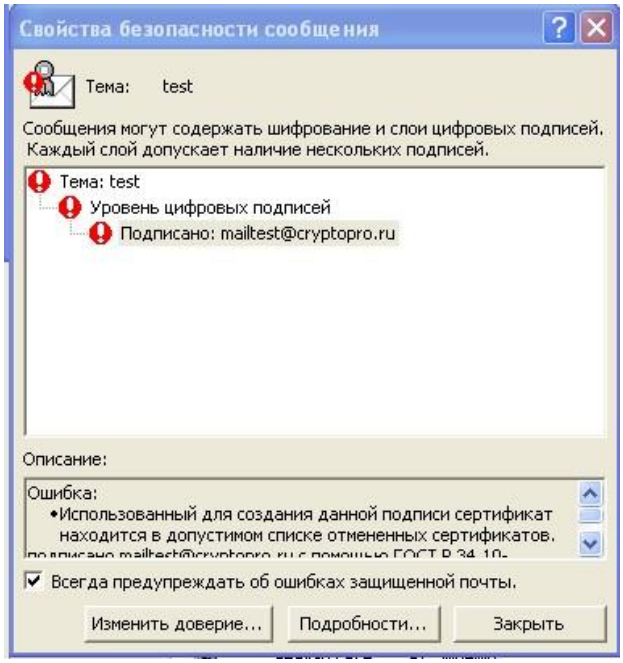
Следующее предупреждение означает, что СОС не установлен либо срок его действия истек. Обновите СОС, хранящийся в локальном справочнике сертификатов с использованием доступных средств.



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



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



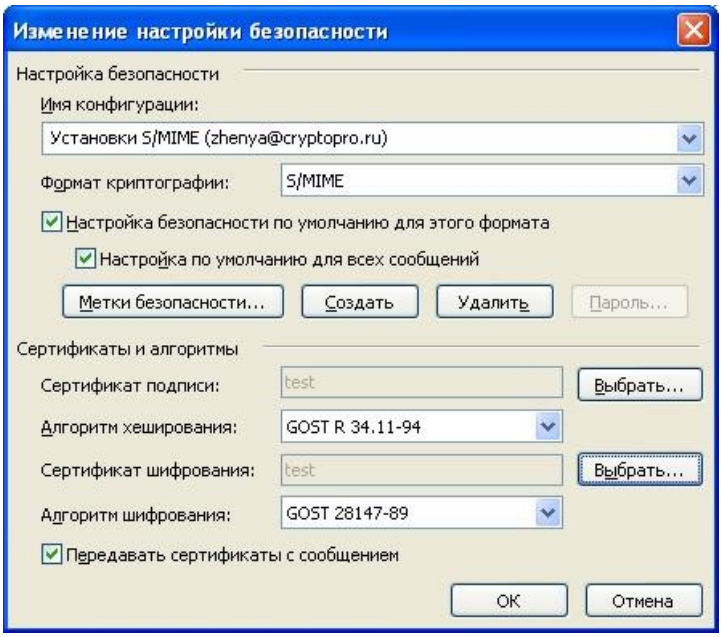
ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В OUTLOOK 2007

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 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**.

Конфигурация Outlook 2007

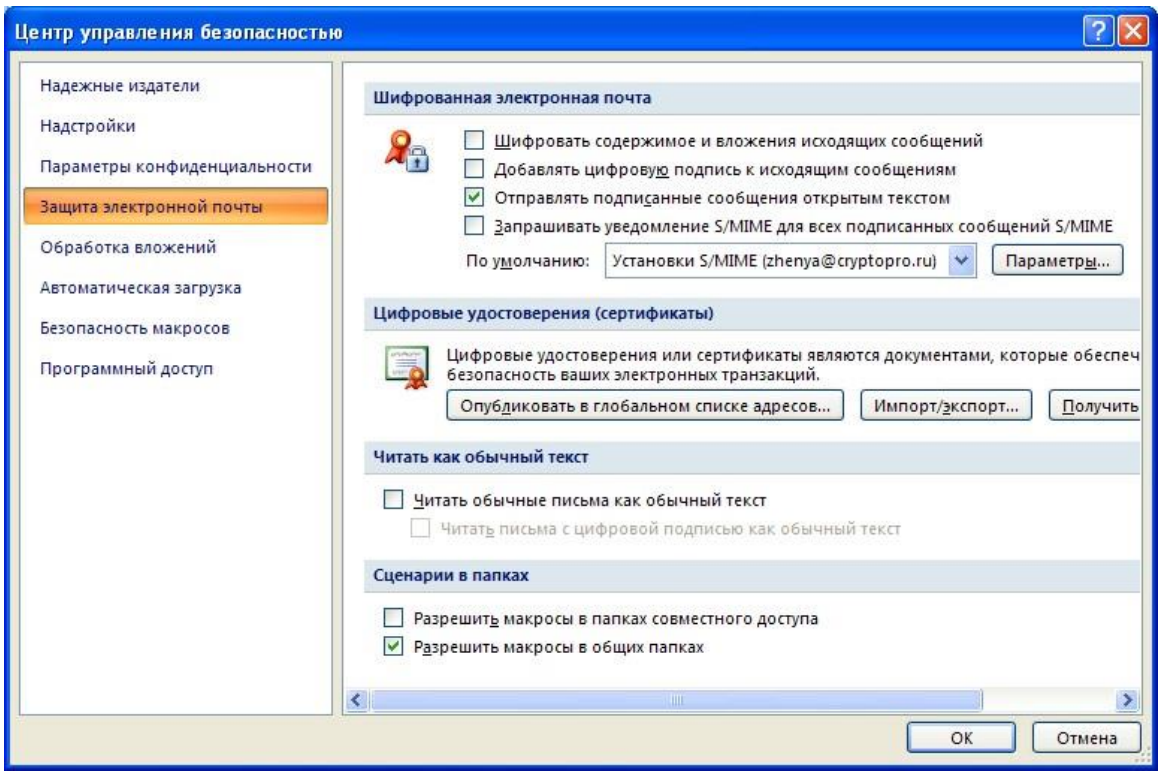
Выберите пункт меню **Сервис, Центр управления безопасностью** и нажмите на закладку **Защита электронной почты**. Нажмите кнопку **Параметры**.



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 сообщения. Если режим выключен - текст сообщения и все вложения объединяются в единое целое и кодируются в соответствии с правилами кодирования BASE64, после чего результат кодирования подписывается.

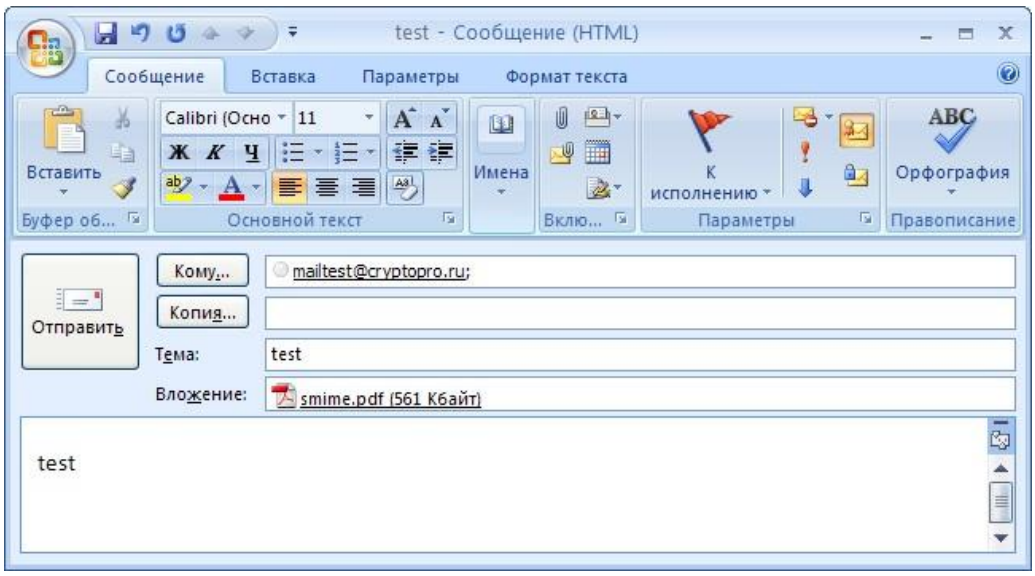
Отправка подписанных сообщений

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

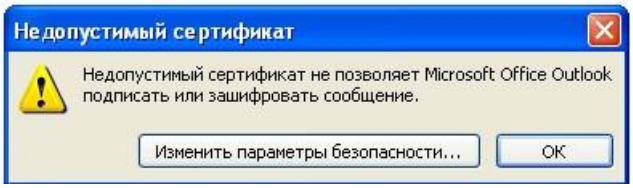
Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить файл**.

Для отправки сообщения в подписанном виде нажмите кнопку  .

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.

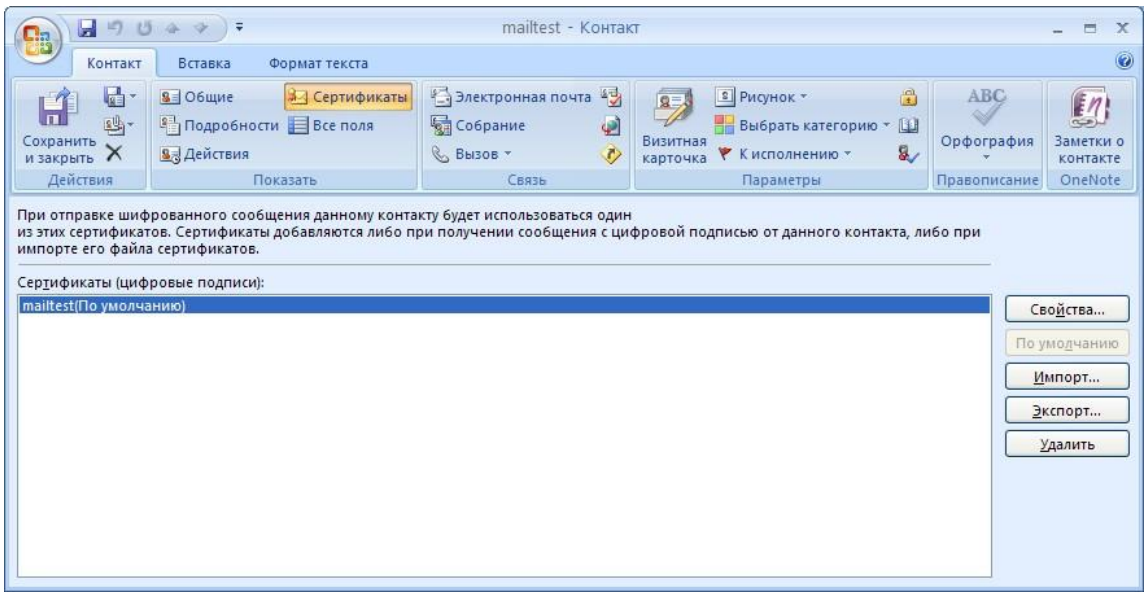


Получение сертификата открытого ключа абонента для шифрования сообщений

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.



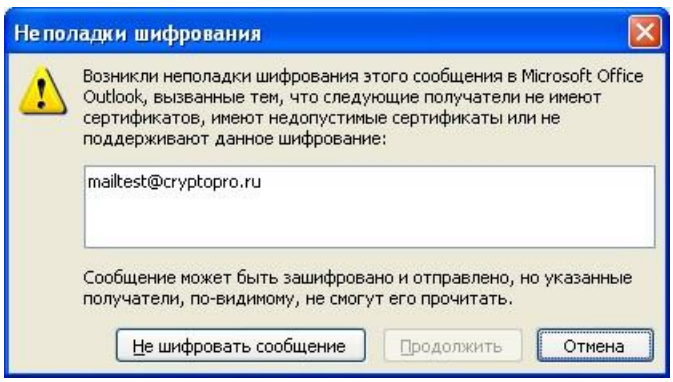
После этого нажмите кнопку Сохранить и закрыть. Если абонент с таким адресом уже существует, программа предложит, либо **добавить новый контакт**, либо **обновить сведения о выделенном контакте**. Выберите второй пункт. При этом в существующий контакт будет добавлен полученный сертификат. Если контакт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

Отправка шифрованных сообщений

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

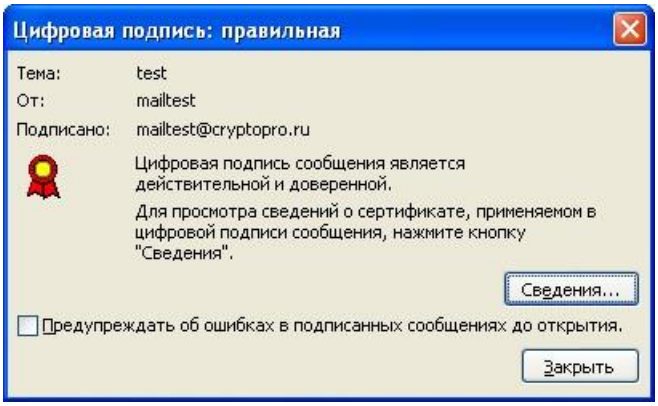
Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить файл**. Для отправки сообщения в зашифрованном виде нажмите кнопку  . После того, как сообщение подготовлено к отправке, нажмите кнопку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

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

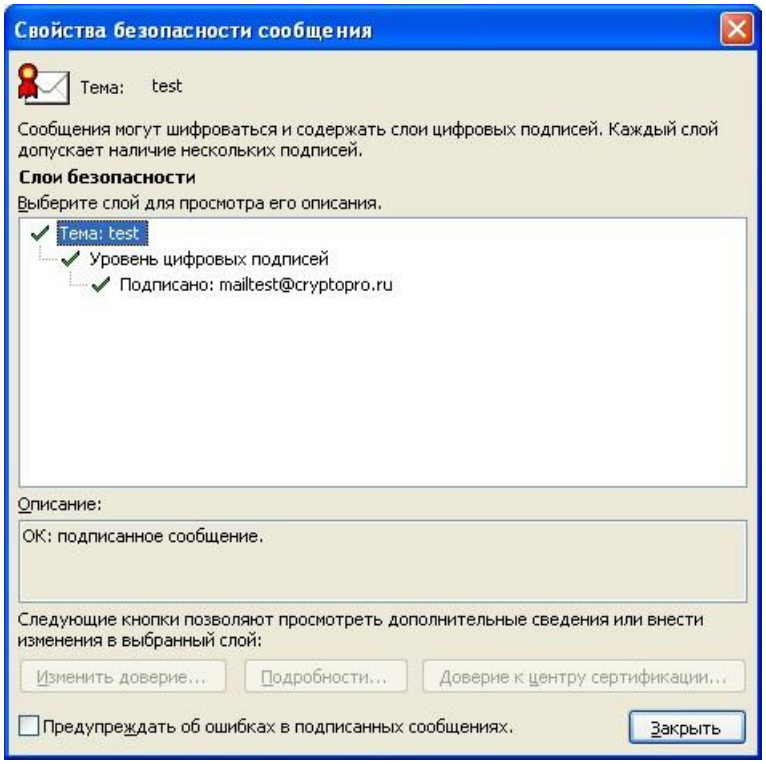


Проверка сертификата на отзыв

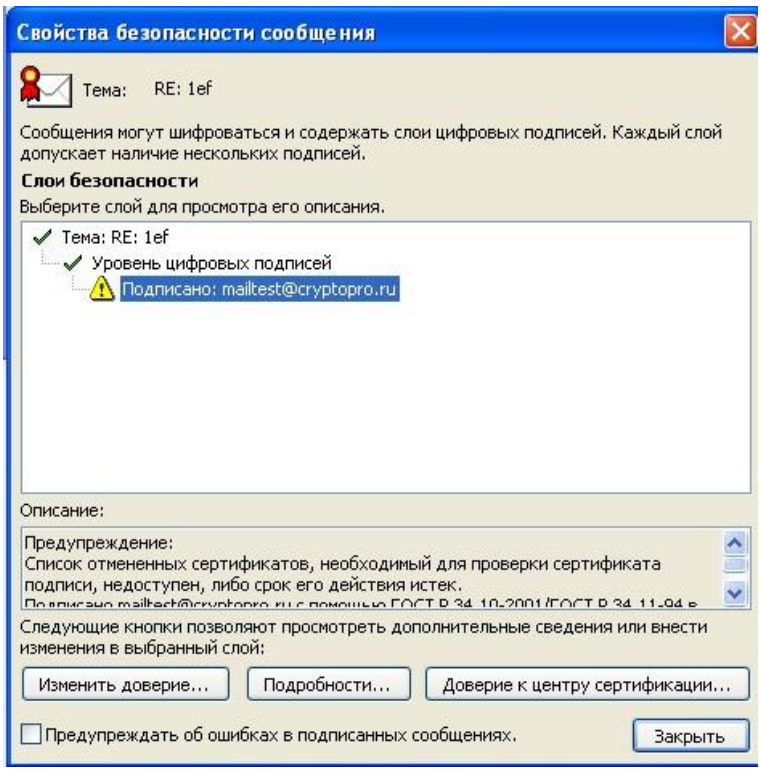
Для контроля проверки сертификатов на отзыв выполните следующие действия. Откройте полученное подписанное письмо. Нажмите кнопку  - признак подписанного сообщения.



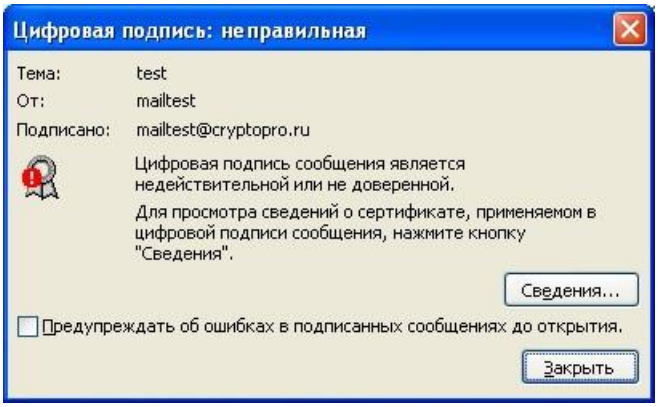
Нажмите кнопку **Сведения**. Если сертификат действительный и не был отозван, то откроется окно, подобное этому:



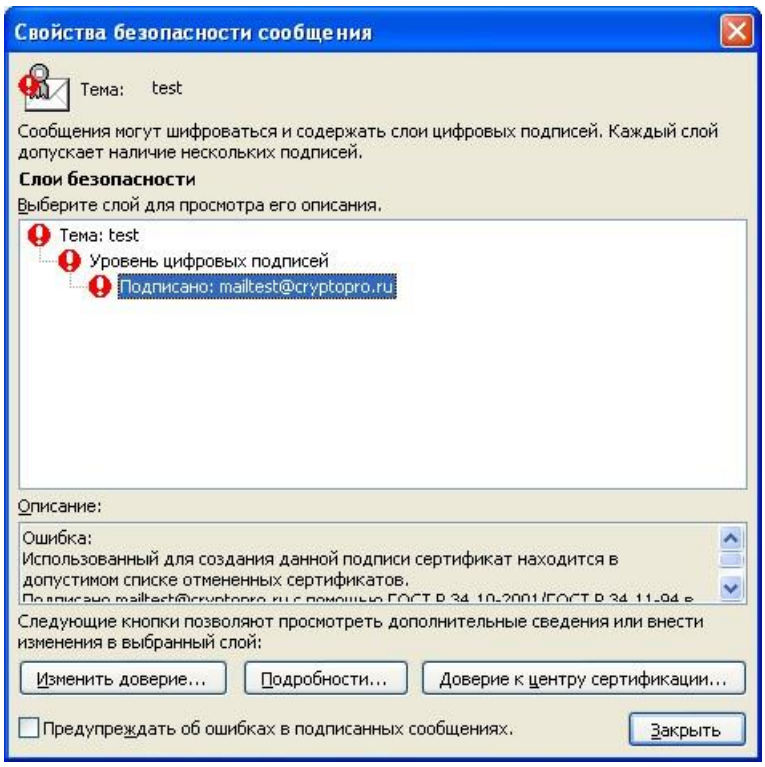
А если открывшееся окно подобно следующему, то СОС не установлен либо срок его действия истек. Обновите СОС, хранящийся в локальном справочнике сертификатов с использованием доступных средств.



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



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

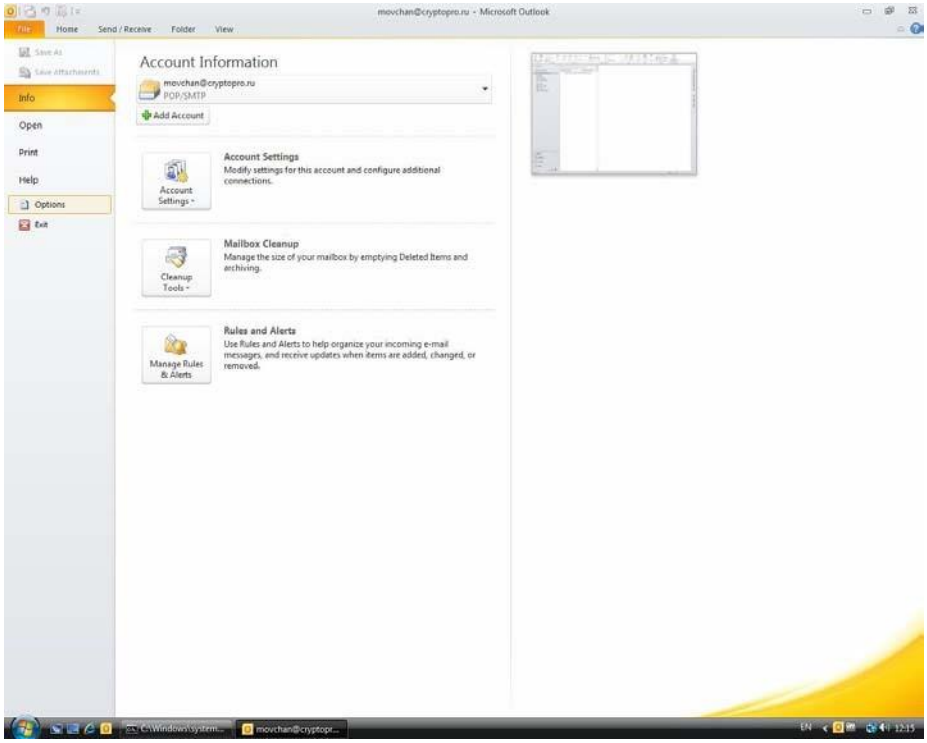

Свойства безопасности сообщения
Тема: test
Сообщения могут шифроваться и содержать слои цифровых подписей. Каждый слой допускает наличие нескольких подписей.
Слои безопасности
Выберите слой для просмотра его описания.
Тема: test
Уровень цифровых подписей
Подписано: mailtest@cryptopro.ru
Описание:
Ошибка:
Использованный для создания данной подписи сертификат находится в допустимом списке отмененных сертификатов.
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

ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В OUTLOOK 2010

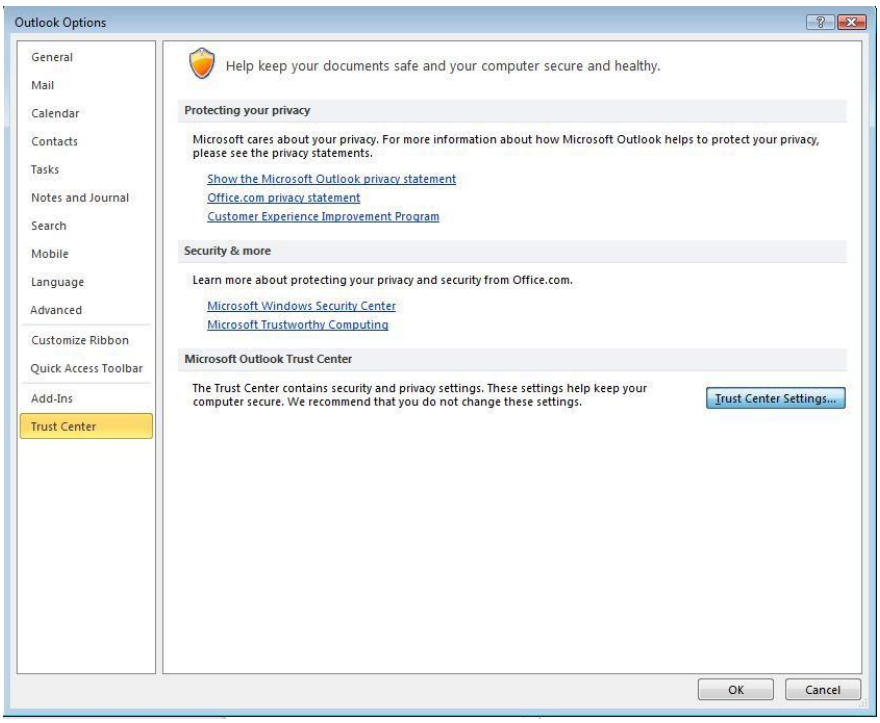
Использование средств криптографической защиты в Outlook 2010 во многом совпадает с использованием в Outlook ранних версий.

Конфигурация Outlook 2010

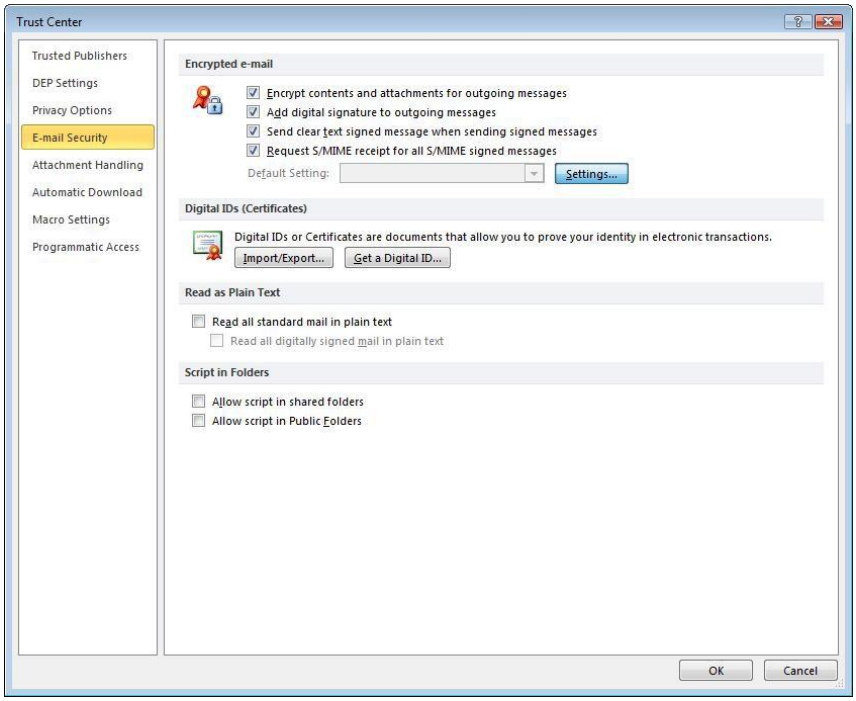
Выберите пункт **Options** (**Параметры**) меню **File** (**Файл**).



В открывшемся окне выберите в закладке **Trust Center** (**Центр управления безопасностью**) пункт **Trust Center Settings** (**Параметры Центра управления безопасностью**).



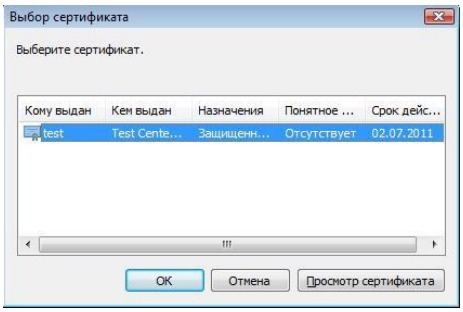
Выберите закладку **E-mail Security** (**Защита электронной почты**).



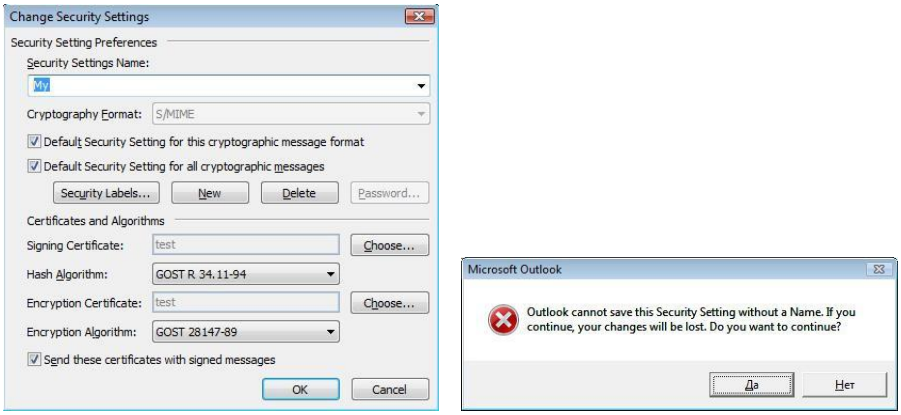
Нажмите **Settings** (**Параметры**).

Выберите личные сертификаты, соответствующие ключам подписи и шифрования, используя кнопку **Choose** (**Выбрать**). 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. Установите флаг **Send these certificates with signed messages** (**Передавать сертификаты с сообщением**).

Окно выбора сертификата:



После выбора сертификата необходимо ввести **Security Settings Name** (**Название параметров безопасности**). В противном случае Outlook выдаст ошибку:



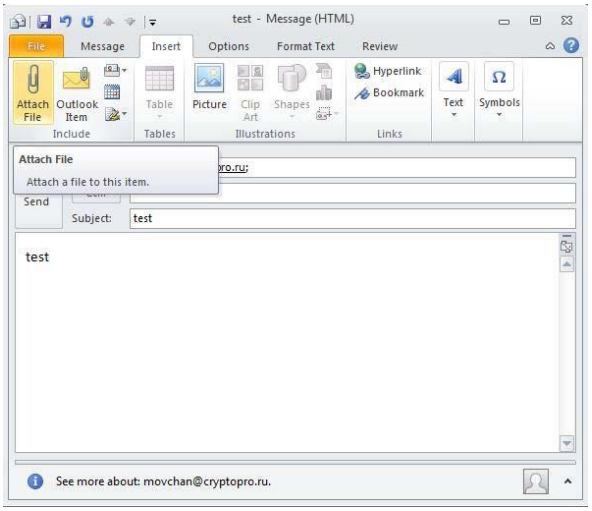
В закладке **E-mail Security** (**Защита электронной почты**) можно включить режимы **Encrypt contents and attachments for outgoing messages** (**Шифровать содержимое и вложения исходящих сообщений**) и **Add digital signature to outgoing messages** (**Добавлять цифровую подпись к исходящим сообщениям**) 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 **Send clear text signed message when sending**

signed messages (**Отправлять подписанные сообщения открытым текстом**). При включенном режиме подпись формируется в виде одного отдельного вложения для сообщения. Если режим выключен - текст сообщения и все вложения объединяются в единое целое и кодируются в соответствии с правилами кодирования BASE64, после чего результат кодирования подписывается.

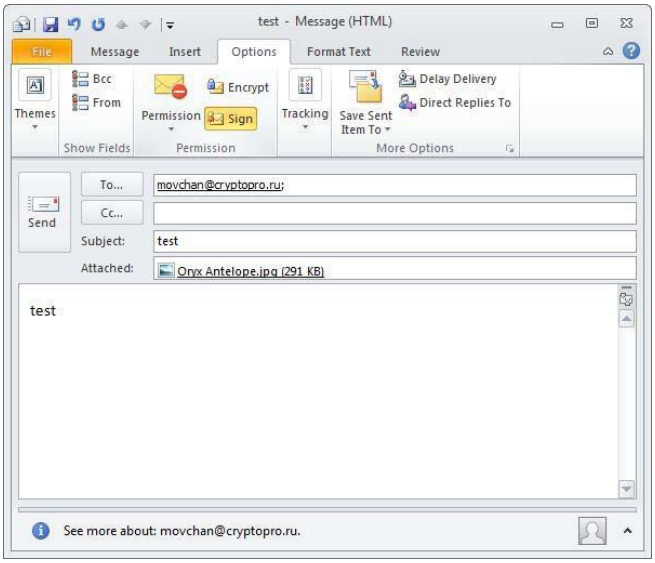
Отправка подписанных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку **New E-mail** (**Создать**).

Выберите получателя сообщения (поле **To**) и введите тему сообщения (**Subject**). Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Attach File** (**Вложить файл**) в закладке **Insert** (**Вставка**).



Для того, чтобы подписать сообщение нажмите на кнопку **Sign** (**Подписать**) в закладке **Options** (**Параметры**).



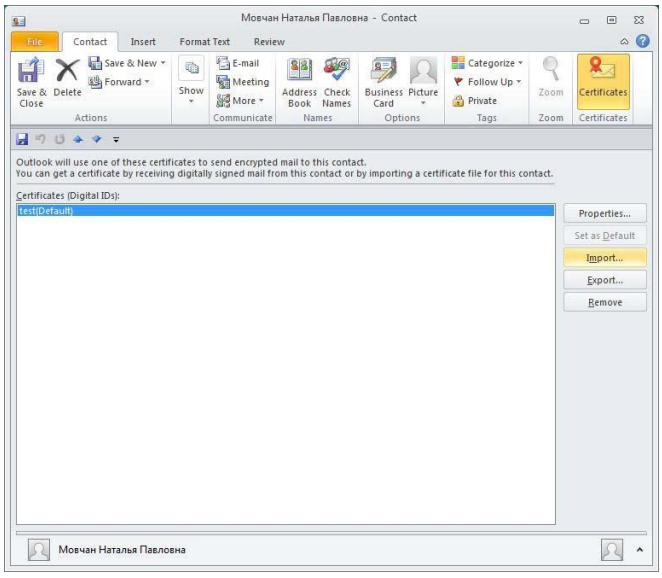
Для отправки сообщения в нажмите кнопку **Send** (**Отправить**).

Если сертификат, с помощью которого подписано сообщение, был отозван или электронный адрес, указанный в сертификате не совпадает с электронным адресом данной учетной записи, 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 **Add to Outlook Contacts** (**Добавить в контакты Outlook**). В отображаемом диалоге нажмите на закладку **Certificates**  (**Сертификаты**) и убедитесь в наличии сертификата отправителя.



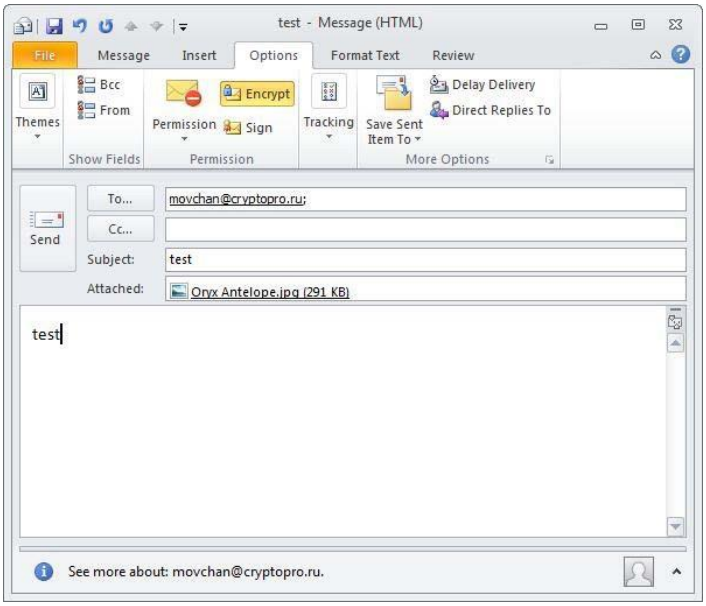
После этого нажмите на кнопку **Save & Close** (**Сохранить и Закрыть**). Если абонент с таким адресом уже существует, программа предложит, либо добавить новый контакт (**Add new Contact**), либо обновить сведения о выделенном контакте (**Update information of selected Contact**). Выберите

второй пункт. При этом в существующий контакт будет добавлен полученный сертификат, а резервная копия будет сохранена в **Deleted Items Folder** (**Удаленные**).

Отправка шифрованных сообщений

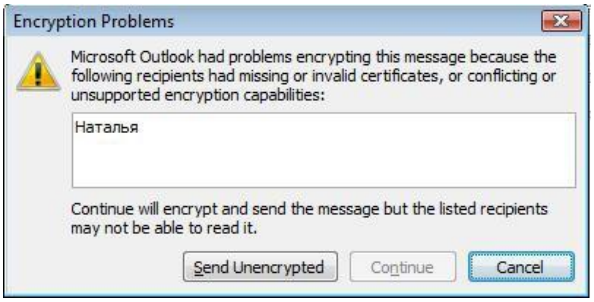
Для создания и отправки шифрованного сообщения нажмите кнопку **New E-mail** (**Создать**).

Выберите получателя сообщения (поле **To**) и введите тему сообщения (**Subject**). Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Attach File** (**Вложить файл**) в закладке **Insert** (**Вставка**). Для отправки сообщения в зашифрованном виде нажмите кнопку **Encrypt** (**Шифровать**).



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

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

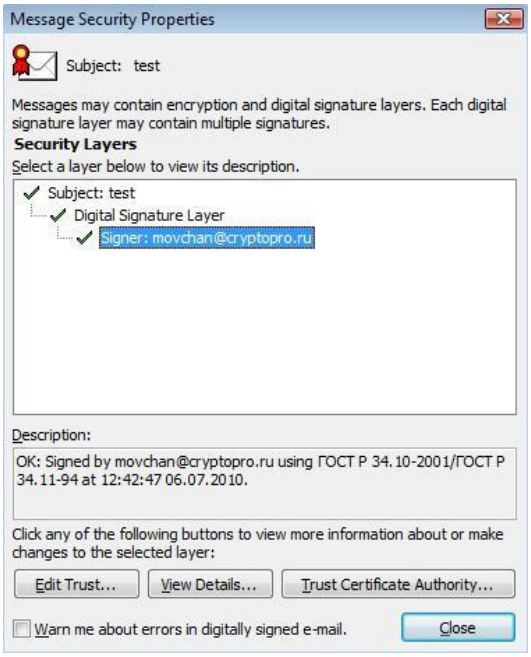


Проверка сертификата на отзыв

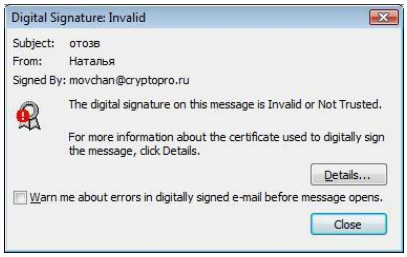
Для контроля проверки сертификатов на отзыв выполните следующие действия. Откройте полученное подписанное письмо. Нажмите кнопку  – признак подписанного сообщения.

Нажмите кнопку **Details** (**Сведения**).

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 окно осталось прежним, то сертификат не был отозван.



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



Нажмите кнопку **Details** (**Сведения**) для просмотра сведений о сертификате.

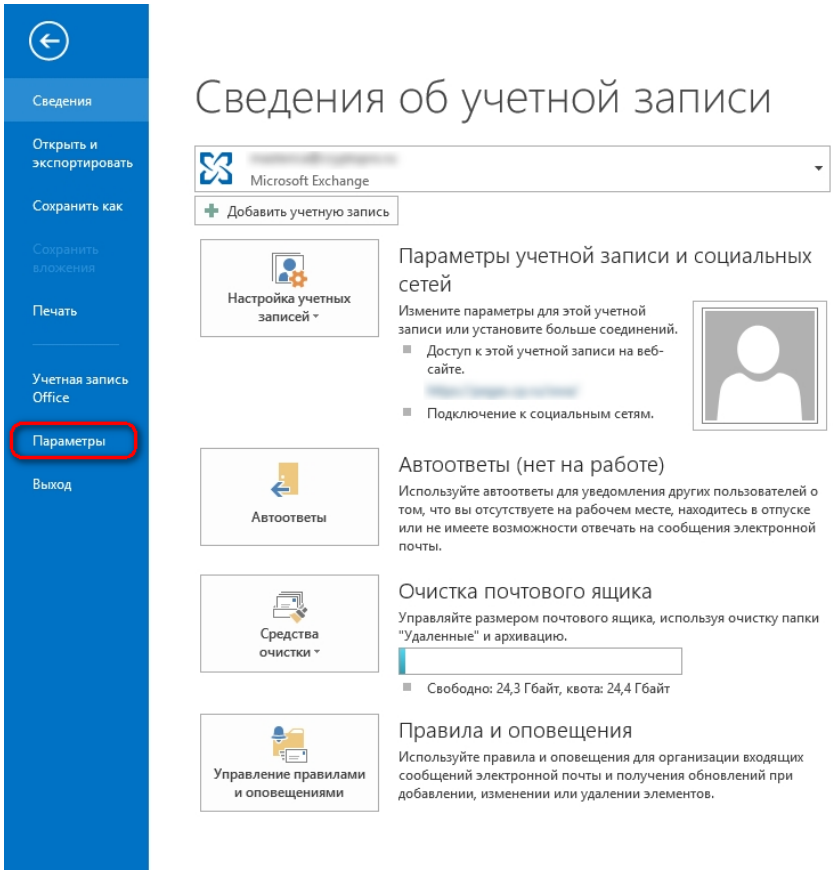

Message Security Properties
Subject: отозв
Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.
Security Layers
Select a layer below to view its description.
Subject: отозв
Digital Signature Layer
Signer: movchan@cryptopro.ru
Description:
Error:
The certificate used to create this signature is on a valid Certificate Revocation List.
Click any of the following buttons to view more information about or make changes to the selected layer:
Edit Trust...
View Details...
Trust Certificate Authority...
Warn me about errors in digitally signed e-mail.
Close

ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В OUTLOOK 2013

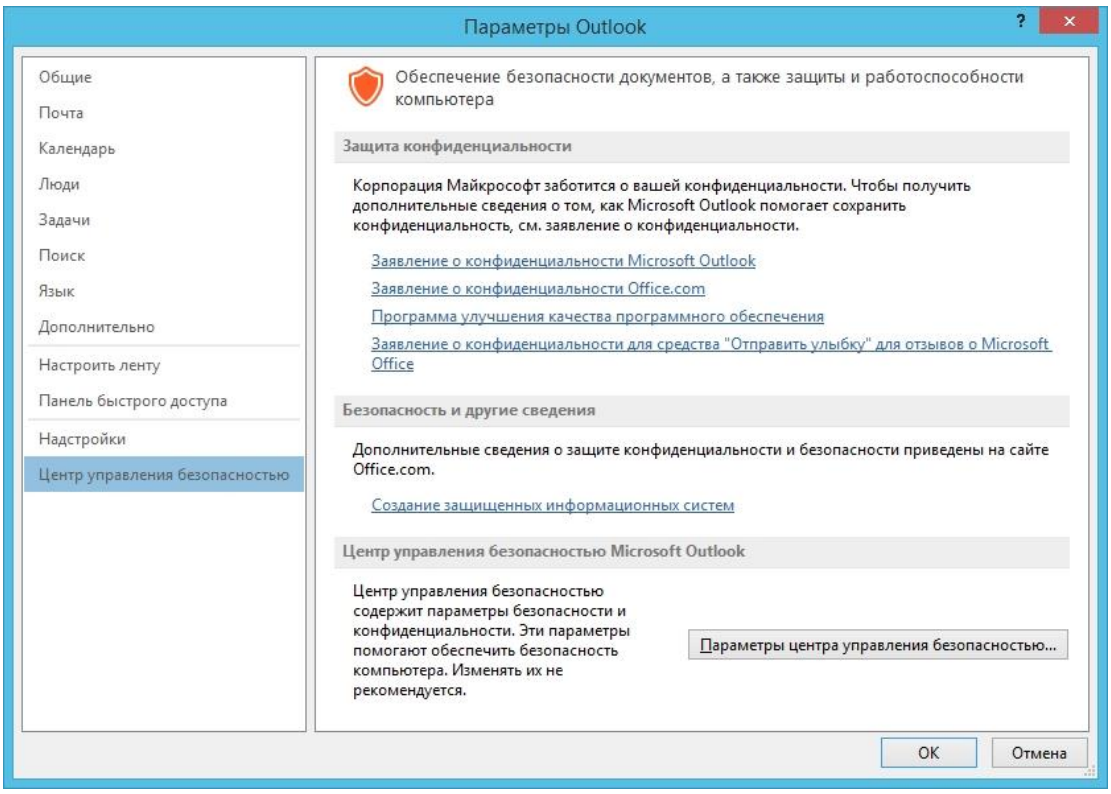
Использование средств криптографической защиты в Outlook 2013 во многом совпадает с использованием в Outlook ранних версий.

Конфигурация Outlook 2013

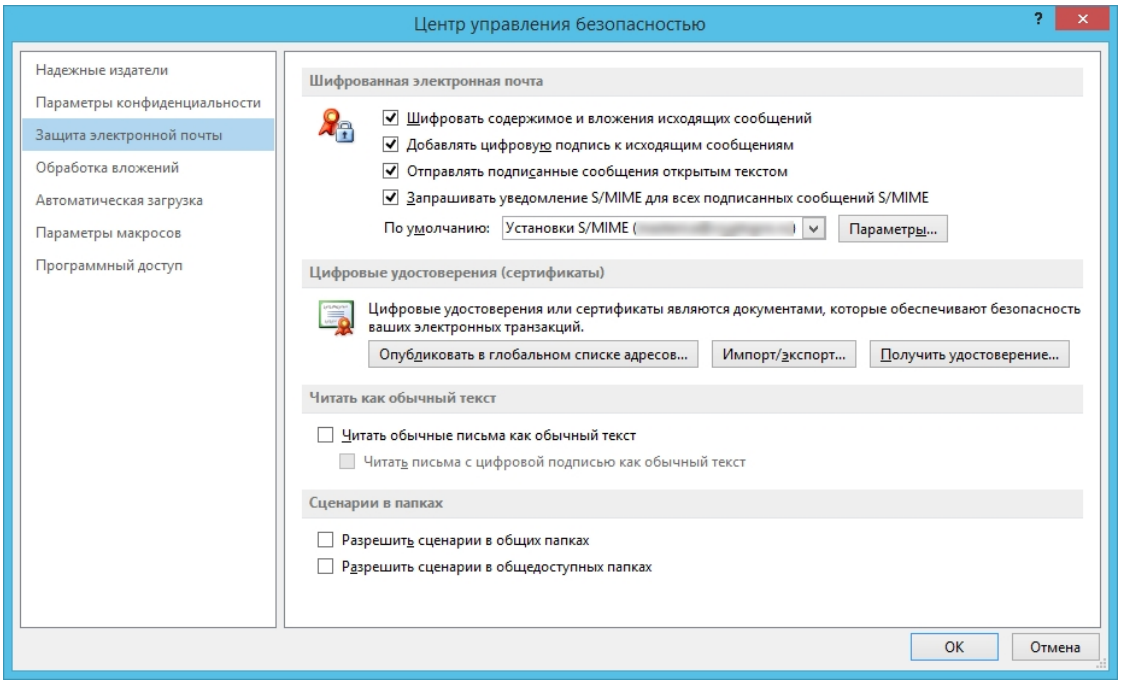
Выберите пункт **Параметры** (**Options**) меню **Файл** (**File**).



В открывшемся окне выберите в закладке **Центр управления безопасностью** (**Trust Center**) пункт **Параметры Центра управления безопасностью** (**Trust Center Settings**).

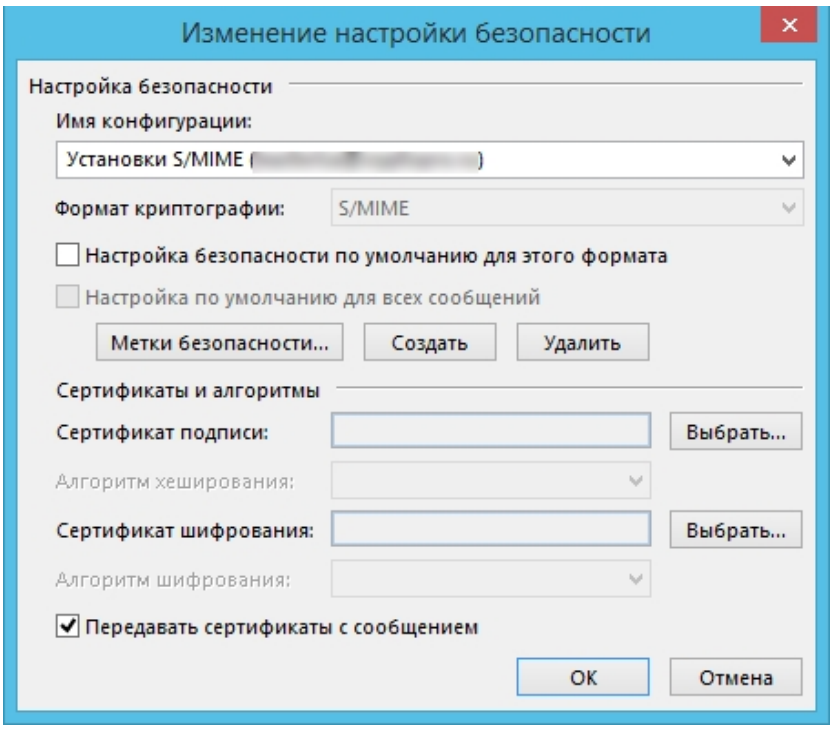


Выберите закладку **Защита электронной почты** (**E-mail Security**).

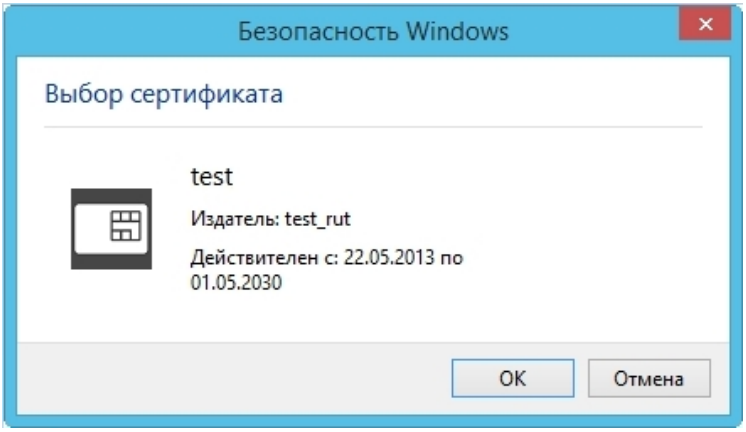


Нажмите **Параметры** (**Settings**).

Выберите личные сертификаты, соответствующие ключам подписи и шифрования, используя кнопку **Выбрать** (**Choose**). 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. Установите флаг **Передавать сертификаты с сообщением** (**Send these certificates with signed messages**).



Окно выбора сертификата:



После выбора сертификата необходимо указать **Имя конфигурации** (**Security Settings Name**). В противном случае Outlook выдаст ошибку.

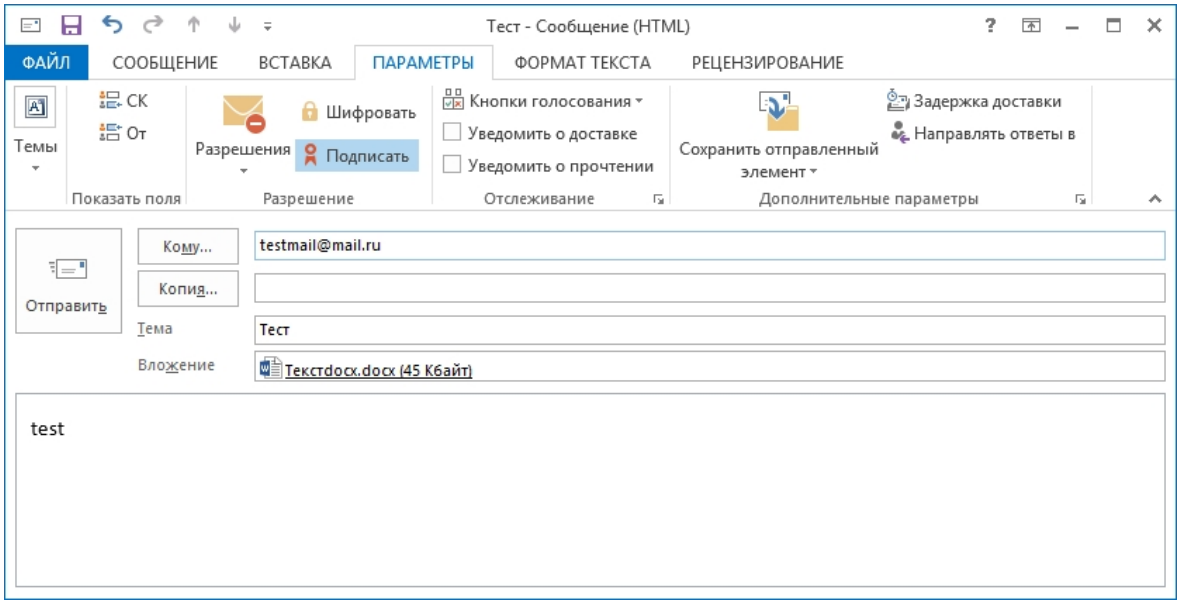
В закладке **Защита электронной почты** (**E-mail Security**) можно включить режимы **Шифровать содержимое и вложения исходящих сообщений** (**Encrypt contents and attachments for outgoing messages**) и **Добавлять цифровую подпись к исходящим сообщениям** (**Add digital signature to outgoing messages**) 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** (**Send clear text signed message when sending signed messages**). При включенном режиме подпись формируется в виде одного отдельного вложения для сообщения. Если режим выключен - текст сообщения и все вложения объединяются в единое целое и

кодируются в соответствии с правилами кодирования BASE64, после чего результат кодирования подписывается.

Отправка подписанных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку **Создать сообщение** (**New E-mail**).

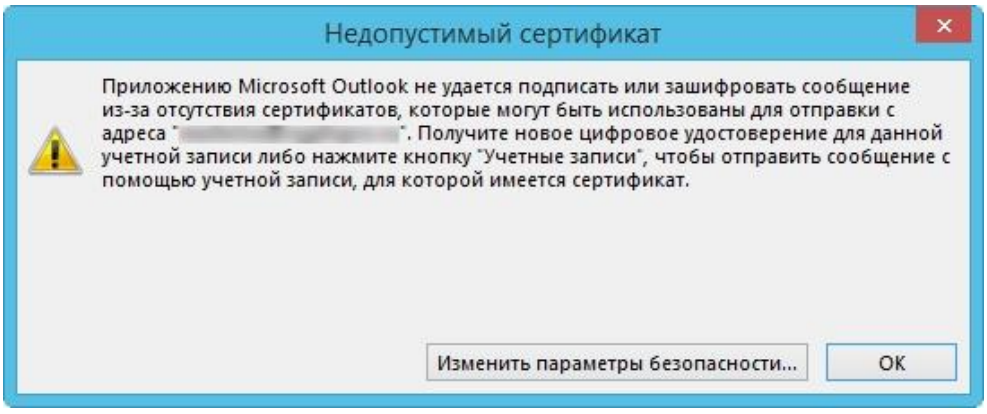
Выберите получателя сообщения (поле **To**) и введите тему сообщения (**Subject**). Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить файл** (**Attach File**).



Для того, чтобы подписать сообщение нажмите на кнопку **Подписать** (**Sign**) в закладке **Параметры** (**Options**).

Для отправки сообщения нажмите кнопку **Отправить** (**Send**).

Если сертификат, с помощью которого подписано сообщение, был отозван или электронный адрес, указанный в сертификате не совпадает с электронным адресом данной учетной записи, то появится следующее предупреждение, а само сообщение не будет отправлено.

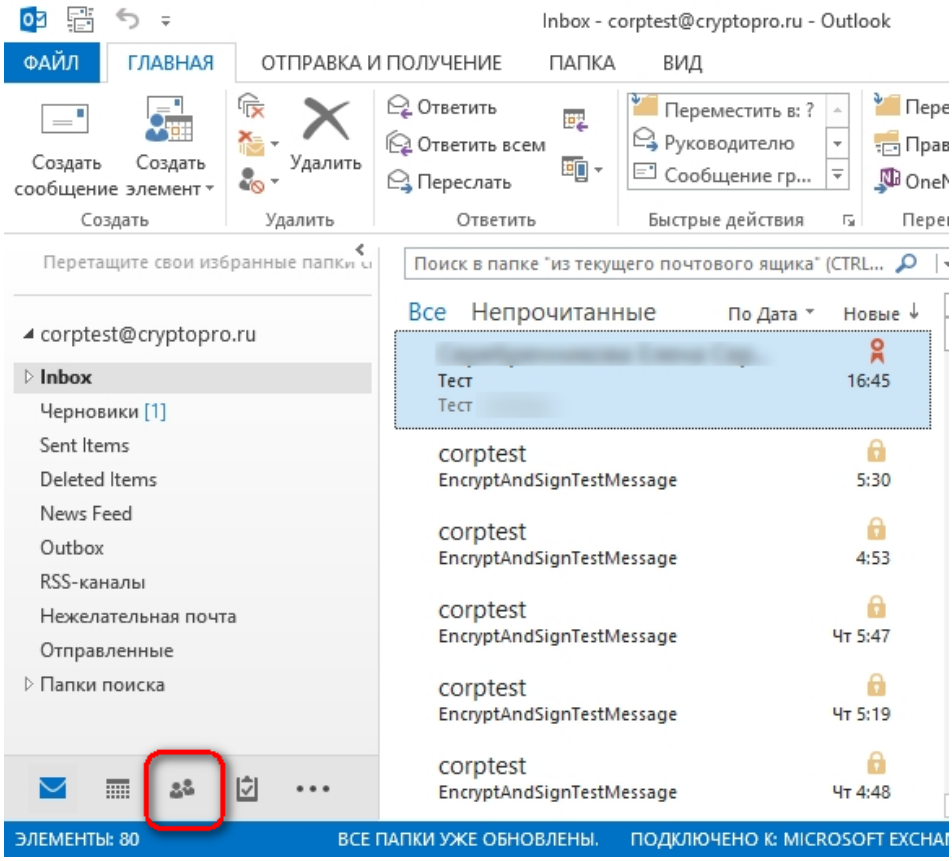


Получение сертификата открытого ключа абонента для шифрования сообщений

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:

1. Откройте локальную адресную книгу, нажав на значок в нижней части области папок.

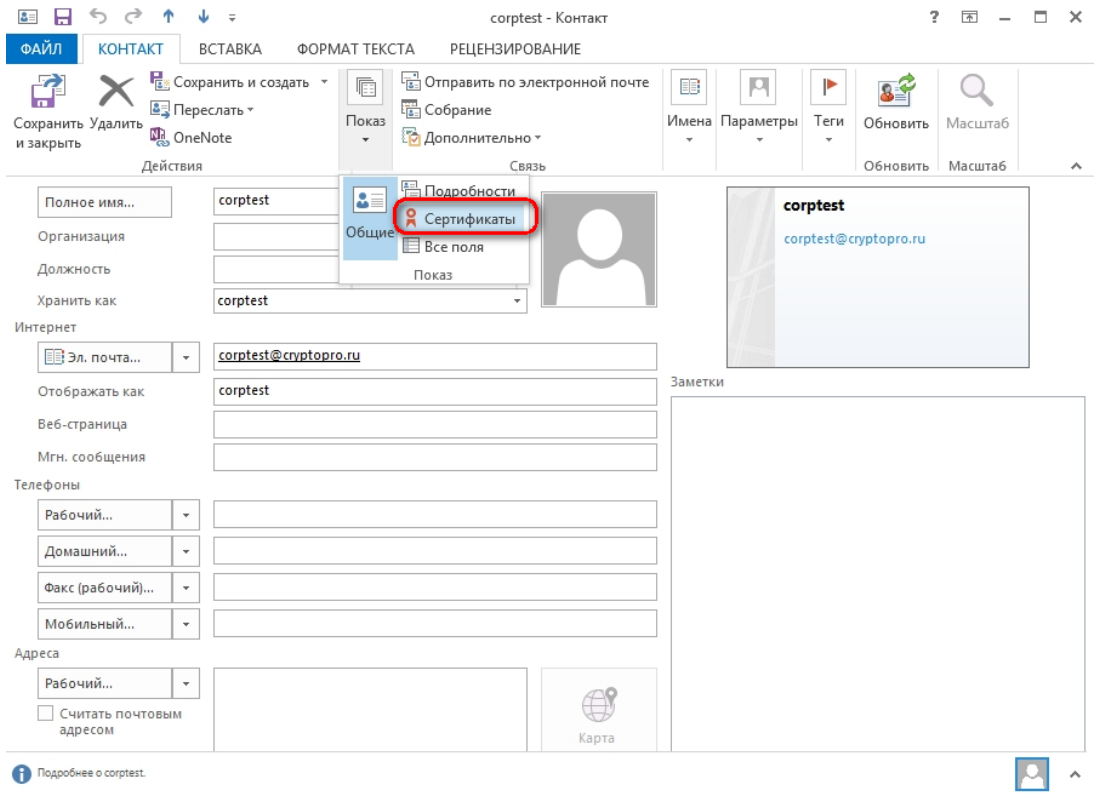


2.

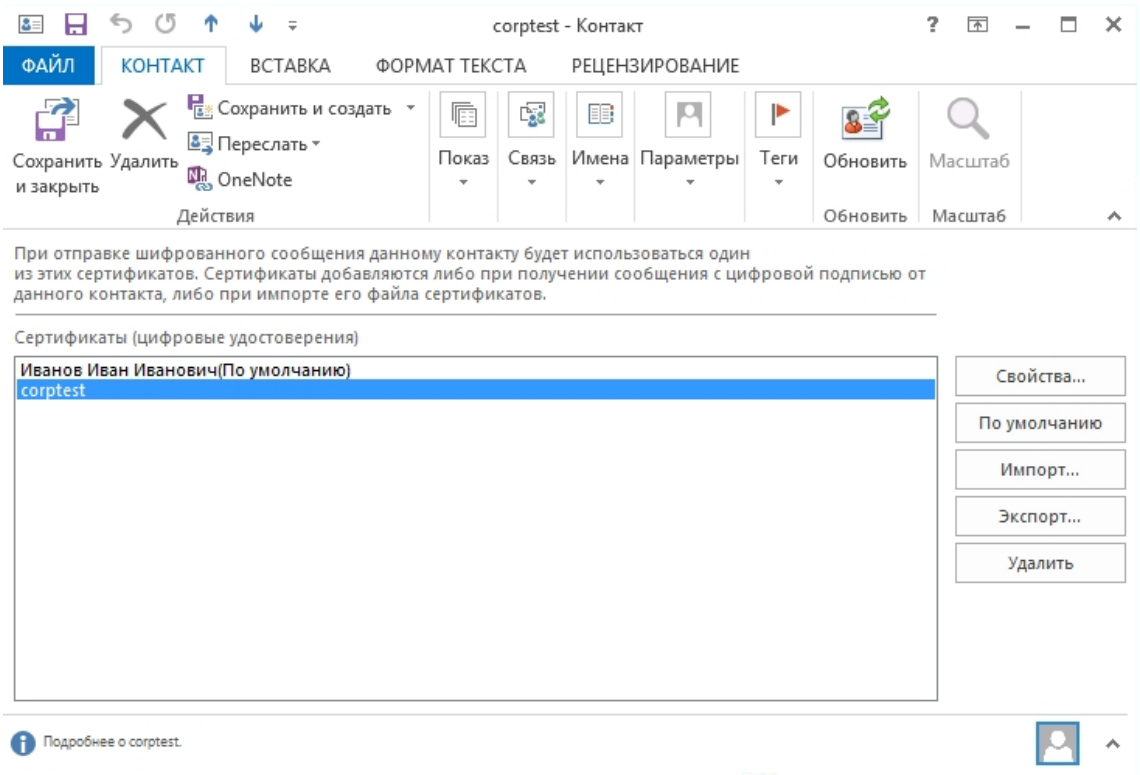
3. В открывшейся форме выберите нужный контакт и откройте двойным кликом.

4. В форме, которая содержит сведения о контакте, выберите **Показ** (**View**), в открывшемся выпадающем меню нажмите Сертификаты 

(Certificates).



В результате откроется список сертификатов, в котором можно увидеть сертификат отправителя.



После этого нажмите на кнопку **Сохранить и Закрыть** 

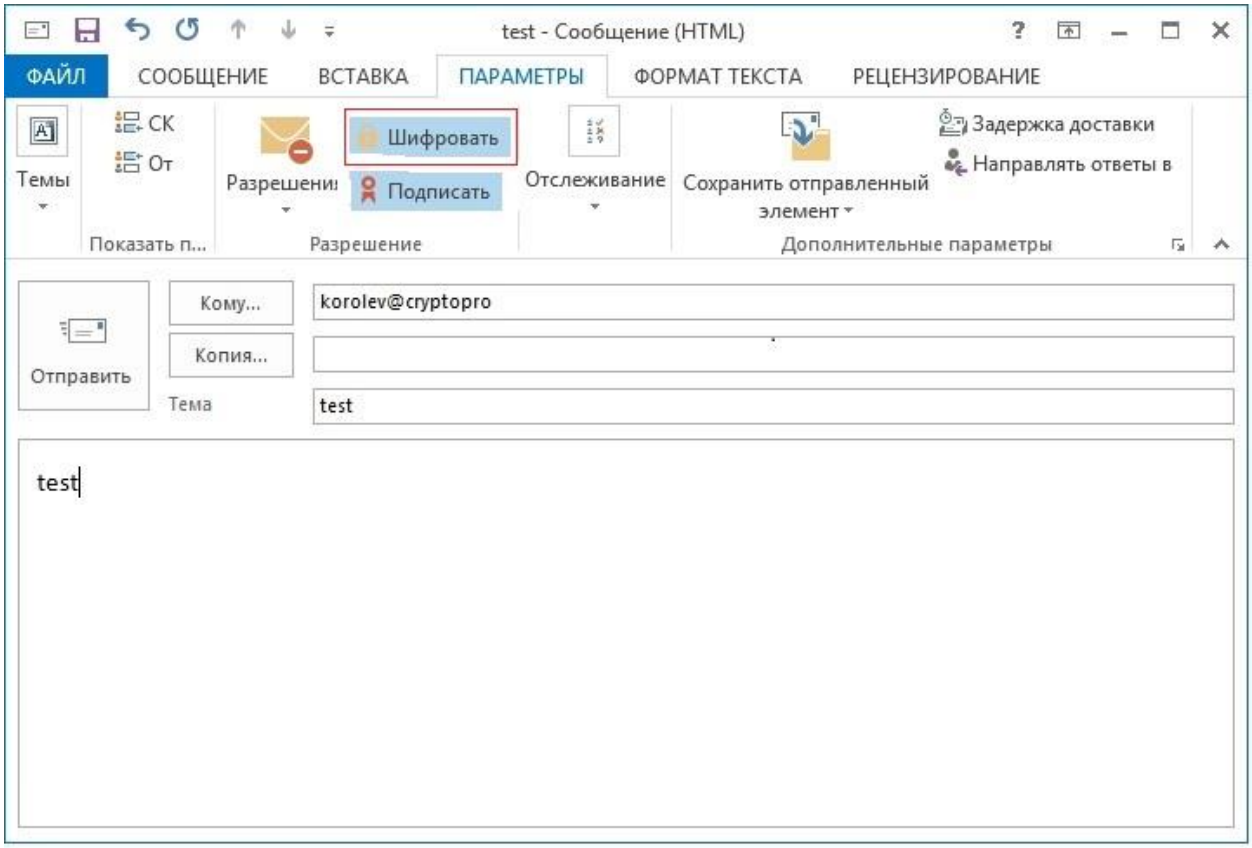
(**Save & Close**). Если абонент с таким адресом уже существует, программа предложит, либо добавить новый контакт (**Add new**

Contact), либо обновить сведения о выделенном контакте (**Update information of selected Contact**). Выберите второй пункт. При этом в существующий контакт будет добавлен полученный сертификат, а резервная копия будет сохранена в **Deleted Items Folder** (**Удаленные**).

Отправка шифрованных сообщений

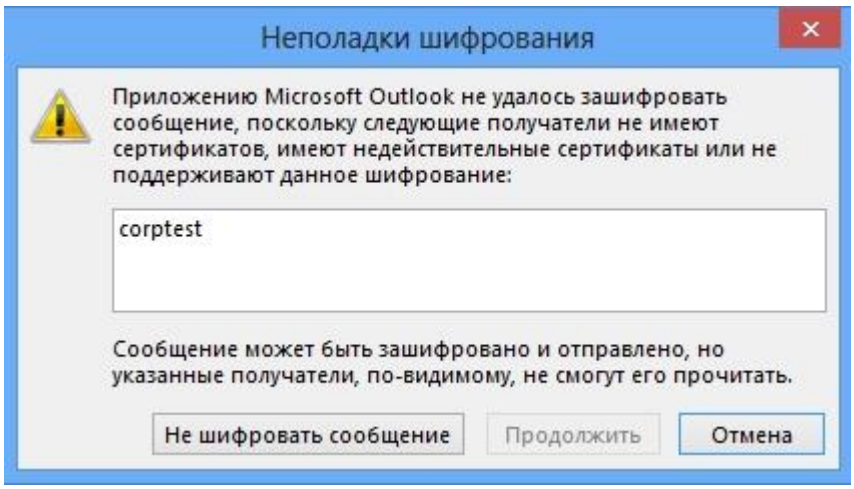
Для создания и отправки шифрованного сообщения нажмите кнопку **Создать** (**New E-mail**).

Выберите получателя сообщения (поле **To**) и введите тему сообщения (**Subject**). Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить файл** (**Attach File**) в закладке **Вставка** (**Insert**). Для отправки сообщения в зашифрованном виде нажмите кнопку **Шифровать** (**Encrypt**).



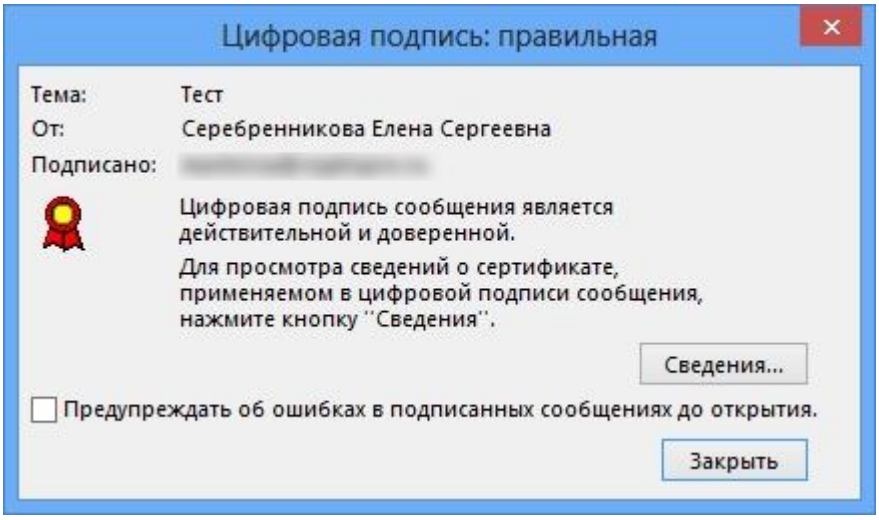
После того, как сообщение подготовлено к отправке, нажмите кнопку **Отправить** (**Send**).

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



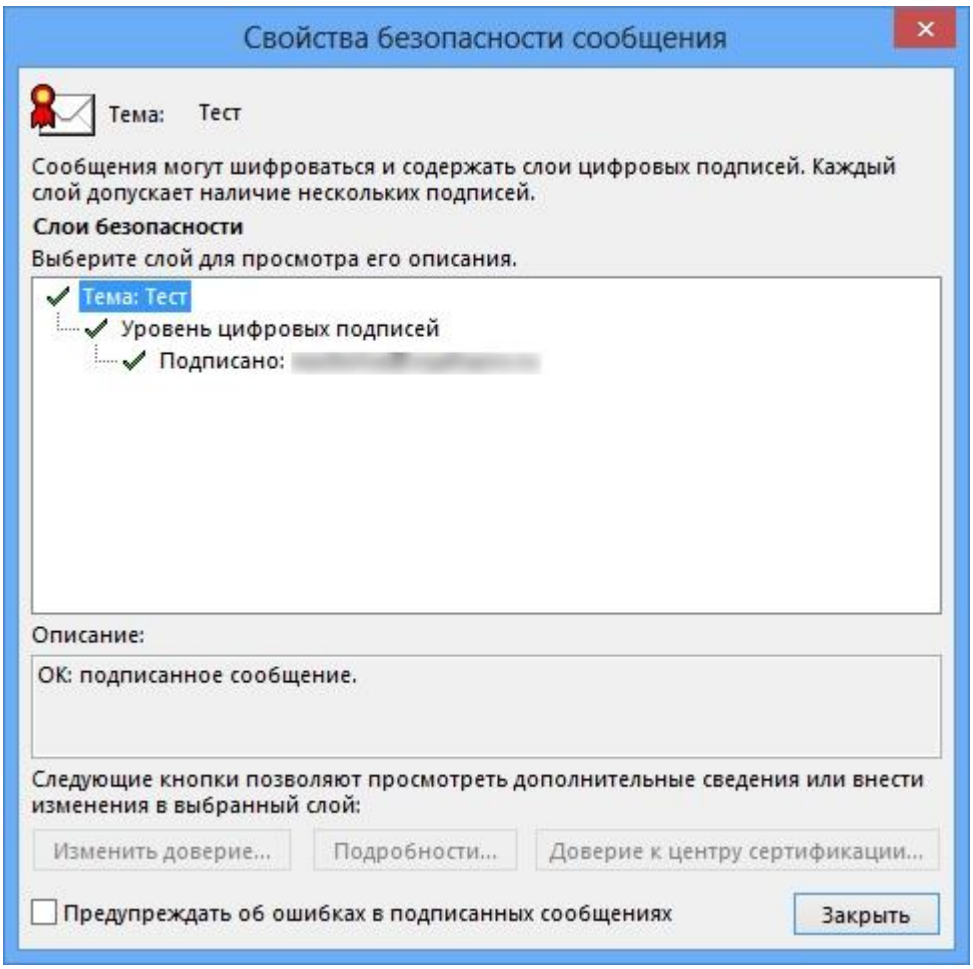
Проверка сертификата на отзыв

Для контроля проверки сертификатов на отзыв выполните следующие действия. Откройте полученное подписанное письмо. Нажмите кнопку  – признак подписанного сообщения.

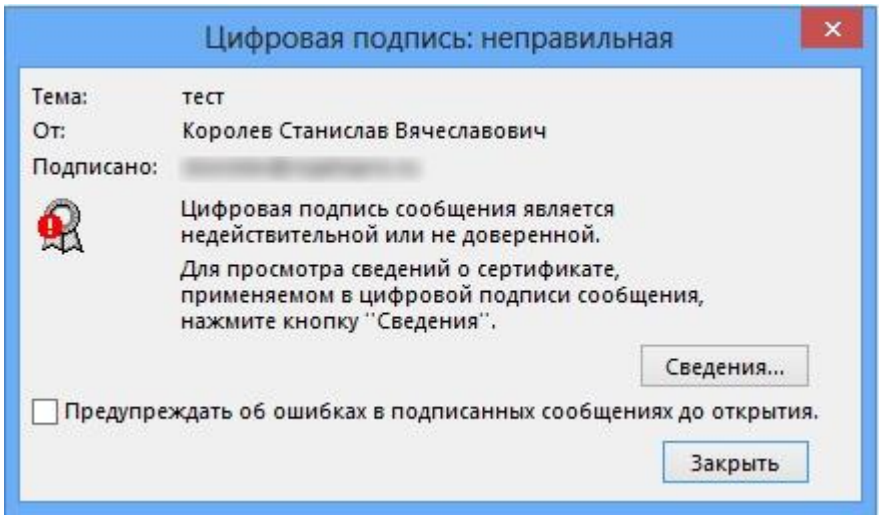


Нажмите кнопку **Сведения** (**Details**).

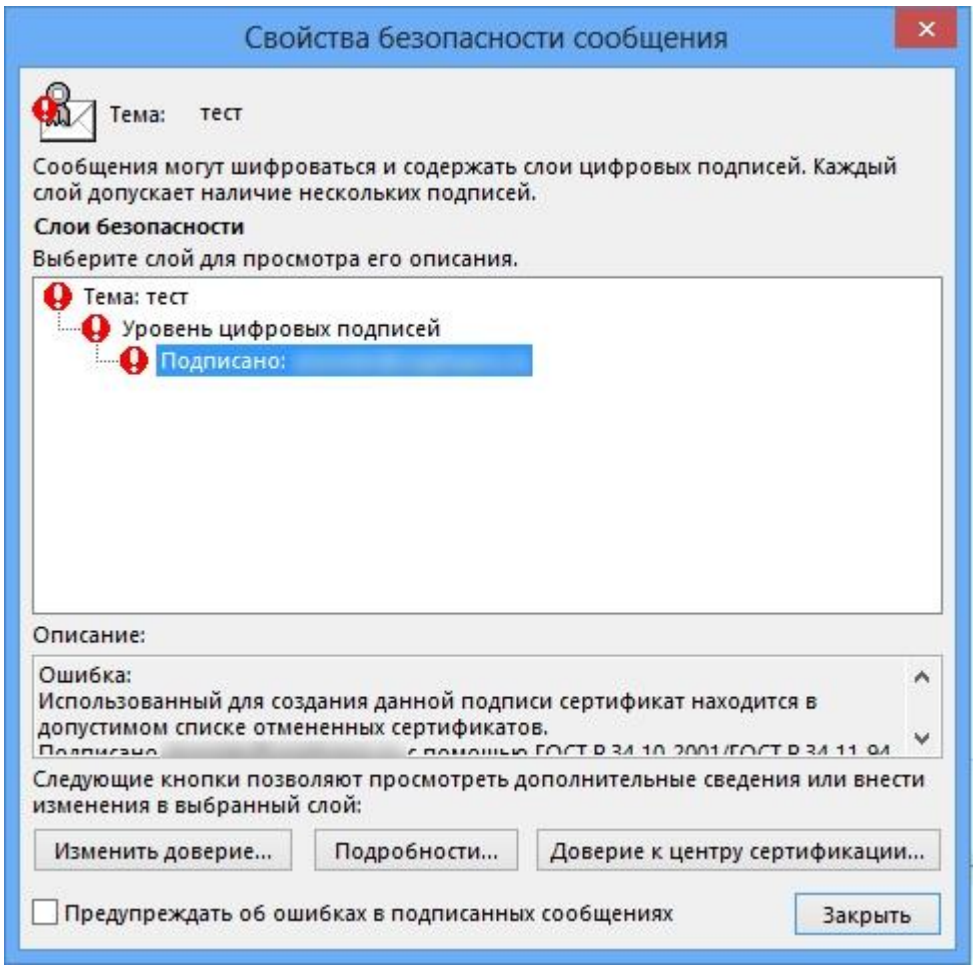
А если открывшееся окно подобно следующему, то СОС не установлен либо срок его действия истек. Обновите СОС, хранящийся в локальном справочнике сертификатов, с использованием доступных средств. Если окно осталось прежним, то сертификат не был отозван.



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



Нажмите кнопку **Сведения** (**Details**) для просмотра сведений о сертификате.


Свойства безопасности сообщения
Тема: тест
Сообщения могут шифроваться и содержать слои цифровых подписей. Каждый слой допускает наличие нескольких подписей.
Слои безопасности
Выберите слой для просмотра его описания.
Тема: тест
Уровень цифровых подписей
Подписано:
Описание:
Ошибка:
Использованный для создания данной подписи сертификат находится в допустимом списке отмененных сертификатов.
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