

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. Microsoft стандарту CSP сертифицированное Реализованное по 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 B 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
V	1СПОЛЬЗОВАНИЕ КРИПТОПРО CSP B 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
V	ІСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В ОUTLOOK 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
k	ІСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В ОUTLOOK 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
V	ІСПОЛЬЗОВАНИЕ 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
V	ІСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В ОUTLOOK 2010	. 62
	Конфигурация Outlook 2010	. 62
	Отправка подписанных сообщений	. 65
	Получение сертификата открытого ключа абонента для шифрования сообщений	. 66
	Отправка шифрованных сообщений	. 67
		2

	Проверка сертификата на отзыв	67
И	СПОЛЬЗОВАНИЕ КРИПТОПРО CSP В ОUTLOOK 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 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 СRL 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" (<u>http://www.cryptopro.ru</u>), 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).

Управл	ение сертификатами	
- andra	Сертификаты используются для удосто подлинности служб сертификации, изда	верения телей и себя.
	<u>Создать сертификат</u>)	Сертификаты
_ Дополн	ительное управление пользозателями —	
S	Локальные пользователи и группы испо дополнительного управления пользоват	льзуются для гелями.
		Дополнительно
Параме	тры безопасной загрузки	
>	Рекомендуется требовать нажатия соче Ctrl-Alt-Delete перед входом в систему. В	тания клавиш то обеспечивает
U	безопасность использования пароля и за от небезопасных программ.	ащищает систему
	Бовать нажатия Ctrl-Alt-Delete перед вхо,	дом в систему.
▼ Ipe		
₽ Ipe		

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 (<u>https://msdn.microsoft.com/en-us/library/windows/desktop/aa376517.aspx</u>). 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 B 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.

Јбщие	Серверь	ы Подключение	Безопасность	Дополнительно
Сертиф	рикат под	писи		
Выб цифр подп	ерите сер ровой код писываниі	пификат подписи. I, который будет и и сообщений с это	. Тем самым вы : іспользоваться п ой учетной записі	зададите ри ью.
<u>С</u> ерт	гификат:	test		Выбрать
Парам	етры шиф	рования		
				_
Выб(вклк ими шиф	ерите сер очаются в могли во рованных	лификат и алгори сообщения с циф спользоваться по сообщений.	пм шифрования. Фровой подписью улучатели при отп	Эти данные с тем, чтобы правке вам
Выбі вклк ими шиф Серт	ерите сер очаются в могли во рованных гификат:	ятификат и алгори в сообщения с циф спользоваться по в сообщений. test	птм шифрования. Фровой подписью олучатели при отп	Эти данные с тем, чтобы іравке вам В <u>ы</u> брать
Выби вклк ими шиф Серт Алго	ерите сер очаются в могли во рованных гификат: іритм:	ятификат и алгори сообщения с циф спользоваться по сообщений. test GOST 28147-89 (птм шифрования. Фровой подписью олучатели при отп 256-bit)	Эти данные с тем, чтобы правке вам Выбрать

Выберите пункт меню Сервис, Параметры... и нажмите на закладку Безопасность.

Оощие	Чтение	Уведа	иления Отправка сообщ		вка сообщений	Co	оздание сообщения
Подписи	Правоп	исание	Безоп	асность	Подключен	ие	Обслуживание
Вь	иберите зону безог (зона Интерне эзона ограниче Предупреждать, е Не разрешать сох изображения	асности дл га (безопас энных узлов сли прилож ранение ил	я обозревал ность ниже (безопасно (ения пытак и открытие	геля Internet но возможн ость выше) отся отправи вложений, к	Explorer: ностей больше) пь почту от моего оторые могут сод	имени. ержать в	ирусы.
Зопасная	і влокироват <u>ь</u> изос я почта	ражения и	другое внеи	инее содерж	имое в сооощени	и в форм	ate HIML.
Ce no	ртификат позволя льзователя при эл	ет удостове ектронном	ерять личнос обмене дан	ть ными.		Свел	дения
Д/ Ш/	ія подписывания о іфрованных сообщ	тправляем: ений нужно	ых сообщені і иметь серт	ий или получ ификат.	ения	<u>с</u> ерги Іолучить	сертификат
	Шифровать содер Подписывать все	жимое и вл отправляен	южения все чые сообще	х исходящих ния	сообщений	Попол	илельно

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.

Дополн	илтельные параметры безопасности 🛛 🛛
Шифро	ванные сообщения
Д	Предупреждать при стойкости шифрования сообщений меньше:
U	168 άντ
	🗹 Шифровать при отправке шифрованной почты самому себе
Сообщ	ения с цифровой подписью
0	Добавлять мой сертификат при отправлении сообщений с подписью
-	Кодировать сообщения перед подписыванием (непрозрачная подпись)
	Автоматически добавлять сертификат отправителя в адресную книгу
Провер	жа отзыва сертификатов
	Проверять, не были ли отозваны сертификаты:
<u></u>	О Іолько при нахождении в сети
	• Никогда не проверять
	ОК Отмена

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.

🗈 test							
файл Правк	ка внд Встдека Формат Серенк Сообщение <u>С</u> правка	4					
Отправить	Вырезать Колировать Вставить Отменить Праволика Вложить Важность Подп	жать Зашифров					
Кону:	maitest@cryptopro.ru						
Копия:							
Тена:	test						
Присоединить:	smime.pdf (560 KE)						
	✓ 単 x K H A 扫扫信信 目 ≤ 目目 - ● ■						
1		M					

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

	Сертификат для данной учетной записи отозван.
	Программе Outlook Express не удалось найти действующего сертификата на этом компьютере. Получить новый сертификат?
_	

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**.

Файл Правка Вид	Сервис Сооби	цение Спра	вка	0	3
Ответить Ответить. От: ПЕ Дата: 13 Кому: mail Тема: test Безопасность: Под	Переслать Добавить в адре Найти Блокировать отп Копировать	Печать эсную книгу правителя	Удалить	Предыду	8
test	Свойства				2

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.

🐋 Адресная книга - Ос	новное уда	остове рение			
<u>Ф</u> айл Правка Вид Серви	с <u>С</u> правка				
создать Свойства	<mark>≻</mark> Удалить	із Поиск людей	Д Печать	& . Действие	
Общие контакты Основное удостовер	Введите <u>и</u> ли	выберите из спи	иска:		Ломация
	mailtest	mailtest@	Pcryptopro.ru	Служеоный телл.	донашни
< >	<				>
1 объекта(-ов)					

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:

test	? 🛽
Общие Подробно Безопасность	
Цифровая подпись	
Подписано: mailtest@cryptopro.ru	
Содержимое не изменено:	Да
Подпись достоверна:	Да
Запрос безопасного уведомления:	н/д
Проверка отзыва сертификата:	Нет
Состояние Проверка отзыва сертифика отзыва:	тов была отключена. 🔗
Метка безопасности:	<
Шифрование	
Содержание и вложения зашифрованы:	Нет
Алгоритм шифрования:	Нет
Просмотр сертификатов Допо	олнительные <u>с</u> ведения
	ОК Отмена

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



Если же сертификат отозвали, то при открытии письма появится предупреждение:

Этот сертификат был отозван.

ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP В ПРОГРАММЕ "ПОЧТА WINDOWS"

Программа "Почта Windows" (Windows Mail) является компонентом только OC 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.

айл Правка Вид 🕻	ервис Сообщение Справка П	оиск	Q		
Создать почтовое со	Доставить почту 🔸 🔀 Дост	авить почту 🔻	-		
🍻 Локальные папки	Синхронизовать все		Получено		
Входящие	Контакты Windows Ctrl+Shift+C		02.07.2010 1		
Отправленны	Добавить отправителя в список контактов		02.07.2010 1		
 Удаленные Удаленные 	Календарь Windows Ctrl+Shift+L	ь в программу Почта Windo	02.07.2010 1		
Черновики Нежелательна	Правила для сообщений 🔸				
Microsoft Commu	Группы новостей Сtrl+W				
	Учетные записи				
	Параметры нежелательной почты				
	Параметры				
	Tema: test1				
	Справка по безопа	сности	5		
	Шифрованные сообщения 🏼 🌈 🖡				
	Это сообщение было зашифровано отправителем	L.			
	При полиции защифророциого сообщения можи	DEITE VPOD			

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

Общие	Серверы	Подключение	Безопасность	Дополнител	њно	
Серти	фикат под	писи				12
Вы код это	берите сер 1, который й учетной	тификат подпи будет использо записью.	іси. Тем самым оваться при по,	і вы зададите дписывании	ецифровой сообщений	c
<u>C</u> ep	отификат:	test			Выбрать	
Парам	иетры шиф	рования –				
БЫ	оерите сер	тификат и алго	ритм шифров	ания. Эти дан	ные	
вкл мог ши Сер	оерите сер ючаются в гли воспол фрованны оти <u>ф</u> икат:	тификат и алго сообщения с взоваться полу х сообщений. test	ритм шифров. цифровой поді учатели при от	ания. Эти дан писью с тем, правке вам	чтобы ими В <u>ы</u> брать	
выл мог ши Сер Алг	оерите сер ючаются в гли воспол фрованны отификат: горитм:	тификат и алго в сообщения с пьзоваться полу х сообщений. test GOST 28147-	ритм шифрова цифровой поді учатели при от 89 (256-bit)	ания. Эти дан писью с тем, правке вам	чтобы ими В <u>ы</u> брать	
выл вкл мол Сер Алг	оерите сер нючаются в гли воспол фрованны отификат: горитм:	тификат и алгс в сообщения с възоваться полу х сообщений. test GOST 28147-	цифровой поді учатели при от 89 (256-bit)	ания, эти ден писью с тем, правке вам	ные чтобы ими В <u>ы</u> брать	

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.

Общие	Чтение	Уведа	мления	Отправ	ка сообщений	Создание с	ообщения
Подписи	Правопи	сание	- Eeson	асность	Подключение	Допол	нительно
Защита от в	ирусов —						
Выбе	ерите зону без	опасности	4:				
	🔘 зона <u>И</u> нте	рнета (без	опасность	ниже, но в	озможностей бол	ьше)	
	Зона о <u>г</u> ран	ниченных	узлов (без	опасность в	ыше)		
V []	редупреждать,	если при	ложения г	нытаются от	править почту от	моего имени.	
[22] L I					4		
<u> </u>	е разрешать с	охранение	е или откр	ытие вложе	нии, которые мог	ут содержать в	ирусы.
Загружать и	зображения						
🔽 <mark>Б</mark> л Н	покироват <u>ь</u> из TML.	ображени	я и другое	внешнее со	одержимое в сооб	щении в форг	иате
Безопасная	почта						
Циф	ровые удостов	ерения (с	ертификат	гы) – это спе	циальные		
доку	менты, дающи	е право н	а подтвер:	ждение лич	ности	50 BC	
поль	зователя при о	обмене да	нными.			<u>С</u> ертифик	аты
Urof				coofmound			
полу	чать шифрова	провую по	бщения, н	еобходимо	иметь	Полу <u>ч</u> ить серт	гификат
цифр	овое удостов	ерение.					
ПШ	ифровать сод	ержимое	и вложени	я всех исход	иящих сообщений	1	
500		• • • • • • • • • • • • • • • • • • • •					
V 🛛	одписывать вс	е <u>о</u> тправл	яемые соо	общения			
					[Лополните	7590
						House	

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.

Цифро	ованные сообщения
9	Предупреждать при стойкости шифрования сообщений меньше:
-	168 бит 🔹
	📝 Шифровать при отправке шифрованной почты самому себе
Сообц	цения с цифровой подписью
9	☑ Добавлять мой сертификат при отправлении сообщений с подписью
• •	Кодировать сообщения перед подписыванием (непрозрачная подпись)
	☑ Двтоматически добавлять сертификат отправителя в контакты Windows.
Прове	рка отзыва сертификатов
	Проверять, не были ли отозваны сертификаты:
	Оправлении в сети
	Никогда не проверять

Отправка подписанных сообщений

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

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**.

Отправить 🔏 🗈	1 7 2 5	Правописание	F7	
🖻 Кому: 🖻 Копия:	constest < constest	Запросить уведомление о прочтении Проверить имена Выбрать получателей	Ctrl+K	
Гема: Бложиты	README.HTM (Контакты Windows Календарь Windows	Ctrl+Shift+C Ctrl+Shift+L	
Arial	- 10 - E	Зашифровать		
		Цифровая подпись		

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

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



Получение сертификата открытого ключа абонента для шифрования сообщений

Для шифрования сообщений в адрес других пользователей необходимо предварительно произвести обмен сертификатами. Для этого обычно достаточно переслать подписанное сообщение в адрес требуемого абонента (сообщение посылается вместе с сертификатом отправителя). После получения сообщения и проверки электронной цифровой подписи производится автоматическое добавление адреса отправителя и его сертификата в список контактов.

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

писи
ования
-89 (256-
вителя
контакто

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. 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**.

Дайл Шракка Вид Вгадкка Формат Сервис Сообщение Справка В Отправить Image: Sorphest Image: Sorphest Image: Sorphest F7 Image: Sorphest Image: Sorphest F7 Image: Sorphest Image: Sorphest	📑 test	_			
Image: Corplest < corplest	Файл Правка Вид III Отправить ∦ III	Вст <u>а</u> вка Фор <u>м</u> ат	С <u>ервис</u> Сооб <u>щ</u> ение <u>С</u> правка Правописание	F7	
I EMA: TEST Вложить: README.HTM Arial ↓ 10 ↓ E test test	📼 Кому: 🖮 Копия:	corptest < corptest	Запросить уведомление о прочтении Проверить имена Выбрать получателей	Ctrl+K	
Аrial • 10 • В Цифровая подпись Запросить безопасное уведомление В	тема: Вложить:	README.HTM (Контакты Windows Календарь Windows	Ctrl+Shift+C Ctrl+Shift+L	
Цифровая подпись Запросить безопасное уведомление	Arial	▼ 10 ▼ ■	Зашифровать		
	test		Цифровая подпись Запросить безопасное уведомление		*

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

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

Ж

Проверка сертификата на отзыв

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

бщие Подробно Безопасность	
	14
цифровая подписв	8
Подписано: corptest@cryptopro.ru	
Содержимое не изменено:	Да
Подпись достоверна:	Да
Запрос безопасного уведомления:	Нет
Проверка отзыва сертификата:	Да
Состояние отзыва: Сертификат не был о не удалось получить информацию об отза	отозван, или
Метка безопасности:	
Шифрование	T
Содержание и вложения зашифрованы:	Нет
Алгоритм шифрования:	н/д
Просмотр сертификатов Дополнительные с	ведения

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

)бщие	Подробно	Безопаснос	СТБ		
Цифр	овая подпи	ісь —			
По,	дписано:	mov	vchan@cryptopro.ru		
Co	держимое н	е изменено	i i i i i i i i i i i i i i i i i i i	Да	
По,	дпись досто	верна:		Да	
3ar	прос безопа	сного уведо	мления:	Дa	
Пр	оверка отзь	ва сертифи	ката:	Да	
Co	стояние отз	ыва:	Этот сертификат был отозван	*	
				-	
Me	тка безопас	ности:		~	
				-	
Шифр	рование				
Co	держание и	вложения з	ашифрованы:	Нет	
Ал	горитм шиф	фрования:		Н/Д	
Про	осмотр серт	ификатов	Дополнительные сведения]	

ИСПОЛЬЗОВАНИЕ КРИПТОПРО CSP B 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.

	rptest) — свойства		
Общие Серверь	ы Подключение Безог	асность Дополнительно	
Сертификат под	лиси		
Выберите сер цифровое удо при подписыв	отификат подписи. Тем са остоверение, которое буд зании сообщений с этой у	амым будет задано ет использоваться четной записью.	
<u>С</u> ертификат:	7777	Выбрать	
Параметры шиф	рования		
Выберите сер включаются в чтобы ими мо	отификат и алгоритм шиф сообщения с цифровой гли воспользоваться пол шифрованных сообщени	рования. Эти данные подписью с тем, лучатели при ий.	
о правке вам			
опіравке вам С <u>е</u> ртификат:	7777	Выбрать	
Сертификат: Алгоритм:	7777 GOST 28147-89 (256-bit	Выбрать	
Сертификат: Алгоритм:	7777 GOST 28147-89 (256-bit	Выбрать	
о правие вам С <u>е</u> ртификат: Алгоритм:	7777 GOST 28147-89 (256-bit	<u>Вы</u> брать	
Свртификат: Алгоритм:	7777 GOST 28147-89 (256-bi	Выбрать	

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.

	Параметры		Надеж	ные отправите	ели
Заблон	кированные отправители	Международные нас	тройки	Фишинг	Безопасност
Защита	а от вирусов Выберите зону безопасно	сти для обозревателя Int	emet Explo	orer:	
	 зона Интернета (о зона ограниченны; 	езопасность ниже, но во: к сайтов (безопасность в	зможност ыше)	ей больше)	
	Предупреждать, если моего имени.	приложения пытаются от	править п	исымо от	
	Не разрешать сохране могут содержать виру	ние или открытие вложе сы.	ний, котор	ые	
Загрузи	ка изображений				
	Блокировать изображи в сообщениях в форма	ения и другое внешнее со ате HTML.	одержимо	8	
	Показывать изобр	ажения и внешнее содер	жимое, от	правленное с	адресов
Безопа	электронной почть сная почта	из списка надежных от	правителе	й.	
Eesona	электронной почте сная почта Цифровые удостоверения специальные документы, и растверскае документы, и	и из списка надежных от (сертификаты) – это зающие возможность	правителе	й. Сертификать	
Eesona	электронной почть сная почта Цифровые удостоверения специальные документы, л подтверждения личности п обмене данными.	и из списка надежных от (сертификаты) – это цающие возможность ользователя при	правителе	й. Сертификать	l
Eesona	электронной почть сная почта Цифровые удостоверения специальные документы, подтверждения личности п обмене данными. чтобы ставыть цифровую г сообщениями или получать сообщения, у вас должен	и из списка надежных от (сертификаты) – это дающие возможность ользователя при подпись под ь шифрованные быть сертификат.	правителе	и. Сертификать лучить сертиф	икат
Eesona	электронной почть сная почта Циеровые удостоеврения специальные документы, и подтверждения личности по обмене данными. Чтобы ставия личности по сообщения, у вас должен сообщения, у вас должен Шифровать содержим	и из описка надежных от (сартификаты) – это закцие возможность польсователя при подпись под в шифрованные быть сертификат.	правителе По дящих соо	й. Сертификать лучить сертиф бщений	икат
Besona	электронной почть сная почта Шикровые удостоверения специальные документы, л подтверждения личности п обмене данными. Чтобы ставция личности п обмене данными. Чтобы ставцить шеровую сообщениям, у вас должен Шифровать содержими Подлисывать все отпр	и из описка надежных от (сертификаты) – это дающие возможность (ользователя при ользователя при цамфрованные быть сертификат. - ре и вложения всех исхо) извляемые сообщения	правителе	й. Сертификать лучить сертиф бщений Дополнительн	икат
Eesona	электронной понть сная почта Циеровые удостоверения специальные документы, и подтверждения личности по обмене данными. Чтобы ставция личности получат сообщения, у вас должен сообщения, у вас должен Шифровать содержими Подлисывать все отпр	и из списка надежных от (сертификаты) – это дающие возможность подпись под в шифрованные быть сертификат. - ре и вложения всех исхо) иавляемые сообщения	правителе	й. Сертификать лучить сертиф бщений Дополнительн	икат

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.

-	
A	Предупреждать при стойкости шифрования сообщений меньше:
	168 бит
	🔽 Всегда шифровать для себя при отправке шифрованной почты
Сооби	цения с цифровой подписью
0	Добавлять мое цифровое удостоверение при отправке сообщений с подписью
	Г Кодировать сообщения перед подписыванием (непрозрачная подпись)
	Aвтоматически добавлять сертификаты отправителей в контакты Windows Live.
Прове	рка отзыва сертификатов
	Проверять, не были ли отозваны цифровые удостоверения:
	Только находясь в сети
	С Никогла не проверять

Отправка подписанных сообщений

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

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

айл Правка Вид Вставка Формат	Сервис Справка			
Подписать Зашифровать Вста	Правописание F7	Вложить	33	R • 0
Кому:	Проверить имена Ctrl+K Выбрать контакт			
Копия:	Важность •			
🛄 Скрытая копия:	Запросить уведомление о прочтении			
Тема:	Зашифровать			
	Цифровая подпись			io ii exportște conine
🕼 Формат 🛛 🙀 Добавить фотографии	Запросить безопасное уведомление	1		

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

	orbeinte beenn. Artepeenn	с доовыть в колстдора здолите		
ыстрые представл	Помек сообщения	test		01.07.2010 1
Непрочитанные сос Непрочитанные сос Непрочитанные веб	oriente oriente anne test	Полите Соларндарь)	далить Нежелательная поч	ra » 🗗 * 🕢 *
Гурторго (согрте te Вюдацие Кс Черновики 1 Отправленные Нежелательная поч Удаленные 1сходящие обавить учетную зап	Общие Сведения Безопасност Цифровая подпись Подписано: porptest@ Содержимое на изменено: Подпись достоверна: Запрос безопасности вуедомил Проверка отзыва цифрового к Состояние отзыва: Сертикен на удол Состояние отзыва: Сертикен на удол о его отз Шифрование Содержение и вложения защи Алгоритм шифрования: Просмотреть сертификать	В В	Сертификат подписи Сертификат шифрования ЗDES Сертификат отправителя	отасности подписью подписью подписью подписью подписьи
Почта		контактах Windows Live.	ОК Отмена	
Календарь Контакты				
Веб-каналы				

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. Создать •

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

айл Правка Ви	а Вст <u>а</u> вка Фор <u>м</u> ат	Сервис Справка		
Подписать 3	ашифровать Вст	Правописание F7	Вложить » 🖹 • 🔞	
		Проверить имена Ctrl+K		
🛄 Кому:		Выбрать контакт		
🛄 Копия:		Важность		
🚺 Скрытая копи	IR:	Запросить уведомление о прочтении		
Тема:		🗸 Зашифровать		
Ар Формат 🖓 Добавить фотографии		Цифровая подпись		
		Запросить безопасное уведомление		

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

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

Предуг	преждение системы безопасности
<u>^</u>	Сертификат шифрования для данной учетной записи отозван.
	ОК

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.

Общие Сведения Безопасность	
Цифровая подпись	
Подписано: corptest@cryptopro.ru	
Содержимое не изменено:	Да
Подлись достоверна:	Дa
Запрос безопасного уведомления:	Нет
Проверка отзыва цифрового сертификата:	Да
Состояние отзыва: Сертификат не был отозва не удалось получить инфор о его отзыве. Метка безопасности:	н, или А мацию У
Шифрование	Une
Содержание и вложения зашифрованы: Алгоритм шифрования:	н/д
Просмотреть сертификаты	
OK	07740447

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

Эбщие	Сведения	Безопасность	
Цифро	вая подписы		
Подг	писано:	van@cryptopro.ru	
Соде	эржимое не і	изменено:	Дa
Подг	лись достове	ерна:	Дa
Запр	оос безопасн	юго уведомления:	Нет
Пров	зерка отзыв	а цифрового сертификата:	Нет
Сост	гояние отзые	за: Проверка отзыва сертификатов была отключена.	- *
			Ŧ
Мет	<a< td=""><td>-</td><td>*</td></a<>	-	*
0es0	ласности:		-
Шифро	вание —		_
Соде	эржание и вл	южения зашифрованы:	Нет
Алго	ритм шифро	вания:	н/д
	иотреть серт	пификаты	
-			

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

Общие Сведения	Безопасность	
Цифровая подпись		-
Подписано:	van@cryptopro.ru	
Содержимое не и	зменено:	Дa
Подпись достове	она:	Дa
Запрос безопасн	ого уведомления:	Нет
Проверка отзыва	цифрового сертификата:	Дa
Состояние отзыв	а: Этот сертификат был отозван	*
		-
Метка		~
оезопасности:		-
Шифрование —		
Содержание и вло	жения зашифрованы:	Нет
Алгоритм шифров	ания:	н/д
Просмотреть серт,	афикаты	

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, (<u>http://office.microsoft.com/ru-ru/officeupdate/CD010225951049.aspx</u>) 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...**.

43

Имя конфигурации:	SOST	
	(Pressed on the second s	-
Формат сообщения:	S/MIME	
🔽 Настройка безопасн	ю, ти по умолчанию для это	л о формата
🔽 Настро <u>й</u> ка по уг	молчанию для всех сообще	ний
		1
	Удали	ть Пароль
ертификаты и алгоритмы	d 	
Сертификат подписи:	mail	Выбрать
Алгоритм хеширования	GOST R 34.11-94 (256-b	it] 💌
Сертификат шифровани	ия: mail	Выбрать
Алгоритм шифрования:	GOST 28147-89 (256-bit)	

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.

Настройки	Почтовые	службы	Coot	бщение	Орфографи
Безопасность		Дополните.	льно	1	Представители
езопасность электрон	ной почты				
<u>) П</u> Шифрова	ть содержимо	е и вложения и	сходящих	сообщений	
💶 🗌 Добавлят	ь цифровую п	юдпись к исхо,	дящим coot	бщениям	
🗌 Отправля	ть подписанн	ые сообщения	открытым	текстом	
Безопасность	по умолчанию	о: Установки	S/MIME	111	
				Изме	нить настройки
				-	
PROPACHOCTE CORPONIA	woro				
собласность содержи					
🚵 Зоны безопас	ного Ности позвол!	яют определит	гь порядок	запуска сц	енариев и активного
Зоны безопас содержимого	ного ности позволя в сообщения»	яют определит «HTML, Выбер	гь порядок ите зону б	запуска сц езопасност	енариев и активного и Internet Explorer.
Зоны безопас содержимого	ности позволя в сообщения»	ают определит «HTML, Выбер	гь порядок ите зону б	запуска сц езопасності	енариев и активного и Internet Explorer.
Зоны безопас содержимого Зона:	ного ности позволя в сообщения: Интернет	яют определит «HTML, Выбер	гь порядок ите зону бо	запуска сц езопасност На	енариев и активного и Internet Explorer. астройки зоны
Зоны безопас содержимого Зона:	ного ности позвол: в сообщения: Интернет	ают определит «HTML. Выбер	гь порядок ите зону б •	запуска сц езопасност На Безоп	енариев и активного и Internet Explorer. астройки зоны асность вложений
Зоны безопас содержимого Зона: Э	ного ности позвол: в сообщения) Интернет ния (сертифи)	ают определит (HTML, Выбер (аты)	гь порядок ите зону б	запуска си езопасності На Безоп	енариев и активного и Internet Explorer. астройки зоны асность вложений
Зоны безопас содержимого Зона: э ифровые удостовере Цифровые уд	ного ности позвол: в сообщения: Интернет ния (сертифи остоверения	ают определит « HTML. Выбер «аты) или сертифика	гь порядок ите зону би • • • • • • • •	запуска сц езопасност На Безоп	енариев и активного и Internet Explorer. астройки зоны асность вложений тами, которые
Зоны безопас содержимого Зона: э ифровые удостовере Цифровые уд	ного ности позвол: в сообщения: Интернет ния (сертифи состоверения т безопасност	ают определит « HTML, Выбер «аты) или сертифика ъ ваших элект	гь порядок ите зону б	запуска сц езопасності На Безоп гся докумеї анзакций.	енариев и активного и Internet Explorer. астройки зоны асность вложений тами, которые
Зоны безопас содержимого Зона: Э ифровые удостовере Цифровые уд обеспечиваю	ного ности позвол: в сообщения: Интернет ния (сертифи состоверения т безопасност Импорт/экспо	ают определит « HTML. Выбер «аты) или сертифика ъ ваших элект рт удостовере	гь порядок ите зону б • • • • • • • • • • • • • • • • • • •	запуска си езопасності На Безоп гся докумен анзакций. Получи	енариев и активного и Internet Explorer. астройки зоны асность вложений нтами, которые нть удостоверение
Зоны безопас содержимого Зона: э ифровые удостовере ифровые удостовере обеспечиваю	ного ности позволя в сообщения Интернет ния (сертифия состоверения т безопасност Импорт/экспо	ают определит « HTML. Выбер «аты) или сертифика ъ ваших элект рт удостовере	гь порядок ите зону б ты являют ронных тр жия	запуска си езопасності На Безоп гся докумен анзакций. Получн	енариев и активного и Internet Explorer. астройки зоны асность вложений птами, которые пть удостоверение

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**.

Параметры сообщения		<u>? ×</u>
а Настройка сообщения Важность: Обычная Поиетка: Обычное Параметры голосования и отслеживания	Безопасность Башифровать сообщение и вло Ф Добавить цифровую подпись и	эжения к исходящему сообщени <u>ю</u>
Кнопки голосовани <u>я</u> : Уведомить о доставке этого о Уведомить о про <u>ч</u> тении этого	сообщения о сообщения	
Параметры отправки Одправлять ответы: После отправки сохранить в:	Отправленные	Выбор имен Об <u>з</u> ор
Не доставлять до: Не действительно после:	▼ ▼	
Кате <u>г</u> ории		Закрыть

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

Файл Правка Вид	, Вст <u>а</u> вка Фор <u>м</u> ат	Сервис Действия	<u>С</u> правка	
🖃 Отправить	X 🖻 🛍 🤻	🕈 📄 Параметры	≫ ∫ Arial	- ×
Komy I somebod	v			
Konug				
Тема <u>:</u> test				
Тема <u>:</u> test				
Тема <u>:</u> test				<u> </u>

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

Microsoft Outlook				×
Данное сообщение невозможно защит почты не совпадает с адресом сертиф сообщение?	ить, используя выбраннук иката, либо возникли друг	о настройку бе гие трудности	зопасности. Возможно адрес вашей электронн с сертификатом. Послать незащищенное	юй
	Да	Нет		

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.

💶 Mailtest - Контакт	<u>_ ×</u>
Файл Правка Вид Вставка Формат Сервис Действия	<u>С</u> правка
🔚 Сохранить и закр <u>ы</u> ть 🔚 🎒 🕕 🔻 伦 🔁 ≫ 🗸	* • • • •
Общие Подробности Действия Сертификаты	Все поля
При отправке данному контакту шифрованного сообщения бу из этих сертификатов. Вы можете получить сертификат, пол цифровой подписью от данного контакта или импортируя его Сертификаты (цифровые подписи):	дет использоваться один учая сообщение с файл сертификатов.
imailtest(По умолчанию)	Свойс <u>т</u> ва
	По умо <u>л</u> чанию
	<u>И</u> мпорт
	Vannum

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:

N=mail	test; C=RU; E=mailtest@cryptopro.ru	_
Лод	пись: достоверна	
~	После подписи сообщения его содержимое не изменилось	
~	Сертификат не отозван	
~	Срок действия сертификата не истек	
~	Сертификат достоверен	
~	Сертификат достоверен	

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



Нажмите кнопку Сведения для просмотра сведений о сертификате:

бщени I=mailt	ие с цифровой подписью от: test; C=RU; E=mailtest@cryptopro.ru	
Подг	пись: недостоверна	
1	После подписи сообщения его содержимое не изменилось	
	Сертификат отозван	
1	Срок действия сертификата не истек	
~	Сертификат достоверен	

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.

 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.

 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**.

Установки S/MIME (mailte	st@cryptopro.i	າບ)	
Формат сообщения:	S/MIME		
 Настройка безопаснос Настройка по умол 	ти по умолчані пчанию для во	ию для этого ф ех сообщений	ормата
Метки безопасности	Создать	Удалить	Пароль
гификаты и алгоритмы			
Сертификат подписи:	mailtest		Выбрат
Алгоритм хеширования:		~	
Сертификат шифрования:	mailtest		Выбраты
опсорити цифрования		-	

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.

		Настройка почты	Сооб	щение	Орфография
Безопас	ность	Дополни	тельно		Представители
зопасность з	лектронно	й почты			
a Fu	ифровать (содержимое и вложени	я исходящих	сообщени	й
🔽 Гд	обавлять ц	ифровую подпись к ис	ходящим сооб	бщениям	
⊽ 0	тправлять	подписанные сообщен	ия открытым	текстом	
Гу	зедомлять	о проверке безопаснос	ти всех подп	исанных со	робщений S/MIME
По ум	олчанию:	Установки S/MIME (n	nailtest@crypt	opro.ru)	💌 Параметры
зопасность о Зоны содер	одержимог безопасною жимого в с	о сти позволяют опреде. сообщениях HTML, Выб	пить порядок іерите зону бе	запуска сі езопасност	ценариев и активного ги Internet Explorer,
зопасность с Зоны содеј Зона:	одержимог безопаснос жимого в с	о сти позволяют опреде: сообщениях НТМL, Выб раниченные узлы	пить порядок іерите зону бе	запуска сі езопасност Н	ценариев и активного ги Internet Explorer. Іастройки зоны
зопасность (Зоны содер Зона:	одержимог безопаснос жимого в с	о сти позволяют определ сообщениях НТМL. Выб раниченные узлы	пить порядок іерите зону бе	запуска сі езопасност Н	ценариев и активного ги Internet Explorer, Іастройки зоны
зопасность с Зоны содеј Зона:	одержимог безопаснос жимого в с Ог Стоверения	о сти позволяют определ сообщениях НТМL, Выб раниченные узлы а (сертификаты)	пить порядок іерите зону бе	запуска сі езопасност Н	ценариев и активного ги Internet Explorer, астройки зоны
зопасность о Зоны содеј Зона фровые удо Цифр обесг	одержимог безопасно жимого в с ООО ОГ стоверения овые удост ечивают б	о сти позволяют опреде сообщениях НТМL. Выб раниченные узлы я (сертификаты) товерения или сертифи езопасность ваших эле	лить порядок ерите зону бо • • • • икаты являют • • жтронных тро	запуска сі взопасност Н гся докуме анзакций.	ценариев и активного ги Internet Explorer. астройки зоны ентами, которые
зопасность о Зоны содеј Зона: фровые удо Цифр	одержимог безопасно эжимого в с Обо Ог стоверения овые удост іечивают б Им	о сти позволяют определ сообщениях НТМL. Выб раниченные узлы я (сертификаты) товерения или сертифи езопасность ваших эле порт/экспорт удостове	пить порядок іерите зону ба т т каты являют жтронных тр врений	запуска сі езопасност Н пся докуме анзакций. Получ	ценариев и активного ги Internet Explorer. астройки зоны энтами, которые иить удостоверение

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**.

Параметры сообщения	? 🛛
Настройка сообщения Безопасность Важность: Обычная Пометка: Обычное Параметры голосования и отслеживания	пасности сообщения.
 Свойства безопасности Шифровать содержимое и вложения сообщений Добавить в сообщение цифровую подпись Добавить в сообщение цифровую подпись Не шифровать подпись сообщения Уведомить о проверке безопасности этого сообщения Параметры безопасности Настройка безопасности: 	Выбор имен Обзор
Классификация: Конфиденциальности:	 <l< td=""></l<>
ОК Отмена	ці й

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

😼 test - Coo	бщение - Microsof	t Word						
Файл Прав	жа <u>В</u> ид Вст <u>а</u> вка	Фор <u>м</u> ат	Сервис	<u>Т</u> аблиц	а <u>О</u> кно	<u>С</u> правка		×
🗗 🖨 日	8 5 6 7	h 🖪	K) +	۵. 🗖	100% -	? 🐥 Arial		• *
🛛 🖃 Отправит	<u>ь</u> Учетные записи •	0 - 0	0 🕵	! +	۳ 🗈 г	адаметры 🔻	HTML	-
🕼 Кому	somebody				See 1 Sector			
🕼 Копия								
к 9 Тема:	test							
something								
	1							J.
Стр. і	9азд	Ha	CT	Кол	ЗАП	ИСПР ВДЛ	ЗАМ англий	ский

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

тедо	пустимый сертификат		
	Недопустимый сертификат н подписать или зашифровать	е позволил Microsoft сообщение.	Outlook
-		016	1

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.

🖭 mailtest - Контакт	
🛛 Файл Правка Вид Вставка Формат Сервис Действия Справка	
🔚 Сохранить и закр <u>ы</u> ть 🛃 🎒 🕴 🤻 🔗 🐁 📎 • 🔺 • • • •	
Общие Подробности Действия Сертификаты Все поля	
При отправке данному контакту шифрованного сообщения будет использоваться од из этих сертификатов. Вы можете получить сертификат, получая сообщение с цифровой подписью от данного контакта или импортируя его файл сертификатов. Сертификаты (цифровые подписи):	цин —
mailtest(По умолчанию)	Свойства
	По умодчанию
	Импорт
	Экспорт
	<u>У</u> далить

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 Шифровать содержимое и вложения сообщений. После того, как сообщение подготовлено к отправке, нажмите кнопку **Отправить**. При

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

Проверка сертификата на отзыв

Для контроля проверки сертификатов на отзыв выполните следующие действия. Откройте

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

Свойст	ва безопасности о	сообщения	? 🔀
k 1	'ема: test		
Сообщен Каждый	ния могут содержать і і слой допускает нали	шифрование и слои ци ичие нескольких подпи	фровых подписей. исей.
Тем	a: test Уровень цифровых по	дписей	
L	🗸 Подписано: zhenya	a@cryptopro.ru	
Описани	e,		
ОК: под	е. писанное сообщение.		
Bcer,	да предупреждать об	ошибках защищенной	і́ почты.
	Изменить доверие	Подробности	Закрыть

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

0	1			
	Тема: RE:1ef			
Сообш Кажді	цения могут содержать и ый слой допускает нали	цифрование и слои ци чие нескольких подп	іфровых подпі исей.	исей
V Te	ема: RE: 1ef			
	Уровень цифровых по,	дписей		
	— <u> П</u> одписано: mailtes	t@cryptopro.ru		
Описа	ние:			
Эписа	ние: зляется сертификат нед	оступным, ливо срок	его деиствия	~
Описа Яв ИС	ние: зляется сертификат нед стек,	оступным, ливо срок	его деиствия	^
Описа Яв ИС ПОДПИ 2001/1	ние: зляется сертификат нед стек. исано mailtest@cryptopro. ГОСТ Р 34.11-94 в 16:52	оступным, лиоо срок .ru с помощью ГОСТ F .22 19.03.2007.	его деиствия 9 34.10-	
Описа яв подпи 2001/I У Все	ние: вляется сертификат нед стек. ссано mailtest@cryptopro. ГОСТ Р 34.11-94 в 16:52: егда предупреждать об	оступным, либо срок .ru с помощью ГОСТ F :22 19.03.2007. ошибках зашищенної	его деиствия 9 34,10- й почты.	
Описа яв ис подпи 2001/I ⊽ Все	ние: вляется сертификат нед стек. исано mailtest@cryptopro. ГОСТ Р 34.11-94 в 16:52: егда предупреждать об	оступным, либо срок .ru с помощью ГОСТ F :22 19.03.2007. ошибках защищенної	его деиствия 9 34.10- й почты.	

Если же СОС обновлен, то при открытии письма, подписанного отозванным сертификатом,

появится следующее предупреждение:



Нажмите кнопку Сведения для просмотра сведений о сертификате:

Тема: test Сообщения могут содержать и Каждый спой вописсает напи	иифрование и слои цио	
 Гообщения могут содержать и Каждый слой допускает нали	инфрование и слои цио	
каждый слой допускает нали	чие нескольких подпи	рровых подписеи сей.
😲 Тема: test		
Уровень цифровых по,	дписей	
— Подписано: mailtes	t@cryptopro.ru	
Описание:		
0		
ошиока;	ания данной подписи (сертификат 🤗
• ИСПОЛЬЗОВАННЫИ // 09 СОЗЛ.		and the second s
 использованный для созд находится в допустимом с 	писке отмененных сер	тификатов. 🚃
•использованный для созд находится в допустимом с поличено mailtest@cryptopro	писке отмененных сер ин с помощью ГОСТ Р	тификатов. 👱
 использованный для созд находится в допустимом с по врисачо mailtest@cryptopro ✓ Всегда предупреждать об 	писке отмененных сер и с вомошью ГОСТ Р ошибках защищенной	тификатов. 👱 за 10. 🖻

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.
- 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.
- 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.

Изменение настройки бе	зопасности	
Настройка безопасности —— Имя конфигурации:		
Установки S/MIME (zhenya	@cryptopro.ru)	~
Формат криптографии:	S/MIME	*
 Настройка безопасности Настройка по умолча Метки безопасности 	по умолчанию для этого формата анию для всех сообщений <u>С</u> оздать Удалит <u>ь</u>	Пароль
Сертификаты и алгоритмы		
Сертификат подписи:	test	Выбрать
<u>А</u> лгоритм хеширования:	GOST R 34.11-94	
Сертификат шифрования:	test	Выбрать
Адгоритм шифрования:	GOST 28147-89	
🗹 Передавать сертификат	ы с сообщением	
	ОК	Отмена

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.

Центр управления безопасностью	
Центр управления безопасностью Надежные издатели Надстройки Параметры конфиденциальности Защита электронной почты Обработка вложений Автоматическая загрузка Безопасность макросов Программный доступ	Шифрованная электронная почта Шифровать содержимое и вложения исходящих сообщений Добавлять цифровую подпись к исходящих сообщениям Добавлять подписанные сообщения открытым текстом Даправивать уведомление S/MIME для всех подписанных сообщений S/MIME По у <u>м</u> олчанию: Установки S/MIME (zhenya@cryptopro.ru) Параметр <u>ы</u> Цифровые удостоверения (сертификаты) Цифровые удостоверения или сертификаты являются документами, которые обеспеч безопасность ваших электронных транзакций. Опубдиковать в глобальном списке адресов Импорт/экспорт Долучить Читать как обычный текст Читать обычные письма как обычный текст Читать письма с цифровой подписью как обычный текст Разрешить макросы в папках совместного доступа Разрешить макросы в общих папках
	ОК Отмена

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.

	044	🗧 🗧 🗧	Сообще	ние (HTML)			- = X
C006	щение В	ставка Параметрь	ι Φο	рмат текста			0
Вставить	Calibri (Осн Ж К Ц Ф - <u>А</u> -	o • 11 • A Ă E • E • ₽ ₽ E = ■	Ш Имена *		к исполнению *		АВС Орфография
Буфер об 🖻	Осн	овной текст 🛛 🖓		Вклю 🖼	Параметры	E)	Правописание
	Кому <u></u> Копи <u>я</u> Т <u>е</u> ма:	mailtest@cryptopro.r	U;				
	вло <u>ж</u> ение:	smime.pdf (561 K6a	<u>йт)</u>				
test							

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

Недол	пустимый сертификат	
	Недопустимый сертификат не позволяет Microsoft Office C подписать или зашифровать сообщение.	outlook
	Изменить параметры безопасности О	

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 Сертификаты и убедитесь в наличии сертификата отправителя.

000	i 4 4) =	mailtest - Контак	т		- = x
Контакт	Вставка Формат текста				۲
Сохранить и закрыть Х	 Общие Сертификаты Подробности Бсе поля Действия 	🔄 Электронная почта 🍕 🙀 Собрание 🥥 & Вызов т 🔗	 Рисунок * Визитная карточка К исполнению * 	АВС Орфография т	Д) Заметки о контакте
Действия	Показать	Связь	Параметры	Правописание	OneNote
импорте его файла Сер <u>т</u> ификаты (циф mailtest(По умолча	а сертификатов. ровые подписи): інию)				ю <u>й</u> ства МО <u>Л</u> ЧаНИЮ МПОрт КСПОрт (далить

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.

Возникли неполадки шифрования этого сообщения в Microsoft Office Outlook, вызванные тем, что следующие получатели не имеют сертификатов, имеют недопустимые сертификаты или не поддерживают данное шифрование:
mailtest@cryptopro.ru
Сообщение может быть зашифровано и отправлено, но указанные получатели, по-видимому, не смогут его прочитать. <u>Не шифровать сообщение</u> <u>Продолжить</u> Отмена

Проверка сертификата на отзыв

Для контроля проверки сертификатов на отзыв выполните следующие действия. Откройте

полученное подписанное письмо. Нажмите кнопку

🙎 - признак подписанного сообщения.

Тема:	test
OT:	mailtest
Подписано:	mailtest@cryptopro.ru
8	Цифровая подпись сообщения является действительной и доверенной.
	Для просмотра сведений о сертификате, применяемом в цифровой подписи сообщения, нажмите кнопку "Сведения".
	Сведения
ППредупре	ждать об ошибках в подписанных сообщениях до открытия.

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

Свойства безопасности сообщения
Ender Tema: 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
<u>О</u> писание:
ОК: подписанное сообщение.
Следующие кнопки позволяют просмотреть дополнительные сведения или внести
изменения в выбранный слой:
Изменить доверие Подробности Доверие к центру сертификации
Предупреждать об ошибках в подписанных сообщениях

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.

Свойства безопасности сообщения
Tema: RE: 1ef
 Сообщения могут шифроваться и содержать слои цифровых подписей. Каждый слой допускает наличие нескольких подписей.
Слои безопасности
Выберите слой для просмотра его описания.
Подписано: mailtest@cryptopro.ru Описание:
Предупреждение: Список отмененных сертификатов, необходимый для проверки сертификата подписи, недоступен, либо срок его действия истек.
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

Если же СОС обновлен, а письмо подписано отозванным сертификатом, то при нажатии

кнопки 🕐 появится следующее предупреждение:

Тема:	test
От:	mailtest
Подписано:	mailtest@cryptopro.ru
	Цифровая подпись сообщения является недействительной или не доверенной.
	Для просмотра сведений о сертификате, применяемом в цифровой подписи сообщения, нажмите кнопку "Сведения".
	Сведения
Предупре	ждать об ошибках в подписанных сообщениях до открытия.

Нажмите кнопку Сведения для просмотра сведений о сертификате:

Свойства безопасности сообщения
ина: test
сообщения могут шифроваться и содержать слои цифровых подписей. Каждый слой допускает наличие нескольких подписей.
Слои безопасности
Выберите слой для просмотра его описания.
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.

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).

SweAs		
Sale Attachesents	Account Information	112 A.
0	POP/SMTP •	
pen	🕸 Add Account	
int In	Account Settings Modify settings for this account and configure additional	
Options	Account Settings -	
to:		
	Chanop Tools -	
	Rules and Alerts Use And Alerts to help organize your incoming e-mail messages, and receive updates when items are added, changed, or removed.	

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).

ust Center	8
Trusted Publishers DEP Settings	Encrypted e-mail
Privacy Options E-mail Security Attachment Handling Automatic Download Macro Settings Programmatic Access	
	Read all digitally signed <u>m</u> ail in plain text Script in Folders Allow script in shared folders Allow script in Public <u>Fo</u> lders
	OK

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).

Security Settings Name:	s			
	0			5
Cryptography Format:	5/M1	IME		
Default Security Setti	ng fa	or this cryptog	raphic message f	ormat
Default Security Setti	ng fa	or all cryptogra	aphic <u>m</u> essages	
Security Labels	ו	New	Delete	Password
Certificates and Algorith	ms			
Signing Certificate:				Choose
Hash Algorithm:	_			
Encryption Certificate:				Choose
Encryption Algorithm:			÷	

Окно выбора сертификата:

	ификат.			
Кому выдан	Кем выдан	Назначения	Понятное	Срок дейс
test	Test Cente	Защищенн	Отсутствует	02.07.2011

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

Security Settings Name:				
My				
		-		
Cryptography Format: S	/MIME	-		
V Default Security Setting	for this cryptographic message form	nat		
Default Security Setting	for all cryptographic messages			
Security Labels	New Delete	Password		
Certificates and Algorithms	,			
Signing Certificate:	ist	Choose		
Hash Algorithm:	OST R 34.11-94 👻	N	licrosoft Outlook	
Encryption Certificate:	st	Choose	Outlook o	annot save this Security Setting without a Name. If you
Encryption Algorithm: G	OST 28147-89 🔹		Continue,	your changes will be lost. Do you want to continue?

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**).

	• • • •	⊮ ∓	test -	Message (HTM	L)		-	• 3
	Message	Insert	Options	Format Text	Review			۵ 🕜
Q		Tabla			Hyperlink 🏑	- Text	Ω	
File	Item 🔉	Tables	Art Illustra	tions	Links	¥	- The symbols	
Attach I Attach	ile a file to this i	tem.	pro.ru;					
Send	Subject:	test						
test								
0	See more abo	ut: movcha	n@cryptopro.ru					2.

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

	Message	Insert Option	s Format Tex	t Review		۵ 🕜
hemes	Bcc From Show Fields	Permission 🔛 Sign Permission	Tracking Save	Sent More Options	ivery plies To	
	To	movchan@cryptopro.r	<u>'u;</u>			
*	Cc					
Jena	Subject:	test				
	Attached:	Cryx Antelope.jp	g (291 KB)			
test						

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** ^{Сентисатес} (Сертификаты) и убедитесь в наличии сертификата отправителя.

2



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).

-	Bcc	Insert Options	Form	Balliest Review	livery	64	
hemes	From	Permission 🚂 Sign	Tracking	Save Sent Item To *	plies To		
	Show Fields	Permission		More Options	G		_
	То	movchan@cryptopro.n	<u>u;</u>				
Send	Cc						
Jenia	Subject:	test					
	Attached:	Cryx Antelope.jpc	(291 KB)				
test							

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

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

A	Microsoft Outlook had problems encrypting this message because the following recipients had missing or invalid certificates, or conflicting or unsupported encryption capabilities:
	Наталья
	Continue will encrypt and send the message but the listed recipients may not be able to read it.

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.

	operties		— ×
Subject: test			
Messages may contain signature layer may co Security Layers	encryption and ontain multiple sig	digital signature li natures.	ayers. Each digital
Select a layer below to	view its descript	ion.	
 Subject: test Digital Signation 	urelaver		
Signer: m	owchan@gryptor	TO TU	
Description:			
<u>D</u> escription: OK: Signed by movcha	an@cryptopro.ru	using FOCT P 34	. 10-2001/FOCT P
Description: OK: Signed by movcha 34.11-94 at 12:42:47	an@cryptopro.ru 06.07.2010.	using FOCT P 34	5. 10-200 1/FOCT P
<u>D</u> escription: OK: Signed by movcha 34.11-94 at 12:42:47	an@cryptopro.ru 06.07.2010.	using FOCT P 34	8. 10-200 1/FOCT P
<u>D</u> escription: OK: Signed by movcha 34, 11-94 at 12:42:47	an@cryptopro.ru 06.07.2010.	using FOCT P 34	1. 10-200 1/FOCT P
<u>D</u> escription: OK: Signed by movcha 34.11-94 at 12:42:47 Click any of the followi	an@cryptopro.ru 06.07.2010. ng buttons to vie	using FOCT P 34	i. 10-2001/FOCT P on about or make
<u>D</u> escription: OK: Signed by movcha 34. 11-94 at 12:42:47 Click any of the followin changes to the selecte	an@cryptopro.ru 06.07.2010. ng buttons to vie d layer:	using FOCT P 34	6. 10-200 1/FOCT P on about or make
Description: OK: Signed by movcha 34. 11-94 at 12:42:47 Click any of the followin changes to the selecte Edit Trust	an@cryptopro.ru 06.07.2010. ng buttons to vie kd layer: View Details	using FOCT P 34 w more informati	1. 10-200 1/FOCT P on about or make rate Authority
Description: OK: Signed by movcha 34. 11-94 at 12:42:47 Click any of the followi changes to the selecte Edit Trust	an@cryptopro.ru 06.07.2010. ng buttons to vie kd layer: <u>Vi</u> ew Details	using FOCT P 34 w more informati	a. 10-200 1/FOCT P on about or make nate Authority

Если же СОС обновлен, а письмо подписано отозванным сертификатом, то при нажатии

кнопки 🥙 появится следующее предупреждение:

Digital Si	gnature: Invalid 🛛 📈
Subject:	0T03B
From:	Наталья
Signed By	: movchan@cryptopro.ru
Q	The digital signature on this message is Invalid or Not Trusted.
~~	For more information about the certificate used to digitally sign the message, click Details.
	Details
🖳 <u>W</u> arn	me about errors in digitally signed e-mail before message opens.
	Close
	Close

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

Message Security F	Properties		
Subject: or	тозв		
Messages may cont signature layer may Security Layers Select a layer below	ain encryption and d contain multiple sign to view its descriptio	igital signature layers. Eacl atures. on.	h digital
Subject: otose Digital Signer	3 nature Layer : movchan@cryptopi	ro.ru	
Description:			
Description: Error: The certificate used Revocation List.	d to create this signa	ture is on a valid Certificat	е _ ~
Description: Error: The certificate used Revocation List. Singed by mouchan Cick any of the follo changes to the select	d to create this signa decreate on using buttons to view cted layer:	ture is on a valid Certificat	e TD rrmake
Description: Error: The certificate used Revocation List. Signed by mouchan Cick any of the follo changes to the select Edit Trust	d to create this signa decuntors or unicod wing buttons to view cted layer: <u>Vi</u> ew Details	ture is on a valid Certificat FOCT P 34 10-2001 /FOCT v more information about o	e TD Tr make

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).

	Параметры Outlook ? 🗙			
Общие Почта	Обеспечение безопасности документов, а также защиты и работоспособности компьютера			
Календарь	Защита конфиденциальности			
Люди Задачи	Корпорация Майкрософт заботится о вашей конфиденциальности. Чтобы получить дополнительные сведения о том, как Microsoft Outlook помогает сохранить конфиденциальность, см. заявление о конфиденциальности.			
Поиск	Заявление о конфиденциальности Microsoft Outlook			
Язык	Заявление о конфиденциальности Office.com			
Дополнительно	Программа улучшения качества программного обеспечения			
Настроить ленту	<u>Заявление о конфиденциальности для средства "Отправить улыбку" для отзывов о Microsoft</u> <u>Office</u>			
Панель быстрого доступа	Безопасность и другие сведения			
Надстройки	Дополнительные сведения о защите конфиденциальности и безопасности приведены на сайте			
Центр управления безопасностью	Office.com.			
	Создание защищенных информационных систем			
	Центр управления безопасностью Microsoft Outlook			
	Центр управления безопасностью содержит параметры безопасности и конфиденциальности. Эти параметры помогают обеспечить безопасность компьютера. Изменять их не рекомендуется.			
J	ОК. Отмена			

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

	Центр управления безопасностью	? ×
Надежные издатели Параметры конфиденциальности Защита электронной почты Обработка вложений Автоматическая загрузка Параметры макросов Программный доступ	Шифрованная электронная почта Шифровать содержимое и вложения исходящих сообщений Добавлять цифровую подпись к исходящим сообщениям Опправлять подпиданные сообщения открытым текстом Запрашивать уведомление S/MIME для всех подписанных сообщений S/MIME По у <u>м</u> олчанию: Установки S/MIME (Чифровые удостоверения (сертификаты) Цифровые удостоверения или сертификаты являются документами, которые обеспечивают безо ваших электронных транзакций. Опубдиковать в глобальном списке адресов Импорт/ <u>э</u> кспорт Читать как обычный текст Читать письма как обычный текст Читать письма с цифровой подписью как обычный текст Разрешить сценарии в общих папках Разрешить сценарии в общедоступных папках	пасность ение
	ОК	Отмена

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**).
стройка безопасности Имя конфигурации: Установки S/MIME () Формат криптографии: S/MIME Настройка безопасности по умолчанию для этого формата	~
имя конфигурации: Установки S/MIME () Формат криптографии: S/MIME Настройка безопасности по умолчанию для этого формата	•
Формат криптографии: S/MIME Настройка безопасности по умолчанию для этого формата	~
Формат криптографии: S/MIME	~
Настройка безопасности по умолчанию для этого формата	
Настройка по умолчанию для всех сообщений	
Метки безопасности Создать Удалить	
Сертификаты и алгоритмы	
Сертификат подписи: Выбрат	ъ
Алгоритм хеширования:	
Сертификат шифрования: Выбрат	ъ
Флгоритм шифрования: 🗸 🗸	
🖌 Передавать сертификаты с сообщением	
ОК Отмен	ia

Окно выбора сертификата:

	Безопасность Windows
Выбор сер	отификата
	test Издатель: test_rut Действителен с: 22.05.2013 по 01.05.2030
	ОК Отмена

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**).

=*	. 5	Ì	ή ψ	Ŧ			Тест - Сообщение (HTN	/IL)		?	1	-	×
ФАЙ	n co	ООБЩЕН	НИЕ	ВСТАВКА	ΠΑΡΑΝ	ІЕТРЫ	ΦΟΡΜΑΤ ΤΕΚCTA	РЕЦЕНЗИРОВАНИЕ					
Гемы Темы		СК От	Разреш	🗧 🔂 Ши ^{јения} 🎗 Под	фровать аписать	₩Кн Уве Уве	опки голосования * едомить о доставке едомить о прочтении	Сохранить отправленны элемент *	🚑 Задержі 🤹 Направл й	са до	ответи	И Ы В	
	Показат	гь поля		Разрешение		0	Отслеживание 🗔	Дополнительн	ые параметрь	ł		E.	^
₹[Отпр	авит <u>ь</u>	Ко <u>м</u> Коп	<u>ı</u> у и <u>я</u>	testmail@ma	il.ru								
		<u>Т</u> ема		Тест									
		Вло <u>ж</u> е	ние	Текстоо	k.docx (45)	<u>(байт)</u>							
test	:												

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.

Недопустимый сертификат	
Приложению Microsoft Outlook не удается подписать или зашифровать сос из-за отсутствия сертификатов, которые могут быть использованы для отпр адреса ". Получите новое цифровое удостоверение учетной записи либо нажмите кнопку "Учетные записи", чтобы отправить с	общение оавки с для данной сообщение
помощью учетнои записи, для которои имеется сертификат.	

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 🤗 Сертификаты (Certificates).

≝ 🗄 S ở ↑ ♦ ∓	corptest - Контакт	? 🛧	- 0	×
ФАЙЛ КОНТАКТ ВСТАВ	КА ФОРМАТ ТЕКСТА РЕЦЕНЗИРОВАНИЕ			
Сохранить и закрыть Сохранить и закрыть	и создать * Править по электронной почте Править почте Править почте Править почте П	Масшта	ю	
Действия	Связь Обновить	Масшта	6	~
Полное имя согр Организация Должность Хранить как согр	ttest Общие Все поля Показ			
Интернет				
📑 Эл. почта 👻 <u>согр</u>	ytest@cryptopro.ru			
Отображать как согр	Заметки			
Веб-страница				
Мгн. сообщения				
Телефоны				
Рабочий 🝷				
Домашний 👻				
Факс (рабочий) 👻				
Мобильный 🝷				
Адреса				
Рабочий Считать почтовым адресом	Карта			
1 Подробнее о corptest.			2	^

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

🖴 🖬 🕤 🗇 🕈 🖌 🖛	corptest	- Контакт		? 🗹 – 🗆 🗙
ФАЙЛ КОНТАКТ ВСТАВКА ФОРМ	ИАТ ТЕКСТА	РЕЦЕНЗИРОВАНИЕ		
Сохранить и создать Удалить и закрыть Удалить Сохранить и создать Сохранить и создать Опереслать Сохранить и создать	Показ Связь	Имена Параметры	Геги Обновить Обновить	С Масштаб Масштаб
При отправке шифрованного сообщения данно из этих сертификатов. Сертификаты добавляются данного контакта, либо при импорте его файла	му контакту буде а либо при получ сертификатов.	т использоваться один чении сообщения с ци	н фровой подписью с	т
Сертификаты (цифровые удостоверения)				
Иванов Иван Иванович(По умолчанию) corptest				Свойства
				По умолчанию
				Импорт
				Экспорт
				Удалить
Togpobhee o corptest.				<u> </u>

После этого нажмите на кнопку Сохранить и Закрыть Сохранить (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).

ФАЙЛ	о 🖸 🛧 🗸	∓ ВСТАВКА ПАР	test - Сообщение АМЕТРЫ ФОІ	(HTML) PMAT TEKCTA PE	? 🗹 🗕	□ ×
Темы • Показ	СК От Разрец ать п	ени: 2 Подписать Разрешение	(т т т т т т т т т т т т т	Сохранить отправле элемент + Дополнит	فَي Задержка доставки پ الما الما الماني الماني عمر الماني ماني ماني ماني م ماني ماني ماني ماني ماني ماني ماني ماني	л ы В Га 🔺
5 - 8	Кому	korolev@cryptopro				
Отправить	Копия			\$		
ompatinte	Тема	test				
test						

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

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

	Неполадки шиф	рования	×
<u>^</u>	Приложению Microsoft Outlook н сообщение, поскольку следующие сертификатов, имеют недействит поддерживают данное шифрован	е удалось зашифро получатели не им ельные сертифика ие:	вать еют гы или не
	corptest		
	Сообщение может быть зашифро	вано и отправлен	о, но

Проверка сертификата на отзыв

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

ест	
anagnauuuuvopa Engua Canraapua	
µфровая подпись сообщения является ействительной и доверенной.	
(ля просмотра сведений о сертификате, ірименяемом в цифровой подписи сообщения, іажмите кнопку ''Сведения''.	
Сведения	
дать об ошибках в подписанных сообщениях до открыти	я.
Закрыть]
	цифровая подпись сообщения является ействительной и доверенной. Иля просмотра сведений о сертификате, ирименяемом в цифровой подписи сообщения, нажмите кнопку "Сведения". Сведения дать об ошибках в подписанных сообщениях до открыти Закрыть

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.

	ойства безопасно	сти сообщения	
Тема: Тест			
			รอมี ห้วาหลายมี
лой допускает наличи	е нескольких подписе	оюй цифровых подпи й.	сеи, каждыи
Слои безопасности			
Зыберите сло <mark>й</mark> для про	смотра его описания.	l	
🗸 Тема: Тест			
Уровень цифро	овых подписей		
Подписано:			
Эписание:			
Описание: ОК: подписанное сооб	шение.		
)писание: ОК: подписанное сооб	щение.		
Описание: ОК: подписанное сооб	щение.		
Описание: ОК: подписанное сооб Следующие кнопки поз	щение. воляют просмотреть /	10ПОЛНИТЕЛЬНЫЕ СВЕДЕН	ния или внести
Описание: ОК: подписанное сооб Гледующие кнопки поз ізменения в выбранны	щение. воляют просмотреть / й слой:	цополнительные сведен	ния или внести
Описание: ОК: подписанное сооб Следующие кнопки поз ізменения в выбранны Изменить доверие	щение. воляют просмотреть / й слой: Подробности	ополнительные сведен Доверие к центру се	ния или внести
Описание: ОК: подписанное сооб Гледующие кнопки поз ізменения в выбранны Изменить доверие…	щение. воляют просмотреть / й слой: Подробности	цополнительные сведен Доверие к центру се	ния или внести :ртификации

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.

	йства безопасно	сти сообщения	×
🔬 Тема: тест			
Сообщения могут шифро слой допускает наличие	оваться и содержать нескольких подписе	слои цифровых подписей. Каждый 1.	
Слои безопасности			
Ф Тема: тест Уровень цифров Подписано:	ных подписей		
Описание:			
Описание: Ошибка: Использованный для соз допустимом списке отме	дания <mark>д</mark> анной подпи ненных сертификато	іси сертификат находится в рв. 	< >
Описание: Ошибка: Использованный для соз допустимом списке отме Полямсано Следующие кнопки позво изменения в выбранный	дания данной подпи ненных сертификато оляют просмотреть д слой:	иси сертификат находится в рв. - ГОСТ в 34 10 2001/ГОСТ в 34 11 04 - ополнительные сведения или внес	< ~ У И
Описание: Ошибка: Использованный для соз допустимом списке отме Полямсано Следующие кнопки позво изменения в выбранный Изменить доверие	дания данной подпи ненных сертификато оляют просмотреть д слой: Подробности	иси сертификат находится в ов. опост в 34 10 2001/гост в 34 11 94 ополнительные сведения или внес Доверие к центру сертификации	л ч ч