# Руководство пользователя по использованию электронной цифровой подписи

### Содержание

I. Инструкция по использованию электронной цифровой подписи в Outlook Express2
1. Отправка подписанных сообщений2
2. Получение сертификата открытого ключа абонента для шифрования сообщений .4
3. Отправка шифрованных сообщений5
4. Проверка сертификата на отзыв6
II. Инструкция по использованию электронной цифровой подписи в Microsoft Office
Outlook 2003
1. Отправка подписанных сообщений8
2. Получение сертификата открытого ключа абонента для шифрования сообщений9
3. Отправка шифрованных сообщений10
4. Проверка сертификата на отзыв11
III. Инструкция по использованию электронной цифровой подписи в Microsoft Office
Outlook 200713
1. Отправка подписанных сообщений13
2. Получение сертификата открытого ключа абонента для шифрования сообщений14
3. Отправка шифрованных сообщений15
4. Проверка сертификата на отзыв15
IV. Инструкция по использованию электронной цифровой подписи в Microsoft Office 2003
1. Порядок подписания файлов в программных продуктах Microsoft Office ( на примере
продукта Microsoft Word)18
V. Инструкция по использованию электронной цифровой подписи в Microsoft Office 2007
1. Порядок подписания файлов в программных продуктах Microsoft Office
VI. Требования к помещениям, где установлены СКЗИ и хранятся ключевые документы к
ним

#### I. Инструкция по использованию электронной цифровой подписи в Outlook Express

1. Отправка подписанных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку создать ... 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 <sup>вложить</sup> Вложить. Для отправки сообщения в Подписать Подписать. Она подписанном виде проверьте состояние кнопки должна быть нажата и должен быть виден признак подписанного сообщения в правой части экрана. (Рисунок 1) Рисунок 1. 12 test Файл Правка Вид Вставка Формат Сервис Сообщение Справка ٩, 5 ABC Ж =0 = = Отправить Вырезать Копировать Отменить Проверить Правописа... Вложить Важность Подписать Зашифров... 🛐 Кому: mailtest@cryptopro.ru 🛐 Копия: Тема: test Присоединить: 📆 smime.pdf (560 КБ) 🔍 🔜 昆 🛪 K H A. 短日健健 自主主目 — 🐁 🖬

После того, как сообщение подготовлено к отправке, нажмите кнопку

отправить Отправить. Если в ответ появится следующее предупреждение, то это означает, что сертификат был отозван. (Рисунок 2)

### Рисунок 2.

Предост	Предостережение системы безопасности						
⚠	Сертификат для данной учетной записи отозван						
	Программе Outlook Express не удалось найти действующего сэртификата на этом компьютере. Получить новый сертификат?						
	Да Отправить, не подписывая Отмена						

# 2. 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. (Рисунок 3)

				Рисунок 3.
🚔 test				
Файл Правка Ви	ид Сервис Сообщени	іе Справка		A.
<ul> <li>Ветить Ответить</li> </ul>	у у Саранија тъ Переслать Г	🍛 Іечать Уд	далить П	оредыду »
От: ла Дата: 13 Кому: ла Тема: tes Безопасность: По,	Добавить в адресну Найти Блокировать отправ Копировать	ю книгу ителя		<b>R</b>
test	Свойства			<

Для того, чтобы проверить наличие сертификата абонента в адресной

книге, нажмите на кнопку Адреса Адреса в основном меню и выберите запись с требуемым абонентом (см. Рисунок 2). Если в записи абонента отсутствует сертификат или сертификат не обновился (у абонента был старый сертификат), удалите полностью запись абонента из адресной книги и получите от него подписанное сообщение еще раз. При этом должно произойти автоматическое создание записи с сертификатом. (Рисунок 4)

#### Рисунок 4.

🍤 Адресная	книга - Ос	новное удо	стове рение			
Файл Правка	: <u>В</u> ид С <u>е</u> рви	іс <u>С</u> правка				
	<b>F</b>	X	<b>B</b>	4	<b>&amp;</b> +	
Создать	Свойства	Удалить	Поиск людей	Печать	 Действие	
06щие	контакты	Введите или	выберите из спи	иска:		
Ссновн	юе удостовер	Имя 🛆	Электр	онная почта	Служебный тел	. Домашни
		📰 mailtest	mailtest@	Deryptopro.ru		
		<.		1111		
1 объекта(-ов)						.:

#### 3. Отправка шифрованных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку

Создать ... 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

	U					
письмо, используя кнопку	Вложить	Вложить. Д	ля отпра	вки сос	общени	ЯВ
		00070000			I = 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 20000 - 20000 - 2000 - 2000 - 2000 - 2000 - 2000 - 20	в
зашифрованном виде	проверьз	те состояни	ие кно	ПКИ	L	
Зашифровать. Она должн	а быть з	нажата и дол	жен быт	ъ виде	н приз	нак
шифрованного сообщения	в г	правой части	экрана.	После	того,	как
		-		1		
сообщение подготовлено к с	этправке	, нажмите кно	ПКУ Отпра	вить От	правит	ГЬ.

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: (Рисунок 5)

	Рис	унок 5
Предос	тережение системы безопасности	×
8	Сертификат шифрования для данной учетной запи	іси отозван.
	ок	

#### 4. 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: (Рисунок 6)

Рисун	ок б
test	?×
Общие Подробно Безопасность	
Цифровая подпись	-
Подписано: mailtest@cryptopro.ru	
Содерхимое не изменено:	Дa
Подпись достоверна:	Дa
Запрос безопасного уведомления:	н/д
Проверка отзыва сертификата:	Нет
Состояние отзыва:	
Метка безопасности:	~
Шифрование	_
Содерхание и вложения зашифрованы:	Нет
Алгоритм шифрования:	Нет
<u>Просмотр сертификатов</u> Дополнительные <u>с</u> ведения.	
ОК Отм	ена

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: (Рисунок 7)

#### Рисунок 7.



А при нажатии кнопки <sup>94</sup>, в открывшемся окне во вкладке **Безопасность** будет значиться: Этот сертификат был отозван.

### II. Инструкция по использованию электронной цифровой подписи в Microsoft Office Outlook 2003

#### 1. Отправка подписанных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку Создать 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 затем кнопку Параметры безопасности, и в отображаемом диалоге установите флаг Добавить в сообщение цифровую подпись (Рисунок 8).

ойка сообщения		Безопас	ность ——					
Важность: О	бычная 🔄	<b>B</b>	Изменени	е парам	етров без	опасности	1 COC	бщения.
лометка: О	бычное 🗾		Параме	етры бе	зопасности	1		
иетры голосования	и отслеживания	a —						
Свойства безопа	асности					? 🛛		
🗖 Шифровать сод	ержимое и влож	ения сооб	щений					
🔽 Добавить в сооб	бщение цифров	ую подпис	ъ					
🔽 Не шифров	ать подпись сос	общения				H	-	Выбор имен
Уведомить	о проверке без	опасности	atoro coof	11.01.040			_	
			310/0 0000	цения		-	-	Обзор
Параметры безопас	ности		310/0 0000	цения				Обзор
Параметры безопас Настройка безопа САвто >	ности		31010 2000	цения			- 	Обзор
Параметры безопас Настройка безопа (<Авто>	ности ———		91010 C000	цения	ь параметр	<u>.</u>	- 	Обзор
Параметры безопас Настройка безопа (<Авто>	ности асности:		<u>_</u>	Ізменит	ь параметр	ЭЫ	- 	Обзор
Параметры безопас Настройка безопа (<Авто> Метка безопаснос Модуль политики	асности асности: ти 1: <			Ізменит	ь параметр Настроит	эы	- 	Обзор
Параметры безопас Настройка безопа (<Авто> Метка безопаснос Модуль политики Классификация:	асности: асности: ти 1;		<u> </u>	Ізменит	ь параметр Настроит	э эы	-	Обзор
Параметры безопас Настройка безопа (<Авто> Метка безопаснос Модуль политики Классификация: Метка	:ности асности: ти 1: <-Нет>		<u> </u>	Ізменит	ь параметр Настроит	эы	-	Обзор
Параметры безопас Настройка безопа (<Авто> Метка безопасное Модуль политики Классификация: Метка конфиденциальн	ности асности: ти 1: <het></het>			Ізменит	ь параметр Настроит	)bl	✓	Обзор

После того, как сообщение подготовлено к отправке, нажмите кнопку **Отправить** (Рисунок 9).

#### Рисунок 9.

📲 test - Coo	бщение - Microsof	t Word					
<u>Ф</u> айл Прав	ка <u>В</u> ид Вст <u>а</u> вка	Фор <u>м</u> ат С	ервис	<u>т</u> аблица <u>(</u>	<u>о</u> кно <u>С</u> прав	ка	×
i 😰 🚔 🔚 🛛	8 🔁 🎒 🕰 🖤	Pa 🛍 🕨	ဂ 🖣 🎑	100	% 🔹 🛛 💝	Arial	- »»
🖃 Отправит <u>ь</u>	₂ Учетные записи т	() <b>-</b> (2	Q, !	+ *	📰 Парамет	ры + НТ	ML -
📴 Кому	somebody						
📴 Копия							
Тема:	test						
something	1						- -
Стр. Р	азд	На	Ст	Кол	ЗАП ИСПР	ВДЛ ЗАМ	английский

Если сертификат, с помощью которого подписано сообщение, был отозван, то появится следующее предупреждение, а само сообщение не будет отправлено. (Рисунок 10)

#### Рисунок 10.



# 2. 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 электронной цифровой получения сообщения И проверки подписи добавление производится автоматическое 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 (Рисунок 11).

#### Рисунок 11.



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.

#### 3. Отправка шифрованных сообщений

Для создания и отправки шифрованного сообщения нажмите кнопку Создать 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 Вложить. Для отправки сообщения в письмо, используя кнопку 📰 Параметры... 🝷 зашифрованном виде нажмите кнопку затем кнопку Параметры безопасности, и в отображаемом диалоге установите флаг Шифровать содержимое и вложения сообщений. После того, как ⊡ отправить Отправить. сообщение подготовлено к отправке, нажмите кнопку При попытке зашифровать письмо на открытом ключе владельца отозванного сертификата возникнет та же ситуация, что и при отправке сообщения, подписанного с помощью отозванного сертификата.

#### 4. 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 (Рисунок 12):

Рисунок 1.
Свойства безопасности сообщения 🛛 🥐 🔀
🔎 Тема: test
Сообщения могут содержать шифрование и слои цифровых подписей. Каждый слой допускает наличие нескольких подписей.
Тема: test Уровень цифровых подписей
🗸 Подписано: zhenya@cryptopro.ru
Описание:
ОК: подписанное сообщение.
🔽 Всегда предупреждать об ошибках защищенной 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 (Рисунок 13).

Рисунок 13
Свойства безопасности сообщения
Тена: RE: lef Сообщення ногут содержать шифрование и слон шифровых подписей. Каждый слой допускает наличие нескольких подписей. Самирание инфровых подписей Уровень шифровых подписей Подписано: mailtest@eryptopro.ru

Если же СОС обновлен, то при открытии письма, подписанного отозванным сертификатом, появится следующее предупреждение (Рисунок 14):

		Рисунок 14.
Цифро	вая подпись: неправильная	? 🗙
Тема: От:	test mailtest	
Цифров сертифи	ая подпись в сообщении недопустима, поскольку отсутствует , кату в сообщении.	доверие к
🔽 Bcer	да предупреждать об ошибках защищенной почты.	
	Показать сообщение Сведения	Отмена

Нажмите кнопку Сведения для просмотра сведений о сертификате (Рисунок 15):

Рисунок 1
Свойства безопасности сообщения 🔹 🤶 🔀
📆 Тема: test
Сообщения могут содержать шифрование и слои цифровы» подписей. Каждый слой допускает наличие нескольких подписей.
Тема: test Уровень цифровых подписей Подписано: mailtest@cryptopro.ru
Описание: Ошибка: •Использованный для создания данной подписи сертификат находится в допустимом списке отмененных сертификатов. По лаиксано maitest@cryptopro rule помощью ГОСТ Р 34.10- Всегда предупреждать об ошибках защищенной почты
Изменить доверие Подробности Закрыть

#### III. Инструкция по использованию электронной цифровой подписи в **Microsoft Office Outlook 2007**

1. Отправка подписанных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку і Создать - Создать или выберите пункт меню Файл – Создать -Сообшение.

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 Отправить (Рисунок 16).

		N			6		-
	0 4 7	),•	test - Cooo	щение (НТМL	)		- 0 X
Coof	щение В	ставка Пар	аметры	Формат текста			0
Вставить	Calibri (Осн Ж К Ц <sup>ађ</sup> - <u>А</u> -				к исполнению -		АВС Орфография
Буфер об 🖻	Осн	овной текст	(e)	Вклю 🖻	Параметры	12	Правописание
 Отправит <u>ь</u>	Кому <u></u> Копи <u>я</u>	<u>mailtest@cryp</u>	otopro.ru;				
	Т <u>е</u> ма:	test					
	Вло <u>ж</u> ение:	🛃 <u>smime.pdf (</u>	561 <u>Кбайт)</u>				
test							- 23 ▲ ■ ■

Если сертификат, с помощью которого подписано сообщение, был отозван, то появится следующее предупреждение, а само сообщение не будет отправлено. (Рисунок 17)



Рисунок 16

# 2. Получение сертификата открытого ключа абонента для шифрования сообщений

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

Для контроля добавления выполните следующие действия. Откройте полученное подписанное письмо. Установите курсор на адрес отправителя и, нажав правую кнопку мыши, выберите пункт Добавить в контакты Outlook. В отображаемом диалоге нажмите на закладку Сертификаты и убедитесь в наличии сертификата отправителя (Рисунок 18).

				1 ncync	<u>JK 10.</u>
0	1 4 4 F	mailtest - Контан	σ		- = x
Контакт	Вставка Формат текста				0
Сохранить и закрыть действия При отправке шиф из этих сертификат импорте его файла Сер <u>т</u> ификаты (циф mailtest(По умолча	Вставка Форматтекста     Общие     Сертификаты     Подробности Все поля     Действия     Показать      показать      пованного сообщения данному конта     сертификаты добавляются либо п     а сертификатов.      ровые подписи):      анию)	<ul> <li>Электронная почта </li> <li>Собрание</li> <li>Вызов &lt;</li> <li>Связь</li> <li>Связь</li> <li>Кту будет использоваться один ри получении сообщения с ци</li> </ul>	<ul> <li>Рисунок *</li> <li>Выбрать категорию *</li> <li>Выбрать категорию *</li> <li>Выбрать категорию *</li> <li>Мараметры</li> <li>Фровой подписью от данного контакта, ли</li> </ul>	АВС Орфография Правописание ибо при	Заметки о контакте OneNote
					модчанию мпорт сспорт /далить

**Ο**μονμοις 18



После этого нажмите на кнопку изакрыть 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.

#### 3. Отправка шифрованных сообщений

Для создания и отправки шифрованного сообщения нажмите кнопку Создать 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 Отправить**.

При попытке зашифровать письмо на открытом ключе владельца отозванного сертификата, появится следующее предупреждение (Рисунок 19).



4. Проверка сертификата на отзыв

Для контроля проверки сертификатов на отзыв выполните следующие

действия. Откройте полученное подписанное письмо. Нажмите кнопку признак подписанного сообщения. (Рисунок 20)

Рисунок 20.



Нажмите кнопку Сведения. Если сертификат действительный и не был отозван, то откроется окно, подобное этому (Рисунок 21):

Рисунок	21.
---------	-----

Свойства безопаснос	ти сообщения	
A Tema: test		
Сообщения могут шифрон допускает наличие неско	ваться и содержать сло опьких подписей.	и цифровых подписей. Каждый слой
Слои безопасности		
Выберите слой для просм	ютра его описания.	
Подписано: 1	nalicescocrypcopro.ru	
<u>О</u> писание:		
Описание: ОК: подписанное сообще	ение.	
<u>О</u> писание: ОК: подписанное сообще Следующие кнопки позви изменения в выбранный о	ение. оляют просмотреть доп глой:	олнительные сведения или внести
Описание: ОК: подписэнное сообще Следующие кнопки позви изменения в выбранный о Изменить доверие	ение. оляют просмотреть доп глой:	олнительные сведения или внести Доверие к центру сертификации
<u>О</u> писание: ОК: подписэнное сообще Следующие кнопки позви изменения в выбранный о <u>И</u> зменить доверие	ение. оляют просмотреть доп слой: Подробности	олнительные сведения или внести Доверие к центру сертификации

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 (Рисунок 22).



Если же СОС обновлен, а письмо подписано отозванным сертификатом, то при нажатии кнопки то при нажатии кнопки появится следующее предупреждение (Рисунок 23):

Рисунок 23. Цифровая подпись: неправильная Тема: test OT: mailtest Подписано: mailtest@cryptopro.ru Цифровая подпись сообщения является 2 недействительной или не доверенной. Для просмотра сведений о сертификате, применяемом в цифровой подписи сообщения, нажмите кнопку "Сведения". Сведения... 🔲 Предупреждать об ошибках в подписанных сообщениях до открытия. <u>З</u>акрыть

Рисунок 24

Нажмите кнопку Сведения для просмотра сведений о сертификате (Рисунок 24):

i ney n	
Свойства безопасности сообщения	×
Tema: test	
Сообщения чогут шифроваться и содержать слои цифровых подписей. Каждый сл допускает наличие нескольких подписей.	юй
Слои безопасности	
Выберите слой для просмотра его описания.	
Ф Тема: təst Уровень цифровых подписей Подписано: mailtest@cryptopro.ru	
Описание:	
Ошибка: Использованный для создания данной подписи сертификат находится в допустимом списке отмененных сертификатов. По вписано pailtect/@cryptopro rule помощью FOCT P 34 10-2001/FOCT P 34 11-94 в	<ul><li></li><li></li></ul>
Следующие кнопки позволяют просмотреть дополнительные сведения или внести изменения в выбранный слой:	и
Изменить доверие Подробности Доверие к центру сертификаци	и
Предупреждать об ошибках в подписанных сообщениях.	ять

### IV. Инструкция по использованию электронной цифровой подписи в Microsoft Office 2003

1. Порядок подписания файлов в программных продуктах Microsoft Office ( на примере продукта Microsoft Word)

Подпись файлов в программных продуктах Microsoft Office сертификатом зарегистрированного пользователя осуществляется следующим образом:

Откройте документ, который необходимо подписать и вставьте ключевой носитель с секретным ключом в АРМ.

На главной панели Microsoft Word откройте вкладку Сервис, в которой выберите пункт Параметры (Рисунок 25.).

Вставка Форма	т Сери	вис	<u>Т</u> аблица	<u>О</u> кно	<u>С</u> правка	Ado <u>b</u> e F	DF	Acrob	at <u>⊂</u> omment
IQ.   ♥ IQ.   - ]	₩ ₩ 3	Пран <u>С</u> пр- <u>Я</u> зы С <u>т</u> а- Обш <u>З</u> ащ <u>Писе</u> <u>Н</u> аст	в <u>о</u> писание, авочные ма к тистика цая рабоча: итить док; ьма и <u>р</u> ассь гройка	 атериаль я об <u>л</u> аст /мент	ы Alt+щ	F7 елчок •	ие	<b>•</b>	<u>(</u> Обычны • 6 • 1 • 7
		Пар	аметры						
				×					

- -

В открывшемся окне выберите вкладку Безопасность (Рисунок 26.) и нажмите на кнопку Цифровые подписи

### Рисунок 26.

Исправления Пользователь Совместимости	ь Расположение
Вид Общие Правка Печать Сохранение Безо	опасность Правописание
Параметры шифрования для данного документа пароль для открытия файла: Параметры совместного использования для данного документа пародь разрешения записи: □ рекомендовать доступ только для чтения □ цифровые подписи Установить защиту Параметры защиты конфиденциальной информации □ удалять личные сведения из свойств файла при сохранени □ предупреждать перед печатью, сохранением и отправкой записанные исправления и примечания ✓ сохранить случайное число для повышения точности слия ✓ показывать скрытую разметку при открытии и сохранения Защита от макросов Изменение уровня безопасности при открытии файлов, которые могут содержать вирусы в макросах, и указание надежных разработчиков макросов.	Дополнительно а ии й файла, содержащего иния и Защита от <u>м</u> акросов

В открывшемся окне можно добавить необходимые цифровые подписи, для этого нажимаем на кнопку **Добавить** (Рисунок 27.). **Рисунок 27.** 

Исправления		Пользователь		Совмест	Совместимость		Расположение		
Вид Общие Правка Печать				Сохранение	Безопаснос	ть Прав	равописани		
Парамет паролы Парамет паро <u>л</u> ы паролы паролы	рышифрова <b>Цифров</b> Подпис Созда легали подпи	ания для да зая подпи жи нная в Offic ыную подпи сях в справ равые подпи	инного доку ись се цифрова ись. См. дол же. си докумен	мента я подпись може полнительные с ита:	т не составля ведения о ци	ж ать фровых			
Napamer y Aa npe san v cox v cox	рі Подг д д р. а	исывающи	ий Цифро	овая подпись вы	ы Дата		го		
Защита ( Измене которь надежн	от Прос	мотр серти Справк	фиката а	Добавитн	»Уда	лить	)сов		

Откроется окно выбора сертификата, в данном случае мы выбираем сертификат Петрова Петра Петровича. Здесь так же мы можем просмотреть сам сертификат, нажав на кнопку **Просмотреть сертификат**. Выделяем сертификат Петрова и нажимаем **ОК** (Рисунок 28.).

		Рисунок
бор сертификата		?
ыберите сертификат.		
Кому выдан	Кем выдан	Срок действия
🔤 Петров Пётр Петр	Informtexcentr	10.02.2010
<		
	Отмена	Просмотр сертификат

Система запросит пин-код на ваш ключевой носитель. Введите пин-код и нажмите **ОК** (Рисунок 29).

				Рису	нок 29.
	Исправления		Польз	ователь	CoBr
	Вид	Общие	Правка	Печать	Сохранен
			A		мента
КриптоПро CSP				? 🔀	
P-					
BaUser-1t	зедите pin o6c3da8-1	4f1-4b16-a5	30-6ad9114	35fd8	
- F					подпись и
Ріп-код:					рлнительн
🗌 Запомнить pin-код					
ОК	<b>—</b>	0.7	мена		a:
			mond		вая подпи
	уда	л			
	🔲 пре,	д			
	запі	11			
	🗹 cox	p.			
	🔽 пок	a			
			исовлиняти	септифик	аты к добав

После ввода пин-кода мы видим что наш сертификат появился в окне **Подписи** (Рисунок 30.). Здесь мы можем просмотреть содержимое сертификата или добавить ещё один сертификат, используя кнопку **Добавить**.

#### Рисунок 30.

Исправления		Пользователь		Совмести	мость	Расположение			
Вид Общие		Правка	Печать	Сохранение	Безопасно	сть	Правопис	зописание	
Парамет пароль парамет паро <u>л</u> ь паро <u>л</u> ь парамет парамет уда зап	ры ш для ры сс разс сомен ле сомен ры за длять длять исанн	ровая под писи зданная в О гальную под альную под алисях в спр фровые под Фровые под Одписываю	пись ffice цифр апись. См. равке. авке. ций Ци атр In	ювая подпись мо: дополнительных имента: ифровая подпись formtexcentr	жет не сост е сведения вы Да 16	гавлять о цифр та .02.200	о оовых 19		
✓ сох ✓ пок Защита Измене которы надежна	рани азыв от ма эние у ые мо ных р	Присоединя Просмотр сер Спра	ать сертик отификата авка	фикаты к добавл а Добави	яемым поді іть	писям Удали От	ть		

Закрываем окна нажатием кнопок ОК. Мы видим, что теперь внизу нашего документа появился красный значок цифровой подписи (Рисунок 31.).

#### Рисунок 31.

СПР	вдл	3AM	русский (Ро	8		

Он означает что ваш документ имеет цифровую подпись. Двойным щелчком по значку цифровой подписи открывается окно подписей, где мы можем просмотреть сертификаты, которыми подписан документ, а так же добавить или удалить сертификат (Рисунок 32.).

#### Рисунок 32.

озданная в Office и егальную подпись. одписях в справке ифровые подписи	ифровая подпись может не См. дополнительные сведе о документа:	составлять ения о цифровы:	
Подписывающий	Цифровая подпись вы	Дата	
🖴 Петров Петр	Informtexcentr	16.02.2009	
Присоединять се	ртификаты к добавляемым	подписям	
Присоединять се Просмотр сертифи	ртификаты к добавляемым ката	подписям Удалить	

При дальнейшем изменении документа его подпись аннулируется. Если есть необходимость редактирования документа, то подписывать необходимо повторно, после завершения его редактирования и сохранения.

Аналогично подписание происходит в других продуктах Microsoft Office.

**Примечание:** При подписании документа в Microsoft Office 2003, проверить подпись и достоверность документа возможно только в этой же версии Microsoft Office.

#### V. Инструкция по использованию электронной цифровой подписи в Microsoft Office 2007

1. Порядок подписания файлов в программных продуктах Microsoft Office

Подпись файлов в программных продуктах Microsoft Office сертификатом зарегистрированного пользователя осуществляется следующим образом:

Вставьте ключевой носитель с секретным ключом в АРМ.

На главной панели нажмите кнопку **Office**, откроется основное меню, в котором необходима открыть вкладку **Подготовить** (Рисунок 33).



После чего необходимо нажать на подменю Добавить цифровую подпись, после чего появится окно предупреждения о возможности получения подписи сторонних партнёров Office (Рисунок 34.). Чтобы это сообщение больше не появлялось, необходимо поставить галочку напротив пункта Больше не показывать это сообщение и нажать ОК.

Рисунок	34.
---------	-----

		ают в сере знакомые черты оры	ичных подписей и удобство	) цифрового формата. Хотя	такая возможность
озволяет польз орпорация Май	зователям убедиться в ц і́крософт не может гаран	елостности документа, юридич тировать, что цифровая подпис	еские нормы в разных стра ъ будет иметь юридическу	нах могут отличаться. Так ю силу. Сторонние постав	им образом, щики услуг цифровой
одписи, которы	ых можно наити в катало	ге решении партнеров Оггісе, мі	огут предложить другие ур	овни гарантии цифровои п	юдписи.
	лазывать это сооощение	-			
Услу	уги подписи из каталога	решении партнеров Orrice		UK	

Далее появится окно выбора сертификата (Рисунок 35). Если сертификат не выбран, нужно нажать на кнопку **Изменить**.

Рисунок 3	35.
-----------	-----

Ополнительные	е сведения о том, что подписываетс	я
документ будет доб росмотре содержимо ель подписания доку	бавлена цифровая подпись. Эта под го документа. умента:	пись не будет видна при
Тема сертификата: Кем выдан:	Петров Пётр Петрович Informtexcentr	Изменить

После чего появится окно выбора сертификата (Рисунок 36). Выбираем наш сертификат и нажимаем **ОК**.

Рисунок	36.
---------	-----

ыберите сертифик	ата			и
Кому выдан	Кем выдан	Понятное имя	Срок действия	
🖾 Петров Пёт	Informtexcentr	Отсутствует	10.02.2010	ть
				мена
(	ĺ	Ш.		

Далее нажимаем на кнопку Подписать (Рисунок 37.).

		Рисунок 3
Подписание		? 🛘
Э Дополнительные	сведения о том, что подписывае	ется
3 документ будет доб просмотре содержимо Цель подписания док	авлена цифровая подпись. Эта по °о документа. /мента:	одпись не будет видна при
Тема сертификата: Кем выдан:	Петров Пётр Петрович Informtexcentr	Изменить
		Подписать Отмена

Появится окно ввода пин-кода в котрое необходимо ввести пин-код соответствующий вашему ключевому носителю (Рисунок 38.).

🗄 КриптоПро CSP 🛛 🔹 💽 💽	3
Введите ріп-код для контейнера RaUser-1b6c3da8-14f1-4b16-a530-6ad911435fd8 Pin-код	
Запомнить ріп-код	?
ИТМена	

Введите пин-код и нажмите ОК. Появится следующее сообщение (Рисунок 39).



Нажмите ОК и документ будет выглядеть теперь следующим образом: на панели справа появится дополнительное окно с фамилией подписавшего этот документ (Рисунок 40.).

#### Рисунок 40.



Выделив подписавшего можно увидеть следующее меню, в котором можно удалить подпись или просмотреть её состав (Рисунок 41.).



Нажав на Состав подписи можно увидеть информацию о подписи (Рисунок 42.) и просмотреть сертификат подписавшего (Рисунок 43.).

#### Рисунок 42.

Состав подписи		? 🔀
Действительная изменялись с мом	подпись. Данная подпись и подписан іента подписания.	ное содержимое не
<u>Ц</u> ель подписания докт	умента:	
Тема сертификата:	Петров Пётр Петрович	
Кем выдан:	Informtexcentr	
Дополнительные свер	ения, которые	Закрыть
рудут включены в по	дпись	

### Рисунок 43.

Сетав подписи Пействительная поллись. Панная подпись и подписанное содержимое не Сертификат Сертификат Сведения о сертификации Сведения о сертификации Сведения о сертификате Этот сертификат предназначается для: -Подтверждает удаленному компьютеру идентификацию вашего компьютера -Зацищает сообщения электронной почты -Пользователь Центра Регистрации, НТТР, TLS клиент -Кому выдан: Петров Пётр Петрович -Кем выдан: Informtexcentr -Действителен с 10.02.2009 по 10.02.2010 Сть закрытый ключ, соответствующий этому сертификату. -Заявление поставщика			•/	
Сертификат Сослав Путь сертификации Сослав Путь сертификации Сведения о сертификате Тот сертификат предназначается для Общие Состав Путь сертификате Подтверждает удаленному компьютеру идентификацию вашего компьютера Защищает сообщения электронной почты Пользователь Центра Регистрации, НТТР, TLS клиент Кому выдан: Петров Пётр Петрович Кем выдан: Informtexcentr Действителен с 10.02.2009 по 10.02.2010 С	остав п	одписи		?
Общие Состав Путь сертификации Сведения о сертификате Этот сертификат предназначается для: -Подтверждает удаленному компьютеру идентификацию вашего компьютера -Защищает сообщения электронной почты -Пользователь Центра Регистрации, НТТР, TLS клиент -Пользователь Центра Регистрации, НТТР, TLS клиент -Кому выдан: Петров Пётр Петрович -Кем выдан: Informtexcentr - Действителен с 10.02.2009 по 10.02.2010 	Серти	твительная поллись. Данная поллись и поллисанное содержимо фикат		
Сведения о сертификате Этот сертификат предназначается для: Подтверждает удаленному компьютеру идентификацию вашего компьютера Эзащищает сообщения электронной почты Эзащищает сообщения электронной почты Пользователь Центра Регистрации, НТТР, TLS клиент Кому выдан: Петров Пётр Петрович Кем выдан: Informtexcentr Действителен с 10.02.2009 по 10.02.2010 Сть закрытый ключ, соответствующий этому сертификату. Заявление поставщика	И Общи	е Состав Путь сертификации		
Этот сертификат предназначается для: •Подтверждает удаленному компьютеру идентификацию вашего компьютера •Зацищает сообщения электронной почты •Пользователь Центра Регистрации, НТТР, TLS клиент •Пользователь Центра Регистрации, НТТР, TLS клиент Кому выдан: Петров Пётр Петрович Кем выдан: Informtexcentr Действителен с 10.02.2009 по 10.02.2010 № Есть закрытый ключ, соответствующий этому сертификату. Заявление поставщика		🔜 Сведения о сертификате		
Кому выдан: Петров Пётр Петрович Кем выдан: Informtexcentr Действителен с 10.02.2009 по 10.02.2010 Р Есть закрытый ключ, соответствующий этому сертификату. Заявление поставщика		<ul> <li>тот сертификат предназначается для:</li> <li>Подтверждает удаленному компьютеру идентификацию вашего компьютера</li> <li>Защищает сообщения электронной почты</li> <li>Пользователь Центра Регистрации, HTTP, TLS клиент</li> </ul>		оыть
Кем выдан: Informtexcentr Действителен с 10.02.2009 по 10.02.2010 У Есть закрытый ключ, соответствующий этому сертификату. Заявление поставщика	2	<b>Кому выдан:</b> Петров Пётр Петрович		
Действителен с 10.02.2009 по 10.02.2010 № Есть закрытый ключ, соответствующий этому сертификату. Заявление поставщика ОК		Кем выдан: Informtexcentr		
Есть закрытый ключ, соответствующий этому сертификату.           Заявление поставщика		<b>Действителен с</b> 10.02.2009 по 10.02.2010		
Заявление поставщика	9	Есть закрытый ключ, соответствующий этому сертификату.		
ОК		Заявление поставщика		
Site Site		ок	5	

При дальнейшем изменении документа его подпись аннулируется. Если есть необходимость редактирования документа, то подписывать необходимо повторно, после завершения его редактирования и сохранения.

Аналогично подписание происходит в других продуктах Microsoft Office.

**Примечание:** При подписании документа в Microsoft Office 2007, проверить подпись и достоверность документа возможно только в этой же версии Microsoft Office.

## VI. Требования к помещениям, где установлены СКЗИ и хранятся ключевые документы к ним

В соответствии с Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации (СКЗИ) с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13.06.2001 г. № 152, к помещениям, где установлены средства криптографической защиты информации, предъявляются следующие требования:

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

Размещение СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае пользователи СКЗИ по согласованию с отделом инфраструктуры и информационной безопасности управления информатизации администрации области обязаны предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в их отсутствие.

Режим охраны помещений пользователей СКЗИ, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает обладатель конфиденциальной информации по согласованию с с отделом инфраструктуры и информационной безопасности управления информатизации администрации области. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать специфику и условия работы конкретных пользователей СКЗИ.

В помещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

При утрате ключа от хранилища или от входной двери в помещение пользователя СКЗИ замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить.

В обычных условиях опечатанные хранилища пользователей СКЗИ могут быть вскрыты только самими пользователями.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководству обладателя конфиденциальной информации и начальнику информационной безопасности отдела инфраструктуры И управления информатизации администрации области. Прибывшие сотрудники данного отдела должны оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации конфиденциальной информации и к замене скомпрометированных криптоключей.