Инструкция по настройке APM пользователя удостоверяющего центра «ТОГУ Информационно-технический центр».

Содержание

1. Настройка рабочего места пользователя.	2
2. Установка и настройка CSP 3.0 с поддержкой rutoken	2
2.1. Установка	2
2.2. Настройка криптопровайдера	7
3. Установка цепочки сертификатов центра сертификации и личного	
сертификата	12
3.1. Установка цепочки сертификатов	12
3.2. Установка личного сертификата	14
4. Проверка достоверности сертификата при получении подписанного пис 21	сьма

1. Настройка рабочего места пользователя.

Перед началом работы с АРМами пользователя ЦР необходимо выполнить следующие процедуры:

• Получить от администратора ЦР или скачать с Web сервера ЦР дистрибутивы программного обеспечения СКЗИ «КриптоПро CSP»

- Установить СКЗИ «КриптоПро СЅР»
- Установить сертификат ЦС

• Установить личный сертификат с ключевого носителя, полученного от администратора ЦР в случае регистрации пользователя в централизованном режиме.

Процедура получения указанных компонент регламентируется политикой конкретного Удостоверяющего Центра. В том случае, если регламентом УЦ разрешена процедура регистрации пользователя в распределенном режиме, то Удостоверяющий Центр должен предоставить пользователю все необходимые компоненты для выполнения процедур настройки рабочего места пользователя.

2. Установка и настройка CSP 3.0 с поддержкой rutoken.

2.1 Установка

Для установки CSP 3.0 с поддержкой рутокена запустим установочный файл и далее следуем инструкциям установки (Рисунок 1).

Рисунок 1.



Нажимаем Далее. Для корректной установки криптопровайдера рутокен не должен быть подсоединён к компьютеру. Если это так, то отсоедините его и ,для продолжения установки, нажмите кнопку **Установить** (Рисунок 2).

Рисунок 2.

КриптоПро CSP 3.0 SP3 с поддержкой Rutoken - InstallShield Wizard 🛛 🔀
КриптоПро CSP 3.0 SP3 с поддержкой Rutoken
Программа готова к началу установки.
СВНИМАНИЕ!
Пожалуйста, не подсоединяйте устройство Rutoken к компьютеру до окончания установки!
Если Rutoken уже подсоединен, отсоедините его.
Нажмите кнопку 'Установить', чтобы начать установку.
Чтобы просмотреть или изменить параметры установки, нажмите кнопку 'Назад'. Нажмите кнопку 'Отмена' для выхода из программы.
InstallShield
< Назад Установить Отмена

Следуйте инструкциям мастера установки нажимая Далее (Рисунок 3).

Рисунок 3.



После прочтения лицензионного соглашения нужно отметить пункт **Я** принимаю условия лицензионного соглашения и нажать Далее (Рисунок 4).

Рисунок 4.

🕼 КриптоПро CSP - InstallShield Wizard	×
Лицензионное соглашение Пожалуйста, внимательно прочтите следующее лицензионное	
соглашение.	
ВНИМАТЕЛЬНО ОЗНАКОМЬТЕСЬ С ЛИЦЕНЗИОННЫМ СОГЛАШЕНИЕМ Н ИСПОЛЬЗОВАНИЕ ИЗДЕЛИ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ	я
1. Термины и определения	
 1.1. Настоящее Лицензионное соглашение является общей офертой между ООО "КРИПТО-ПРО" и Пользователем - физическим или юридическим лицом. Настоящее Лицензионное соглашение в случае согласия, выраженного в форме молчания в течение 7 дней с момента приобретения права на использование Изделия, в соответствии со ст. 433 ГК РФ имеет силу договора. 1.2. Под Изделием понимается программа/комплекс программ для ЭВМ, включая носители и документацию, авторские права на которые принадлежат ООО «КРИПТО- 	
 Я принимаю условия лицензионного соглашения Я не принимаю условия лицензионного соглашения 	
InstallShield < Назад Далее > Отмен	a

Далее необходимо ввести ваши лицензионные данные. Заполните все поля в соответствии с вашим именем пользователя и данными полученными с лицензией на криптопровайдер (Рисунок 5). После того как все поля заполнены, нажимаем кнопку Далее.

Рисунок	5.
v	

🔀 КриптоПро CSP - InstallShield Wizard	×
Сведения о пользователе Укажите сведения о себе.	
Пользователь: user	
	,
Серийный номер:]
Введите серийный номер, соответствующий лицензионному Без заданного серийного номера срок действия продукта 30	соглашению. дней.
InstallShield	
< <u>Н</u> азад Да	лее > Отмена

В следующем окне выбираем обычную установку и нажимаем Далее (Рисунок 6).

Рисунок 6.

🛃 КриптоПро С	SP - InstallShield Wizard 🛛 💈	K)
Вид установки Выбор наибол	ее подходящего вида установки.	
Выберите вид	установки.	
💿 Обычная	Будет установлен стандартный набор компонент.	
Овыбороць	120	
	Выбор необходимых компонентов программы и папки, в которой они будут установлены. Рассчитана на опытных пользователей.	
InstallShield ———	< Назад Далее > Отмена)

Программа готова к установке. Нажимаем кнопку **Установить** и затем **Готово** (Рисунок 7,8).

Рисунок 7.

😸 КриптоПро CSP - InstallShield Wizard	×
Готова к установке программы Программа готова к началу установки.	
Нажмите кнопку "Установить", чтобы начать установку. Чтобы просмотреть или изменить параметры установки, нажмите к Нажмите кнопку "Отмена" для выхода из программы.	нопку "Назад".
InstallShield	
< Назад Установит	ь Отмена

Рисунок 8.



Для окончания установки необходимо перезагрузить компьютер. Выберите пункт Да, перезагрузить компьютер сейчас и нажмите Готово (Рисунок 9).

Рисунок 9.

КриптоПро CSP 3.0 SP3 с	поддержкой Rutoken - InstallShield Wizard
	Программа InstallShield Wizard завершена Установка КриптоПро CSP 3.0 SP3 с поддержкой Rutoken на компьютер завершена.
Num Based	 Да, перезагрузить компьютер сейчас. Нет, перезагрузить компьютер позже. Нажмите кнопку 'Готово' для завершения установки.
	< Назад Готово Отмена

2.2 Настройка криптопровайдера

После перезагрузки необходимо в криптопровайдер добавить считыватель реестр. Для этого откроем Пуск → Панель управления → КриптоПроСSP (Рисунок 10).



В открывшемся окне выберем вкладку Оборудование и нажмём на кнопку Настроить считыватели... (Рисунок 11).

Рисунок	11.
---------	-----



В следующем окне нажмём кнопку Добавить... (Рисунок 12).

Рисунок 12.

Управление считывателями	×
Считыватели	
Установлены следующие считыватели:	
Aktiv Co. ruToken 0	
	-
Добавить Удалить Свойства	ן כ
ОК Отмена	3

Далее увидим окно мастера установки и нажмём Далее (Рисунок 13).

Рисунок 13.



В следующем окне нам предоставлен выбор считывателей. Выбираем считыватель **Реестр** и нажимаем **Далее** (Рисунок 14).

Рисунок 14.

Мастер установки считыва	теля 🔀
Выбор считывателя Какой считыватель необх	ходимо установить?
Выберите считыватель, котор Производители	ный следует добавить, и нажмите кнопку "Далее". Постипные силтыватели:
(Все производители)	Aktiv Co. ruToken 1
Компания Крипто-Про	Aktiv Co. ruToken 2
	Установить с диска
	 Казад Далее > Отмена

Мастер установки спросит как назвать данный считыватель. Можно оставить предлагаемый вариант и нажать Далее (Рисунок 15).

Рисунок 15.

Мастер установки считывателя
Имя считывателя Требуется назначить имя для этого считывателя
Можно либо ввести желаемое имя для этого считывателя, либо использовать предложенное ниже имя. Чтобы продолжить установку после выбора имени, нажмите кнопку "Далее".
Имя считывателя:
< Назад Далее > Отмена

Завершаем установку считывателя нажатием кнопки Готово в следующем окне (Рисунок 16).

Рисунок 16.



Теперь мы видим, что в окне считывателей появился новый считыватель **Реестр.** Закрываем окна нажатием на кнопку **ОК** (Рисунок 17,18).

Рисунок 17.

Управление считывателями	×
Считыватели	
Установлены следующие считыватели:	
aktiv Co. ruToken 0	1
臺 Дисковод, А 译 Реестр	
Добавить Удалить Свойства)
ОК Отмена	5

Рисунок 18.

Свойства: КриптоПр	oo CSP	
Дополнительно Общие	Алгоритмы Оборудование	Безопасность Сервис
Считыватели закрытых ключей Позволяет добавить новые и удалить не нужные считыватели закрытых ключей. Настроить считыватели		не нужные читыватели
Датчики случайных Позволя датчики	к чисел ет добавить новые и удалить случайных чисел. Настрои	ь не нужные пь ДСЧ
Ключевые носители Позволя носители	и ет добавить новые и удалить и секретных ключей. Настроит	ь не нужные ь носители
	ОК От	мена Применить

Криптопровайдер успешно установлен и готов к работе.

3. Установка цепочки сертификатов центра сертификации и личного сертификата

3.1 Установка цепочки сертификатов

Для установки цепочки сертификатов центра сертификации необходимо нажать правой кнопкой мыши на файле цепочки. В появившемся меню выбрать пункт Установить сертификат (Рисунок 19).



Далее следуем инструкциям мастера установки и нажимаем Далее (Рисунок 20).



12

Мастер установки попросить указать хранилище для установки сертификата. Выбираем Поместить все сертификаты в следующее хранилице, нажимаем Обзор и выбираем Доверенные корневые центры сертификации. Нажимаем ОК и кнопку Далее (Рисунок 21).

ри	Рисун мпорта сертификатов
	ине сертификатов
(ран (ран	илища сертификатов - это области системы в которых производится нение сертификатов.
зыбо	ор хранилища может быть произведен Windows автоматически, или же
10жн	ю указать размещение сертификата вручную.
0	 Автоматически выбрать хранилище на основе типа сертификата
C	Опоместить все сертификаты в следующее хранилище
	Хранилище сертификатов:
	Обзор
	< Назад Далее > От

В окне завершения работы мастера нажимаем Готово (Рисунок 22).

		Рисунок 22
Мастер импорта сертификат	10 B	\mathbf{X}
	Завершение работы мас импорта сертификатов Работа мастера импорта сертификатов завершена. Были указаны следующие параметры:	с тера успешно
	Выбранное хранилище сертификатов Содержание Имя файла	Автоматическ Сертификаты C:\Documents
	< Назад Готово	Отмена

Система безопасности выдаст следующее предупреждение (Рисунок 23). На вопрос «Установить данный сертификат?» отвечаем Да.

<mark>Треду</mark> пр	реждение системы безопасности	×
1	Готовится установка сертификата от центра сертификации (ЦС) в этом домене: Informtexcentr	
	Не удается проверить, что сертификат принадлежит "Informtexcentr". Обратитесь к "Informtexcentr" и подтвердите его происхождение. Следующие числа будут полезны для данного процесса:	
	Отпечаток (sha1) : F35EC874 BE3FF918 7286FC47 A6142335 8B26FBCF	
	Предупреждение: Если установить данный корневой сертификат, то Windows автоматически будет доверять любому сертификату, выданному ЦС. Установка сертификата без отпечатка может привести к риску безопасности. "Да" указывает, что риск принимается.	
	Установить данный сертификат?	
	Да Нет	

И получаем сообщение об успешном окончании установки (Рисунок 24).

Нажимаем Ок.



Рисунок 23.

Сертификат центра сертификации и список отозванных сертификатов успешно установлены.

3.2 Установка личного сертификата

Для установки личного сертификата в систему откроем криптопровайдер. Пуск →Панель управления → КриптоПроСSP (Рисунок 25).



На вкладке Сервис нажмём на кнопку Просмотреть сертификат в контейнере (Рисунок 26).



Вставим рутокен в компьютер и в открывшемся окне нажмём кнопку Обзор для выбора контейнера (Рисунок 27).

	Рисунок 27
Сертификаты в контейнере закрытого ключа	×
Контейнер закрытого ключа Введите или укажите контейнер закрытого ключа для просмотра сертификатов в этом контейнере	
Имя ключевого контейнера:	
	Обзор
Введенное имя задает ключе	вой контейнер:
Выберите CSP для поиска ключевых контейнеров:	
Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider	•
< Назад Далее >	Отмена

Выбираем наш рутокен и нажимаем ОК (Рисунок 28).

Рисунок 28.

🗖 Выбор ключевого контейнера 🛛 🛛 🔀
В списке показывать: Эдружественные имена ОУникальные имена
Список ключевых контейнеров пользователя:
Считыватель 🔻 Имя контейнера
🗞 Aktiv Co. ruToken 0 🛛 RaUser-1b6c3da8-14f1-4b16-a530-6ad911
Cancel OK

Теперь мы видим имя нашего рутокена в строке имени ключевого контейнера. Нажимаем Далее (Рисунок 29).

Рисунок	29.
---------	-----

Сертификаты в контейнере закрытого ключа 🛛 🔀
Контейнер закрытого ключа Введите или укажите контейнер закрытого ключа для просмотра сертификатов в этом контейнере
Имя ключевого контеинера: ВаШеер 166е3da8.14f1.4b16.a530.6ad911435fd8
Введенное имя задает ключевой контейнер:
О Пользователя
🔾 Компьютера
Выберите СSP ала поиска к акцерых контейнеров:
Crupto-Pro GOST B 34 10-2001 Cruptographic Service Provider
< Назад Далее > Отмена

В следующем окне мы видим информацию о сертификате, который находится на данном ключевом носителе. Нажимаем кнопку **Свойства** (Рисунок 30).

Рисунок 30.

Сертификаты в ко	нтейнере закрытого ключа 🛛 🔀
Сертификат для Просмотрите и	просмотра і выберите сертификат
Сертификат:	Петров Пётр Петрович
Субъект:	E=uc@itc.tambov.gov.ru, C=RU, L=Тамбов, О=ТОГУ, CN=Петров Пётр
Поставщик:	E=uc@itc.tambov.gov.ru, O=TOГУ Информтехцентр, S=Tамбовская об
Действителен с:	10 февраля 2009 г. 12:27:00
Действителен по:	10 февраля 2010 г. 12:36:00
Серийный номер:	1F33 081D 0000 0000 000F
	Свойства
	Обзор
	< Назад Готово Отмена

Открылось окно нашего личного сертификата. Нажимаем на кнопку Установить сертификат (Рисунок 31).

Рисунок 31.

roperty Page Select Cert ?
Общие Состав Путь сертификации
🔛 Сведения о сертификате
Этот сертификат предназначается для:
 Подтверждает удаленному компьютеру идентификацию вашего компьютера
•Защищает сообщения электронной почты
to be a considering a conception of the part of the pa
Кому выдан: Петров Пётр Петрович
Кемвыдан: Informtexcentr
Действителен с 10.02.2009 по 10.02.2010
🌮 Есть закрытый ключ, соответствующий этому сертификату.
Установить сертификат Заявление поставщика
ОК

Откроется мастер установки сертификатов. Нажимаем Далее (Рисунок 32).

Рисунок 32.



В окне выбора хранилища выбираем пункт Поместить все сертификаты в следующее хранилище и нажимаем кнопку Обзор (Рисунок 33).

Рисунок 33.

	ертификатов
Хранилища хранение с) сертификатов - это области системы в которых производится ертификатов.
Выбор хра можно ука	чилища может быть произведен Windows автоматически, или же зать размещение сертификата вручную. матически выбрать хранилище на основе типа сертификата
U I IOME	стить все сертификаты в следующее хранилище
Xpar	илище сертификатов: Обзор

В открывшемся окне выбираем папку Личные и нажимаем ОК (Рисунок

Рисунок 34.



Хранилище выбрано. Нажимаем Далее (Рисунок 35).

Рисунок 35.

Мастер импорта сертификатов
Хранилище сертификатов
Хранилища сертификатов - это области системы в которых производится хранение сертификатов.
Выбор хранилища может быть произведен Windows автоматически, или же можно указать размещение сертификата вручную. О Автоматически выбрать хранилище на основе типа сертификата Поместить все сертификаты в следующее хранилище
Хранилище сертификатов:
Личные Обзор
< Назад Далее > Отмена

Завершаем работу мастера нажатием кнопки Готово (Рисунок 36).

Рисунок 36.

Мастер импорта сертификатов		
	Завершение работы мастера импорта сертификатов Работа мастера импорта сертификатов успешно	
	завершена.	
	Содержание	
	< Назад Готово Отмена	

И видим сообщение об успешном импорте сертификата. Нажимаем ОК (Рисунок 37).

Рисунок 37.



Ваш личный сертификат успешно установлен на компьютер.

4. Проверка достоверности сертификата при получении подписанного письма

Получая электронное письмо, подписанное ЭЦП, (в данном случае от Петрова) в почтовой программе, открыв это письмо, мы видим следующее сообщение (Рисунок 38).

Рисунок 38.

! 0	1	От	Тема	Получено 🗸	^
		Щ Петров	Письмо Петрова	22.05.2009 8:45	
		👷 Удостоверяющий центр		05.05.2009 10:42	*
От: Пе	тров К	ому: Удостоверяющий центр			
Тема:	Письмо Г	Тетрова			
				<u> </u>	^
			Справка по без	вопасности 🦰	
		Co	общения с цифровой		
	Это подп	сообщение было подг иси.	исано отправителем с испол	ъзованием цифровой	
	Подг подл пред пере	исанное сообщение с инность сообщения - полагаемого отправи дачи.	от других пользователей позн что это сообщение действит птеля и что его текст не был н	золяет проверять ельно исходит от его никем изменен во время	
	Любые неполадки с подписанным сообщением будут упомянуты в предупреждении безопасности, которое может последовать за данным предупреждением. При получении такого предупреждения следует считать, что либо сообщение было изменено при передаче, либо оно не исходит от предполагаемого отправителя.				
			Больше не выводить это окно.		
			Продолжить		
1			Defense over		
			🚐 Работа в сети		

Для прочтения самого письма необходимо нажать на кнопку **Продолжить.** После чего мы сможем просмотреть содержимое письма (Рисунок 39).

Рисунок 39.

! 0 7	₽ От	Тема	Получено 🗸	^
	💁 Петров	Письмо Петрова	22.05.2009 8:45	-
	👷 Удостоверяющий центр		05.05.2009 10:42	~
От: Петров Тема: Письм	Кому: Удостоверяющий центр о Петрова		8	2
Текст пись	ма			~

В правой части колонки, подсвеченной синим цветом, мы видим значок цифровой подписи, который становится цветным если навести на него курсор (Рисунок 40). Нажав на этот значок, мы можем просмотреть сертификат пользователя, который подписал это письмо, и проверить достоверность этого сертификата.

Рисунок 40.



В открывшемся окне на вкладке **Безопасность** нужно нажать на кнопку **Просмотр сертификатов...** (Рисунок 41).

Рисунок 41.

Письмо Петрова	?×
Общие Подробно Безопасность	
Цифровая подпись	_
Подписано: uc@itc.tambov.gov.ru	
Содержимое не изменено:	Дa
Подпись достоверна:	Дa
Запрос безопасного уведомления:	н/д
Проверка отзыва сертификата:	Нет
Состояние Проверка отзыва сертификатов была отключена. отзыва:	
Метка безопасности:	
Шифрование	_
Содержание и вложения зашифрованы:	Нет
Алгоритм шифрования:	Нет
Просмотр сертификатов Дополнительные сведени:	A
ОК От	мена

После чего мы можем просмотреть сертификат отправителя, нажав на кнопку Сертификат отправителя (Рисунок 42).

Рисунок 42.

Просмотр сертификатов	? 🗙
Подписи	
Выберите "Сертификат подписи" для просмотра сертификата, используемого для подписи данного сообщения.	Сертификат подписи
Шифрование	
Сообщение не было зашифровано.	Сертификат шифрования
Предпочтения отправителя	
Рекомендуемый алгоритм шифрования:	3DES
Выберите "Сертификат отправителя" для просмотра сертификата, рекомендуемого для шифрования сообщений отправителю.	Сертификат отправителя
Выберите "Добавить в адресную книгу", чтобы сохранить в адресной книге предпочтения шифрования сообщений данному отправителю.	Добавить в адресную книгу
	ОК Отмена

После чего откроется окно сертификата, в котором можно просмотреть информацию о самом сертификате и его владельце (Рисунок 43).

Рисунок 43.

Свойства се ртифика	та подписи ? 🔀
Общие Состав Путь	сертификации Доверие
Сведения Этот сертификат	о сертификате г предназначается для:
Кому выдан:	Петров Пётр Петрович
Кем выдан:	Informtexcentr
Действителен	н с 10.02.2009 по 10.02.2010
	Заявление поставщика
	ОК

На вкладке **Состав** в пункте **Субъект** мы можем увидеть информацию о владельце сертификата (Рисунок 44). Здесь можно увидеть Ф.И.О. субъекта, организацию, отдел, город, регион и адрес электронной почты.

Рисунок 44.

Свойства сертификата подпи	си ?	
Общие Состав Путь сертифика	зции Доверие	
Показать: <Все>	~	
Поле	Значение	
Версия Серийный номер Алгоритм подписи Поставщик Действителен с Действителен по Субъект Открытый ключ	V3 1f 33 08 1d 00 00 00 00 00 00 0f ГОСТ Р 34.11/34.10-2001 Informtexcentr, RU, Тамбов, Т 10 февраля 2009 г. 12:27:00 10 февраля 2010 г. 12:36:00 Петров Пётр Петрович, ТОГ ГОСТ Р 34.10-2001 (512 Bits)	
CN = Петров Пётр Петрович D = TOГУ L = Тамбов C = RU E = uc@itc.tambov.gov.ru		
Lec	йства Копировать в файл	

На вкладке **Путь сертификата** можно просмотреть, действителен ли сертификат, и проследить путь сертификации до удостоверяющего центра, которым выдан данный сертификат (Рисунок 45).

Свойства сертификата подписи	? 🗙
Общие Состав Путь сертификации	Доверие
Informtexcentr Петров Пётр Петрович	
	Просмотр сертификата
Состояние сертификата:	
Этот сертификат действителен.	
	ОК

Рисунок 45.

В графе Состояние сертификата мы видим, что сертификат действителен. Значит владелец сертификата на момент подписи имел право подписывать письмо своим личным сертификатом.