127 018, Москва, Сущевский Вал, 18 Телефон: (495) 995 4820 Факс: (495) 995 4820 <u>http://www.CryptoPro.ru</u> E-mail: <u>info@CryptoPro.ru</u>



Средство

Криптографической

Защиты

Информации

КриптоПро CSP

Версия 4.0 КС2

2-Base

Инструкция по

использованию СКЗИ

под управлением ОС

Windows

ЖТЯИ.00088-01 92 01 Листов 122

© ООО «КРИПТО-ПРО», 2000-2016. Все права защищены.

Авторские права на средства криптографической защиты информации типа КриптоПро CSP и эксплуатационную документацию к ним зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент).

Настоящий Документ входит в комплект поставки программного обеспечения СКЗИ КриптоПро CSP версии 4.0; на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО "КРИПТО-ПРО" документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

		Содержание	
1.	Инста	алляция СКЗИ КриптоПро CSP	5
2.	Интер	офейс СКЗИ КриптоПро CSP	11
21	Лоступ	ик панели управления СКЗИ	11
2.1.	Общие		12
2.2.	Оощие		12
2.3.	вод се	ерииного номера лицензии криптопроваидера «криптопро CSP»	12
2.4.	настро	Иса оборудования СКЗИ	13
	2.4.1.	Изменение наоора устроиств считывания ключевой информации	14
		2.4.1.1. Доодвление считывателя	14 18
			10 18
	242	Изменение набора устройств хранения ключевой информации	
		2.4.2.1. Добавление носителя	
		2.4.2.2. Удаление ключевого носителя	
		2.4.2.3. Просмотр свойств ключевого носителя	23
	2.4.3.	Настройка датчиков случайных чисел (ДСЧ)	23
		2.4.3.1. Добавление ДСЧ	23
		2.4.3.2. Удаление ДСЧ	26
		2.4.3.3. Просмотр свойств ДСЧ	26
2.5.	Работа	а с контейнерами и сертификатами	27
	2.5.1.	Тестирование, копирование и удаление контейнера закрытого ключа	27
		2.5.1.1. Тестирование контейнера закрытого ключа	27
		2.5.1.2. Копирование контейнера закрытого ключа	29
		2.5.1.3. Удаление контейнера закрытого ключа	32
	2.5.2.	Просмотр и установка личного сертификата, хранящегося в контейнере зан 33	крытого ключа
		2.5.2.1. Просмотр сертификата, хранящегося в контейнере закрытого ключа	33
		2.5.2.2. Установка личного сертификата, хранящегося в контейнере зан	срытого ключа
		36	
	2.5.3.	Установка личного сертификата, хранящегося в файле	26
	2.5.4.		
		Управление паролями доступа к закрытым ключам	40
		Управление паролями доступа к закрытым ключам 2.5.4.1. Изменение пароля на доступ к закрытому ключу	40 40
		Управление паролями доступа к закрытым ключам 2.5.4.1. Изменение пароля на доступ к закрытому ключу 2.5.4.2. Удаление запомненных паролей	40 40 41
2.6.	Установ	Управление паролями доступа к закрытым ключам 2.5.4.1. Изменение пароля на доступ к закрытому ключу 2.5.4.2. Удаление запомненных паролей вка параметров безопасности	40 40 41 41
2.6. 2.7.	Установ Дополн	Управление паролями доступа к закрытым ключам 2.5.4.1. Изменение пароля на доступ к закрытому ключу 2.5.4.2. Удаление запомненных паролей вка параметров безопасности чительные настройки	40 40 41 41 41
2.6. 2.7.	Установ Дополн 2.7.1.	Управление паролями доступа к закрытым ключам 2.5.4.1. Изменение пароля на доступ к закрытому ключу 2.5.4.2. Удаление запомненных паролей вка параметров безопасности чительные настройки Просмотр версий используемых файлов	40 40 41 41 41 44 44
2.6. 2.7.	Установ Дополн 2.7.1. 2.7.2.	Управление паролями доступа к закрытым ключам 2.5.4.1. Изменение пароля на доступ к закрытому ключу 2.5.4.2. Удаление запомненных паролей вка параметров безопасности чительные настройки Просмотр версий используемых файлов Установка времени ожидания ввода информации от пользователя	40 40 41 41 41 44 44 44
2.6. 2.7. 2.8.	Установ Дополн 2.7.1. 2.7.2. Выбор	Управление паролями доступа к закрытым ключам 2.5.4.1. Изменение пароля на доступ к закрытому ключу 2.5.4.2. Удаление запомненных паролей ивка параметров безопасности чительные настройки просмотр версий используемых файлов Установка времени ожидания ввода информации от пользователя пара метров криптографических алгоритмов	40 41 41 41 41 44 44 44 44
2.6. 2.7. 2.8. 2.9.	Установ Дополн 2.7.1. 2.7.2. Выбор Настроі	Управление паролями доступа к закрытым ключам 2.5.4.1. Изменение пароля на доступ к закрытому ключу 2.5.4.2. Удаление запомненных паролей ивка параметров безопасности чительные настройки Просмотр версий используемых файлов Установка времени ожидания ввода информации от пользователя пара метров криптографических алгоритмов ийка аутентификации в домене Windows.	40 41 41 41 44 44 44 44
2.6. 2.7. 2.8. 2.9. 2.10.	Установ Дополн 2.7.1. 2.7.2. Выбор Настрої Настрої	Управление паролями доступа к закрытым ключам 2.5.4.1. Изменение пароля на доступ к закрытому ключу 2.5.4.2. Удаление запомненных паролей извка параметров безопасности нительные настройки просмотр версий используемых файлов Установка времени ожидания ввода информации от пользователя пара метров криптографических алгоритмов ийка аутентификации в домене Windows ийки TLS	40 41 41 41 44 44 44 46 46 47
2.6. 2.7. 2.8. 2.9. 2.10. 3.	Установ Дополн 2.7.1. 2.7.2. Выбор П Настрої Иастрої Интер	Управление паролями доступа к закрытым ключам 2.5.4.1. Изменение пароля на доступ к закрытому ключу 2.5.4.2. Удаление запомненных паролей	40 40 41 41 44 44 44 46 46 46 47 49
2.6. 2.7. 2.8. 2.9. 2.10. 3. 3.1.	Установ Дополн 2.7.1. 2.7.2. Выбор Настрої Настрої Интер Генера	Управление паролями доступа к закрытым ключам	40 40 41 41 44 44 44 46 46 46 46 47 49 49
2.6. 2.7. 2.8. 2.9. 2.10. 3.1. 3.2.	Установ Дополн 2.7.1. 2.7.2. Выбор Настрої Настрої Интер Генераї Создані	Управление паролями доступа к закрытым ключам 2.5.4.1. Изменение пароля на доступ к закрытому ключу 2.5.4.2. Удаление запомненных паролей	40 40 41 41 44 44 44 46 46 46 47 49 49 49 50
 2.6. 2.7. 2.8. 2.9. 2.10. 3.1. 3.2. 	Установ Дополн 2.7.1. 2.7.2. Выбор П Настрої Интер Генераї Создані 3.2.1.	Управление паролями доступа к закрытым ключам	40 40 41 41 44 44 44 46 46 46 47 49 49 50
 2.6. 2.7. 2.8. 2.9. 2.10. 3.1. 3.2. 	Установ Дополн 2.7.1. 2.7.2. Выбор I Настроі Настроі Интер Генерая Создані 3.2.1. 3.2.2.	Управление паролями доступа к закрытым ключам	40 40 41 41 44 44 44 46 46 46 46 47 49 49 50 50
2.6. 2.7. 2.8. 2.9. 2.10. 3.1. 3.2.	Установ Дополн 2.7.1. 2.7.2. Выбор I Настрої Настрої Интер Генераї Создані 3.2.1. 3.2.2. 3.2.3.	Управление паролями доступа к закрытым ключам	40 41 41 41 44 44 44 46 46 46 47 49 49 50 50 50
2.6. 2.7. 2.8. 2.9. 2.10. 3.1. 3.2.	Установ Дополн 2.7.1. 2.7.2. Выбор П Настрой Настрой Интер Генерая Создан 3.2.1. 3.2.2. 3.2.3. 3.2.4.	Управление паролями доступа к закрытым ключам	40 40 41 41 44 44 44 46 46 46 47 49 49 50 50 50 50 51
2.6. 2.7. 2.8. 2.9. 2.10. 3.1. 3.1. 3.2.	Установ Дополн 2.7.1. 2.7.2. Выбор I Настроі Настроі Интер Генеран Создані 3.2.1. 3.2.2. 3.2.3. 3.2.4.	Управление паролями доступа к закрытым ключам	40 40 41 41 44 44 44 46 46 46 46 47 49 49 50 50 50 51
2.6. 2.7. 2.8. 2.9. 2.10. 3.1. 3.2.	Установ Дополн 2.7.1. 2.7.2. Выбор I Настрої Настрої Интер Генеран Создані 3.2.1. 3.2.2. 3.2.3. 3.2.4.	Управление паролями доступа к закрытым ключам	40 41 41 41 44 44 44 46 46 47 49 49 49 49 50 50 50 51 51
2.6. 2.7. 2.8. 2.9. 2.10. 3.1. 3.2.	Установ Дополн 2.7.1. 2.7.2. Выбор Настрої Настрої Интер Генеран Создани 3.2.1. 3.2.2. 3.2.3. 3.2.4.	Управление паролями доступа к закрытым ключам	40 41 41 41 44 44 44 46 46 46 47 49 49 50 50 50 50 51 52 52
 2.6. 2.7. 2.8. 2.9. 2.10. 3.1. 3.1. 3.2. 	Установ Дополн 2.7.1. 2.7.2. Выбор I Настрої Настрої Интер Генеран Создані 3.2.1. 3.2.2. 3.2.3. 3.2.4.	Управление паролями доступа к закрытым ключам	40 41 41 41 44 44 44 46 46 46 47 49 49 50 50 50 50 51 51 52 52 52 53
 2.6. 2.7. 2.8. 2.9. 2.10. 3.1. 3.2. 3.3. 	Установ Дополн 2.7.1. 2.7.2. Выбор I Настрої Настрої Интер Генеран Создані 3.2.1. 3.2.2. 3.2.3. 3.2.4. Открыт 3.3.1.	Управление паролями доступа к закрытым ключам	40 41 41 41 44 44 44 46 46 46 46 47 49 49 50 50 50 50 51 51 52 52 53
 2.6. 2.7. 2.8. 2.9. 2.10. 3.1. 3.2. 3.3. 	Установ Дополн 2.7.1. 2.7.2. Выбор I Настрої Настрої Интер Генеран Создан 3.2.1. 3.2.2. 3.2.3. 3.2.4. Открыт 3.3.1. 3.3.2.	Управление паролями доступа к закрытым ключам	40 40 41 41 41 44 44 44 44 44
 2.6. 2.7. 2.8. 2.9. 2.10. 3.1. 3.2. 3.3. 	Установ Дополн 2.7.1. 2.7.2. Выбор I Настрої Интер Генеран Создані 3.2.1. 3.2.2. 3.2.3. 3.2.4. Открыт 3.3.1. 3.3.2.	Управление паролями доступа к закрытым ключам	40 40 41 41 41 44 44 44 44 44

Проверка пароля при разделении ключа между несколькими носителями..54 3.3.2.3. 4. Описание использования, настроек и управления ключами модуля сетевой аутентификации КриптоПро TLS55 4.1. Установка IIS на сервере......55 4.2. Установка КриптоПро CSP......55 Установка корневого сертификата в хранилище компьютера......56 4.3. 4.4. Установка сертификата IIS......60 4.4.1. Настройка IIS с указанием сертификата......63 4.4.2. 4.4.3. Проверка соединения по HTTPS......65 5. Описание использования, настроек и управления ключами на сервере ISA/TMG72 5.1. Размещение сертификата аутентификации сервера на сервере ISA/TMG......72 5.2. Размещение сертификата клиентской аутентификации на сервере ISA/TMG......73 5.3. Настройка соединения с Web-клиентом.....74 5.4. Публикация Web-сервера в сети Интернет......77 6. Описание использования, настроек и управления ключами в КриптоПро Winlogon 80 6.2. 6.2.1. 6.3. Требования к сертификату контроллера домена95 6.3.1. 6.4. 6.5. 6.5.1. 6.6. Настройка Active Directory и контроллера домена для входа по смарт-картам с помощью групповой политики при использовании стороннего центра сертификации. 103 Указания по настройке......103 6.6.1. 6.6.1.1. Добавление независимого корневого центра сертификации к доверенным 6.6.1.2. Добавление сторонних выпускающих центров сертификации в хранилище NTAuth службы Active Directory......105 6.6.1.3. Запрос и установка сертификата контроллеров домена на контроллер(ы) домена. 105 6.6.2. 7. Использование Крипто Про CSP при работе с почтовым клиентом The Bat! 109 7.1. Настройка параметров S/МІМЕ почтового клиента......109 7.2. 7.3. 8. Использование КриптоПро CSP при работе с почтовым клиентом Outlook 2013 114 8 1 8.2. Отправка подписанных сообщений......116 8.3. 8.4. 8.5.

1. Инсталляция СКЗИ КриптоПро СSP

Установка дистрибутива СКЗИ КриптоПро CSP должна производиться пользователем, имеющим права администратора.

Для установки программного обеспечения вставьте компакт-диск в дисковод.

КриптоПро CSP 4.0 (Disk 1 of 1)		
	Начало	
	<mark>Язык</mark> <u>S</u> witch to english	
	Установка <u>А</u> рхитектура x86/x64 Архитектура <u>I</u> tanium	
	Информация Примечания к выпуску Обзор <u>а</u> окументации	
Крипто <mark>Про</mark> CSP	<u>О</u> бзор диска <u>С</u> айт ООО КРИПТО-ПРО	
4.0		Выход

Рисунок 1. Установка СКЗИ КриптоПро CSP

Выберите удобный для Вас язык установки и дистрибутив, соответствующий используемой операционной системе.

Примечание. также установка может производиться с дистрибутива, полученного с сайта ООО КРИПТО-ПРО. В таком случае пользователю нужно запустить файл дистрибутива CSPSetup.exe.

Перед запуском мастера установки выводится диалоговое окно, в котором доступен выбор уровня защищенности (кнопка **Опции**).

Þ	CSPSetup ×					
K	КРИПТО-ПРО - ключевое слово в защите информации					
h	http://www.cryptopro.ru					
Б Д Е	ілагодарим за выбор КриптоПро CSP. Іля продолжения установки нажимте "Далее", іля установки специфических настроек - "Опции". Если вы не знаете, что выбирать, нажмите Далее".					
	Опции Далее Отмена					

Рисунок 2. Начало установки

В СКЗИ КриптоПро реализованы классы защиты КС1, КС2, КС3 согласно требованиям ФСБ России.

<u>k</u>		CSP	Setup		×
Язык уста	новки:				
• Русский	i				
🔵 English					
Уровень б	езопасни	ости:			
● KC1					
○кс2					
○ксз					
Скрыть			Далее	Отмена	а
-					

Рисунок З. Выбор уровня безопасности

Укажите требуемый уровень безопасности, если он отличается от значения по умолчанию. После этого можно переходить к работе с мастером установки.

谩	Устан	овка "КриптоПро CSP"	×
		Вас приветствует программа установки "КриптоПро CSP (КС2)"	
		Программа выполнит установку "КриптоПро CSP " на компьютер. Для продолжения нажмите кнопку "Дале	:e".
Крип	то <mark>Про</mark> CSP 4.0	ПРЕДУПРЕЖДЕНИЕ: Данная программа защищена закона об авторских правах и международными соглашениями.	эми
		< Назад Далее > Отмена	

Рисунок 4. Приветственное окно мастера установки

Если на машине была установлена более ранняя версия СКЗИ КриптоПро CSP, то в окне появится информация об обновляемой версии:



Рисунок 5. Установка с замещением компонентов

Для продолжения установки КриптоПро CSP нажмите **Далее**.

Внимательно прочитайте лицензионное соглашение, которое выводится при первой установке. Дальнейшая установка производится в соответствии с сообщениями, выдаваемыми мастером. В процессе установки может быть предложено:

- о ввести серийный номер лицензии криптопровайдера;
- о зарегистрировать дополнительные считыватели ключевой информации;
- настроить дополнительные датчики случайных чисел;

Эти параметры можно изменить после завершения установки через панель свойств КриптоПро CSP. Для корректной работы КриптоПро CSP после завершения установки необходимо перезагрузить компьютер в случае, если пользователю предлагается перезагрузка.

В процессе установки мастером может быть предложен выбор наиболее подходящего вида установки.

i	Установка "КриптоПро CSP"	×
Вид установ и Выбор наибо	ки подходящего вида установки.	
Выберите ви	ид установки.	
Обычная С	я Будет установлен стандартный набор компонент.	
Выбороч	чная Выбор необходимых компонентов программы и папки установки. Рассчитана на опытных пользователей.	
	< Назад Далее > Отмена	

Рисунок 6. Выбор вида установки

По умолчанию (вид установки «Обычная») устанавливаются только основные файлы для работы СКЗИ (для Windows Server 2008 по умолчанию также устанавливается «Драйверная библиотека CSP»). При необходимости можно изменить набор компонентов для установки:

🔋 Установ	ка "КриптоПро	CSP"	×
Выборочная установка Выберите компоненты программы, к	оторые необходимо	установить.	
Щелкните значок в списке ниже, чтоб	ы изменить способ у ть с продуктами М ядра ОС 20 CSP 3.6 20 CSP 3.0 >	истановки компонента. Описание компонента Файлы, необходимые д работы продукта.	ля
Папка: C: \Program Files (x86) \Crypto Pro \CSP \		Измен	ИТЬ
Подсказка	< Назад	Далее > От	чена

Рисунок 7. Выборочная установка

Расширенная совместимость с продуктами Microsoft – Обеспечивает совместимость с такими приложениями, как Microsoft Office, Outlook Express. Необходима для входа в систему по смарт-картам.

Служба хранения ключей – Обеспечивает хранение, использование и кэширование ключей в отдельном сервисе ОС. По умолчанию включена для уровня безопасности КС2 и КС3 (подробно описана в разделе <u>Установка параметров безопасности</u>).

Revocation Provider - Механизм проверки текущего статуса сертификата с использованием OCSP. Является дополнением к стандартному механизму Windows проверки статуса сертификата на основе списка отозванных сертификатов (COC, CRL). Кроме этого предоставляет возможность использования COC, выпущенных по правилам, описанным в RFC 3280.

Криптопровайдер уровня ядра ОС- Необходим для работы криптопровайдера в службах и ядре Windows (TLS-cepвep, EFS, IPsec).

Совместимость с КриптоПро CSP 3.6 - Регистрирует имена провайдеров, совместимые с КриптоПро CSP 3.6. Необходимо только при наличии в хранилище «Личные» сертификатов, установленных с КриптоПро CSP 3.6.

Совместимость с КриптоПро CSP 3.0 - Регистрирует имена провайдеров, совместимые с КриптоПро CSP 3.0. Необходимо только при наличии в хранилище «Личные» сертификатов, установленных с КриптоПро CSP 3.0.

Примечание. В состав КриптоПро CSP SDK, входит описание параметров командной строки установщика Windows (\CHM\msi-readme.txt), которые удобно использовать для автоматического развертывания дистрибутива.

После нажатия на **Далее** мастером установки предлагается запланировать или отменить установку библиотек поддержки считывателей, а также принять решение о включении функционала накопления информации об использованных съёмных ключевых носителях. Помимо этого, также необходимо включить режим усиленного контроля использования ключей. Данный режим осуществляет контроль срока действия долговременных ключей электронной подписи и ключевого обмена, контроль доверенности ключей проверки электронной подписи и контроль корректного использования программного датчика случайных чисел. Использование СКЗИ КриптоПро CSP 4.0 без включения режима усиленного контроля использования ключей разрешается только в тестовых целях.

юследние приготовения к ус	тановке программ	ы	
Программа готова к началу уста	новки.		
Выберите требуемые библиотек	ки поддержки (можно	настроить позже):	
🔽 Зарегистрировать считыв	атель "Реестр"		
📝 Зарегистрировать считыв	атель смарт-карт		
🔽 Зарегистрировать считыв	атель съемных носит	елей	
📝 Не сохранять информацию	об использованных	съемных носителях	
👿 Усиленный контроль испол	пьзования ключей		
Нажмите кнопку "Установить", ч	чтобы начать устано	вку.	
Чтобы просмотреть или изменит Нажмите кнопку "Отмена" для в	ъ параметры установ ыхода из программы.	зки, нажмите кнопку	/ "Назад".
	13		

Рисунок 8. Установка усиленного контроля использования ключей

При установке СКЗИ с включением режима усиленного контроля использования ключей будут запрошены данные с датчика случайных чисел. В случае ошибки получения данных будет отображено окно, пример которого приведён на Рисунок 9. В этом случае при начале работы пользователя в системе с установленным СКЗИ КриптоПро CSP 4.0 необходимо проверить, что зарегистрирован хотя бы один физический датчик случайных чисел (например, внешняя гамма или аппаратный ДСЧ), и выполнить команду:

csptest.exe -keyset -verifycontext -hard_rng.

После завершения установки СКЗИ с включённым режимом усиленного контроля использования ключей **необходимо в обязательном порядке** установить доверенные корневые сертификаты в хранилище сертификатов локального компьютера CryptoProTrustedStore («Доверенные корневые сертификаты КриптоПро CSP», «CryptoPro CSP Trusted Roots») с помощью оснастки Сертификаты либо с помощью утилиты certmgr.exe:

certmgr.exe -inst -cert -silent -store mCryptoProTrustedStore -file ca.cer

После этого следует осуществить перезагрузку компьютера.

Установ Устаная	ака "КриптоПро СSP 4.0.9702" вливаются выбранные компоненты программы.	
P	Дождитесь окончания установки "КриптоПро CSP". Это может занят несколько минут.	ть
		Σ
	чисслатеред использованием криптопро сог пеооходимо	
	установить ДСЧ и получить инициализирующие данные с помощью вызова "csptest.exe -keyset -verifycontext -hard_rng"	
	установить ДСЧ и получить инициализирующие данные с помощью вызова "csptest.exe -keyset -verifycontext -hard_rng"	ОК
	установить ДСЧ и получить инициализирующие данные с помощью вызова "csptest.exe -keyset -verifycontext -hard_rng"	

Рисунок 9. Окно ошибки получения данных с датчика случайных чисел при инсталляции СКЗИ.

2. Интерфейс СКЗИ КриптоПро CSP

2.1. Доступ к панели управления СКЗИ

Контрольная Панель управления средства криптографической защиты информации (СКЗИ) КриптоПро CSP доступна как отдельный пункт в группе программ «КРИПТО-ПРО» (меню **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP**).

Приложения				
по имени 🗸				
КРИПТО-ПРО	Диспетчер задач			
КриптоПро CSP	Защитник Windows			
КриптоПро РКІ	Командная строка			
Сертификаты	Панель управления			
Управление лицензиями	Проводник			
Служебные — Windows	Программы по умолчанию			

Рисунок 10. Доступ к оснастке

Панель управления СКЗИ КриптоПро CSP осуществляет доступ к настройке функций с помощью вкладок:

- <u>Общие;</u>
- Оборудование;
- <u>Сервис;</u>
- <u>Алгоритмы</u>;
- Безопасность;
- <u>Winlogon;</u>
- <u>Настройки TLS;</u>
- Дополнительно.

	Крипто	Про CSP		
Алгоритмы	Безопасность	Winlogon	Настройки TLS	
Общие	Оборудование	Сервис	Дополнительно	
<u>(0 r</u>	<u>птоПро CSP</u> Ве Е Сомпания КРИПТО-ПРО	рсия ядра СКЗІ ерсия продукт . Все права заш	И: а: ищены.	
<u>Запусти:</u>	гь с правами админист;	ратора		
Лицензия				
Серийный	номер: 4040EG0037E	K8R3C6K4		
Владелец:	Владелец:			
Организац	ия:			
Срок дейс	твия 22.05.2014			
Тип лицен Первая ус	зии: Серверная гановка: 20.02.2014	Ве	од лицензии	
Язык				
Выберите CSP вашей	язык для отображения учетной записи:	<ум	олчание систен 🗸	
Выберите CSP польз (умолчани	язык для отображения рвателей, не задавших е системы):	а окон (язык	кий 🗸	
	0	КОт	иена Примени	

Рисунок 11. Панель управления

2.2. Общие параметры СКЗИ

Вкладка **Общие** (см. Рисунок 11) панели управления СКЗИ КриптоПро CSP предназначена для просмотра информации о версии установленного ПО СКЗИ КриптоПро CSP, информации о лицензии и ввода нового серийного номера (подробнее см. <u>Ввод серийного номера лицензии криптопровайдера</u> <u>«КриптоПро CSP»</u>), изменения языка работы пользователя с данным ПО.

2.3. Ввод серийного номера лицензии криптопровайдера «КриптоПро CSP»

При установке программного обеспечения КриптоПро CSP пользователю предлагается ввести данные лицензии. Без ввода лицензии пользователю предоставляется ознакомительная лицензия с ограниченным сроком действия, для использования КриптоПро CSP после окончания этого срока нужно ввести серийный номер с бланка Лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта. Если КриптоПро CSP используется на клиентской машине, то требуется лицензия клиентского типа, если на сервере, то серверная лицензия.

Для ввода лицензии после установки КриптоПро CSP воспользуйтесь кнопкой Ввод лицензии на вкладке Общие <u>панели управления</u> КриптоПро CSP. Откроется окно «Сведения о пользователе» (см. Рисунок 13).

Также можно ввести лицензию с помощью утилиты Управление лицензиями КриптоПро РКІ. Для этого выполните **Пуск > Программы > КриптоПро > Управление лицензиями КриптоПро РКІ.** В оснастке Управление лицензиями КриптоПро РКІ выберите продукт, лицензию на который Вы хотите ввести. В контекстном меню выберите **Все задачи - Ввести серийный номер** (см. Рисунок 12).



Рисунок 12. Ввод серийного номера

Откроется окно «Сведения о пользователе», в котором необходимо указать сведения о пользователе, организации, а также ввести **серийный номер** с бланка **Лицензии** в соответствующие поля ввода (см. Рисунок 13).

😸 КриптоПро CSP	×
Сведения о пользователе Укажите сведения о себе.	
Пользователь: 	
<u>С</u> ерийный номер: Введите серийный номер, соответствующий лицензионному Серийный номер расположен на Вашем бланке «Лицензия на одном рабочем месте MS Windows программного продукта Кр	соглашению. право использования на оиптоПро CSP»
	ОК Отмена

Рисунок 13. Ввод данных лицензии

После ввода и нажатия клавиши ОК данные о лицензии сохранятся или обновятся.

2.4. Настройка оборудования СКЗИ

Вкладка **Оборудование** контрольной панели СКЗИ предназначена для изменения набора устройств <u>хранения</u> и <u>считывания</u> ключевой информации и <u>датчиков случайных чисел</u> (ДЧС).

По умолчанию поддерживаются все считыватели смарт-карт (и соответствующие им типы носителей), все дисководы съемных дисков, в том числе flash-носители.

訬	Установка "КриптоПро CSP"	×
п	оследние приготовения к установке программы Программа готова к началу установки.	
	Выберите требуемые библиотеки поддержки (можно настроить позже): ✓ Зарегистрировать считыватель "Реестр" ✓ Зарегистрировать считыватель смарт-карт ✓ Зарегистрировать считыватель съемных носителей	
	Не сохранять информацию об использованных съемных носителях Не разрешать интерактивные сервисы Windows Нажмите кнопку "Установить", чтобы начать установку. Чтобы просмотреть или изменить параметры установки, нажмите кнопку "Назад". Нажмите кнопку "Отмена" для выхода из программы.	
	< Назад Установить Отмена	

Рисунок 14. Настройка оборудования по уровню защиты КС1

В исполнении по уровню защиты КС1 предустановлен Биологический ДСЧ. В исполнениях по уровням защиты КС2 и КС3 Биологический ДСЧ или аппаратный ДСЧ «Соболь»/ АПМДЗ-У М-526Б (КРИПТОН ЗАМОК/У) можно добавить в процессе установки криптопровайдера.

謾	Установка "КриптоПро CSP"						
No T	Последние приготовения к установке программы Программа готова к началу установки.						
E	Выберите требуемые библиотеки поддержки (можно настроить позже): Зарегистрировать считыватель "Реестр" Зарегистрировать считыватель смарт-карт Зарегистрировать считыватель съемных носителей						
ł	 Зарегистрировать датчик случайных чисел "Соболь" Зарегистрировать биологический датчик случайных чисел (не рекомендуется) Не сохранять информацию об использованных съемных носителях Не разрешать интерактивные сервисы Windows Нажмите кнопку "Установить", чтобы начать установку. Чтобы просмотреть или изменить параметры установки, нажмите кнопку "Назад". Нажмите кнопку "Отмена" для выхода из программы. 						
	< Назад Установить Отмена						

Рисунок 15. Настройка оборудования по уровням защиты КС2 и КС3

2.4.1. Изменение набора устройств считывания ключевой информации

2.4.1.1. Добавление считывателя

Для того, чтобы добавить считыватель, откройте <u>Панель управления</u> СКЗИ КриптоПро CSP. Панель управления долж на быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить считыватели.**

	Крип	тоПро С	SP	
Алгоритмь	Безопасност	ьWir	logon	Настройки TLS
Общие	Оборудование	Cep	вис	Дополнительно
Считыват	ели закрытых ключ Позволяет добавит закрытых ключей.	ей ъ или удал	ить счит	ыватели
		Настр	оить счи	тыватели
Типы клю	чевых носителей Позволяет добавит носителей.	На ть или удал	астроить ить типь	а дСЧ
_	ļ	Настрои	ить типь	і носителей

Рисунок 16. Контрольная панель. Вкладка «Оборудование»

Откроется окно «Управление считывателями» (см. Рисунок 17).

⊵ Управление считывателями	×
Считыватели	
Установлены следующие считыватели:	
Все считыватели смарт-карт Все съемные лиски	
Ет Реестр	
	1
Добавить Удалить Свойства	1
ОК Отмена	

Рисунок 17. Окно «Управление считывателями»

Для того чтобы в КриптоПро CSP стало доступным использование нового считывателя, нажмите кнопку **Добавить**. Запустится мастер установки считывателя (см. Рисунок 18).



Рисунок 18. Запуск мастера установки считывателя

Нажмите кнопку **Далее**, чтобы перейти к шагу «Выбор считывателя» (см. Рисунок 19). Выберите из списка считыватель, который следует добавить.

Þ	Мастер ус	тановки считывателя	×	
Выбор считывателя Какой считыватель необходимо установить?				
Выберите считы	затель, который сле	адует добавить, и нажмите кнопку "Далее".		
Производители:	Дос	тупные считыватели:		
(Все производи	тели)	Dallas (DS1410E)		
Компания КРИ	пто-про 🛛 👲	Dallas (DS9097E)		
		Dallas (DS9097U)		
		Соболь		
		< Назад Далее > Отми	ена	

Рисунок 19. Окно «Выбор считывателя»

В зависимости от выбранного считывателя может потребоваться выбор соединения для этого устройства. В таком случае на следующем шаге мастера выводится окно «Выбор соединения» (см. Рисунок 20). В этом окне выберите соединение для считывателя и нажмите кнопку **Далее.**

	Мастер установки считывателя
Выбор со Требуе	единения. тся выбрать соединение для этого устройства
Выбери Чтобы і	те соединение, которое следует использовать для данного соединения. продолжить установку после соединения, нажмите кнопку "Далее".
	Доступные соединения: LPT1 LPT2
	< Назад Далее > Отмена

Рисунок 20. Окно «Выбор соединения»

На следующем шаге выводится окно «Имя считывателя» (см. Рисунок 21). В этом окне введите имя выбранного считывателя и нажмите кнопку **Далее.**

Þ	Мастер установки считывателя ×
Им	ия 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: Dallas (DS1410E), LPT1
	< Назад Далее > Отмена

Рисунок 21. Окно «Имя считывателя»

Последний шаг - «Завершение работы мастера установки считывателя» (см. Рисунок 22). Внимательно прочитайте текст в этом окне, нажмите кнопку **Готово** и перезагрузите компьютер, если это требуется.

📙 Ma	стер установки считывателя	x
	Завершение работы мастера установки считывателя	
	Выбранный Вами считыватель требует дополнительной установки драйвера устройства от производителя данного устройства. Вы можете получить эти драйверы на веб-сервере компании Крипто-Про по адресу http://www.cryptopro.ru/cryptopro/products/csp/readers.htm.	
	Чтобы закончить установку считывателя, нажмите кнопку "Готово". После завершения установки рекомендуется ПЕРЕЗАГРУЗИТЬ компьютер. Нажмите кнопку "Назад", если требуется изменить параметры установки.	
	< Назад Готово Отмена	3

Рисунок 22. Завершение мастера установки считывателя

Примечание. Имеется возможность установки драйверов сторонних производителей, обеспечивающие взаимодействие КриптоПро CSP с аппаратной частью в случае, если они не входят в состав дистрибутива СКЗИ. Для их установки следует воспользоваться программой установки, поставляемой производителями таких устройств. Например, если КриптоПро CSP уже установлено, и нужно использовать новые устройства, необходимо установить поддерживающие драйвера и другие модули от производителей этих устройств.

2.4.1.2. Удаление считывателя

Для того, чтобы удалить считыватель, откройте <u>Панель управления</u> СКЗИ КриптоПро CSP. Панель управления долж на быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить считыватели.**

Откроется окно «Управление считывателями» (см. Рисунок 17). Выберите считыватель, который требуется сделать недоступным, и нажмите кнопку **Удалить.**

В открывшемся диалоге подтвердите удаление считывателя, нажав ОК.

Þ	Подтверждение на удаление считывателя
	Подтвердите удаление считывателя: Dallas (DS1410E), LPT1
	ОК Отмена

Рисунок 23. Окно «Подтверждение на удаление считывателя»

После подтверждения использование считывателя СКЗИ станет недоступно.

2.4.1.3. Просмотр свойств считывателя

Чтобы просмотреть свойства считывателя откройте <u>Панель управления</u> СКЗИ КриптоПро CSP и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP (см. Рисунок 16) нажмите кнопку **Настроить считыватели**.

Откроется окно «Управление считывателями» (см. Рисунок 17). Выберите считыватель, свойства которого требуется просмотреть, и нажмите кнопку **Свойства.**

Выведется справочная информация о выбранном считывателе, в том числе, и данные о состоянии устройства. После просмотра свойств считывателя нажмите кнопку **ОК.**

Da	Ilas (DS1410E), LPT1
Устро подсо	йство чтения Touch-memory DS1410E, единяемое к LPT порту.
Соединение:	LPT1
Считыватель:	
Состояние:	Недоступен
Изготовитель:	Dallas Semiconductor
Версия:	Неизвестна
Библиотека сопря	жения:
Состояние:	Установлены
Изготовитель:	Компания КРИПТО-ПРО
Версия:	
	ОК Отмена

Рисунок 24. Свойства считывателя

2.4.2. Изменение набора устройств хранения ключевой информации

2.4.2.1. Добавление носителя

Для того, чтобы сделать доступным носитель ключевой информации, откройте <u>Панель управления</u> СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить типы носителей.**

Откроется окно «Управление ключевыми носителями» (см. Рисунок 25).

Носители Магистра, Магистра Сбербанк/BGS, Оскар, Оскар CSP 2.0, РИК являются смарткартами. Носители типа Rutoken и eToken являются USB-ключами.

Þ	Управление ключевыми носителями
Клю	учевые носители
9	-7
1 2	3
Уст	ановлены следующие ключевые носители:
	Athena IDProtect (E)
	ESMART Token 32K
	ESMART Token 64K
IP IP	INPASPOT
IP	INPASPOT, SCone
IP	INPASPOT1
IP I	INPASPOT2
	ISBC J2A/J3A
	Добавить Удалить Свойства
	ОК Отмена

Рисунок 25. Окно «Управление ключевыми носителями»

Для того, чтобы сделать доступным ключевой носитель, нажмите кнопку **Добавить**. Запустится мастер установки ключевого носителя (см. Рисунок 26).

📙 Мастер	установки ключевого носителя	×
	Мастер установки ключевого носителя	
	Мастер установки помогает выполнить установку и настройку ключевых носителей.	
	Чтобы приступить к установке, нажмите кнопку "Далее".	
	< Назад Далее > Отмен	а

Рисунок 26. Запуск мастера установки ключевого носителя

Нажмите кнопку **Далее**, чтобы перейти к шагу выбора ключевого носителя (см. Рисунок 27). Выберите ключевой носитель, который следует сделать доступным, и нажмите кнопку **Далее.**



Примечание. Запрещается использовать несъемные носители, а также носители, для которых не обеспечивается непрерывный контроль.

Выберите ключевой носитель, который следует добавить, и нажмите кнопку "Далее".					
Γ	Іроизводители:	Доступные ключевые носители:			
	(Все производители)	DS199x	^		
	Charismathics GmbH	ESMARTToken			
	Компания КРИПТО-ПРО				
	Компания ПрограмПарк	MPCOS-GEMALTO			
		MPCOSEMV			
			h d		

Рисунок 27. Окно «Выбор ключевого носителя»

После выбора ключевого носителя откроется окно «Имя ключевого носителя» (см. Рисунок 28). В этом окне введите имя выбранного носителя и нажмите кнопку **Далее.**

Þ	Мастер установки ключевого носителя
Имя ки Тре	пючевого носителя вбуется назначить имя для этого ключевого носителя
Мол исп выб	жно либо ввести желаемое имя для этого ключевого носителя, либо ользовать предложенное ниже имя. Чтобы продолжить установку после бора имени, нажмите кнопку "Далее".
	Имя ключевого носителя: MPCOSEMV
	< Назад Далее > Отмена

Рисунок 28. Окно «Имя ключевого носителя»

В зависимости от типа ключевого носителя следующие шаги мастера могут различаться, так для MPCOS/EMV будет отображено окно «Разметка карты» (см. Рисунок 29). В этом окне нужно указать разметку карты, после чего перейти к следующему шагу.

<u>le</u>	Мастер установки ключевого носителя
Какая разм Установ	иетка карты? ите параметры разметки карты
ATR:	3B2A008065A201010072D641
Маска:	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Приложение	CPCSP
	< Назад Далее > Отмена

Рисунок 29. Окно «Разметка карты»

Откроется окно «Завершение работы мастера установки ключевого носителя» (см. Рисунок 30). Нажмите в нем кнопку **Готово**.

📃 Мастер	установки ключевого носителя
	Завершение работы мастера установки ключевого носителя
	Чтобы закончить установку ключевого носителя, нажмите кнопку "Готово". Нажмите кнопку "Назад", если требуется изменить параметры установки.
	< Назад Готово Отмена

Рисунок 30. Завершение мастера установки ключевого носителя

Установленный ключевой носитель отобразится в списке окна «Управление ключевыми носителями (см. Рисунок 25).

2.4.2.2. Удаление ключевого носителя

Для того чтобы сделать недоступным ключевой носитель откройте <u>Панель управления</u> СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить типы носителей.**

В открывшемся диалоге подтвердите удаление ключевого носителя, нажав ОК.



Рисунок 31. Окно «Подтверждение на удаление ключевого носителя»

После подтверждения ключевой носитель станет недоступен для использования в работе криптопровайдера.

2.4.2.3. Просмотр свойств ключевого носителя

Для того, чтобы просмотреть свойства ключевого носителя, откройте <u>Панель управления</u> СКЗИ КриптоПро CSP и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP (см. Рисунок 16) нажмите кнопку **Настроить типы носителей.**

В открывшемся окне «Управление ключевыми носителями» (см. Рисунок 25) выберите ключевой носитель, свойства которого требуется просмотреть, и нажмите кнопку **Свойства.**

Откроется окно «Свойства: Имя носителя» (см. Рисунок 32), в котором отображается справочная информация о выбранном ключевом носителе, в том числе, и данные о состоянии устройства. После просмотра свойств ключевого носителя нажмите кнопку **ОК.**

l <mark>e</mark> I	NPASPOT, SCone
Общие Настройка р	азметки
INPAS	POT
ß	
Библиотека сопрях Состояние:	жения:
Изготовитель:	Inpas Ltd
Версия:	1.0.0.0
	ОК Отмена

Рисунок 32. Окно «Свойства: имя носителя»

2.4.3. Настройка датчиков случайных чисел (ДСЧ)

2.4.3.1. Добавление ДСЧ

При настройке ДСЧ и загрузке динамических библиотек должно быть установлено программное обеспечение, соответствующее аппаратному средству. Подключение ДСЧ должно соответствовать установкам программно-аппаратного комплекса.

Для того чтобы добавить ДСЧ, откройте <u>Панель управления</u> СКЗИ КриптоПро CSP. Панель управления долж на быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить ДСЧ.**

Откроется окно «Управление датчиками случайных чисел» (см. Рисунок 33).

⊵ Управление датчиками случайн	ых чисел 🖻
Датчики случайных чисел	
[1001110 [110010 011000	
Становлены следующие датчики случаиных Биологический ДСЧ	чисел:
	1
	t
Добавить Удалить	Свойства
ОК Отдена	Применить

Рисунок 33. Окно «Управление датчиками случайных чисел»

Для того, чтобы добавить ДСЧ, нажмите кнопку **Добавить**. Запустится мастер установки ДСЧ (см. Рисунок 34). Нажмите кнопку **Далее**, чтобы перейти к следующему шагу.

Þ	Мастер установки ДСЧ	×
	Мастер установки ДСЧ	
	Мастер установки помогает выполнить установку и настройку датчиков случайных чисел (ДСЧ).	
	Чтобы приступить к установке, нажмите кнопку "Далее".	
	< Назад Далее > Отмен	a

Рисунок 34. Запуск мастера установки ДСЧ

Откроется окно «Выбор ДСЧ» (см. Рисунок 35). В этом окне выберите датчик случайных чисел, который требуется добавить, и нажмите кнопку **Далее**, чтобы перейти к следующему шагу.

Выбор ДСЧ	
какои доч неооходимо ј	установить /
Выберите ДСЧ, который сле,	дует добавить, и нажмите кнопку "Далее".
Производители:	Доступные ДСЧ:
(Все производители)	🕼 АПМДЗ ДСЧ
Компания КРИПТО-ПРО	🖫 КриптоПро Исходный Материал
SAA TRUNKING HONOU	0000NB

Рисунок 35. Окно «Выбор ДСЧ»

Откроется окно «Имя ДСЧ» (см. Рисунок 36). В этом окне введите имя выбранного датчика случайных чисел и нажмите кнопку **Далее.**

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

Рисунок 36. Окно «Имя ДСЧ»

Последним шагом мастера откроется окно «Завершение работы мастера установки ДСЧ» (см. Рисунок 37). Нажмите в нем кнопку **Готово** и перезагрузите компьютер.

le.	Мастер установки ДСЧ	×
	Завершение работы мастера установки ДСЧ	
	Чтобы закончить установку ДСЧ, нажмите кнопку "Готово". После завершения установки рекомендуется ПЕРЕЗАГРУЗИТЬ компьютер.	
	Нажмите кнопку "Назад", если требуется изменить параметры установки. < Назад Готово Отмена	3
	< Назад Готово Отмена	3

Рисунок 37. Завершение мастера установки ДСЧ

2.4.3.2. Удаление ДСЧ

Для того, чтобы удалить ДСЧ, откройте <u>Панель управления</u> СКЗИ КриптоПро CSP. Панель управления долж на быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить ДСЧ**.

В открывшемся окне «Управление датчиками случайных чисел» (см. Рисунок 33) выберите датчик, который требуется удалить, и нажмите кнопку **Удалить.**

В появившемся диалоге нажмите ОК.

녩 Подт	верждение на удаление датчика случайных чи 🗙
1	Подтвердите удаление датчика случайных чисел: Соболь
	ОК Отмена

Рисунок 38. Окно «Подтверждение на удаление ДСЧ»

После подтверждения ДСЧ будет удалён.

2.4.3.3. Просмотр свойств ДСЧ

Для того чтобы просмотреть свойства ДСЧ, Для того чтобы добавить ДСЧ, откройте <u>Панель</u> <u>управления</u> СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить ДСЧ**.

Откроется окно «Управление датчиками случайных чисел» (см. Рисунок 33). Выберите датчик, свойства которого требуется просмотреть, и нажмите кнопку **Свойства**.

Откроется окно «Свойства: Имя ДСЧ» (см. Рисунок 39), в котором отображается справочная информация о выбранном датчике случайных чисел, в том числе и данные о состоянии устройства. После просмотра свойств ДСЧ нажмите кнопку **ОК.**

<u>le</u>	Биол	огический	ДСЧ		×
Общие					
F.	Биологиче	екий ДСЧ.			
Библио	тека сопряжени	19:			
Состоя	ние:	Подключены			
Изгото	зитель:	Компания КРИ	ПТО-ПРО		
Версия	:	4.0.4548.0			
			ок	Отмена	3

Рисунок 39. Окно «Свойства: имя ДСЧ»

Примечание. Если в СКЗИ настроено несколько датчиков случайных чисел, то при формировании исходной ключевой информации будет использоваться ДСЧ, находящийся в верхней строке списка установленных ДСЧ, если ДСЧ не установлен, то будет использован следующий и т.д. Например, если установлено два датчика случайных чисел - БиоДСЧ и ДСЧ Электронного замка «Соболь», они находятся в состоянии – «подключен» и в верхней строке списка датчиков случайных чисел указан ДСЧ Электронного замка «Соболь», то формирование исходной ключевой информации будет осуществляться на ДСЧ Электронного замка «Соболь».

Для использования БиоДСЧ, необходимо с помощью кнопок **М** перемест верхнюю позицию в списке.

переместить его на

2.5. Работа с контейнерами и сертификатами

Вкладка **Сервис** контрольной панели СКЗИ КриптоПро CSP предназначена для выполнения следующих операций:

• Копирование и удаление закрытого ключа, находящегося в существующем контейнере;

• <u>Тестирование</u> (проверка работоспособности) и отображение свойств ключа (ключей) и сертификата (сертификатов) в существующем контейнере;

• <u>Просмотр</u> и <u>установка</u> сертификата, находящегося в существующем контейнере закрытого ключа на носителе;

• Осуществление связки между существующим сертификатом из файла и существующим контейнером закрытого ключа на носителе;

• <u>Изменение</u> и <u>удаление</u> сохраненных паролей (PIN-кодов) доступа к носителям закрытых ключей;

• <u>Очистка информации</u> о ранее использованных съёмных носителях, на которых располагались контейнеры закрытых ключей.

2.5.1. Тестирование, копирование и удаление контейнера закрытого ключа

2.5.1.1. Тестирование контейнера закрытого ключа

Для того чтобы провести тест работоспособности контейнера закрытого ключа, откройте <u>Панель</u> <u>управления</u> СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 40). Нажмите кнопку **Протестировать.**

		IIIIOI	IDO CSP	
Алгоритмы	Безопасно	ость	Winlogon	Настройки TLS
Общие	Оборудовани	ие	Сервис	Дополнительно
Контейнер Эти мастер удалить ко Протести;	закрытого ключ а позволяют про нтейнер закрыт ровать С	на отестир ого клн жопиро	оовать, скоп оча с носите вать	ировать или ля. Удалить
Сертифика				
Этот масте в контейне сертифика	р позволяет про ре закрытого кл гов.	смотре юча, и	ть сертифик установить	аты, находящиеся их в хранилище
	Просмо	треть	сертификаты	в контейнере
Личный сер	тификат			
Этот масте контейнеро хранилище	р позволяет свя ом закрытого кл	зать се юча, ус	ртификат из становив это	файла с г сертификат в
	Ус	танови	ть личный се	ртификат
Пароли зак	рытых ключей			
Эти мастер ключей или	а позволяют изн 1 удалить запом	ченить ненные	пароли <mark>(ПИН</mark> ранее парол	-коды) закрытых и.
Измен	нить пароль	2	Удалить запо	мненные пароли

Рисунок 40. Контрольная панель. Вкладка «Сервис»

Откроется окно «Тестирование контейнера закрытого ключа» (см. Рисунок 41).

<u>e</u>	Тестирование контейнера закрытого ключа 🛛 🗙
Кон	атейнер закрытого ключа Введите или укажите контейнер закрытого ключа, который необходимо протестировать
Имяк	лючевого контейнера: Обзор
Введе	иное имя задает ключевой контейнер: По сертификату Пользователя Компьютера
Выбер	рите CSP для поиска ключевых контейнеров: Crypto-Pro GOST R 34. 10-2001 Cryptographic Service Provider 🛛 🗸 🗸
	< пазад Далее > Отмена

Рисунок 41. Окно «Тестирование контейнера закрытого ключа»

На этой форме необходимо заполнить поле **Имя ключевого контейнера**. Оно может быть введено вручную или найдено в списках контейнеров (кнопка **Обзор**) или сертификатов (кнопка **По** сертификату).

Опции поиска:

- Введенное имя задает ключевой контейнер переключатель устанавливается в положение Пользователь или Компьютер, в зависимости от того, в каком хранилище (Личные или Локального компьютера соответственно) расположен контейнер. Для тестирования контейнера закрытого ключа из хранилища Локального компьютера необходимы права администратора.
- Выберите CSP для поиска ключевых контейнеров необходимый криптопровайдер (CSP) выбирается из предлагаемого списка.

После того, как все поля заполнены, нажмите кнопку Далее.

Если на доступ к закрытому ключу установлен пароль, то он будет запрошен. Введите пароль и нажмите кнопку **ОК**.

После этого откроется форма с результатом тестирования (см. Рисунок 42), в котором будет выведена информация о данном контейнере и результат теста.

е Тестирова	ние контейнера закрытого Работа мастера провер завершена	ключа ×
	Проверка завершена успешно Контейнер закрытого ключа имя уникальное имя FQCN проверка целостности контейнера Ключ обмена длина ключа экспорт открытого ключа импорт открытого ключа подпись проверка <	ошибок не обнару: ∧ ivanovcert ivanovcert \\. \REGISTRY\jvanc успешно успешно успешно успешно успешно успешно успешно успешно успешно успешно успешно
	< Назад Го	тово Отмена



2.5.1.2. Копирование контейнера закрытого ключа

Для того чтобы скопировать контейнер закрытого ключа, откройте <u>Панель управления</u> СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 40). Нажмите кнопку **Скопировать**. Откроется окно «Копирование контейнера закрытого ключа» (см. Рисунок 43).

<u>e</u>	Копирование контейнера закрытого кл	юча 🗙
Конте Вв ск	йнер закрытого ключа едите или укажите контейнер закрытого ключа, который не опировать	обходимо
Имя клю	евого контейнера:	
I		Обзор
Введенн К	е имя задает ключевой контейнер: ользователя омпьютера	По сертификату
Выберит	е CSP для поиска ключевых контейнеров:	
Cryp	to-Pro GOST R 34.10-2001 Cryptographic Service Provider	¥
	< Назад Далее	е > Отмена

Рисунок 43. Окно «Копирование контейнера закрытого ключа»

На этой форме необходимо заполнить поле **Имя ключевого контейнера**. Оно может быть введено вручную или найдено в списках контейнеров (кнопка **Обзор**) или сертификатов (кнопка **По** сертификату).

Опции поиска:

- Введенное имя задает ключевой контейнер переключатель устанавливается в положение Пользователь или Компьютер, в зависимости от того, в каком хранилище (Личные или Локального компьютера соответственно) расположен контейнер. Для работы с контейнером закрытого ключа из хранилища Локального компьютера необходимы права администратора.
- Выберите CSP для поиска ключевых контейнеров необходимый криптопровайдер (CSP) выбирается из предлагаемого списка.

После того, как все поля заполнены, нажмите кнопку Далее.

	Крипт	оПро CSP	
Выбор ключевог	о контейнера		0:09:38
В списке показ	ывать:		
Дружестве	нные имена	О Уникальны	ые имена
Список ключевь	іх контейнеро	в пользователя:	
Считыватель	Имя контейн	epa	
Реестр	ivanovcert		
Реестр	petrovcert		
		ОК	Отмена

Рисунок 44. Выбор ключевого контейнера

Þ	Безопасность Windows
Выбор сер Выберите сер пользователя	ртификата ртификат из хранилища "Личные" текущего я.
	semenov Издатель: Test Center CRYPTO-PRO Действителен с: 25.02.2014 по 04.10.2014 Просмотреть свойства сертификата
	petrov Издатель: Test Center CRYPTO-PRO Действителен с: 25.02.2014 по 04.10.2014
Ħ	ivanovii Издатель: Test Center CRYPTO-PRO Действителен с: 25.02.2014 по 04.10.2014
	ОК Отмена

Рисунок 45. Выбор сертификата

Если на доступ к закрытому ключу установлен пароль, то он будет запрошен. Введите пароль и нажмите кнопку **ОК**.

Откроется окно ввода параметров нового контейнера закрытого ключа (см. Рисунок 46). Введите имя нового ключевого контейнера и установите переключатель **Введенное имя задает ключевой** контейнер в положение **Пользователь** или **Компьютер**, в зависимости от того, в каком хранилище требуется разместить скопированный контейнер.

Þ	Копирование контейнера закрытого кл	юча 🗙
Ко	нтейнер закрытого ключа Введите контейнер закрытого ключа, на который необходимо скопировать	
Имян	ключевого контейнера:	
	ivanovcopy	
Введ (енное имя задает ключевой контейнер: ● Пользователя ● Компьютера	
Выбе	рите CSP для поиска ключевых контейнеров:	
	Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider	¥
	< Назад Готов	во Отмена

Рисунок 46. Окно «Копирование контейнера закрытого ключа»

После ввода нажмите кнопку **Готово**. Откроется окно, в котором необходимо выбрать носитель для скопированного контейнера (см. Рисунок 47).

3	к	риптоПро CSP	×
Све	Вставьте и выбери закрытого ключа дения	ите носитель для хранения контейне; "ivanovcopy".	0:09:54 pa
	Устройства:	Вставленный носитель:	
		ОК Отмена Сведени	ія <<

Рисунок 47. Окно выбора носителя

Вставьте носитель в считыватель, выберите носитель из перечня устройств и нажмите кнопку **ОК**. Откроется окно создания пароля на доступ к закрытому ключу (см. Рисунок 48). Введите пароль, подтвердите его.

3	КриптоПро CSP	×
Задайте парол "ivanovcopy".	ль для создаваемого контейнера	0:09:14
 Установить новый п Новый пароль: 	пароль	EN
Подтверждение:		
ОК	Отмена Подр	обнее >>

Рисунок 48. Окно ввода пароля

После ввода необходимых данных нажмите кнопку **ОК**. СКЗИ «КриптоПро CSP» осуществит копирование контейнера закрытого ключа.

2.5.1.3. Удаление контейнера закрытого ключа

Для того чтобы удалить контейнер закрытого ключа откройте <u>Панель управления</u> СКЗИ КриптоПро CSP, перейдите на вкладку **Сервис** (см. Рисунок 40) и нажмите кнопку **Удалить контейнер**.

Откроется окно «Удаление контейнера закрытого ключа» (см. Рисунок 49).

го ключа ите контейнер закри ра:	ытого ключа, і	который нео	обходимо	
pa:				
pa:				
			063	op
ючевой контейнер:	:		По серти	фикату
а ключевых контей 4, 10-2001 Cryptogra	неров: phic Service Pro	ovider	~	
	< Назад	Готов	30 (Отмена
	ючевой контейнер а ключевых контей 4. 10-2001 Cryptogra	ючевой контейнер: а ключевых контейнеров: 4. 10-2001 Cryptographic Service Pro < Назад	ючевой контейнер: а ключевых контейнеров: 4. 10-2001 Cryptographic Service Provider < Назад Готов	ючевой контейнер: По сертил а ключевых контейнеров: 4. 10-2001 Cryptographic Service Provider v < Назад Готово (

Рисунок 49. Окно «Удаление контейнера закрытого ключа»

На этой форме необходимо заполнить поле **Имя ключевого контейнера**. Оно может быть введено вручную или найдено в списках контейнеров (кнопка **Обзор**) или сертификатов (кнопка **По** сертификату).

Опции поиска:

- Введенное имя задает ключевой контейнер переключатель устанавливается в положение Пользователь или Компьютер, в зависимости от того, в каком хранилище (Личные или Локального компьютера соответственно) расположен контейнер. Для удаления контейнера закрытого ключа из хранилища Локального компьютера необходимы права администратора.
- Выберите CSP для поиска ключевых контейнеров необходимый криптопровайдер (CSP) выбирается из предлагаемого списка.

После того, как все поля заполнены, нажмите кнопку Готово.

В диалоге подтверждения удаления ключевого контейнера (см. Рисунок 50) нажмите кнопку Да.



Рисунок 50. Окно подтверждения удаления ключевого контейнера

2.5.2. Просмотр и установка личного сертификата, хранящегося в контейнере закрытого ключа

2.5.2.1. Просмотр сертификата, хранящегося в контейнере закрытого ключа

Для того чтобы просмотреть сертификат, хранящийся в контейнере закрытого ключа, откройте <u>Панель управления</u> СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 40), нажмите кнопку **Просмотреть сертификаты в контейнере**.

Откроется окно «Сертификаты в контейнере закрытого ключа» (см. Рисунок 51).

Þ	Сертификаты в контейнере закрытого кл	тюча ×
Конт В	ейнер закрытого ключа ведите или укажите контейнер закрытого ключа для просмотр ертификатов в этом контейнере	
Имя клк	учевого контейнера:	Обзор
Введени ОГ	ное имя задает ключевой контейнер: Тользователя Компьютера	По сертификату
Выбери	те CSP для поиска ключевых контейнеров: /pto-Pro GOST R 34.10-2001 Cryptographic Service Provider	*
	, , , , , , , , , , , , , , , , , , ,	
	< Назад Далее	> Отмена

Рисунок 51. Окно «Сертификаты в контейнере закрытого ключа»

На этой форме необходимо заполнить поле **Имя ключевого контейнера**. Оно может быть введено вручную или найдено в списках контейнеров (кнопка **Обзор**) или сертификатов (кнопка **По** сертификату).

Опции поиска:

- Введенное имя задает ключевой контейнер переключатель устанавливается в положение Пользователь или Компьютер, в зависимости от того, в каком хранилище (Личные или Локального компьютера соответственно) расположен контейнер. Для просмотра контейнера закрытого ключа из хранилища Локального компьютера необходимы права администратора.
- Выберите СЅР для поиска ключевых контейнеров необходимый криптопровайдер (СЅР) выбирается из предлагаемого списка.

После того, как все поля заполнены, нажмите кнопку Далее.

Если сертификата в контейнере закрытого ключа нет, об этом появится сообщение (см. Рисунок 52).



Рисунок 52. Окно, информирующее об отсутствии сертификата

Если сертификат в выбранном контейнере имеется, откроется окно «Сертификат для просмотра» (см. Рисунок 53).

Сертификат для Просмотрите и	просмотра 1 выберите сертификат	P
Сертификат:	petrov	
Субъект:	CN=petrov, C=RU	
Поставщик:	E=info@cryptopro.ru, C=RU, O=CRYPTO-PRO, CN=Te	st Center CRYPT
Действителен с:	25 февраля 2014г. 16:55:03	
Действителен по:	4 октября 2014 г. 11:09:41	
Серийный номер:	6DB0 80F2 0002 0006 9670	
	Установить	Свойства
		Обзор

Рисунок 53. Окно «Сертификаты в контейнере закрытого ключа»

Для просмотра основных свойств сертификата нажмите кнопку **Свойства** в окне «Сертификаты в контейнере закрытого ключа» (см. Рисунок 53). Откроется окно просмотра свойств сертификата (см. Рисунок 54).

	Сертификат	x	
Общие	Общие Состав Путь сертификации		
	Сведения о сертификате		
Эт	Этот сертификат предназначается для:		
	 Подтверждает удаленному компьютеру идентификацию вашего компьютера 		
Ko	мувыдан: реточ		
Ke	теst Center CRYPTO-PRO		
	Действителен с 25.02.2014 по 04.10.2014		
1	💡 Есть закрытый ключ для этого сертификата.		
	Установить сертификат Заявление поставщика		
	OK		

Рисунок 54. Окно просмотра свойств сертификата

На вкладке «Путь сертификации» можно просмотреть все сертификаты до корневого УЦ, если они содержатся в контейнере.

2.5.2.2. Установка личного сертификата, хранящегося в контейнере закрытого ключа

Примечание. В данном разделе руководства под установкой личного сертификата понимается установка сертификата в хранилище **Личные** с формированием ссылки на закрытый ключ, соответствующий данному сертификату.

Реализация КриптоПро CSP позволяет хранить личные сертификаты пользователя не только в локальном справочнике сертификатов компьютера, а также вместе с личными ключами пользователя на ключевом носителе (при условии, что ключевой носитель имеет достаточный объем памяти для записи сертификата). Хранение сертификата на ключевом носителе позволяет пользователю переносить всю необходимую ключевую информацию с компьютера, где был сформирован ключ пользователя на другие рабочие места.

Для того чтобы воспользоваться личными ключами и сертификатами пользователя в различных приложениях на другом компьютере, необходимо на этом компьютере установить пользовательский сертификат в локальный справочник и создать ссылку, которая будет однозначно связывать сертификат с личным ключом пользователя.

Для того чтобы установить личный сертификат, откройте его для просмотра, для этого выполните последовательность действий, указанных в пункте 2.5.2.1.

В окне «Сертификаты в контейнере закрытого ключа» (см. Рисунок 53) нажмите кнопку Установить.

Сертификат будет установлен в хранилище «Личные» текущего пользователя или компьютера, в зависимости от опции, выбранной при поиске контейнера.

Если сертификат уже есть в хранилище, будет выдано предупреждение о перезаписи прежнего сертификата (см. Рисунок 55).



Рисунок 55. Предупреждение о перезаписи сертификата

В случае успеха появится сообщение о завершении операции (см. Рисунок 56).



Рисунок 56. Окно завершения установки сертификата

При таком способе установки сертификатов в соответствующие хранилища также устанавливаются сертификаты корневых и промежуточных УЦ, если они содержатся в контейнере закрытого ключа.

2.5.3. Установка личного сертификата, хранящегося в файле

Примечание. В данном разделе инструкции под установкой личного сертификата понимается установка сертификата в хранилище **Личные** с формированием ссылки на закрытый ключ, соответствующий данному сертификату.

Для того чтобы установить личный сертификат откройте <u>Панель управления</u> СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 40), нажмите кнопку **Установить личный сертификат**.
В окне «Расположение файла сертификата» (см. Рисунок 57) будет предложено указать **Имя** файла сертификата. Выберите путь к файлу с помощью кнопки Обзор, после чего нажмите кнопку Далее.

Þ	Мастер установки личного сертификата 🛛 🗙
Pac	положение файла сертификата Зведите или укажите расположение файла устанавливаемого сертификата
Имя ф	айла сертификата: Обзор
	Формат файла может одним из следующих: Файл сертификата - X.509 (.CER.,CRT) Сообщение стандарта РКСS #7 (.P7B,.P7M,.DER) Хранилище сериализованных сертификатов (.SST) Замечание: Некоторые форматы файлов могут содержать в одном файле более одного сертификата.
	< Назад Далее > Отмена

Рисунок 57. Окно «Расположение файла сертификата»

Откроется просмотр основной информации сертификата для установки (см. Рисунок 58). Нажав на кнопку **Свойства** можно просмотреть подробную информацию о сертификате в стандартном окне просмотра свойств сертификата.

<u>e</u> N	Ластер установки личного сертификата	>
Сертификат для Просмотрите	а установки и выберите сертификат для установки	
Сертификат:	ivanovii	
Субъект:	CN=ivanovii, C=RU	
Поставщик:	E=info@cryptopro.ru, C=RU, O=CRYPTO-PRO, CN=Test	Center CRYPTO-
Действителен с:	25 февраля 2014 г. 15:39:04	
Действителен по:	4 октября 2014 г. 11:09:41	
Серийный номер:	6D6A C5EF 0002 0006 965C	
		Свойства
		Обзор
	< Назад Далее >	Отмена

Рисунок 58. Окно «Сертификат для установки»

Нажмите кнопку Далее. Откроется окно «Контейнер закрытого ключа» (см. Рисунок 59).

<u>le</u>	Мастер установки личного сертификата
Контейнер з	закрытого ключа
Введите и	или укажите контейнер закрытого ключа, который соответствует
выбранно	ому сертификату
Найти ко	онтейнер автоматически
Имя ключевого	контейнера:
Введенное имя Пользов Компьют	задает ключевой контейнер: ателя тера
Выберите CSP д	иля поиска ключевых контейнеров:
Crypto-Pro C	GOST R 34.10-2001 Cryptographic Service Provider v
	< Назад Далее > Отмена

Рисунок 59. Окно «Контейнер закрытого ключа»

На этой форме необходимо заполнить поле **Имя ключевого контейнера**. Оно может быть введено вручную или найдено в списках контейнеров (кнопка **Обзор**) или сертификатов (кнопка **По** сертификату). Для автоматического поиска подходящего контейнера среди доступных можно воспользоваться опцией **Найти контейнер автоматически**.

Опции поиска:

- Введенное имя задает ключевой контейнер переключатель устанавливается в положение Пользователь или Компьютер, в зависимости от того, в каком хранилище (Личные или Локального компьютера соответственно) расположен контейнер.
- Выберите CSP для поиска ключевых контейнеров необходимый криптопровайдер (CSP) выбирается из предлагаемого списка.

После того, как все поля заполнены, нажмите кнопку Далее.

Если на доступ к закрытому ключу установлен пароль, то он будет запрошен. Введите пароль и нажмите кнопку **ОК**.

На следующем шаге с помощью кнопки **Обзор** выберите хранилище для установки сертификата. Сертификат будет установлен в хранилище пользователя или компьютера, в зависимости от расположения контейнера закрытого ключа (см. предыдущий пункт).

Þ	Мастер установки личного сертификата
Храни Ук сер	лище сертификатов ажите хранилище сертификатов для установки выбранного ранее ртификата.
Указанны компьюте Имя хран	ый ранее флаг использования ключевых контейнеров пользователя или ера определяет выбор необходимых хранилищ сертификатов иилища сертификатов:
Личн	ное Обзор
🗸 Устан	Используются хранилища сертификатов: Пользователя Компьютера овить сертификат в контейнер
	< Назад Далее > Отмена

Рисунок 60. Окно «Хранилище сертификатов»

Одновременно сертификат можно записать в ключевой контейнер для удобства поиска сертификата при переносе контейнера на другой компьютер. Для этого служит опция «Установить сертификат в контейнер» (см. Рисунок 60).

На последнем шаге «Завершение работы мастера установки личного сертификата» (см. Рисунок 61) нужно проверить правильность указанных параметров и для выполнения установки сертификата нажать кнопку **Готово**.

📃 Мастер	о установки личного с	ертификата
	Завершение рабо установки личной Работа мастера установки завершена. Были указаны следующие г	оты мастера го сертификата личного сертификата успешно параметры:
	Взять сертификат из файла имя сертификата субъект поставщик действителен с действителен по серийный номер	 C:\ss.cer ivanovii CN=ivanovii, C=RU E=info@cryptopro.ru, C=R 25 февраля 2014 г. 15:35 4 октября 2014 г. 11:09:4 6D6A C5EF 0002 0006 96 ∨
	Убедитесь, что выбраны пр нажмите кнопку "Готово" д	авильные параметры и ля выполнения установки.
	< Назад	Готово Отмена

Рисунок 61. Завершение работы мастера установки личного сертификата

2.5.4. Управление паролями доступа к закрытым ключам

2.5.4.1. Изменение пароля на доступ к закрытому ключу

Для того, чтобы изменить пароль на контейнер, откройте <u>Панель управления</u> СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 40), нажмите кнопку **Изменить пароль**.

Откроется окно «Контейнер закрытого ключа» (см. Рисунок 62).

2	Изменение	пароля конт	тейнера закр	оытого	ключа	
Конте Вве изм	йнер закрытого н адите или укажите н ненить пароль.	илюча контейнер закры	отого ключа, на	котором н	необходимо	
Имя ключ	евого контейнера:				Обзор	
Введенно По Ко	е имя задает ключе ильзователя мпьютера	евой контейнер:			По сертифика	ту
Выберите	: CSP для поиска кли	ючевых контейн 1-2001 Cryptograf	неров: phic Service Provic	lor	v	
стур	0410 0031 K 34.10	-2001 Cryptograp	June Service F10Vic		•	

Рисунок 62. Окно «Контейнер закрытого ключа»

На этой форме необходимо заполнить поле **Имя ключевого контейнера**. Оно может быть введено вручную или найдено в списках контейнеров (кнопка **Обзор**) или соответствующих им сертификатов (кнопка **По сертификату**).

Опции поиска:

- Введенное имя задает ключевой контейнер переключатель устанавливается в положение Пользователь или Компьютер, в зависимости от того, в каком хранилище (Личные или Локального компьютера соответственно) расположен контейнер. Автоматически ставится в нужное положение, если выбор производился по сертификату. Для работы с контейнером закрытого ключа из хранилища Локального компьютера необходимы права администратора.
- Выберите CSP для поиска ключевых контейнеров необходимый криптопровайдер (CSP) выбирается из предлагаемого списка.

После того, как все поля заполнены, нажмите кнопку Готово.

Откроется окно ввода пароля на доступ к закрытому ключу выбранного контейнера (см. Рисунок 63). Введите указанный пароль и нажмите кнопку **ОК.**

3	КриптоПро CSP	×
Введите парол Пе-13f1b328-8	њ для контейнера f40-41a8-afd5-05e9776c87ae"	0:09:58
		EN
Пароль:		
Запомнить пароль		
ОК	Отмена	

Рисунок 63. Ввод пароля на доступ

Если пароль введен верно, откроется окно ввода нового пароля на доступ к закрытому ключу (см. Рисунок 64). Введите дважды новый пароль и нажмите кнопку **ОК.**

3	КриптоПро CSP	×
Введите дваж 13f1b328-8f40	ды новый пароль для контейнера " -41a8-afd5-05e9776c87ae"	0:09:58 e-
• Установить новый г	ароль	EN
Новый пароль:		
Подтверждение:		
ОК	Отмена Подробн	iee >>

Рисунок 64. Ввод нового пароля

После подтверждения ввода пароля СКЗИ «КриптоПро CSP» осуществит смену пароля на доступ к закрытому ключу. Более подробно работа по установке пароля и дополнительных параметров защиты контейнера описана в пункте <u>Выбор способа защиты доступа к закрытому ключу</u>.

Примечание. Вместо установки пароля на доступ к закрытому ключу СКЗИ «КриптоПро CSP» позволяет зашифровать данный закрытый ключ на другом закрытом ключе, а также разделить закрытый ключ на несколько ключевых носителей. Подробнее об этом в разделе 3.2.4.

2.5.4.2. Удаление запомненных паролей

СКЗИ «КриптоПро CSP» позволяет сохранить в специальном хранилище локального компьютера пароли на доступ к контейнеру закрытого ключа (в случае, если пользователь ставит флаг **Запомнить пароль** в окне ввода пароля на доступ к закрытому ключу). Когда пароль сохранен, при обращении к закрытому ключу он не запрашивается. В это же хранилище записывается точный путь к ключевому контейнеру (связка между именем контейнера и уникальным именем контейнера).

Для того, чтобы удалить запомненный пароль, откройте <u>Панель управления</u> СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 40), нажмите кнопку **Удалить запомненные пароли.**

Откроется окно «Удаление запомненных паролей» (см. Рисунок 65).

Þ	Удаление запомненных паролей 🛛 🗙
Удалит	ть все запомненные пароли закрытых ключей:
	ользователя
K	омпьютера
Удалит	гь информацию об использованных съемных носителях:
	ользователя
K	омпьютера
	ОК Отмена

Рисунок 65. Окно «Удаление запомненных паролей»

В этом окне установите флаги **Пользователя/Компьютера** для удаления сохраненных на локальном компьютере в специальном хранилище паролей и нажмите кнопку **ОК**. Если сохраненных паролей нет, то соответствующая область будет затемнена.

СКЗИ «КриптоПро CSP» осуществит удаление сохраненных паролей только из специального хранилища на локальном компьютере; пароль на доступ к закрытому ключу не удаляется.

Кроме того, в этом же окне можно отдельно удалить информацию о физических характеристиках носителей, на которых расположены ключевые контейнеры, использовавшиеся ранее на данном компьютере. Это полезно, если ключевой контейнер на новом носителе имеет то же имя, что один из ранее использовавшихся на данном компьютере контейнеров.

2.6. Установка параметров безопасности

Вкладка **Безопасность** контрольной панели СКЗИ КриптоПро CSP предназначена для выбора параметров безопасности при работе со СКЗИ «КриптоПро CSP».

Для того, чтобы установить параметры безопасности, откройте <u>Панель управления</u> СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 11). После перезапуска перейдите на вкладку **Безопасность** (см. Рисунок 66).

	Оборудование	Сервис	Дополнительно
Алгоритмы	Безопасность	Winlogon	Настройки TLS
Назначенны GOST R 34.	ые по умолчанию CSP д 10-2001 Signature with	ля указанных т Diffie-Hellman Ke	ипов ey Exchange:
Crypto-Pro	GOST R 34.10-2001 Cr	yptographic Serv	vice Provider 🔹 👻
GOST R 34	10-2012 (256) Signature	e with Diffie-Hellr	man Key Exchange:
Crypto-Pro	GOST R 34. 10-2012 Cr	yptographic Serv	vice Provider 🔹
GOST R 34.	10-2012 (512) Signature	e with Diffie-Hellr	man Key Exchange:
Crypto-Pro	GOST R 34. 10-2012 St	rong Cryptograp	hic Service Pro 💌
Усилени Выберите	ный контроль использо CSP для настройки:	вания ключей	
- <u>Service activity</u>	GOST R 34.10-2001 Cr	ptographic Serv	rice Provider 🔹
Crypto-Pro		ожений	
Сгурtо-Рго Э Храните Исполь: Включи	ь ключи в памяти прил зовать службу хранени ть кэширование	ія ключей <u>Уст</u> Размер к	ановить зша: 8

Рисунок 66. Контрольная панель. Вкладка «Безопасность»

На вкладке Безопасность можно выбрать режим работы: с хранением ключей в памяти приложений либо с хранением ключей в службе хранения ключей. При хранении ключей в службе хранения ключей все операции с закрытым ключом производятся внутри службы, внешнему приложению выдается только результат, что более безопасно, чем хранить ключи непосредственно в памяти приложений. В исполнениях СКЗИ, сертифицированных по уровню КС2 или КС3, режим работы с хранением ключей в службе является единственным доступным (см. Рисунок 67).

Оощие	Оборудование	Сервис	Дополнительн
Алгоритмы	Безопасность	Winlogon	Настройки TL
Назначенны GOST R 34.	ые по умолчанию CSP д . 10-2001 Signature with	іля указанных т Diffie-Hellman Ke	ипов ey Exchange:
Crypto-Pro	GOST R 34.10-2001 Cr	yptographic Serv	vice Provider 🛛 🔻
GOST R 34.	. 10-2012 (256) Signature	e with Diffie-Hellr	nan Key Exchange
Crypto-Pro	GOST R 34.10-2012 Cr	yptographic Serv	vice Provider 🔹 👻
GOST R 34.	. 10-2012 (512) Signature	e with Diffie-Hellr	nan Key Exchange
Crypto-Pro	GOST R 34.10-2012 St	rong Cryptograp	hic Service Pro 🔻
Режим рабо	оты CSP ять <mark>информацию об ис</mark>	тользованных с	ъемных носителя
Режим рабо	оты CSP ять информацию об исі ный контроль использо CSP аля настройки:	пользованных с вания ключей	ъемных носителя
Режим рабо Сохран: Усилени Выберите (Стурto-Pro	оты CSP ять информацию об исп ный контроль использо CSP для настройки: GOST R 34, 10-2001 Cr	пользованных с ования ключей yptographic Serv	ъемных носителя ice Provider 🗸 🔻
Режим рабо Сохрана Усилени Выберите (Стурto-Pro	оты CSP ять информацию об ис ный контроль использо CSP для настройки: GOST R 34.10-2001 Cr ь ключи в памяти прил	пользованных с ования ключей yptographic Serv ожений	ъемных носителя ice Provider 🛛 🔻
Режим рабо Сохранз Усилени Выберите (Сrypto-Pro Хранить О Использ	оты CSP ять информацию об исп ный контроль использо CSP для настройки: GOST R 34, 10-2001 Cr ь ключи в памяти прил зовать службу хранени	пользованных с вания ключей yptographic Serv ожений вя ключей	ъемных носителя ice Provider 🛛 🔻
Режим рабо Сохрана Усилени Выберите (Сгурто-Рго Хранить О Использ Включи	оты CSP ять информацию об ис ный контроль использо CSP для настройки: GOST R 34, 10-2001 Cr в ключи в памяти прил зовать службу хранени пъ кэширование	тользованных с вания ключей yptographic Serv ожений яя ключей Размер к	ъемных носителя ice Provider ▼ эша; 8 <u>*</u>

Рисунок 67. Вкладка Безопасность, уровень защиты КС2 или КС3

При хранении ключей в службе хранения ключей возможно применение кэширования контейнеров закрытых ключей. Кэширование заключается в том, что считанные с носителя ключи остаются в памяти сервиса.

Ключ из кэша является доступным и после извлечения ключевого носителя из считывателя, а также после завершения работы загрузившего этот ключ приложения. Каждый ключ из кэша доступен любому приложению, которое работает под той же учётной записью, что и приложение, поместившее этот ключ в кэш. Все ключи из кэша доступны до завершения работы службы хранения ключей. При переполнении кэша очередной ключ записывается на место самого раннего ключа, помещённого в кэш.

Кэширование контейнеров позволяет увеличить производительность приложений за счет более быстрого доступа к закрытому ключу, т.к. считывание ключа осуществляется только один раз.

Размер кэша задает количество ключей, которые одновременно могут храниться в памяти.

Для того чтобы включить кэширование, необходимо установить флаг в поле **Включить** кэширование. Необходимо также задать размер кэша в соответствующем поле ввода.

Примечание. Если на доступ к закрытому ключу установлен пароль, пароль не сохранен на локальном компьютере, закрытый ключ находится в кэше (ранее к нему уже был осуществлен доступ), то обращение к данному закрытому ключу произойдет без появления окна ввода пароля пользователя – ключ автоматически считывается из кэша.

СКЗИ «КриптоПро CSP» осуществляет кэширование закрытых ключей, связанных с сертификатами, установленными в хранилище сертификатов Локального компьютера (например, закрытых ключей Центра сертификации, Web-сервера) только для конкретного пользователя.

На вкладке «Безопасность» также можно включить режим усиленного контроля использования ключей, если он не был включён при установке СКЗИ КриптоПро CSP. После включения режима через контрольную панель в обязательном порядке необходимо:

- 1) осуществить запуск утилиты csptest.exe
 - csptest.exe -keyset -verifycontext -hard_rng
- 2) установить доверенные корневые сертификаты в хранилище сертификатов локального компьютера CryptoProTrustedStore («Доверенные корневые сертификаты КриптоПро

CSP», «CryptoPro CSP Trusted Roots») с помощью оснастки Сертификаты либо с помощью утилиты certmgr.exe:

certmgr.exe -inst -cert -silent -store mCryptoProTrustedStore -file ca.cer

3) перезагрузить компьютер.

2.7. Дополнительные настройки

Вкладка **Дополнительно** контрольной панели СКЗИ КриптоПро CSP предназначена для:

- <u>просмотра версий и путей размещения</u> используемых СКЗИ «КриптоПро CSP» файлов;
- установки времени ожидания ввода информации от пользователя.

2.7.1. Просмотр версий используемых файлов

Для просмотра версий и путей размещения используемых СКЗИ «КриптоПро CSP» файлов откройте <u>Панель управления</u> СКЗИ КриптоПро CSP и перейдите на вкладку **Дополнительно** (см. Рисунок 68).

	Безопасности	5 L	Winlogon	Настройки TLS
Общие	Оборудование	0	Сервис	Дополнительно
Версии файл	OB			
Имя	Версия	Тип	Путь	^
advapi32.d	6.3.9600.16384	x64	C:\Windo	ws\system32\ad
advapi32.d	6.3.9600.16384	x86	C:\Windo	ws\SysWOW64\
crypt32.dll	6.3.9600.16384	x64	C:\Windo	ws\system32\cry
crypt32.dll	6.3.9600.16384	x86	C:\Windo	ws\SysWOW64\
inetcomm.d	6.3.9600.16384	x64	C:\Windo	ws\system32\ine
inetcomm.d	6.3.9600.16384	x86	C:\Windo	ws\SysWOW64\i 🗸
<				>
	C	Скопиров	вать в буф	ер обмена
				-
Время ожида	ния ввода			
	оты CSP на экран	е могут	быть пока	заны диалоговые
Во время ра				
Во время ра окна, требу	ощие ввода инфо	рмации	от пользов	ателя.
Во время ра окна, требу Злесь можни	ощие ввода инфо	рмации (от пользов	ателя.
Во время ра окна, требу Здесь можно которого эт	ощие ввода инфо) настроить интер 1 окна будут закр	рмации вал врег ыты, ка	от пользов мени, по за к будто по	ателя. авершению ользователь
Во время ра окна, требу Здесь можно которого эт нажал на кн	ощие ввода инфо настроить интер и окна будут закр эпку "Отмена".	рмации вал вреі ыты, ка	от пользов мени, по за к будто по	ателя. вершению ользователь
Во время ра окна, требу Здесь можно которого эт нажал на кн	ощие ввода инфо настроить интер и окна будут закр опку "Отмена". Устан	рмации вал вреі ыты, ка новить в	от пользое мени, по за к будто по время ожи	ателя. вершению ильзователь цания ввода

Рисунок 68. Контрольная панель. Вкладка «Дополнительно»

В разделе **Версии файлов** в табличной форме представлена информация о версиях и путях размещения использующихся СКЗИ «КриптоПро CSP» файлов. Данную информацию можно скопировать в буфер обмена, нажав на соответствующую кнопку.

2.7.2. Установка времени ожидания ввода информации от пользователя

Во время работы СКЗИ «КриптоПро CSP» на экране могут появляться диалоговые окна, требующие ввода пользователем определенных данных (например, ввод пароля на доступ к закрытому ключу).

Для того, чтобы установить интервал времени, по завершении которого эти окна будут автоматически закрыты (действие, эквивалентное нажатию пользователем кнопки **Отмена**), откройте <u>Панель управления</u> СКЗИ КриптоПро CSP и перейдите на вкладку **Дополнительно** (см. Рисунок 68).

Нажмите кнопку Установить время ожидания ввода.

Откроется окно «Интервал времени ожидания ввода» (см. Рисунок 69). Установите необходимые значения переключателей **Значение пользователя** и **Значение по умолчанию для всего компьютера**.

_		
	⊵ Интервал времени ожидания ввода	×
	Введите интервал времени ожидания ввода пользователя в диалоговых окнах КриптоПро CSP в секундах:	
	Значение пользователя:	
	• Использовать системное значение по умолчанию	
	О Установить бесконечное ожидание	
	🔿 Установить интервал: 600 🜲 секунд	
	Значение по умолчанию для всего компьютера:	
	🔘 Установить бесконечное ожидание	
	🖲 Установить интервал: 600 🗼 секунд	
	ОК Отмена	

Рисунок 69. Окно «Интервал времени ожидания ввода»

В этом окне установите необходимые значения переключателей Значение пользователя и Значение по умолчанию для всего компьютера.

Переключатель Значение пользователя можно установить в одно из следующих положений:

• Использовать системное значение по умолчанию – устанавливает значение, определенное переключателем Значение по умолчанию для всего компьютера; это значение установлено по умолчанию;

• Установить бесконечное ожидание – устанавливает бесконечное ожидание ввода данных пользователя;

• Установить интервал – определяет интервал времени, во время которого пользователь должен ввести данные.

Изменить переключатель **Значение по умолчанию для всего компьютера** может только администратор локального компьютера. При этом, если в панели КриптоПро CSP активна ссылка «Запустить с правами администратора» (см. Рисунок 40), то её нужно нажать.

По умолчанию установлено ожидание ввода в течение 600 секунд.



Примечание. Значение пользователя имеет больший приоритет по отношению к Значению по умолчанию для всего компьютера (например, если значение переключателя Значение по умолчанию для всего компьютера установлено в положение Установить интервал - 600 секунд, а переключатель Значение пользователя в положение Установить бесконечное ожидание, то действительным будет значение – Установить бесконечное ожидание).

2.8. Выбор параметров криптографических алгоритмов

Вкладка **Алгоритмы** контрольной панели СКЗИ КриптоПро CSP предназначена для установки различных параметров реализованных криптографических алгоритмов.

Для установки параметров криптографических алгоритмов откройте <u>Панель управления</u> СКЗИ КриптоПро CSP и перейдите на вкладку **Алгоритмы** (см. Рисунок 70):

	Крипто	Tpo CSP			
Общие Оборудование Сервис Дополнительно					
Алгоритмы	Безопасность	Winlogon	Настройки TLS		
Параметры Выберите GOST R 3 Пар ГО Пар ГО	алгоритмов тип CSP для настройки 4.10-2001 Signature with аметры алгоритма шиф CT 28147-89, параметр аметры алгоритма под CT P 34.10-2001, парам аметры алгоритма Диф CT P 34.10-2001, парам	параметров: n Diffie-Hellman K pования: ы по умолчаник писи: етры по умолча фи-Хеллмана: етры обмена по	iey Exchange V V		
	Of	СОтм	ена Применит		

Рисунок 70. Контрольная панель. Вкладка «Алгоритмы»

На закладке **Алгоритмы** можно выбрать тип криптопровайдера, для которого будет осуществляться настройка (в версии КриптоПро CSP 3.6 доступен единственный тип криптопровайдера: GOST R 34.10-2001 Signature with Diffie-Hellman Key Exchange), после чего для соответствующих криптографических алгоритмов реализована возможность установки параметров:

• установка параметров алгоритма шифрования – ГОСТ 28147-89.

• установка параметров алгоритма выработки и проверки электронной цифровой подписи - ГОСТ Р 34.10-2001;

• установка параметров алгоритма Диффи-Хеллмана - ГОСТ Р 34.10-2001.

2.9. Настройка аутентификации в домене Windows.

Вкладка **Winlogon** контрольной панели СКЗИ КриптоПро CSP предназначена для настройки аутентификации в домене с использованием алгоритмов ГОСТ.

Для настройки Winlogon откройте <u>Панель управления</u> СКЗИ КриптоПро CSP и перейдите на вкладку **Winlogon** (см. Рисунок 71):

Общие	Оборудование	Сервис	Дополнительно		
Алгоритмы	Безопасность	Winlogon	Настройки TL		
Ключевой считыватель по умолчанию					
Выберите С	SP для настройки:				
Crypto-Pro	GOST R 34.10-2001 Cr	yptographic Se	rvice Provider 🛛 🗸		
Выберите с	читыватель:				
Не установ	злен		~		
Параметры					
Параметры					
Параметры	ить КриптоПро Winlog	on			
Параметры	ить КриптоПро Winlog		KDC		
Параметры	ить КриптоПро Winlog овать алгоритмы Криг	on ттоПро CSP на	KDC		
Параметры Отключи	и ть КриптоПро Winlog овать алгоритмы Криг	on iтoПpo CSP на	KDC		
Параметры Отключи	ить КриптоПро Winlog овать алгоритмы Криг	on птоПро CSP на	KDC		
Параметры – Отключи Использо	ить КриптоПро Winlog овать алгоритмы Криг	on птоПро CSP на	KDC		
Параметры – Отключи Использо Идентифика	ить КриптоПро Winlog овать алгоритмы Криг аторы контроллеров д	оп птоПро CSP на цомена	KDC		
Параметры Отключи Использо Идентифика Контроллер	ить КриптоПро Winlog овать алгоритмы Криг аторы контроллеров д домена:	оп птоПро CSP на цомена	KDC		
Параметры Отключи Использо Идентифика Контроллер	ить КриптоПро Winlog овать алгоритмы Криг аторы контроллеров д домена:	оп птоПро CSP на цомена у	КDC Экспортировать		
Параметры Отключи Использо Идентифика Идентифика	ить КриптоПро Winlog овать алгоритмы Криг аторы контроллеров д домена: атор контроллера дом	оп птоПро CSP на цомена чена:	КDC Экспортировать		
Параметры Отключи Использо Идентифика Идентифика	ить КриптоПро Winlog овать алгоритмы Криг аторы контроллеров д домена: атор контроллера дом	оп птоПро CSP на цомена чена:	КDС Экспортировать Шаблоны		
Параметры – Отключи Использо Идентифика Идентифика	ить КриптоПро Winlog овать алгоритмы Криг аторы контроллеров д домена: атор контроллера дом	оп птоПро CSP на цомена нена:	КDС Экспортировать Шаблоны		

Рисунок 71. Контрольная панель, вкладка Winlogon

При установке на контроллер домена будет доступна для выбора опция **Использовать** алгоритмы КриптоПро CSP на KDC и будут заполнены поля идентификаторов контроллера домена. Подробно о настройке Winlogon см. соответствующую документацию.

При необходимости можно полностью отключить использование алгоритмов ГОСТ при аутентификации в домене. Для этого предназначена опция **Отключить КриптоПро Winlogon**.

2.10. Настройки TLS.

Вкладка **Настройка TLS** на контрольной панели СКЗИ КриптоПро CSP предназначена для настройки протокола TLS, обеспечивающем аутентификацию связывающихся сторон, конфиденциальность и целостность пересылаемой информации.

Для настройки TLS откройте <u>Панель управления</u> СКЗИ КриптоПро CSP и перейдите на вкладку **Настройка TLS** (см. Рисунок 72).

КриптоПро CSP			
Общие Оборудование Сервис Дополнительно			
Алгоритмы	Безопасность	Winlogon	Настройки TLS
Клиент			
Использ	овать протокол OCSP		
Не прове	ерять сертификат сер	вера на отзыв	
Не прове	ерять назначение соб	ственного серти	фиката
Ина истор		ciober suite	
	воовать устаревшие	uprici sulterbi	
Сервер			
Использ	овать протокол OCSP		
Не проверять сертификат клиента на отзыв			
Не проверять назначение собственного сертификата			
Не испол	њзовать устаревшие	cipher suite-ы	
Поддерж	кивать RFC 5746 (Ren	egotiation Indica	tion)
Пребова	ть поддержку RFC 57	'46 (Renegotiatio	n Indication)
Писнользовать сертификат компьютера по умолчанию			
Размер кэша сессии: 64 🚽			
Максимальное число ЦС в запросе сертификата: 100 🚖			
	0	С Отме	на Примени
	0		- ipencin

Рисунок 72. Контрольная панель, вкладка Настройка TLS

В параметрах клиента:

флаг **Использовать протокол OCSP** – клиентом осуществляется протокол проверки сертификата по базе сервера OCSP Responder;

флаг Не проверять сертификат сервера на отзыв – клиентом не производится проверка сертификатов на принадлежность списку отозванных сертификатов (CRL);

флаг Не проверять назначение собственного сертификата -

флаг Не использовать устаревшие cipher suite-ы – отключается возможность использования cipher suite, в которых были обнаружены уязвимости.

Необходимо требовать поддержку RFC 5746.

В параметрах сервера:

флаг Использовать протокол OCSP – сервером осуществляется протокол проверки сертификата по базе сервера OCSP Responder.

Путем установления соответствующих флагов в полях сервера достигается отключение сервером проверки сертификата клиента на наличие в списке отозванных сертификатов, проверки назначения собственного сертификата, использование cipher suite, в которых были обнаружены уязвимости.

Посредством установления/снятия флагов, связанных с расширением Renegotiation Indication, контролируется требование безопасного связывания нескольких фаз handshake (см. RFC 5746).

В соответствующих полях настраивается размер кэша сессий и максимальное число центров сертификации в запросе сертификата.

3. Интерфейс генерации ключей

КриптоПро CSP может использоваться различными приложениями, в том числе для создания контейнеров на платформе Windows с использованием службы сертификации Windows Server.

Примечание. В операционных системах Windows в случае использования службы хранения ключей для уровня КС1 (см. раздел <u>Установка параметров безопасности</u>) или использования Биологического датчика случайных чисел для уровней КС2/КС3 (см. раздел <u>Настройка датчиков случайных чисел</u>) диалоги выбора считывателя и генерации ключа появляются на сервисном десктопе.

3.1. Генерация ключей и получение сертификата при помощи УЦ

Для формирования личных ключей и получения сертификатов можно воспользоваться тестовым Центром Сертификации <u>https://www.cryptopro.ru/certsrv</u>.

< 🕞 🖛 https://	www.cryptopro.ru/certsrv/certrqma.asp 🔎 🗧 🖒 🍋 Службы сертификации Ас 🗴					
Microsoft Службы сертификации Active Directory Test Center CRYPTO-PRO						
Расширенный з	апрос сертификата					
Идентифицирующи	е сведения:					
Имя:	Сидоров Иван Иванович					
Электронная почта:	sidorov@mail.ru					
Организация:	ACME					
Подразделение:	Маркетинг					
Город:	Москва					
Область, штат:						
Страна, регион:	RU					
Type of Certificate N	leeded:					
	Сертификат проверки подлинности клиента 🗸					
Параметры ключа:						
	Осоздать новый набор ключей Оспользовать существующий набор ключей					
С	SP: Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider					
Использование ключ	ней: 🔿 Exchange 🔿 Подпись 💿 Оба					
Размер клю	рча: 512 Минимальный:512 (стандартные размеры ключей: <u>512</u>)					
	• Автоматическое имя контейнера ключа					
	🗌 Пометить ключ как экспортируемый					
	🗌 Включить усиленную защиту закрытого ключа					
	Использовать локальное хранилище компьютера для сертификата Сохраняет сертификат в локальном хранилище вместо пользовательского хранилища сертификатов. Не устанавливает корневой сертификат ЦС. Необходимо быть администратором, чтобы создать локальное хранилище.					

Рисунок 73. Генерация ключа при помощи УЦ

В диалоге создания ключа и формирования запроса на сертификат задайте "Имя Владельца" сертификата и введите свой адрес электронной почты "Адрес E-Mail".

Если запрашиваемый сертификат предполагается использовать в электронной почте, выберите Сертификат защиты электронной почты **Область применения ключа**.

Если запрашиваемый сертификат предполагается использовать в протоколе TLS, выберите Сертификат аутентификации клиента в разделе Область применения ключа.

Примечание. Если введенный адрес почты не совпадает с зарегистрированным адресом в

Outlook Express (Outlook), использовать криптографические функции в электронной почте будет невозможно.

3.2. Создание ключевого контейнера

3.2.1. Выбор ключевого носителя

При создании ключевого контейнера откроется окно выбора ключевого носителя (см. Рисунок 74).

🗏 КриптоПро CSP	×			
0:0 Вставъте и выберите носитель для хранения контейнера закрытого ключа "Test_1".				
Устройства:	Вставленный носитель:			
C	Ж Отмена <u>С</u> ведения <<			

Рисунок 74. Выбор ключевого носителя

Это окно отображается в том случае, когда пользователь имеет несколько устройств, служащих ключевыми считывателями. В случае, когда ключевой считыватель только один, он выбирается автоматически, и это окно не отображается.

После того, как ключевой считыватель выбран, нажмите кнопку ОК.

3.2.2. Генерация начальной последовательности ДСЧ

После выбора ключевого считывателя, если в системе не установлен аппаратный ДСЧ, откроется окно «Биологический датчик случайных чисел» (см. Рисунок 75).

КриптоПро CSP	×			
(779) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	0:09:25			
Биологический датчик случайны	іх чисел			
Нажимайте клавиши или перемещайте указатель				
мыши над этим окном до тех пор, пока ключ не будет				
Нет				
<u>О</u> тмена				

Рисунок 75. Биологический датчик случайных чисел

Биологический датчик случайных чисел предназначен для генерации начальной последовательности датчика случайных чисел.

Для генерации необходимо нажимать на клавиши или двигать мышью.

3.2.3. Ввод пароля на доступ к закрытому ключу

После завершения работы биологического датчика случайных чисел откроется окно ввода пароля на доступ к закрытому ключу создаваемого контейнера (см. Рисунок 76).

3	КриптоПро CSP	×		
Задайте ba9a2690	Задайте пароль для создаваемого контейнера "e- ba9a269d-1f98-4849-b468-52db54c72cd3".			
Установить но Новий ворода	овый пароль	RU		
Подтвержден	ие:			
ОК	Отмена	Подро <u>б</u> нее >>		

Рисунок 76. Ввод пароля на доступ к закрытому ключу

В поле Новый пароль пользователь должен ввести текстовый пароль на доступ к закрытому ключу создаваемого контейнера и подтвердить его повторным вводом в поле Подтверждение.

После ввода пароля нажмите кнопку ОК.

Если ключ генерируется на носитель, поддерживающий аппаратный пароль или пин-код, то необходимо ввести тот пароль (пин-код), который установлен на этот ключевой носитель.

3.2.4. Выбор способа защиты доступа к закрытому ключу

Помимо ввода пароля в СКЗИ «КриптоПро CSP» существуют другие средства защиты доступа к закрытому ключу. Для выбора подходящего средства защиты в окне ввода пароля на доступ к закрытому ключу создаваемого контейнер (см. Рисунок 76) нажмите кнопку **Подробнее**. Откроется окно выбора способа защиты доступа к закрытому ключу создаваемого контейнера (см. Рисунок 77). Защита носителей, поддерживающих аппаратный пароль (пин-код), возможна только на этом пароле (пин-коде).

3	КриптоПро CSP		×	
0:09:50 Задайте пароль для создаваемого контейнера "le- 5ea9ac9f-3cc5-40dc-85ed-f8351b05dbf7".				
• Установить новый	пароль		RU	
Новый пароль:				
Подтверждение:				
Установить мастер	о-ключ			
<u>И</u> мя контейнера:		<u>В</u> ыбрать		
Создать новы	й контейнер			
<u>Разделить ключ на</u>	а несколько носителей	i		
<u>К</u> оличество носит	елей для загрузки	3		
Общее <u>ч</u> исло носн	телей	5		
ОК	Отмена	Подро <u>б</u> нее	<<]	

Рисунок 77. Выбор средства защиты доступа к закрытому ключу

В этом окне содержатся следующие поля:

Установить новый пароль – ввод текстового пароля;

• <u>Установить мастер-ключ</u> – зашифрование данного закрытого ключа на другом закрытом ключе (из другого ключевого контейнера);

• Разделить ключ на несколько носителей – разделение данного закрытого ключа на несколько носителей для обеспечения доступа к нему.

3.2.4.1. Установка нового пароля

Если переключатель на поле **Установить новый пароль** (см. Рисунок 77), то СКЗИ КриптоПро CSP осуществит защиту ключа при помощи пароля на доступ, введенного с клавиатуры. Необходимо осуществить действия, описанные в пункте <u>Ввод пароля на доступ к закрытому ключу</u>.

3.2.4.2. Установка мастер-ключа

Если переключатель на поле **Установить мастер-ключ** (см. Рисунок 77), то СКЗИ КриптоПро CSP осуществит защиту ключа при помощи зашифрования данного закрытого ключа на другом закрытом ключе.

Для этого необходимо ввести имя контейнера (или выбрать контейнер из списка с помощью кнопки **Выбрать**), содержащего закрытый ключ, на котором будет осуществлено зашифрование исходного закрытого ключа. При нажатии кнопки **Выбрать** откроется список существующих контейнеров (см. Рисунок 78).

КриптоПро CSP					
0:09:51 Выбор ключевого контейнера					
В списке показ	В списке показывать:				
Дружестве	Дружественные имена ОУникальные имена				
Список ключевь	Список ключевых контейнеров пользователя:				
Считыватель	Имя контейнера	^			
REGISTRY	le-023c8983-fbcc-4d53-9db9-6072e0149706				
REGISTRY	le-226a15ad-4e2a-4405-b26f-1ae5c86cc797				
REGISTRY	le-ba9a269d-1f98-4849-b468-52db54c72cd3				
REGISTRY	test_0	× -			
<	>				
ОК Отмена					

Рисунок 78. Список существующих контейнеров

После выбора необходимого контейнера нажмите кнопку **ОК**. При этом произойдет зашифрование данного закрытого ключа на ключе выбранного контейнера.

СКЗИ КриптоПро CSP позволяет осуществлять зашифрование данного ключа не только на существующем закрытом ключе. При установке флага напротив поля **Создать новый контейнер** (см. Рисунок 77) аналогично будет создан новый контейнер и на его ключе зашифрован закрытый ключ данного контейнера.

3.2.4.3. Разделение ключа на несколько носителей

Если переключатель установлен в поле **Разделить ключ на несколько носителей** (см. Рисунок 77), то СКЗИ «КриптоПро CSP» осуществит защиту ключа при помощи разделения доступа к нему между несколькими ключевыми носителями. Каждый из этих носителей является самостоятельным контейнером с собственным паролем на доступ к закрытому ключу.

Заполните следующие поля:

• Количество носителей для загрузки – число носителей, необходимых для доступа к закрытому ключу.

• Общее количество носителей – общее количество носителей, между которыми ключ будет разделен.

После заполнения этих полей начнётся процесс создания новых контейнеров, участвующих в разделении исходного ключа. Количество создаваемых контейнеров равно значению, указанному в поле **Общее количество носителей**:

1. Для каждого создаваемого контейнера откроется окно выбора ключевого носителя (см. Рисунок 74). В этом окне выберите носитель, который будет участвовать в разделении ключа.

2. После того, как для всех контейнеров выбраны носители, откроется окно ДСЧ.

3. После завершения генерации откроется окно ввода пароля на доступ к закрытому ключу для каждого создаваемого контейнера (см. Рисунок 76). В этом окне нужно ввести или выбрать другое средство защиты доступа к закрытому ключу при помощи кнопки **Подробнее** (см. Рисунок 77).

После создания всех контейнеров, участвующих в разделении ключа, будет обеспечена защита доступа к закрытому ключу.

3.3. Открытие ключевого контейнера

3.3.1. Отсутствие ключевого носителя

В случае отсутствия ключевого носителя при открытии ключевого контейнера появится окно, сообщающее об отсутствии носителя (см. Рисунок 79).

🗐 КриптоПро CSP	×
Вставьте ключевой н "testL1".	0:09:47 носитель
Устройства:	Вставленный носитель: Состояние:
	Отмена Сведения <<

Рисунок 79. Отсутствие необходимого носителя

После того, как носитель будет подключен, откроется следующее окно.

Если требуемый носитель установить не удается, нажмите кнопку Отмена.

Когда необходимый ключевой носитель подключен, окно, сообщающее об отсутствии ключевого носителя, не отображается.

3.3.2. Проверка пароля на доступ к закрытому ключу

После того, как ключевой носитель установлен, потребуется подтверждение пароля на доступ к закрытому ключу контейнера.

3.3.2.1. Проверка текстового пароля

Если устанавливалась защита доступа к закрытому ключу с помощью пароля (см. пункт 3.2.4.1), то будет отображено окно проверки пароля для доступа к закрытому ключу открываемого контейнера (см. Рисунок 80).

КриптоПро CSP	×
Введите пароль для контейнера "test_0"	0:09:54
	EN
Пароль:	
🗌 Запомнить пароль	
ОК Отмена	

Рисунок 80. Проверка пароля на доступ к закрытому ключу

Если ранее во время ввода пароля на доступ к закрытому ключу флаг напротив поля **Сохранить пароль** был установлен, то пароль был сохранен в реестре. Повторный ввод (проверка) этого пароля не требуется, поэтому окно проверки пароля отображено не будет.

Если пароль введен неверно, будет предложено повторно ввести пароль.

Примечание. Носители, имеющие аппаратный пин-код, могут иметь ограничение на количество неудачных попыток ввода пароля. Превышение этого предела приводит к блокированию носителя или контейнера.

3.3.2.2. Проверка пароля при зашифровании ключа на другом ключе

Если защита доступа к закрытому ключу была осуществлена при помощи зашифрования данного закрытого ключа на другом закрытом ключе (см. пункт 3.2.4.2), то будет отображено окно проверки пароля для доступа к закрытому ключу контейнера, на ключе которого проводилось зашифрование (см. Рисунок 80).

После того, как был получен доступ к ключу расшифрования, произойдет расшифрование ключа открываемого контейнера.

3.3.2.3. Проверка пароля при разделении ключа между несколькими носителями

Если защита доступа к закрытому ключу осуществлялась при помощи разделения ключа между носителями (см. пункт 3.2.4.3), то проверку требуется осуществить для такого количества носителей, какое было указано в поле **Количество носителей для загрузки** при создании контейнера. При нахождении одного из ключей будет произведена стандартная проверка пароля для ключа-части.

При открытии одного из носителей, участвующего в разделении ключа некоторого контейнера (а все они в свою очередь также являются носителями), проверка пароля на доступ к закрытому ключу проводится в соответствии со способом защиты доступа к ключу, примененным к данному носителю. В общем случае, для разных носителей, участвующих в разделении закрытого ключа одного и того же контейнера, могут быть применены разные способы защиты доступа к ключу.

4. Описание использования, настроек и управления ключами модуля сетевой аутентификации КриптоПро TLS

Для настройки двустороннего соединения (клиент-сервер) по протоколу TLS пользователю с правами администратора необходимо выполнить следующие действия:

- 1. Установить IIS
- 2. Установить КриптоПро СЅР
- 3. Установить корневой сертификат в хранилище компьютера
- 4. <u>Установить сертификат в IIS и настроить двустороннюю аутентификацию</u>
- 5. <u>Установить сертификат пользователя</u>
- 6. Выполнить проверку соединения

Для выпуска сертификатов в качестве примера используется Тестовый ЦС на сайте cryptopro.ru

4.1. Установка IIS на сервере.

В случае, если службы IIS не установлены в операционной системе Windows используемой версии по умолчанию, необходимо выполнить установку с помощью пользовательского интерфейса через Компоненты Windows. Для этого через меню Пуск откройте Панель управления, найдите Программы и компоненты, выберите включение и отключение компонентов Windows.

В диалоговом окне Компоненты Windows выберите службы IIS. Для работы по TLS обязательно должны быть указаны службы интернета и средства управления веб-сайтом:

Control Panel	📴 Windows Features		ograms and Features 👂
Control Panel Home View installed updates Turn Windows features on or off	Turn Windows features on or off To turn a feature on, select its check box. To turn a fe check box. A filled box means that only part of the features Games	eature off, clear its ature is turned on.	ange, or Repair.
	Indexing Service		8== 👻 🔮
-0	Internet Explorer 8		Installed On
	FTP Server		
	B Web Management Tools		
	🛞 🔳 🚺 IIS 6 Management Compatibility		
	IS Management Console		
	IS Management Scripts and Tools		
	IS Management Service		
	World Wide Web Services		
	Application Development Features		
	Common HTTP Features		
	Security		
	Internet Information Services Hostable Web	b Core	
	Media Features		
	⊞		
	⊕ □ ↓ Microsoft Message Queue (MSMQ) Server	*	
	OK	Cancel	,

Рисунок 81. Включение компонентов IIS

Нажмите ОК для выполнения настройки сервера.

4.2. Установка КриптоПро CSP

Установка КриптоПро CSP выполняется запуском файла CSPSetup.exe, далее пошагово с помощью мастера установки (см. <u>Инсталляция СКЗИ КриптоПро CSP</u>) При выборе вида установки укажите выборочную установку, чтобы иметь возможность включить компоненты, не входящие в стандартный набор по умолчанию.

В диалоге выборочной установки необходимо указать, что приложение будет использовано в качестве криптопровайдера уровня ядра ОС:

遢	Установка "КриптоПро CSP"
Выбор Выбе	ите компоненты программы, которые необходимо установить.
Щелкн	 Ссновные файлы Основные файлы (х64) Расширенная совместимость с продуктами Служба хранения ключей Revocation Provider Криптопровайдер уровня ядра ОС
	 Данный компонент будет установлен на локальный жесткий диск. Данный компонент и все подкомпоненты будут установлены на локальный жесткий диск.
< Папка:	 Данный компонент будет установлен для запуска по сети. Данный компонент и все подкомпоненты будут установлены для запуска по сети. Данный компонент будет недоступен.
1	одсказка < Назад Далее > Отмена

Рисунок 82. Включение компонентов КриптоПро CSP при установке

Далее установка производится с рекомендуемыми по умолчанию параметрами. По завершении установки перезагрузите компьютер.

Для того, чтобы ввести лицензию на TLS или проверить её наличие, воспользуйтесь оснасткой Управление лицензиями КриптоПро PKI, которая открывается через меню Пуск (Все программы → КРИПТО-ПРО →КриптоПро PKI)

4.3. Установка корневого сертификата в хранилище компьютера

Для корректной работы сервера в хранилище сертификатов должен быть установлен сертификат корневого удостоверяющего центра. Для получения сертификата используется ntcnjdsq центр сертификации КриптоПро.

Браузер, через который осуществляется доступ к веб-интерфейсу центра сертификации, нужно открыть от имени администратора. Откройте веб-интерфейс центра сертификации КриптоПро <u>https://www.cryptopro.ru/certsrv/</u>

Для корректной работы с функционалом выпуска сертификатов необходимо добавить адрес центра сертификации в доверенные сайты в настройках браузера. Для этого в свойствах браузера выберите вкладку Безопасность, в список надежных сайтов добавьте узел <u>https://www.cryptopro.ru/</u> и сохраните изменения свойств.

Из списка действий выберите получение сертификата удостоверяющего центра.

(+ https://www.cryptopro (+ C + Certification Authority ×	₼ ☆ 🕸
Файл Правка Вид Избранное Сервис Справка	
КРИПТО Тестовый центр сертификации	^
English version	
Внимание.	
Центр сертификации использует криптопровайдер КриптоПро СSP версии 3.6. Пользователи с установленным криптопровайдером КриптоПро CSP версии 1.1 не смогут проверить ЭЦП центра. Криптопровайдер можно получить <u>здесь</u> .	
Центр реализован на основе службы сертификации, входящей в состав операционной системы Windows Server 2003.	
Центр предназначен только для целей тестирования криптопровайдера КриптоПро CSP и не должен использоваться для других цел	тей.
Воспользоваться услугами действующего Удостоверяющего центра ООО "Крипто-Про"можно обратившись по адресу info@cryptopro.ru или по телефону +7 (495) 780 4820.	
Вы можете использовать тестовый центр для того чтобы получить цифровой сертификат открытого ключа для различных приложени	й.
С помощью цифрового сертификата Вы сможете обеспечить целостность, авторство и конфиденциальность передаваемой в сети информации.	
Для получения цифрового сертификата Вы должны будете сформировать закрытый и открытый ключи и ввести данные, которые используются для связывания открытого ключа и Владельца сертификата.	
Подробнее о цифровых сертификатах можно узнат	ь здесь.
Выберите пункт из меню и нажмите кнопку "Дальше"	
 Сформировать ключи и отправить запрос на сертификат 	
 Получить сертификат Удостоверяющего Центра или действующий список отозванных сертификатов 	
О Проверить наличие выпущенного сертификата	
На главную страницу Дальше >>>	~
٢	>

Рисунок 83. Тестовый ЦС

Далее выполняется загрузка сертификата центра сертификации. Выберите метод шифрования и нажмите на ссылку «Загрузка сертификата ЦС».

	- • •
🧲 🔄 🕶 https://www.cryptopro 🔎 – 🔒 С 🕽 🕶 Службы сертификации А 🗙	ଳ 🖈 🔅
Файл Правка Вид Избранное Сервис Справка	
Citysca ceptingwaaquid Active Directory (with obort) - Test Center CRTFTC-PRC	
Загрузка сертификата ЦС, цепочки сертификатов или CRL	
Чтобы доверять сертификатам, выданным этим центром сертификации, установите эту цепочку сертификатов ЦС.	
Чтобы загрузить сертификат ЦС, цепочку сертификатов или список отзыва сертификатов (CRL), выберите этот сертификат и метод шифрования.	
Сертификат ЦС: Текущий [Test Center CRYPTO-PRO(2)]	
Метод шифрования:	
ODER Ø Deres 64	
Загрузка целочки сертификатов ЦС	
Загрузка последнего базового СКL	
Jarpyska последнего разностного CKL	

Рисунок 84. Загрузка сертификата ЦС

При получении сертификата нужно выбрать «Открыть сертификат». Если данный сертификат ранее не был установлен в хранилище доверенных корневых центров сертификации, его необходимо установить.

Сертификат	x
Общие Состав Путь сертификации	
Сведения о сертификате	-
Нет доверия к этому корневому сертификату центра сертификации. Чтобы включить доверие, установите этот сертификат в хранилище доверенных корневых сертификатов центров сертификации.	
Кому выдан: Test Center CRYPTO-PRO	
Кем выдан: Test Center CRYPTO-PRO	
Действителен с 07. 04. 2009 по 04. 10. 2014	
Установить сертификат Заявление поставщика Подробнее о сертификатах	
OK	

Рисунок 85. Просмотр сертификата ЦС

В окне просмотра сведений о сертификате нажмите кнопку «Установить сертификат», откроется мастер импорта сертификатов.

В диалоге выбора хранилища сертификатов укажите «Поместить сертификаты в следующее хранилище», при выборе хранилища поставьте флажок «Показать физические хранилища», укажите в доверенных корневых центрах сертификации хранилище локального компьютера.

Сертифика	т	X	
Общие с	остав Путь сертификации		
нет д цент устан дове	Сведения о сертификате цоверия к этому корневому ра сертификации. Чтобы вкл ювите этот сертификат в х ренных корневых сертифик	сертификату пючить доверие, ранилище катов центров	
Ceph	Мастер импорта сертифика	этов	8
Кому	Хранилище сертификатов Хранилища сертифика хранятся сертификат	атов - это системные области, в которых ы.	
Кем в	Выбор хранилища мож можно указать размец О Автоматически О Поместить все с	кет быть произведен Windows автоматически, или же цение сертификата вручную. выбрать хранилище на основе типа сертификата сертификаты в следующее хранилище	
	Хранилище серт	тификатов:	
		Обзор	
Подробне		Выбор хранилища сертификата 🛛 🔀	
		Выберите хранилище сертификатов.	
	Подробнее о <u>хранилищах</u>	Доверенные корневые центры серти Реестр Локальный компьютер Смарт-карта Ловерительные отношения в прелпри Ш Н	ia
		✓ Показать физические хранилища ОК Отмена	

Рисунок 86. Установка сертификата ЦС

Завершите установку сертификата следуя дальнейшим указаниям мастера.

Для проверки правильности установки сертификата воспользуйтесь оснасткой для управления сертификатами КриптоПро CSP. В меню Пуск выберите Все программы → КРИПТО-ПРО → Сертификаты. Из списка действий выберите получение сертификата удостоверяющего центра (Корневой сертификат необходимо получать доверенным образом).



Рисунок 87. Хранилище Доверенные корневые центры сертификации

4.4. Установка сертификата IIS

Для того, чтобы настроить соединение с сервером по протоколу TLS, необходимо предпринять следующие шаги:

- 1. выпустить сертификат IIS, если он не был выпущен ранее и установить его в соответствующее хранилище
- 2. настроить IIS с указанием сертификата
- 3. проверить соединение по HTTPS

4.4.1. Выпуск сертификата IIS

Для получения сертификата используется центр сертификации КриптоПро.

Браузер, через который осуществляется доступ к веб-интерфейсу центра сертификации, нужно открыть от имени администратора.

Откройте веб-интерфейс центра сертификации КриптоПро <u>https://www.cryptopro.ru/certsrv/</u> и из списка действий выберите «Сформировать ключи и отправить запрос на сертификат».

← → https://www.cryptopro ♀ ← ▲ ♂	🟠 🖈 🛱
Файл Правка Вид Избранное Сервис Справка	
КРИПТО Тестовый центр сертификации	^
English version	
Внимание.	
Центр сертификации использует криптопровайдер КриптоПро СSP версии 3.6. Пользователи с установленным криптопровайдером КриптоПро СSP версии 1.1 не смогут проверить ЭЦП це Криптопровайдер можно получить <u>здесь</u> .	ентра.
Центр реализован на основе службы сертификации, входящей в состав операционной системы Windows Server 2003.	
Центр предназначен только для целей тестирования криптопровайдера КриптоПро CSP и не должен использоваться,	для других целей.
Воспользоваться услугами действующего Удостоверяющего центра ООО "Крипто-Про"можно обратившись info@cryptopro.ru или по телефону +7 (495) 780 4820.	» по адресу
Вы можете использовать тестовый центр для того чтобы получить цифровой сертификат открытого ключа для различн	ных приложений.
С помощью цифрового сертификата Вы сможете обеспечить целостность, авторство и конфиденциальность передавает информации.	мой в сети
ля получения цифрового сертификата Вы должны будете сформировать закрытый и открытый ключи и ввести данны используются для связывания открытого ключа и Владельца сертификата.	іе, которые
Подробнее о цифровых сертификата	ах можно узнать здесь.
Выберите пункт из меню и нажмите кнопку "Дальше"	
 Сформировать ключи и отправить запрос на сертификат 	
О Получить сертификат Удостоверяющего Центра или действующий список отозванных сертификатов	
О Проверить наличие выпущенного сертификата	
На главную страницу	Дальше >>>
٢	>

Рисунок 88. Создание ключа и сертификата в тестовом ЦС

На следующем шаге выберите действие «Создать и выдать запрос к этому ЦС».

🗲 🗇 🕶 https://www.cryptopro 🔎 – 🚔 С 🤇 🛩 Службы сертификации А 🗙	
Microsoft Спухбы сертификации Active Directory - Test Center CRYPTO-PRO	Домой 📈
Расширенный запрос сертификата	
Политика ЦС определяет типы сертификатов, которые вы можете запрашивать. Выберите нужное действие: Создать и выдать запрос к этому ЦС.	
Выдать запрос, используя base-64 шифрованный файл PKCS #10, или выдать запрос обновления, используя base-64 ш	ифрованный файл PKCS #7.

Рисунок 89. Выбор запроса сертификата

В появившемся диалоге подтвердите выполнение операции с сертификатом от имени пользователя.

В открывшейся форме заполните данные сертификата. При заполнении поля Имя (Common Name) необходимо учитывать, что имя сертификата должно совпадать с доменом, обслуживаемым сервером IIS, для которого выпускается сертификат.

Microsoft Службы серт	ификации Active Directory Test Center CRYPTO-PRO	Домо
Расширенный зап	рос сертификата	
Идентифицирующие с	ведения:	
Имя: test	-srv.local	
Электронная почта:		
Организация:		
Подразделение:		
Город:		
Область, штат:		
Страна, регион: RU		
Type of Certificate Nee	ded:	
	Сертификат проверки подлинности сервера 👻	
Тараметры ключа:		
· ·	Осоздать новый набор ключей Пспользовать существующий набор ключей	
CSP:	Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider 🔹	
Использование ключей:	💿 Exchange 💿 Подпись 💿 Оба	
Размер ключа:	512 Минимальный:512 Максимальный:512 (стандартные размеры ключей: <u>512</u>)	
	⊚ Автоматическое имя контейнера ключа 🛛 🔘 Заданное пользователем имя контейнера к	люча
	🗹 Пометить ключ как экспортируемый	
	Включить усиленную защиту закрытого ключа	
Дополнительные пара	метры:	
Формат запроса:		
Алгоритм хеширования:	FOCT P 34.11-94 ▼	
	Используется только для подписания запроса.	
	Сохранить запрос	
Атрибуты:	۵. ۳	
, , , , , , , , , , , , , , , , , , , ,	٠	
Понятное имя:	Cert for test server	
	Bugar. N	1
	редате >	J.

Рисунок 90. Заполнение параметров сертификата IIS в тестовом ЦС

Заполните необходимые поля, укажите тип сертификата «Сертификат проверки подлинности сервера», в параметрах ключа укажите «Использовать новый набор ключей» и выберите CSP: Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider. Если в дальнейшем предполагаются манипуляции с ключом сертификата, для удобства можно пометить ключ как экспортируемый и в дополнительных параметрах указать понятное имя. Остальные параметры рекомендуется оставить по умолчанию.

После заполнения полей формы нажмите кнопку «Выдать».

В диалоговом окне будет предложено указать пароль для сертификата. В данном случае пароль не требуется, поля нужно оставить пустыми и нажать кнопку ОК. После завершения работы биологического датчика в браузере открывается страница со ссылкой для установки выпущенного сертификата:

🏉 Службы сертификации Active Directory (Microsoft) - Windows Internet Explorer	- • •
🚱 💿 🗢 https://www.cryptopro.ru/certsrv/certfnsh.asp 🔹 🔒 😽 🗙 🕨 Bing	- م
🚖 Favorites 🛛 🖛 Службы сертификации Active Directory (Micros	
Microsoft Службы сертификации Active Directory Test Center CRYPTO-PRO	Доной
Сертификат выдан	
Запрошенный вами сертификат был вам выдан.	
Установить этот сертификат	
ПСохранить ответ	

Рисунок 91. Установка созданного через тестовый ЦС сертификата IIS

Нажмите «Установить этот сертификат». На странице появится сообщение об успешной установке сертификата.

Для проверки правильности установки сертификата воспользуйтесь оснасткой для управления сертификатами КриптоПро. В меню Пуск выберите Все программы → КРИПТО-ПРО → Сертификаты.

Сертификат службы IIS должен находиться в хранилище Личное локального компьютера.

🗐 Сертификаты		
🗐 Файл Действие Вид Окно Справка		_ 8 ×
🗢 🔿 🖄 🖬 🔏 🖦 🔀 🖬 👔		
Корень консоли Корень консоли Корень консоли Сертификаты - текущий пользователь Сертификаты (локальный компьютер) Ceртификаты Сертификаты Доверенные корневые центры сертификации Доверенные издатели Сертификаты, к которым нет доверия Соронние корневые центры сертификаци Доверенные лица Доверенные лица Доверенные корневые сертификаты сма Доверенные устройства	Кому выдан 管算 test-snv.local	Кем выдан Test Center CRYPTO-PRO
4	< III	4
Хранилище Реестр содержит 1 сертификат.		

Рисунок 92. Проверка наличия сертификата IIS в хранилище локального компьютера

Если сертификат не попал в хранилище Личное локального компьютера, то найдите его в хранилище текущего пользователя через оснастку Сертификаты и перенесите в указанное хранилище.

4.4.2. Настройка IIS с указанием сертификата

Откройте диспетчер служб IIS одним из следующих способов:

- откройте Панель управления → Администрирование → Диспетчер служб IIS;
- вызовите командную строку комбинацией клавиш Win+R и введите команду inetmgr

В Диспетчере служб IIS щелкните правой кнопкой мыши на Веб-узел по-умолчанию (Default Web Site) и выберите в контекстном меню Изменить привязки... (Edit Bindings...)

	USER-PC Sit	ianager tes 🕨 Default	Web Site 🕨							
File View He	lp									
Connections				<i></i>					Ac	tions
2		🥑 D	efault Wel	o Site He	ome				B	Explore
⊿ · · GIN USER-PC (us	er-PC\user)	Eilton		- 010 Go -		Group has				Edit Permissions
- 🏠 Applicati	on Pools	Ther.		• 66 00	SHOW AII	Group by.		Ŧ		Edit Site
⊿ Sites	It Mich Site	115	0		·····			Â		Bindings
Co Delat	int web site	A.		0	II	404				Basic Settings
		Authentic	. Compression	Default	Directory	Error Page	s Handler			View Applications
ĺ	Site Bindings						? ×			View Virtual Directories
									M	anage Web Site 🛛 🙆
	Type Hos	t Name	Port IP A	ddress	Binding Infor	ma	Add		2	Restart
	http		80 *				Edit	=	▶	Start
							Euren			Stop
							Remove			Browse Web Site
							Browse		•	Browse *:80 (http)
										Advanced Settings
	•					- F				Configure
										Limits
							Close		0	Help
l		_								Online Help
		Features \	/iew ि Conte	nt View						
Ready										6

Рисунок 93. Диспетчер IIS

В списке привязок сайта нажмите кнопку Добавить... (Add...).

onnections							Actio	ns
		Default \	Neb Sit	e Home			D E	xplore
USER-PC (user-PC\user)	E3	top	- 00	Go Show	Group ha		E	dit Permissions
Application Pools	vite Bindinas				E E	dit Site		
Sites Default Web Site							В	indings
	Туре	Host Name	Port	IP Address	Binding Informa	Add	В	asic Settings
	http		80	*		Edit	ע ר	iew Applications
		dd Site Rinding				2 2		iew Virtual Directories
	~	ad site binding					na	ge Web Site
		Туре:	IP addr	ess:	Port:		R	estart
		https	◄ All Un	assigned			SI	tart
	•	Host name:					St	top
							B	rowse Web Site
		SSL certificate:					В	rowse *:80 (http)
		cert for test server			View		A	dvanced Settings
		certific test server					C	onfigure
							Li	imits
				L	OK Ca	ancel	О н	lelp
						÷.	0	Inline Help

Рисунок 94. Добавление сертификата SSL

В открывшемся диалоге добавления привязки сайта укажите тип протокола подключения (Туре) HTTPS, а в выпадающем списке Сертификаты SSL (SSL certificate) выберите сертификат, созданный для служб IIS. Нажмите ОК для сохранения параметров, закройте Привязки сайта и перезапустите IIS, нажав Перезапустить (Restart) в окне диспетчера.

ЖТЯИ.00088-01 92 01. КриптоПро CSP. Инструкция по использованию



Рисунок 95. Перезапуск IIS

4.4.3. Проверка соединения по HTTPS

Для локальной проверки соединения используйте ссылку в левой части окна менеджера IIS, которая показана на следующем рисунке, или через браузер пройдите по ссылке https:/<domainname>//, где <domainname> – доменное имя настраиваемого сайта (где предварительно должен быть настроен DNS).

СКЗИ «КриптоПро CSP», функционирующее в ОС Windows 10, также поддерживает работу в рамках HTTP/2 при взаимодействии с Internet Explorer/Edge и Internet Information Services (IIS). Для обратной совместимости с протоколом HTTP в случае возникновения проблем, связанных с отсутствием поддержки HTTP/2 на клиенте/сервере, необходимо в настройках Internet Explorer/Edge/IIS отключить поддержку HTTP/2 (на сервере отключается параметром HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters\EnableHttp2Tls REG_DWORD 0).



Рисунок 96. Проверка соединения с сервером по HTTPS

Если службы IIS настроены правильно, в браузере отобразится соответствующая страница:



Рисунок 97. Результат проверки соединения с сервером по HTTPS

Для того, чтобы сервер IIS поддерживал двустороннюю аутентификацию с браузером пользователя, нужно выставить в параметрах IIS соответствующие требования. Для этого в Диспетчере служб IIS выделите Beб-узел по-умолчанию (Default Web Site) и выберите в открывшемся меню Параметры SSL (SSL settings).

🛐 Internet Information Services (IIS) N	Aanager	- • ×
G Since	ites 🕨 Default Web Site 🕨	🖅 🖂 🚱 🗸
File View Help		
Connections	Default Web Site Home Filte: 	Actions Actions Edit Stelore Edit Site Bindings Basic Settings View Virtual Directories Manage Web Site Call Content of the State Start Start Start Start Start
Ready	SSL Settings Management Configurat Editor	Browse Web Site Srowse %80 (http) Advanced Settings Configure Limits Help Online Help

Рисунок 98. Настройка двусторонней аутентификации

В параметрах SSL проставьте флажок «Требовать SSL» (Require SSL) и укажите для сертификатов клиента «Требовать» (Require).

File View Help		
Connections	SSL Settings This page lets you modify the SSL settings for the content of a Web site or application. Require SSL Client certificates: Gamma Gamma Gamm	Actions Apply Cancel Online Help

Рисунок 99. Параметры SSL для двусторонней аутентификации

После этого нажмите «Применить» (Apply) для сохранения изменений и перезапустите IIS описанным выше способом.

4.5. Установка личного сертификата пользователя

Для успешной работы пользователя с сервером по протоколу TLS, необходимо:

- 1. Установить на компьютер пользователя КриптоПро СЅР
- Выпустить личный сертификат пользователя, если он не был выпущен ранее и установить его в хранилище Личное текущего пользователя или на носитель другого типа, доступный для считывания на компьютере пользователя
- 3. Выполнить проверку связи с сервером

Используя установочный файл CSPSetup.exe установите КриптоПро CSP на компьютер пользователя. Для решения текущей задачи достаточно принять при установке параметры, рекомендуемые по умолчанию.

Сертификат пользователя можно получить через центр сертификации КриптоПро https://www.cryptopro.ru/certsrv/

На первой странице центра сертификации выберите «Сформировать ключи и отправить запрос на сертификат.



Проверить наличие выпущенного сертификата

На главную страницу

Дальше >>>

Рисунок 100. Запрос сертификата пользователя на тестовом ЦС

Далее следует выбрать ссылку «Создать и выдать запрос к этому ЦС»

Расширенный запрос сертификата

Политика ЦС определяет типы сертификатов, которые вы можете запрашивать. Выберите нужное действие:

Test Cer

Создать и выдать запрос к этому ЦС.

Выдать запрос, используя base-64 шифрованный файл PKCS #10, или выдать запрос обновления, используя base-64 шифрованный файл PKCS #7.

Рисунок 101. Расширенный запрос сертификата

В форме создания запроса обязательно заполните следующие параметры: имя пользователя, в качестве типа сертификата укажите сертификат проверки подлинности клиента, выберите CSP: Crypto - Pro GOST R 34.10-2001 Cryptographic Service Provider, при необходимости дальнейших манипуляций с ключом поставьте флажок «Пометить ключ как экспортируемый». Нажмите кнопку «Выдать».

Расширенный за Идентифицирующие Имя: Те Электронная почта:	прос сертификата сведения:
Идентифицирующие Имя: Те Электронная почта:	сведения:
Имя: Те Электронная почта:	st user
Электронная почта:	
onekipennan neara.	
Организация:	
Подразделение:	
Город:	
Область, штат:	
Страна, регион: RU	
Type of Certificate Ne	eded:
	Сертификат проверки подлинности клиента 🔻
Параметры ключа:	
	💿 Создать новый набор ключей 🛛 🔘 Использовать существующий набор ключей
CSP	Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
Использование ключей	: 💿 Exchange 💿 Подпись 💿 Оба
Размер ключа	: 512 Минимальный:512 (стандартные размеры ключей: <u>512</u>) Максимальный:512 (стандартные размеры ключей: <u>512</u>)
	💿 Автоматическое имя контейнера ключа 🛛 🔘 Заданное пользователем имя контейнера ключа
	🗷 Пометить ключ как экспортируемый
	🔲 Включить усиленную защиту закрытого ключа
Дополнительные пар	аметры:
Формат запроса	© CMC © PKCS10
Алгоритм хеширования	: FOCT P 34.11-94 🔻
	Используется только для подписания запроса.
	П Сохранить запрос
	A
Атриоуты	
Понятное имя	: Test User
	Выдать >

Рисунок 102. Параметры запроса сертификата пользователя

После срабатывания биологического датчика КриптоПро CSP предлагает задать пароль для создаваемого контейнера. Затем нужно установить выданный сертификат.

На открывшейся странице нажмите ссылку «Установить этот сертификат».

🍘 Службы сертификации Active Directory (Microsoft) - Windows Internet Explorer	- • •
🚱 🕞 🗢 https://www.cryptopro.ru/certsrv/certfnsh.asp 🔹 🔒 😽 🗙 📴 Bing	+ م
🚖 Favorites 🛛 🕶 Службы сертификации Active Directory (Micros	
Microsoft Службы сертификации Active Directory - Test Center CRYPTO-PRO	Домой
Сертификат выдан	
Запрошенный вами сертификат был вам выдан.	
Установить этот сертификат	
Сохранить ответ	



При установке сертификата в хранилище текущего пользователя запрашивается пароль для контейнера. После ввода пароля сертификат установлен.

Проверить наличие сертификата в хранилище Личное текущего пользователя можно с помощью оснастки «Сертификаты».

🗐 Сертификаты		- • •
🗊 File Action View Window Help		_ 8 ×
🗢 🔿 🙍 🚮 🤞 💺 🗐 😖 🛛	? 📷	
📔 Корень консоли 🔺	Issued To	Issued By
🛛 🔊 Сертификаты - текущий пользов	🔚 Test user	Test Center CRYPTO-PRO
a 🚞 Personal		
Registry		
Certificates		
Trusted Root Certification Auth		
Enterprise Trust		
Intermediate Certification Auth		
Active Directory User Object		
Trusted Publishers		
Untrusted Certificates		
Third-Party Root Certification 4		
Trusted People		
Certificate Enrollment Requests		
Smart Card Trusted Roots		
🔺 छ Сертификаты (локальный компь		
Personal		
Trusted Root Certification Auth		
4	•	4
Registry store contains 1 certificate.		

Рисунок 104. Проверка наличия сертификата пользователя в хранилище

Сертификат пользователя в составе контейнера закрытого ключа также может быть сохранён на различных типах носителей.

4.6. Проверка двусторонней аутентификации клиент-сервер

Для проверки соединения с сервером по протоколу TLS нужно зайти через браузер на страницу сервера https://domainname>//, где <domainname> - имя домена сервера.

Если настройка соединения выполнена правильно, то при переходе на страницу откроется диалог с выбором сертификата.



Рисунок 105. Выбор сертификата

После выбора сертификата будет запрошен пароль к контейнеру сертификата пользователя.

🔄 КриптоПро CSP		—
Введите парол Те-7208962f-26	њ для контейнера 6c4-4e28-bfac-a6c48f8454a0"	0:09:46
		EN
Пароль:		
🔲 Запомнить пароль		
ОК	Отмена	

Рисунок 106. Ввод пароля контейнера закрытого ключа

При вводе правильного пароля пользователю открывается доступ к сайту.

Примечание. При получении сертификата пользователя необходимо убедиться в том, что поле «Улучшенный ключ» содержит значение «Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)», а поле «Использование ключа» - значения «Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)». В случае отсутствия одного из этих значений в указанных полях двусторонняя аутентификация «клиент-сервер» может быть невозможна.

5. Описание использования, настроек и управления ключами на сервере ISA/TMG

5.1. Размещение сертификата аутентификации сервера на сервере ISA/TMG

На компьютере с сервером ISA/TMG сертификат аутентификации сервера должен быть размещен в хранилище **Локальный компьютер\Личные** с привязкой к ключевому контейнеру локального компьютера. Сертификат Центра сертификации, выдавшего этот сертификат - в хранилище **Локальный** компьютер\Доверенные корневые Центры Сертификации (если этот ЦС корневой) или **Локальный** компьютер\Промежуточные Центры Сертификации (если этот ЦС подчинённый. В этом случае все вышестоящие сертификаты промежуточных ЦС и корневой сертификат должны быть установлены в соответствующие хранилища локального компьютера).

Если ключевой контейнер, соответствующий этому сертификату, расположен в реестре компьютера, то необходимо добавить права на чтение-запись для служебной учётной записи **Network** Service на раздел реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings\Keys**

Проверить наличие необходимых сертификатов можно с помощью оснастки "Сертификаты" – специально настроенной консоли MMC Windows. Для запуска консоли нужно выполнить **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **Сертификаты**



Рисунок 107. Запуск консоли Сертификаты

После запуска открывается консоль:


Рисунок 108. Корень консоли Сертификаты

Установите курсор на сертификат сервера ISA:



Рисунок 109. Хранилище Личное текущего пользователя

С использованием функции «Копировать», занесите сертификат в буфер обмена.

После этого установите курсор на разделе «Личные» сертификатов локального компьютера и выполните функцию «Вставить».

После установки сертификата серверной аутентификации ISA, таким же образом установите сертификат центра сертификации в хранилище «Доверенные корневые центры сертификации» хранилища локального компьютера.

5.2. Размещение сертификата клиентской аутентификации на сервере ISA/TMG

Если между сервером ISA/TMG и конечным веб-сервером требуется шифрование трафика по TLS с аутентификацией по сертификату клиента, то выпускается сертификат клиентской аутентификации. На компьютере с сервером ISA/TMG этот сертификат должен быть размещен в хранилище **Локальный** компьютер\Личные с привязкой к ключевому контейнеру локального компьютера. Сертификат Центра

сертификации, выдавшего этот сертификат - в хранилище Локальный компьютер\Доверенные корневые Центры Сертификации (если этот ЦС корневой) или Локальный компьютер\Промежуточные Центры Сертификации (если этот ЦС подчинённый. В этом случае все вышестоящие сертификаты промежуточных ЦС и корневой сертификат должны быть установлены в соответствующие хранилища локального компьютера).

Если ключевой контейнер, соответствующий этому сертификату, расположен в реестре компьютера, то необходимо добавить права на чтение-запись для служебной учётной записи **Network** Service на раздел реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings\Keys**

5.3. Настройка соединения с Web-клиентом

После установки сертификатов открытых ключей, необходимо установить и настроить Слушателя для внешнего IP адреса сервера (IP адрес сетевого интерфейса, доступного из внешней сети).

Установка и настройка Слушателей осуществляется на вкладке Incoming Web Requests окна свойств ISA сервера (Рисунок 110):

В окне ISA Management установить курсор на имя сервера и нажать правую кнопку мыши.

В появившемся меню выбрать пункт Properties.

В окне свойств сервера выбрать закладку Incoming Web Requests.

Выберите режим индивидуального Слушателя для каждого IP адреса в поле Identification.

MASLOV Properties			<u>? ×</u>	
General Incoming Web Requests A	Uuto Discovery	itgoing Web R Performance	equests Безопасность	
Identification C Use the same listener configuration for all IP addresses C Configuration for all IP addresses				
Server IP Address	Display N	Authentic	Server C	
/ 	\ <u>d</u> d	<u>R</u> emove	<u>E</u> dit	
SSL port: 443		E <u>n</u> able SSL list	eners	
Connections Connection settings: Ask unauthenticated u	sers for identific	ation	<u>C</u> onfigure	
	OK	Отмена	При <u>м</u> енить	

Рисунок 110. Установка и настройка Слушателей

Добавьте нового Слушателя в список слушателей ISA сервера.

Установите имя сервера.

Установите внешний IP-адрес, на который будет настроен Слушатель.

Введите имя, с которым будет отображаться данный Слушатель в дальнейшем (опционально).

Add/Edit Listeners		? ×
Ser <u>v</u> er:	MASLOV	•
I <u>P</u> Address:	192.168.68.5	•
Displ <u>a</u> y Name:	pif.nikoil.ru	
□ <u>U</u> se a server certificate t	o authenticate to web clie	ents
		<u>S</u> elect
Authentication		
		Select domain
Digest with this domain	J	Jelest domain
		Select do <u>m</u> ain
✓ Integrated		
<u>C</u> lient certificate (secu	re channel only)	
	OK	Cancel

Рисунок 111. Добавление Слушателя/редактирование свойств Слушателя(1)

Для настройки защищенного соединения по протоколу TLS с двухсторонней аутентификации сервера ISA необходимо:

В окне добавления Слушателя или в окне редактировании свойств Слушателя, указать на использование сертификата сервера при аутентификации с Web-клиентом.

Add/Edit Listeners	<u>?</u> ×
Ser <u>v</u> er:	MASLOV
I <u>P</u> Address:	192.168.68.5
Displ <u>a</u> y Name:	pif.nikoil.ru
✓ Use a server certificate	to authenticate to web clients
	<u>S</u> elect
Authentication ———	
□ <u>B</u> asic with this domain	κ
	Select domain
Digest with this domai	n:
	Select do <u>m</u> ain
✓ Integrated	
🔲 🖸 <u>C</u> lient certificate (secu	ire channel only)
	OK Cancel

Рисунок 112. Добавление Слушателя/редактирование свойств Слушателя(2)

Выбрать сертификат сервера, который будет использоваться для аутентификации. Нажать кнопку Select.

В появившемся окне выбрать из списка сертификат открытого ключа сервера:

Sel	ect Certificate				? ×
:	Select a certificate server: Certificates:	from the list of certif	icates available on	the specified	
	Issued To	Issued By	Expiration Date	Friendly Name	
	pif.nikoil.ru	CA TEST MA	24.10.2002		
			ОК	Cancel	

Рисунок 113. Выбор сертификата открытого ключа сервера

Указать на использование сертификата клиента (опция Client certificate (secure channel only)).

Add/Edit Listeners		?×
Ser⊻er:	MASLOV	•
I <u>P</u> Address:	192.168.68.5	•
Displ <u>a</u> y Name:	pif.nikoil.ru	
✓ Use a server certificate	to authenticate to web cli	ents
pif.nikoil.ru		<u>S</u> elect
Authentication	n:	
		Select domain
Digest with this doma	in:	
		Select domain
✓ Integrated		
Client certificate (sec	ure channel only)	
	ОК	Cancel

Рисунок 114. Добавление Слушателя/редактирование свойств Слушателя(3)

После установки сертификата (сертификатов) открытых ключей, необходимо установить и настроить Слушателя (Web listener) для внешнего IP адреса сервера (IP адрес сетевого интерфейса, доступного из внешней сети).

Установка и настройка Слушателей осуществляется по документации на ISA сервер.

В окне добавления Слушателя или в окне редактировании свойств Слушателя необходимо указать на использование сертификата сервера при аутентификации с Web-клиентом и выбрать настроенный в п. <u>3.5</u>. сертификат сервера, который будет использоваться для аутентификации.

Для настройки защищенного соединения по протоколу TLS с двухсторонней аутентификацией необходимо дополнительно указать на требование сертификата клиента.

5.4. Публикация Web-сервера в сети Интернет

В этом разделе рассматривается порядок действий при опубликовании Web-сервера, расположенного во внутренней сети. При этом соединение сервера ISA и Web-сервера будет установлено по протоколу SSL.

Для публикации Web-сервера во внешнюю сеть необходимо:

1. Получить и установить на публикуемый Web-сервер сертификат открытого ключа, который будет использоваться для серверной аутентификации.

Требования к сертификату:

- Имя сертификата (Common name) должно совпадать с доменным именем Web-сервера, указываемого для редиректа поступающих запросов (вкладка Action окна свойств правила Web публикации);
- Область использования ключа должна содержать «Аутентификация Сервера».
- 2. Установить сертификат корневого ЦС в цепочке сертификатов Web-сервера на сервере ISA, в хранилище Локальный компьютер\Доверенные корневые Центры Сертификации.
- 3. Настроить Web-сервер для поддержки SSL соединения.

Настройка Web-сервера производится в соответствии с документацией соответствующего Webсервера.

4. Создать и настроить правила публикации на сервере ISA.

В окне ISA Management установить курсор на Web Publishing Rules, находящийся в группе Publishing

Нажать правую кнопку мыши и в появившемся меню выбрать последовательно **New** и **Rule** В открывшемся окне, с помощью Мастера создания Правила Web публикации, создать правило. Ввести имя публикации (произвольное имя) и нажать «Далее»

New Web Publishing Rule Wiz	ard	×
	Welcome to the New Web Publishing Rule Wizard This wizard helps you create a new Web publishing rule. Web publishing rules map incoming requests to the appropriate Web servers. Note: Be sure to create new policy elements required by the rule before you use this wizard. Web publishing rule name: pif.nikoil.ru To continue, click Next.	
	< <u>Н</u> азад Далее > Отмена	

Рисунок 115. Окно Мастера создания Правила Web

В окне **Destination Sets** оставить значение, предлагаемое по умолчанию (любые назначения) и нажать «Далее».

New Web Publishing Rule Wizard	×
Destination Sets Select the destinations to which this rule applies.	
Apply this rule to: All destinations	
< <u>Н</u> азад Дал	пее > Отмена

Рисунок 116. Окно установки назначения

Этой установкой определяется, что данное правило публикации (фактически редирект) будет применяться ко всем Web-запросам, прошедшим через Слушателей, вне зависимости от того, какой ресурс из внутренней сети они запросили. В случае публикации нескольких Web-серверов, необходимо создать и применять в правилах публикации назначения.

В окне Client Туре оставить значение, предлагаемое по умолчанию (любые запросы) и нажать «Далее»

New Web Publishing Rule Wizard			×
Client Type You can specify client type by user name, y	group name, or IP a	ddress.	
Apply the rule to requests from:			
© Specific <u>c</u> omputers (client address sets)			
Specific users and groups			
	< <u>Н</u> азад	Далее >	Отмена

Рисунок 117. Окно типа клиента

В этом окне мы указываем, что правило применяется ко всем Web-запросам, вне зависимости от того клиента, кто сформировал запрос.

В окне Rule Action выбрать редирект запросов во внутренний Web-сервер (Redirect the request to this \dots)

Ввести доменное имя публикуемого Web-сервера и нажать «Далее».

ew Web Publishing Rule Wizard	×
Rule Action Specify how you want this rule to respond to requests from clients.	
Response to client requests: Discard the request Redirect the request to this internal Web server (name or IP address): efo.nikoil.rul Browse Send the original host header to the publishing server instead of the actual one (specified above). Connect to this port when bridging request as HTTP: 80 Connect to this port when bridging request as SSL: 443 Connect to this port when bridging request as ETP: 21	
< <u>Н</u> азад Далее> От	гмена

Рисунок 118. Окно ввода доменного имени

Установив правило редиректа таким образом, все запросы, пришедшие к Слушателю на 80 порт, будут редиректироваться на 80 порт Web-сервера. Тоже самое будет происходить с запросами, поступившими на 443 порт (по протоколу TLS).

Завершить работу Мастера, нажав «Готово».

В списке правил Web-публикации появится новая строка, соответствующая созданному нами правилу.



Рисунок 119. Список правил Web-публикации

6. Описание использования, настроек и управления ключами в КриптоПро Winlogon

Для реализации первоначальной аутентификации пользователя протокола Kerberos V5 по сертификату и ключевому носителю, выпущенными в соответствии с алгоритмами **ГОСТ Р 34.10-2001** или **ГОСТ Р 34.10-2012** с использованием сертифицированного **СКЗИ КриптоПро CSP** нужно выполнить следующие действия:

- 1. Установить и настроить контроллер домена на сервере (Active Directory Domain Services настраивается согласно стандартной документации Windows).
- Установить СКЗИ КриптоПро CSP на сервер, на котором разворачивается контроллер домена, на сервер Центра сертификации (в случае, если служба ЦС располагается на отдельном сервере) и на компьютеры пользователей домена.
- 3. Установить и настроить службу сертификации Active Directory (ЦС).
- 4. Выпустить сертификат контроллера домена.
- 5. Выпустить сертификат Агента регистрации.
- 6. Выпустить смарт-карту пользователя домена.

Для работы КриптоПро Winlogon необходима специальная лицензия (для сервера и клиентского ПК). Эта лицензия может входить в лицензию КриптоПро CSP, или выдаваться отдельно. Ввести серийный номер лицензии можно с помощью утилиты Управление лицензиями КриптоПро PKI (подробнее см. ссылку на раздел в инструкции).

6.1. Установка и настройка службы сертификации Active Directory (ЦС)

Сертификаты контроллера домена и пользователей домена запрашиваются через оснастку Сертификаты на сервере, на котором настроен ЦС Предприятия (Enterprise CA) или через вебинтерфейс Центра Сертификации лицом, имеющим право выпуска сертификатов. Далее рассматривается вариант развертывания ЦС на сервере.

Перед установкой и настройкой ЦС Предприятия на сервере должен быть установлен **КриптоПро СSP**, также потребуются права группы **Администраторы Предприятия (Enterprise Administrators)**. Для установки ЦС Предприятия нужно добавить роль Центра сертификации.

Для этого в диспетчере серверов нужно выбрать **Добавить роли и компоненты**.

На шаге выбора роли сервера необходимо отметить **Службы сертификатов Active Directory**.

a	Мастер добавления ролей и компонентов	
Выбор ролей сер	овера	КОНЕЧНЫЙ СЕРВЕР DC1.test.loc
Перед началом работы	Выберите одну или несколько ролей для установки на этом	сервере.
Тип установки	Роли	Описание
Выбор сервера Роли сервера Компоненты Подтверждение Результаты	 DHCP-сервер DNS-сервер (Установлено) Hyper-V Be6-сервер (IIS) ✓ Доменные службы Active Directory (Установленс Сервер приложений Службы Active Directory облегченного доступа в Службы aktube Directory of deservices Службы печати и документов Службы политики сети и доступа Службы развертывания Windows Службы сертификатов Active Directory Службы удаленных рабочих столов 	Службы сертификатов Active Directory (AD CS) предназначены для создания центров сертификации и связанных служб ролей и позволяют выдавать сертификаты для множества приложений и управлять этими сертификатами.
	× IIII /	
	< Назад Далее	> Установить Отмена

Рисунок 120. Добавление роли ЦС

При этом добавляются необходимые компоненты:

	ЖТЯИ.00088-01	92 01.	КриптоПро	CSP.	Инструкция	по	использованию
--	---------------	--------	-----------	------	------------	----	---------------



Рисунок 121. Добавление компонентов для роли ЦС

Далее принимаются по умолчанию компоненты и на следующем шаге выбирается служба ролей Центр сертификации.

b	Мастер добавления ролей и компонентов	_ 🗆 X
Выбор служб рол Перед началом работы Тип установки Выбор сервера Роли сервера Компоненты Служба сертификации А Служба ролей Подтверждение	Мастер добавления ролей и компонентов ПСЙ Выберите службы ролей для установки для Службы сертиф Службы ролей У Центр сертификации Веб-служба политик регистрации сертификатов Веб-служба регистрации сертификатов Сетевой ответчик Служба регистрации в центре сертификации чере: Служба регистрации на сетевых устройствах	сертификации (ЦС) икатов Active Directory. Описание Центр сертификации (ЦС) используется для выпуска сертификатов и управления ими. Несколько объединенных ЦС образуют инфраструктуру открытых ключей.
Результаты	< ш > < Назад Дале	е > Установить Отмена

Рисунок 122. Выбор службы роли ЦС

На шаге **Подтверждение** после просмотра выбранных для установки компонентов нажмите кнопку **Установить**.

Ъ	Мастер добавления ролей и компонентов	x
Компоненты Службы ролей Подтверждение у Перед началом работы Тип установки Выбор сервера Роли сервера Компоненты Служба сертификации А Службы ролей Подтверждение	Мастер добавления ролей и компонентов	×
Результаты	Средства удаленного администрирования сервера Средства администрирования ролей Средства служб сертификации Active Directory Средства управления центра сертификации Экспорт параметров конфигурации Указать альтернативный исходный путь	
	< Назад Далее > Установить Отмена	

Рисунок 123. Подтверждение установки компонентов роли ЦС

По окончании установки компонентов, требующихся для роли Центра сертификации нужно настроить службы сертификатов. Для этого нажмите «Настроить службы сертификатов Active Directory на конечном сервере».

b	Мастер добавления ролей и компонентов	_		x
Ход установки	KO	нечныі DC	Й СЕРВ I1.test.l	EP oc
Перед началом работы	Просмотр хода установки			
Тип установки	Установка компонента			
Выбор сервера				
Роли сервера	Требуется настройка. Установка выполнена на DC1.test.loc.			
Компоненты	Службы сертификатов Active Directory			
Служба сертификации А	Чтобы настроить службы сертификатов Active Directory на конечном сервере, тр	ебую	тся	
Службы ролей	дополнительные деиствия. Настроить службы сертификатов Active Directory на конечном сервере			
Подтверждение	Центр сертификации			
Результаты	Средства удаленного администрирования сервера Средства администрирования ролей Средства служб сертификации Active Directory Средства управления центра сертификации			
	Этот мастер можно закрыть, не прерывая выполняющиеся задачи. Наблюда выполнения задачи или откройте эту страницу снова, выбрав на панели ком "Уведомления", а затем "Сведения о задаче". Экспорт параметров конфигурации	йте за анд пу	ходоі інкт	и
	< Назад Далее > Закрыть	C	тмен	a

Рисунок 124. Настройка службы сертификатов AD на конечном сервере Откроется мастер настройки конфигурации службы сертификатов.

a	Конфигурация службы сертификатов Active Directory		
Учетные данные	КОНЕЧНЫЙ СЕРВЕР DC1.test.loc		
Учетные данные	Укажите учетные данные для настройки служб роли		
Службы ролей			
Подтверждение	Чтобы установить следующие службы роли, необходимо быть членом локальной группы "Администраторы":		
	 Автономный центр сертификации Служба регистрации в центре сертификации через Интернет Сетевой ответчик 		
	Чтобы установить следующие службы роли, необходимо быть членом группы "Администоаторы поедприятия":		
	 Центр сертификации предприятия Веб-служба политик регистрации сертификатов Веб-служба регистрации сертификатов Служба регистрации на сетевых устройствах 		
	Учетные данные: TEST \Администратор Изменить		
	Дополнительные сведения о ролях серверов AD CS		
	< Назад Далее > Настроить Отмена		

Рисунок 125. Учетные данные службы сертификатов AD

Укажите учетные данные для настройки и на следующем шаге выберите роль «Центр сертификации».

B	Конфигурация службы сертификатов Active Directory	_ 🗆 X
Службы ролей		КОНЕЧНЫЙ СЕРВЕР DC1.test.loc
Учетные данные	Выберите службы роли для настройки	
Службы ролей Вариант установки Тип ЦС Закрытый ключ Шифрование Имя ЦС Срок действия База данных сертификат Подтверждение Ход выполнения Результаты	 ✓ Центр сертификации Служба регистрации в центре сертификации через Интернет Сетевой ответчик Служба регистрации на сетевых устройствах Веб-служба регистрации сертификатов Веб-служба политик регистрации сертификатов 	
	Дополнительные сведения о ролях серверов AD CS	
	< Назад Далее >	Настроить Отмена

Рисунок 126. Выбор службы роли для настройки ЦС

Нажмите Далее и выберите вариант установки.



Рисунок 127. Выбор варианта установки ЦС

На следующем шаге укажите тип ЦС (корневой/подчиненный).

B	Конфигурация службы сертификатов Active Directory	-		x
Тип ЦС	KOHE	IHЫЙ DC1	CEPB .test.l	EP oc
Учетные данные Службы ролей Вариант установки Тип ЦС Закрытый ключ Шифрование Имя ЦС Срок действия База данных сертификат Подтверждение Ход выполнения Результаты	Укажите тип ЦС При установке служб сертификатов Active Directory (AD CS) вы создаете или раст иерархию инфраструктуры открытых ключей (PKI). Корневой ЦС расположен на иерархии инфраструктуры открытых ключей и выдает собственный самозаверя сертификат. Подчиненный ЦС получает сертификат от другого ЦС, расположенние иерархии инфраструктуры открытых ключей. Корневой ЦС Корневой ЦС Корневой ЦС Сорневые ЦС настраиваются в иерархии инфраструктуры открытых ключей по настройка других ЦС может не потребоваться. Подчиненный ЦС Для работы подчиненных ЦС требуется установленная иерархия инфраструкто открытых ключей; они авторизованы для выдачи сертификатов центром серти- расположенным выше в иерархии.	ширяет верши юго вы ервым уры ифика	те ине ыше в ии;	3
	Подробнее о типе ЦС			
	< Назад Далее > Настроить	От	мена	

Рисунок 128. Выбор типа ЦС

После этого нужно создать закрытый ключ ЦС.



Рисунок 129. Выбор типа закрытого ключа для ЦС

Далее выберите из доступного списка поставщика служб шифрования и проставьте флажок «Разрешить взаимодействие с администратором, если ЦС обращается к закрытому ключу».

<u>Примечание</u>: В некоторых версиях Windows Server данный флажок называется «Разрешить CSP доступ к рабочему столу». Если это свойство отключено, системные службы не смогут взаимодействовать с рабочим столом пользователя, который вошел в систему.

B	Конфигурация службы сертификатов Active Directory
Шифрование для	я ЦС конечный сервер DC1.test.loc
Учетные данные Службы ролей Вариант установки Тип ЦС Закрытый ключ	Укажите параметры шифрования Выберите поставщик служб шифрования: Длина ключа: Сrypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Pr 💌 1024
закрытый ключ Шифрование Имя ЦС Срок действия База данных сертификат	Выберите хэш-алгоритм для подписывания сертификатов, выдаваемых этим ЦС: ГОСТ Р 34.11-2012 512 бит
подіверждение Ход выполнения Результаты	✓ Разрешить взаимодействие с администратором, если ЦС обращается к закрытому ключу.
	Подробнее о шифровании
	< Назад Далее > Настроить Отмена

Рисунок 130. Выбор параметров шифрования для ЦС

На следующем шаге задается имя ЦС.



Рисунок 131. Ввод общего имени ЦС

После этого указывается срок действия ключа и расположение базы данных сертификатов.

B	Конфигурация службы сер	тификатов Active Directory 📃 🗖 🗙
Подтверждение		КОНЕЧНЫЙ СЕРВЕР DC1.test.loc
Учетные данные Службы ролей Вариант установки	Чтобы настроить следующие р "Настроить".	ооли, службы ролей или компоненты, нажмите кнопку Active Directory
Тип ЦС	Центр сертификации	
закрытым ключ Шифрование Имя ЦС	Тип ЦС: Поставщик служб шифрования: Алгоритм хеширования:	Корень предприятия Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider ГОСТ Р 34.11-2012 512 бит
Срок действия База данных сертификат	Длина ключа: Разрешить взаимодействие с	1024 Включено
Подтверждение Ход выполнения Результаты	администратором: Срок действия сертификата: Различающееся имя: Расположение базы данных	18.03.2019 16:11:00 CN=test-DC1-CA,DC=test,DC=loc C:\Windows\system32\CertLog
	сертификатов: Расположение журнала базы данных сертификатов:	C:\Windows\system32\CertLog
		< Назад Далее > Настроить Отмена

Рисунок 132. Подтверждение параметров ЦС

Все указанные параметры ещё раз выводятся на шаге **Подтверждение**. Нажмите **Настроить** для того, чтобы сконфигурировать службы в соответствии с этими параметрами.

В процессе создания закрытого ключа для ЦС выводится окно Биологического датчика случайных чисел (ДСЧ) и криптопровайдер запрашивает пароль на создаваемый контейнер (пароль в данном случае указывать не нужно).

Ē.	Конфигурация службы сертификатов Active Directory	_ D X
Ход выполнения		КОНЕЧНЫЙ СЕРВЕР DC1.test.loc
Учетные данные	Настраиваются следующие роли, службы ролей и компоненты:	
Службы ролей	Настройка	
Вариант установки		
Тип ЦС	Службы с 🦉 КриптоПро СЅР 🔼	
Закрытый ключ	U:09:27 Биологический датчик случайных чисел	
Шифрование	Ser Shorten in cooling at since ity instances incent	
Имя ЦС	Нажимайте клавиши или перемещайте указатель мыши над этим окном до тех пор, пока ключ не будет	
Срок действия	создан	
База данных сертификат	Нет	
Подтверждение		
Ход выполнения	Отмена	
Результаты		
	< Назад Далее > Наст	роить Отмена

Рисунок 133. Выполнение конфигурирования ЦС

По окончании выполнения конфигурирования выводится информация об успешной настройке службы ЦС.

После выполнения данной задачи корневой сертификат ЦС можно увидеть в хранилище Доверенные корневые центры Локального компьютера через оснастку Сертификаты.

<u>Примечание:</u> если изменения не вступили в силу, для обновления групповой политики в командной строке выполните gpupdate /force.

6.2. Добавление шаблонов сертификатов на сервере

Для того, чтобы контроллер домена поддерживал Winlogon, необходимо выпустить сертификат для контроллера домена. Чтобы пользователь с ролью Агента регистрации мог производить выпуск сертификатов для других пользователей, нужно выпустить сертификаты Агента регистрации и входа по смарт-карте.

Шаблоны для вышеуказанных сертификатов по умолчанию могут быть отключены, поэтому нужно проверить их наличие в списке шаблонов сертификатов и включить недостающие. Для этого на сервере, на котором установлена служба ЦС, откройте оснастку центра сертификации: Панель управления – Администрирование – Центр Сертификации. В список шаблонов сертификатов необходимо включить шаблоны:

Контроллер домена,

Агент регистратор,

Вход со смарт-картой.

Для этого выберите Шаблоны сертификатов, затем из контекстного меню Создать – Выдаваемый шаблон сертификата.

🧔 certsrv -	[Центр серти	фикации (Локальны	й)\test-DC1-CA	🛾 🔲 🗖 🕹
Файл Действие	Вид Справка			
🗢 🔿 🖄	≩ [?			
🚋 Центр сертифика	ации (Локальнь	Имя		Назначение
⊿ 🍶 test-DC1-CA		🚇 Почтовая репликац	ия каталога	Почтовая репликация службы катало
📔 Отозванні	ые сертификать	🚇 Проверка подлинно	сти контролле	Проверка подлинности клиента, Про
📔 Выданные	е сертификаты	🗵 проверка подлинно	сти Kerberos	Проверка подлинности клиента, Про
📔 Запросы і	в ожидании	🗷 Агент восстановлен	ия EFS	Восстановление файлов
📃 Неудачны	іе запросы	🗟 Базовое шифровані	e EFS	Шифрующая файловая система (EFS)
Шаблонь	Управлени	ие		Проверка подлинности клиента, Про
	Создать	×	Выдаваемы	й шаблон сертификата
	Вид	•		Шифрующая файловая система (EFS)
	Обновить		сертификации	<bce></bce>
	Экспортир	овать список		Подписывание списка доверия (Micr
	Справка			
< III			-	
Включение дополни	тельных шаблон	юв сертификатов на это	м центре сертифи	ікации

Рисунок 134. Добавление шаблонов сертификатов

Откроется окно включения шаблонов сертификатов, в котором нужно выделить шаблоны и нажать

ОΚ.

Включение шаблонов сертификатов				
Выберите один шаблон сертификата для использования Примечание. Если созданный шаблон сертификата не о время, пока информация о шаблоне не будет реплициро Не все шаблоны сертификатов в организации могут быт	в этом центре сертификации (ЦС). тображается в списке, подождите некоторое вана на все контроллеры домена. ть доступны для вашего ЦС.			
Дополнительную информацию см. в разделе Основ	зные сведения о шаблонах сертификатов.			
Имя	Назначение	~		
IPSec	IKE-посредник IP-безопасности			
🚇 IPSec (автономный запрос)	IKE-посредник IP-безопасности			
🗷 RAS-и IAS-серверы	Проверка подлинности клиента, Проверка по			
📟 Агент восстановления ключей	Агент восстановления ключей			
🗷 Агент регистрации (компьютер)	Агент запроса сертификата			
🗷 Агент регистрации Exchange (автономный запрос)	Агент запроса сертификата			
💀 Маршрутизатор (автономный запрос)	Проверка подлинности клиента			
風 Перекрестный центр сертификации	<bce></bce>			
風 Подписывание кода	Подписывание кода			
🖳 Подписывание отклика OSPC	Подписание OCSP	$\mathbf{\mathbf{v}}$		
< III	>			
	ОК Отмена	3		

Рисунок 135. Включение шаблонов сертификатов

Далее администратору домена необходимо обновить шаблоны через Панель управления СКЗИ КриптоПро CSP. Для этого на вкладке Winlogon нужно нажать кнопку Шаблоны.

<u>e</u>	КриптоГ	Tpo CSP	x			
Общие Алгоритм	Оборудование ы Безопасность	Сервис Winlogon	Дополнительно Настройки TLS			
Ключево Выбери	Ключевой считыватель по умолчанию Выберите CSP для настройки:					
Сгурто- Выбери Не уста	Рго GOST R 34,10-2001 Cr ге считыватель: ановлен	yptographic Serv	vice Provider V			
Парамет Откл Испо	ры ючить КриптоПро Winlog льзовать алгоритмы Криг	on птоПро CSP на К	DC			
Идентиф	оикаторы контроллеров д ілер домена:	омена				
DC1.tes	t.loc	¥ [Экспортировать			
Идентиф {f1fd77	DC1.test.loc Экспортировать Идентификатор контроллера домена: [f1fd7703-cd5d-4ac6-9262-7e677dd27116]					
	Of	СОтм	ена Применить			

После выполнения этого действия появится сообщение о том, что все шаблоны успешно обновлены, можно будет приступать к созданию заявок на сертификаты.

Если редактируются или добавляются новые шаблоны для контроллера домена и агента регистрации, данное действие нужно производить в обязательном порядке.

6.2.1. Настройка шаблонов сертификатов

Для того, чтобы сертификаты можно было использовать в Winlogon, нужно, чтобы они удовлетворяли определённым требованиям к сертификатам Контроллера домена, Агента регистратора, Входа по смарт-карте. Подробнее данные требования описаны в документации Microsoft http://support.microsoft.com/kb/281245/en-us

Если существующий шаблон не удовлетворяет требованию, к составу сертификата, необходимо его изменить. Для этого нужно создать копию шаблона, отредактировать её и включить в список шаблонов ЦС.

Откройте оснастку Центра сертификации (Пуск – Панель управления – Администрирование – Центр сертификации).

В оснастке выберите свой ЦС, откройте Шаблоны сертификатов.В контекстном меню нажмите Управление.

違 certsrv - [Центр сертификаци	и (Локальный)\test-SERVDC-	СА\Ш	аблоны сертификатов] 🗕 🗖 📑	x
Файл Действие Вид Справка				
🗢 🄿 🖄 🙆				
謆 Центр сертификации (Локальный)	Имя		Назначение	^
⊿ 🝶 test-SERVDC-CA	🚇 Вход со смарт-картой УЭК		Вход со смарт-картой, Проверка под	
📔 Отозванные сертификаты	🚇 Веб-сервер TLS		Проверка подлинности сервера	
📔 Выданные сертификаты	🚇 Вход со смарт-картой		Вход со смарт-картой, Проверка под	
🧮 Запросы в ожидании	🚇 Агент регистрации		Агент запроса сертификата	
📔 Неудачные запросы	🚇 Контроллер домена		Проверка подлинности сервера, Про	
Шаблоны сертификатов		7	Проверка подлинности клиента, Вход	
	Управление		Агент запроса сертификата	_
	Создать 🕨	p)	Агент запроса сертификата	=
	Вид 🕨		Защищенная электронная почта, Пр Почтовая репликация службы катало	
	Обновить	лле	Проверка подлинности клиента, Про	
	Экспортировать список	s	Проверка подлинности клиента, Про	
	Справка	-	Восстановление файлов	
	😑 разовос тифрование ст э		Шифрующая файловая система (EFS)	
	🗏 🖳 Контроллер домена		Проверка подлинности клиента, Про	
	🖩 🗟 Веб-сервер		Проверка подлинности сервера	
	💹 Компьютер		Проверка подлинности клиента, Про	
	🔲 🖾 Пользователь		Шифрующая файловая система (EFS)	$\mathbf{\mathbf{Y}}$
Запуск оснастки шаблонов сертификато	в			

Запустится оснастка шаблонов сертификатов. В ней нужно выбрать редактируемый шаблон и нажать в контекстном меню «Скопировать шаблон».

	Консоль ша	блонов сертификатов		_ D X
Файл Действие Вид Сп	равка			
(= =) 🖬 🗙 🗐 🗟	?			
🗵 Шаблоны сертификатов (s	Отображаемое имя шаблон	а Версия схемы	^	Действия
	🚇 Шифрование СЕР	1		Шаблоны сертифика 🔺
	🚇 ЦС Exchange	2		
	🖳 🖳 Только подпись пользова	ателя 1		дополнительные деи 🕨
	🛛 🚇 Только подпись Exchange	e 1		Контроллер домена1 🔺
	🖳 🖳 Проверка подлинности р	абочей ста 2		Дополнительные дей 🕨
	🛛 🚇 Проверка подлинности к	онтроллер 2		
	🚇 проверка подлинности Ке	erberos 2		
	🖳 🖳 Проверенный сеанс	1		
	🛛 🕮 Почтовая репликация кат	галога 2	=	
	🕮 Пользователь со смарт-к	артой 1		
	🕮 Пользователь Exchange	1		
	🕮 Пользователь	1		
	🔤 Подчиненный центр серт	ификации і		
	🔤 Подписывание списка до			
		1		
	🚇 Подписывание кода	ификации 2		
	🚇 Маршрутизатор (автоном	иный запрос) 1		
	Корневой центр сертифи	кации 1		
	🖳 Контроллер домена			
	🚇 Контроллер домена	Скопировать шаолон		
	🚇 Компьютер	Подать повторную заявку для все	х вла,	дельцев сертификатов
	🗵 Вход со смарт-карто	Изменить имена		
	🚇 Вход со смарт-карто	Все задачи		•
	Вход со смарт-карто Веб-сервер	Удалить		
< III >		Свойства		
При использовании данного ш	аблона в качестве базово	Справка		

Откроется форма, в которой можно изменить свойства шаблонов так, чтобы они соответствовали требованиям, описанным в п.п. Требования к сертификату контроллера домена, Требования к сертификату для входа по смарт-карте.

	Свойства нов	вого шаблона	a	×
Шифрование	Аттестация ключей	Имяс	ибъекта	Сервер
Требования выдачи	Устаревшие шабл	оны Расши	ирения	Безопасность
Совместимость	Общи	1e	Обработ	ка запроса
Отображаемое имя ша Копия "Контроллер до Имя шаблона: Копия "Контроллер до Период действия: 1 г. v Опубликовать серт Не использоват сертификат уже	блона: мена" Период обновл 6 нед. ификат в Active Directory в автоматическую переза существует в Active Direc	тения: ✓ аявку, если такой ctory		
	OK	Отмена	Примен	ить Справка

После сохранения нового шаблона нужно добавить его через список шаблонов способом, описанным в п. 6.2 Добавление шаблонов сертификатов на сервере.

6.3. Выпуск сертификата контроллера домена

Выпуск сертификата контроллера домена должен производиться на сервере, на котором развёрнуты службы AD, пользователем с правами администратора домена. Для этого через меню Пуск можно открыть оснастку mmc Сертификаты, затем в хранилище Личное Локального компьютера выбрать Все задачи – Запросить новый сертификат.

	Сертиф	фикаты	_	
🗐 Файл Действие Вид Окно Спра	вка			_ 5 ×
Корень консоли) Э Сертификаты - текущий пользовате Э Э Сертификаты - текущий пользовате Э Э Сертификаты - текущий пользовате Э Э Сертификаты компьют Ф Э Лочное Ф Э Ресстр Э Сертификаты В Все за В Э Доверенные корневі В Доверенные издател В Сертификаты, к кот Сертификаты, к кот Сертификаты, к кот В Сертификаты, к кот В Сертификаты сертиф В Сертификаты сертиф	Кому выдан ^ © DC1.test.loc © test-DC1-CA ачи / окно отсюда ить отировать список ка	Кем выдан test-DC1-CA test-DC1-CA Запросить новый сертификат. Импорт Дополнительные операции	Срок действия 20.03.2015 18.03.2019	Назначени Проверка г <bce></bce>
Удаленный рабочий стол Запросы заявок на сертификат Запросы заявок на сертификат Э Зоверенные корневые сертифии Э Доверенные устройства	<	Ш	1	>
Запросить новый сертификат от центра серт	ификации (ЦС) в этом домен	e		

Рисунок 136. Запрос сертификата контроллера домена

Откроется мастер регистрации сертификатов. Наж мите Далее.

	- D X
📮 Регистрация сертификатов	
Перед началом работы	
Следующие шаги помогут установить сертификаты, являющиеся цифровыми учетными используемыми для подключения к беспроводным сетям, защиты контента, идентифика задач безопасности.	і данными, зции и иных
Прежде чем запрашивать сертификат, убедитесь, что:	
этот компьютер подключен к сети; имеются учетные данные, которые могут быть использованы для подтверждения права н получение сертификата.	на
Подробнее о <u>цифровых сертификатах</u>	
Далее	Отмена

Рисунок 137. Мастер регистрации сертификатов

Откроется диалог выбора политики регистрации.

Регистрация сертификатов Выбор политики регистрации сертификатов	
Политика регистрации сертификатов позволяет регистрировать сертификаты на основании заданны заранее шаблонов сертификатов. Политика регистрации сертификатов уже могла быть настроена.	
Настраиваемые администратором	
Политика регистрации Active Directory	~
Настраиваемые пользователем	Добавить
Подробнее о <u>политике регистрации сертификатов</u>	

Рисунок 138. Выбор политики регистрации сертификатов

В данном окне нужно оставить параметры по умолчанию и перейти к следующему шагу, нажав Далее.

Из списка типов сертификатов выберите Контроллер домена.

систрация сертификатов				
and pagin coping naroo				
Запрос сертификатов				
Surper cepting incures				
Вы можете запросить следующ запросить, и нажмите кнопку "3	ие тиг аявка	пы сертификатов. Выберите серти ".	фикаты, которые хотите	
🗹 Контроллер домена		🤹 Состояние: Доступно	Подробности 🔨	-
Следующие параметры ог сертификата:	редел	пяют характер использования и ср	оок действия данного типа	
Использование ключа	Циф	ровая подпись		
Подитики применения	Шиф	рование ключей верка подлинности клиента		:
ries in the reprinter card	Про	верка подлинности сервера		
Срок действия (дней):	365			
			Свойства	
🗌 Почтовая репликация ката	лога	Остояние: Доступно	Подробности 🗸	
Показать все шаблоны				
Подробнее о <u>сертификатах</u>				
			Заявка Отм	ен

Рисунок 139. Запрос сертификата контроллера домена

Проверьте правильность и при необходимости выберите поставщика службы шифрования в Свойствах на вкладке Закрытый ключ.

Для того, чтобы выпустить сертификат на контроллер домена, нажмите кнопку **Заявка**. При выпуске сертификата предлагается установить новый пароль на контейнер. В процессе создания

закрытого ключа для контроллера домена выводится окно Биологического ДСЧ и криптопровайдер запрашивает пароль на создаваемый контейнер (пароль в данном случае указывать не нужно).

После завершения работы Биологического ДСЧ откроется окно, информирующее об успешной установке сертификата.

	×
ификатов	
олучены и установлены на данном компь Directory	ютере.
🖌 Состояние: Успешно	Подробности 🗸
	Готово
	ификатов олучены и установлены на данном компь Directory ✔ Состояние: Успешно

Рисунок 140. Результат установки сертификата контроллера домена Развернув Подробности можно просмотреть сведения о сертификате.

	Результаты установки сертификатов Следующие сертификаты были получены и установлены на данном	компьютере.
	Политика регистрации Active Directory	
	Контроллер домена Состояние: Успешно Следующие параметры определяют характер использования и сертификата:	Подробности ^ срок действия данного типа
	Сертификат	
0	бщие Состав Путь сертификации	
	Сведения о сертификате	Просмотреть сертификат
	Этот сертификат предназначается для: • Обеспечивает получение идентификации от удаленного компьютера • Подтверждает удаленному компьютеру идентификацию вашего компьютера	Готово
	Кону выдан: DC1.test.loc	
	Кем выдан: test-DC1-CA	
	Действителен с 20.03.2014 по 20.03.2015 Р Есть закрытый ключ для этого сертификата.	
ļ	Заявление поставщика Подробнее о <u>сертификатах</u>	

Рисунок 141. Просмотр сведений о сертификате

Сертификат контроллера домена в результате должен быть установлен в хранилище сертификатов локального компьютера. После выпуска сертификата контроллер домена необходимо перезагрузить.

<u>Примечание:</u> Для сертификатов с ГОСТ-ключами функции автоматического выпуска сертификатов контроллера домена недоступны, поэтому необходимо следить за валидностью сертификата DC и обновлять его до истечения срока действия.

6.3.1. Требования к сертификату контроллера домена

- Сертификат должен иметь расширение точки распространения CRL, который указывает на действительный сертификат список отзыва (CRL), Например:
- [1] Точка распределения списка отзыва (CRL)

Имя точки распространения:

Полное имя:

URL=http://server1.name.com/CertEnroll/caname.crl

- При необходимости раздел субъекта сертификата должен содержать путь к каталогу серверного объекта (имя), например:
- CN=Server1.northwindtraders.com OU = Domain Controller, DC = northwwindtraders, DC = com
- Раздел Использование должен содержать:

Цифровая подпись, Шифрование ключей

• Раздел Основные ограничения должен содержать:

[Тип темы = Конечный субъект, ограничения на длину пути = Отсутствует]

• Раздел расширенного использования ключа сертификата должен содержать:

Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

- Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
 - Раздел Дополнительное имя субъекта должен содержать DNS-имя. При использовании SMTPрепликации раздел дополнительное имя субъекта сертификата должен также содержать глобальный уникальный идентификатор (GUID) объекта контроллера домена в каталоге. Например:

Другое имя: 1.3.6.1.4.1.311.25.1 = ac 4b 29 06 aa d6 5d 4f a9 9c 4c bc b0 6a 65 d9 DNS Name=server1.northwindtraders.com

• Шаблон сертификата должен иметь расширение со значением BMP «DomainController»

6.4. Выпуск сертификата Агента регистрации.

По умолчанию разрешение на запрос сертификатов от лица пользователя предоставляется только администраторам домена. Однако пользователю, не являющемуся администратором домена, может быть предоставлено разрешение стать агентом регистрации.

Для выпуска смарт-карт агента регистрации и пользователей домена должна быть также установлена поддержка необходимых считывателей (ссылка на раздел в основной инструкции).

<u>Примечание:</u> Наличие сертификата агента регистрации позволяет подавать заявки на получение сертификатов и создавать смарт-карты от имени любого пользователя в составе организации. Полученная таким образом смарт-карта может затем использоваться для входа в сеть под именем пользователя без его ведома. Поскольку сертификат «Агент регистрации» предоставляет широкие возможности, настоятельно рекомендуется придерживаться в организации строгих политик безопасности для этих сертификатов.

Чтобы стать агентом регистрации, необходимо подать заявку на сертификат **Агент регистрации** через оснастку **Сертификаты – Текущий пользователь**.

			_		x
истрация сертификатов					
апрос сертификатов					
ы можете запросить следующие т апросить, и нажмите кнопку "Заяв	ипы сертификатов. Выберите сертифи ка".	каты, которы	е хотит	re	
······································					_
Политика регистрации Active D	irectory				^
— Агент восстановления EFS	(i) Состояние: Доступно	Подро	бност	и∨	_
🖌 Агент регистрации	Остояние: Доступно	Подро	бност	ил	=
Следующие параметры опред сертификата:	еляют характер использования и срок	действия дан	ного ті	ипа	
Использование ключа: Ци Политики применения: Аг	іфровая подпись ент запроса сертификата				
Срок действия (дней): 73	D				
		Ce	ойств	a	
					\sim
Показать все шаблоны					
		Заявка		Отме	ена

Рисунок 142. Выбор заявки Агента регистрации

Необходимо отредактировать шаблон сертификата, нажав на кнопку Свойства. На вкладке Закрытый ключ в поле Поставщик службы шифрования нужно указать поставщика.

Свойства сертификата
Общие Субъект Расширения Закрытый ключ Центр сертификации
Поставщик службы шифрования
Поставщик службы шифрования (СУР) - это программа, создающая открытыи и закрытый ключи, которые используются во многих процессах, связанных с сертификатами.
Выберите поставщика службы шифрования:
Мicrosoft Strong Cryptographic Provider (Подпись)
Сrypto-Pro GOST R 34.10-2001 Cryptographic Service Provider (Подпись)
🗌 Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider (Подпись)
✓ Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider (Подпись)
Microsoft Base Cryptographic Provider v1.0 (Подпись)
Microsoft Pace DSS and Diffic Hollman Countegraphic Drovider (Beaguer)
Показать всех поставщиков служб шифрования
Параметры Юноча
Тип ключа 🗸
ОК Отмена Применить

Рисунок 143. Выбор поставщика службы шифрования

На вкладке Центр сертификации обязательно должен быть указан соответствующий ЦС.

	C	войства серти	фиката		x
Общие Субъект	Расширения	Закрытый ключ	Центр серт	гификации	
Сервер регистр подключается запросов на се	ации необходи с серверам рег этификаты.	ім для выдачи и г истрации из след	продления с ующего спі	сертификатов иска для обра	. Система ботки
На каждом сер диагностики по	зере регистрац лезно определ	ии доступны не в ить все доступнь	все шаблон не серверы ј	ы сертификат регистрации.	ов. В целях
Центр сертиф ∳test-DC1-CA	ікации	Тип: Корі	невой ЦС пр	редприятия	
	CEDREDH DEFM	трации			
Подробнее о се	рверах регистр	ации			
			ОК	Отмена	Применить

Рисунок 144. Выбор центра сертификации

После сохранения изменений нужно нажать кнопку Заявка для того, чтобы начать формирование контейнера с сертификатом и закрытого ключа.

Если доступно более одного считывателя, отобразится диалог выбора считывателя, в котором нужно указать, куда поместить создаваемый контейнер.

В процессе создания закрытого ключа выводится окно Биологического ДСЧ и криптопровайдер запрашивает пароль на создаваемый контейнер. После ввода пароля и выводится сообщение об успешном выпуске сертификата

^у езультаты установки сертификатов		
Политика регистрации Active	Directory	····
🗹 Агент регистрации	🗸 Состояние: Успешно	Подробности

Рисунок 145. Результат выполнения установки сертификата Агента регистратора

6.5. Выпуск сертификатов для входа по смарт-карте.

На компьютере в домене, на котором предварительно установлен КриптоПро CSP, пользователь, являющийся членом группы Пользователи и имеющий сертификат Агента регистратора, может выпускать сертификаты для других пользователей домена.

Для этого в оснастке **Сертификаты** нужно развернуть узел **Личные** и выбрать пункт Сертификаты, в котором выполнить Все задачи – Дополнительные операции – Зарегистрироваться от имени.

🗐 Сертификаты 🗕 🗖 🗙						
🗐 Файл Действие Вид Окно Справка 📃 🗗 🗵						
🗢 🔿 🙍 🗊 📋 🗟 🙀						
Корень консоли Сертификаты - текущий пользов Личное Сертификаты Сертификаты Сертификаты Сертификаты Сертификаты Сертификаты Сертификаты Сертификаты	Кому выдан Сар servdc.test.local Сар servdc.test.local	Кем выдан test-SERVDC-CA test-SERVDC-CA test-SERVDC-CA	Срок дейсти 12.03.2015 14.03.2015 12.03.2019			
▷ C Об1 Обновить	Дополнительные опе	рации 🕨	Создать настраиваемый запро	oc		
р Дов Справка		L	Зарегистрироваться от имени			
 ▶ Сторонние корневые центры ▶ Доверенные лица ▶ Поставщики сертификатов п ▶ Доверенные корневые сертис ▲ Осертификаты (локальный компь ▲ Личное ▲ Ресстр Сертификаты ▶ Доверенные корневые центри ▶ Доверительные отношения в 						
	< III		>			
З&арегистрироваться от имени						

Рисунок 146. Выпуск сертификата пользователя смарт-карты

Перейдите к сертификату Агента регистрации, который будет использоваться для подписывания обрабатываемого запроса сертификата.

🔄 Регистрация сертификатов	
Выберите сертификат агента регистрации	
Сертификат агента регистрации неооходим для подписи запроса на сертификат от имен пользователей. Нажмите кнопку "Обзор", чтобы найти сертификат подписи, а затем ще "Далее".	ни других 2лкните
Сертификат полписи:	
	Обзор
	Отмена

Рисунок 147. Выбор сертификата Агента регистрации

После выбора сертификата Агента регистрации из списка доступных сертификатов запрашивается пароль на доступ к этому сертификату.

Регистрация сертифі Выберите сертиф	икатов Икат агента регистрации	_ D X
Сертификат агента рег пользователей. Нажми "Далее".	истрации необходим для подписи запроса на сертификат от име те кнопку "Обзор", чтобы найти сертификат подписи, а затем ще КриптоПро CSP	ни других елкните
Сертификат подписи: Агент регистрации	0:09:45 Введите пароль для контейнера Te-EnrollmentAgent-dab12db5-728d-4ba6-8575-31bd62531: RU Пароль:	Обзор
Подробнее о <u>подаче за</u>	ОК Отмена	
	Далее	Отмена

Рисунок 148. Ввод пароля для сертификата Агента регистрации

В мастере регистрации сертификатов указывается тип сертификата **Вход со смарт-картой**. Необходимо отредактировать параметры выпуска сертификата, для этого нажмите кнопку **Свойства**.

Запрос сертификатов		
Вы можете запросить следую запросить, и нажмите кнопку	цие типы сертификатов. Выберите сертиф "Далее".	икаты, которые хотите
	ч · · · ·	· 9
Вход со смарт-картой	(i) Состояние: Доступно	Подробности 🔨
Следующие параметры с сертификата:	определяют характер использования и сро	к действия данного типа
Использование ключ	а: Цифровая подпись Шифрование ключей	
Политики применени	ия: Проверка подлинности клиента Вход со смарт-картой	
Срок действия (дней):	365	
		Свойства
Показать все шаблоны		

Рисунок 149. Выбор типа сертификата

Нужно указать поставщика службы шифрования и центр сертификации на соответствующих вкладках:

Свойства сертификата				
Закрытый ключ Центр сертификации				
Поставщик службы шифрования ^				
закрытый ключи, которые используются во многих процессах, связанных с сертификатами.				
Выберите поставщика службы шифрования:				
Microsoft Strong Cryptographic Provider (Шифрование)				
🗌 Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider (Шифрование)				
🗌 Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider (Шифрование)				
✓ Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider (Шифрование)				
☐ Microsoft Base Cryptographic Provider v1.0 (Шифрование)				
Microsoft Pace DCC and Diffie Hellman Comtegraphic Drovider (Illuchnonauus)				
Показать всех поставщиков служб шифрования				
Подробнее о <u>закрытых ключах</u>				
ОК Отмена Применить				

Рисунок 150. Выбор поставщика службы шифрования

Для сохранения выбранных параметров нужно нажать кнопку **Применить** и закрыть форму. В мастере создания сертификата нажмите **Далее**, чтобы перейти к следующему шагу и выбрать пользователя домена.

Выберите пользователя			
Чтобы запросить сертификат от имен доменное имя. Например, используй "домен\имя_пользователя".	и другого пользователя, введ ге формат "имя фамилия", "и	ите его формальное мя_пользователя" и	е имя или или
Прежде чем запрашивать сертифика должен быть установлен, подключен	пользователя, убедитесь, что 5.	устройство, на кот	ором он
Имя пользователя или псевдоним: TEST0\testuser			Обзо
Имя пользователя или псевдоним: TEST0\testuser			Обзо
Имя пользователя или псевдоним: TEST0\testuser			0630

Рисунок 151. Выбор пользователя, для которого выпускается смарт-карта

Нажмите на кнопку Заявка, чтобы начать формирование контейнера и ключа.

Далее выбирается устройство для записи на носитель. Считыватель должен быть подключен к компьютеру, а смарт-карта определяться. В процессе формирования контейнера выводится окно Биологического ДСЧ и запрашивается пароль для нового контейнера.

В диалоге выбора пароля нужно ввести пароль для создаваемого контейнера. Для правильной работы со смарт-картой пароль для создаваемого контейнера и смарт-карты должен быть одним.

В результате выводится сообщение об успешной записи контейнера на смарт-карту.

			_ 0	2
егистрация сертификатов				
Результаты установки се	ртификатов			
C				
Следующие сертификаты были	получены и установлены на данном	и компьютере.		
Политика регистрации Activ	e Directory			
💿 Вход со смарт-картой	4 Состояние: Успешно	Под	робности	^
Следующие параметры оп сертификата:	ределяют характер использования и	і срок действия данн	юго типа	
Использование ключа:	Цифровая подпись Шифрование ключей			
Политики применения:	Проверка подлинности клиента			
Coor 10 ⁸ (110 ⁸)	Вход со смарт-картой 265			
Срок деиствия (днеи):	202	Просмотреть се	ртификат	
	Следую	ций пользователь	Закр	ыть

Рисунок 152. Результат выпуска сертификата

После того, как контейнер записывается на носитель, вход с доменной учетной записью пользователя может осуществляться с авторизацией по смарт-карте.





Для авторизации пользователя домена к компьютеру, с которого осуществляется вход в домен, нужно подключить считыватель и вставить в него смарт-карту, затем из параметров входа выбрать значок «Смарт-карта» и ввести ПИН-код.

6.5.1. Требования к сертификату для входа по смарт-карте

• Точка распространения CRL (где CRL - список отзыва сертификата) должна быть заполнена, доступна и находиться в оперативном режиме. Например:

[1]Точка распространения CRL Имя точки распространения: Полное имя: URL=http://server1.name.com/CertEnroll/caname.crl

- Использование ключа = Цифровая подпись
- Основные ограничения [Тип темы=Конечный субъект, Ограничения длины пути=нет] (Необязательно)
- Использование улучшенного ключа =

Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) (Проверка подлинности клиента (OID) требуется только в случаях, когда сертификат используется для проверки подлинности по протоколу SSL.)

- Вход в систему с помощью смарт-карты (1.3.6.1.4.1.311.20.2.2)
- Дополнительное имя субъекта = другое имя: Основное имя пользователя = (UPN). Например:

основное имя пользователя = user1@name.com UPN Другое имя OID: "1.3.6.1.4.1.311.20.2.3" UPN Другое имя значение: Это должна быть ASN1-кодированная строка UTF8

• Тема = Различающееся имя пользователя. Это поле является обязательным дополнением, но заполнять его необязательно.

6.6. Настройка Active Directory и контроллера домена для входа по смарт-картам с помощью групповой политики при использовании стороннего центра сертификации

Для проверки подлинности с помощью смарт-карты в Active Directory необходимо, чтобы рабочие станции со смарт-картами, Active Directory и контроллеры доменов Active Directory были правильно настроены. Чтобы выполнить проверку подлинности пользователей на основе сертификатов от центра сертификации, нужно, чтобы приложение Active Directory доверяло этому центру сертификации. И рабочие станции со смарт-картами, и контроллеры доменов должны быть настроены с правильно настроенными сертификатами.

При любой реализации инфраструктуры открытого ключа (РКІ) необходимо, чтобы все участники доверяли корневому центру сертификации, к которому привязывается выпускающий центр сертификации. И контроллеры доменов, и рабочие станции со смарт-картами доверяют этому корневому центру.

Для настройки Active Directory и контроллера домена необходимы следующие условия:

- Чтобы выполнить проверку подлинности пользователей в Active Directory, сторонние выпускающие центры сертификации должны находиться в хранилище NTAuth.
- Чтобы выполнять проверку подлинности пользователей с помощью смарт-карт, контроллеры доменов должны быть настроены с сертификатом контроллера домена.
- Также можно настроить Active Directory так, чтобы независимые корневые центры сертификации распространялись в хранилища доверенных корневых центров сертификации всех членов домена с помощью групповой политики.

6.6.1. Указания по настройке

Для настройки необходимо иметь независимый корневой сертификат в кодировке Base64 X.509, а также сертификаты выпускающих ЦС.

6.6.1.1. Добавление независимого корневого центра сертификации к доверенным корневым центрам в объект групповой политики службы Active Directory.

Настройка групповой политики в домене Windows для распространения независимых корневых центров сертификации в хранилища доверенных корневых центров всех компьютеров домена производится следующим образом:

- 1. Откройте в консоли ттс оснастку Управление групповой политикой.
- Разверните в открывшейся оснастке элементы: Управление групповой политикой → Лес:
 <имя домена> → Домены. На соответствующем домене выберите в контекстном меню Изменить.

\overline Консоль1 - [Корень конс	соли\Упра	вление групповой	политикой\Лес: test.local\Домен	ны\test.local \Default 💻 🗖 🗙
🚟 Файл Действие Вид Изб	іранное Ок	но Справка		_ & ×
🗢 🔿 🖄 🖬 🗶 🙆	▶ <u>:</u>			
📔 Корень консоли		Default Domain Pol	icy	Действия
⊿ ⊆ Управление групповой пол Долу test la sel	литикой	Область Сведения П	араметры Делегирование	Default Domain Policy
а 🔝 Лес: test.iocai		Связи		Дополнительные действия
⊿ 🙀 test.local		Показать связи в распо	ложении: test.local 🗸	
🛒 Default Doma		0.000	ие сайты, домены и подразделения:	
⊳ 🖬 Domain	Изменить		Принудительн	
р 📑 test	 ▶ ■ test ▶ □ Oбъекть ▶ □ Oбъекть ▶ □ Cвязь включена ▶ □ Фильтры 		Нет	
р 📑 Фильтрь				
þ 🛅 Началы	Сохранить с	отчет		
▷ 🙀 Сайты	Вид	•		
😰 Моделировани	Новое окно	отсюда		
е сультатытру	Новый вид г	панели задач		
	Удалить		ти	
	Переимено	вать	экта групповой политики применяются	
	Обновить		вателей и компьютеров:	
	Справка			
			_*	

Рисунок 154. Оснастка Управление групповой политикой

Откроется окно Редактора управления групповыми политиками

3. В редакторе управления групповыми политиками разверните **Конфигурация компьютера** → Политики → Конфигурация Windows → Параметры безопасности → Политики открытого ключа → Доверенные корневые центры сертификации. В это хранилище импортируйте корневой сертификат ЦС, открыв через контекстное меню мастер импорта сертификатов и следуя указаниям мастера.

Редактор управления группо	вы	ми политиками	_ 🗆 X
Файл Действие Вид Справка			
(= -) 2 🗊 🖹 🙆 🛃 🖬			
Политика Default Domain Policy [DC1.TEST.LOC]	~	Кому выдан	Кем выдан
⊿ 👰 Конфигурация компьютера		🔄 test-DC1-CA	test-DC1-CA
⊿ 🧰 Политики			
🔈 🚞 Конфигурация программ			
🛛 🧮 Конфигурация Windows			
Политика разрешения имен			
📄 Сценарии (запуск/завершение)			
⊿ 🚡 Параметры безопасности			
Политики учетных записей			
þ 🝶 Локальные политики	≡		
🔈 🝶 Журнал событий			
Гід Группы с ограниченным доступом			
В Системные службы			
þ 📴 Реестр			
Файловая система			
Политики проводной сети (IEEE 802.3)			
Брандмауэр Windows в режиме повышенной безопасно			
🚞 Политики диспетчера списка сетей			
Политики беспроводной сети (IEEE 802.11)			
Политики открытого ключа			
📔 Шифрованная файловая система (EFS)			
🛗 Защита данных			
📔 Шифрование диска BitLocker			
📔 Сертификат сетевой разблокировки для шифровани	\$		
📔 Параметры автоматического запроса сертификатов			
📔 Доверенные корневые центры сертификации			
Доверительные отношения в предприятии			
📔 Промежуточные центры сертификации	$\overline{}$		
< III >		< 111	>
Хранилище Доверенные корневые центры сертификации содержит 1 сертиф	икат		

Рисунок 155. Добавление сертификата доверенного УЦ в групповые политики

6.6.1.2. Добавление сторонних выпускающих центров сертификации в хранилище NTAuth службы Active Directory.

Сертификат входа по смарт-карте должен быть выпущен центром сертификации, находящимся в хранилище NTAuth. Корневые сертификаты центров сертификации Microsoft Enterprise CA автоматически добавляются в хранилище NTAuth, а сертификаты сторонних центров сертификации необходимо поместить в хранилище вручную или с помощью утилиты certutil, которая присутствует в поставке Microsoft Windows.

Хранилище NTAuth для всего леса находится в контейнере конфигурации. Примерное расположение:

LDAP://server1.name.com/CN=NTAuthCertificates,CN=Public Key Services,CN=Services,

CN=Configuration,DC=name,DC=com

По умолчанию это хранилище создается при установке центра сертификации Microsoft Enterprise.

Для того, чтобы поместить сертификат в хранилище NTAuth с помощью certutil сохраните его в файл и выполните следующую команду:

> certutil -dspublish -f <filename> NTAuthCA

Здесь <filename> – имя файла с сертификатом.

После помещения сертификатов независимого центра сертификации в хранилище NTAuth групповая политика на базе домена размещает раздел реестра (отпечаток сертификата) на всех компьютерах домена в следующем разделе:

HKEY_LOCAL_MACHINE\Software\Microsoft\EnterpriseCertificates\NTAuth\Certificates

Обновление на рабочих станциях происходит каждые восемь часов (стандартный интервал групповой политики). При необходимости можно принудительно применить групповую политику с помощью команды на сервере gpupdate /force

6.6.1.3. Запрос и установка сертификата контроллеров домена на контроллер(ы) домена.

Каждый контроллер домена, выполняющий проверку подлинности пользователей по смарт-картам, должен иметь сертификат контроллера домена. При установке центра сертификации Microsoft Enterprise в лес службы Active Directory все контроллеры домена отмечаются в сертификате контроллеров домена автоматически. Формат сертификата должен отвечать требованиям к сертификату контроллера домена.

Подробно запрос и установка сертификата рассматривается в разделе Выпуск сертификата контроллера домена.

6.6.2. Вход в домен по УЭК

В КриптоПро Winlogon реализована возможность использования УЭК для авторизации в домене. Для того, чтобы настроить эту функцию, нужно выполнить на сервере AD следующие действия:

1. Включить в настройках групповой политики AD параметр, разрешающий при входе выбор из сертификатов, содержащих электронную подпись.

Параметр **Разрешить ключи подписей для входа** включается в редакторе групповых политик (gpedit.msc) на контроллере домена в узле **Конфигурация компьютера** — **Административные** шаблоны — Компоненты Windows — Смарт-карта.



Рисунок 156. Разрешение входа в домен по ключам подписей

- Обеспечить доверие ко всей цепочке сертификатов на сервере и распространить его с помощью групповой политики (см. п.п. <u>6.6.1.1</u> и <u>6.6.1.2</u>)
- 3. Обеспечить доступ к списку отзыва сертификатов (CRL).

На ЦС, выпускающем сертификат для УЭК должен быть использован шаблон с именем «Вход со смарт-картой». Выпуск сертификата подробно описан в п.п. <u>6.2</u> и <u>6.5</u>.

- На клиентской машине необходимо:
- 1. Установить СКЗИ КриптоПро УЭК СSP.
- 2. Обеспечить взаимодействие с СV-сервисом по 443 порту.

Для проверки доступности CV-сервиса откройте утилиту настройки УЭК (Пуск ⇒ Программы ⇒ КриптоПро ⇒ UEC tool), введите адрес сервера, на котором расположен сервис, нажмите кнопку «Тест».

•	Настройки УЭК		
Сервер ✓ cvservice.uec Использовать	ard.ru : 443 системный прокси-сервер	Тест	
Файл Создать зап	Операция завершена	х вдать	
Установить Хранилище аутен	Тестирование успешно завершено	новить	
 Реестр W Смарт-ка; 	ОК		
Провайдер			
Считыватель	~	Обновить	
Работа с ПИН Предъявить к	од разблокировки ПИН (КРП)	Ввести	
Работа с картой Удалить ауте	нтификационную информацию	Удалить	
Сбросить настройк	Сохранить настройки	Закрыть	

Рисунок 157. Проверка доступности СV-сервиса

3. Через панель управления СКЗИ КриптоПро УЭК CSP нужно указать в свойствах носителя, что он зарегистрирован в Smartcard Winlogon.

Для этого откройте панель управления (Пуск ⇒ Программы ⇒ КриптоПро ⇒ КриптоПро УЭК CSP), на вкладке Оборудование нажмите «Настроить типы носителей...» Выберите из предложенного списка тип носителя, соответствующий используемой УЭК и откройте свойства носителя. На вкладке Свойства карты должен быть проставлен флажок «Зарегистрирован в smartcard winlogon».



⊵ КриптоПро УЭК СЅР 🔽
Алгоритмы Безопасность Winlogon Настройки TLS
Общие Оборудование Сервис Дополнительно
Считыватели закрытых ключей
😪 🔢 Управление ключевыми носителями 🔽
Ключевые носители
Датчики слу По По ЧИ Установлены следующие ключевые носители:
Гипы ключее UEC2
Но Общие Свойства карты
ATR: 387013000080640000000730000008100
Macka: FFF0FFFF00000000FF000000F00
Приложение: 0801
Japeгистрирован в smartcard winlogon
Настройка УЭК
ОК Отмена

Рисунок 158. Настройка параметров ключевого носителя

Если флажок не проставлен, то нужно удалить ключевой носитель в форме **Управление ключевыми носителями**, добавить его заново и проставить этот параметр при добавлении.

4. Подключить к компьютеру пользователя считыватель смарт-карт, соответствующий спецификации для доступа к смарт-картам PC/SC (при необходимости установить драйвер считывателя вручную).

После включения всех вышеперечисленных настроек нужно убедиться, что групповая политика применена к клиентским учетным записям и компьютерам, и авторизоваться в домене с помощью УЭК.
7. Использование КриптоПро CSP при работе с почтовым клиентом The Bat!

Для того, чтобы использовать защиту переписки через электронную почту по стандарту протокола S/MIME в почтовом клиенте The Bat! с использованием ГОСТ-алгоритмов при шифровании и подписывании сообщений нужно выполнить ряд настроек.

- 1. указать параметры S/MIME в настройках почтового клиента;
- 2. настроить почтовый ящик;
- 3. <u>обменяться сертификатами с другими участниками переписки</u> и поместить их в хранилища сертификатов.

Предварительно на компьютере пользователя должно быть установлено СКЗИ КриптоПро CSP.

- 7.1. Настройка параметров S/MIME почтового клиента
- 1. В главном меню The Bat! выберите Свойства S/MIME и TLS...
- 2. В окне Параметры S/MIME и TLS укажите следующие настройки:
 - в блоке Реализация S/MIME и сертификаты TLS выберите Microsoft CryptoAPI;
 - флаг Всегда шифровать отправителю ставится, если необходимо, чтобы исходящая почта шифровалась с помощью сертификата получателя в случае, если такой сертификат есть;
 - Криптопровайдер выберите из выпадающего списка поставщика служб шифрования;
 - флаг Никогда не использовать других криптопровайдеров ставится, если данный почтовый клиент не планируется использовать с другими поставщиками служб шифрования;
 - Алгоритм шифрования указывается алгоритм шифрования, соответствующий выбранному криптопровайдеру;
 - Хэш-алгоритм подписи указывается хэш-алгоритм подписи;
 - Помнить связи e-mail адресов с сертификатами для подписи ставится для автоматического выбора сертификатов;
 - Помнить связи e-mail адресов с сертификатами для шифрования ставится для автоматического выбора сертификатов.

M	Параметры S/MIME и TLS	×
Реализация S/MIME и сертификаты О Внутренняя Microsoft CryptoAPI	īLS	
 Всегда шифровать отправителю Криптопровайдер 		
Crypto-Pro GOST R 34.10-2001 Crypto	graphic Service Provider	~
Никогда не использовать других Алгоритм шифрования	криптопровайдеров	
GOST 28147-89		~
Хеш-алгоритм подписи		
GOST R 34.11-94		~
🖌 Помнить связи e-mail адресов с с	ертификатами для подписи	
🗹 Помнить связи e-mail адресов с с	ертификатами для шифрования	
	ОК Отмена Спр	равка

Рисунок 159. Настройка параметров S/MIME и TLS

3. Сохраните настройки, нажав кнопку ОК.

- 7.2. Настройка почтового ящика
- 1. Для изменения параметров почтового ящика выделите почтовый ящик и в главном меню The Bat! выберите **Ящик Свойства почтового ящика...**
- В окне Свойства почтового ящика выберите раздел Параметры. В блоке «Редактор писем» должно быть отмечено флажком поле Авто-S/MIME. Также можно включить опции Подписать перед отправкой и Зашифровать перед отправкой.

	Свойства почтового ящика - TEST	×
 Общие сведения Транспорт Управление почтой Параметры Файлы и каталоги Шаблоны Новое письмо Ответ Подтверждение проч Сохранение в файл Быстрый ответ Девизы Заметки 	Свойства почтового ящика - TEST Проверка почтового ящика Проверять при запуске The Bat! Проверять с интервалом в Помечать письмо как прочит. при показе в теч. С помечать письмо как прочитанное при открытии в отдельном окне Помечать отвеченное письмо как прочитанное автоматически Расширенное журналирование Максимальный размер файла <u>журнала</u> работы: 20 Кбайт Игнорировать команду проверки всех ящиков	
	 Очищать корзину при выходе из The Bat! Очищать корзину при выходе из The Bat! Сжать все папки при выходе из The Bat! Редактор писем Подтверждать немедленную отправку Авто - OpenPGP Подписать перед отправкой ✓ Авто - S/MIME Зашифровать перед отправкой Подтверждать незашифрованную отправку 	
	ОК Отмена Справка	

Рисунок 160. Редактирование свойств почтового ящика

3. Сохраните настройки, нажав кнопку ОК.

Примечание. В почтовом клиенте The Bat! возможно настроить только один почтовый ящик, работающий с электронной подписью и шифрованием писем.

7.3. Обмен сертификатами

Для того, чтобы подписывать письма и шифровать их в адрес получателя при отправке с помощью почтового клиента, в хранилищах сертификатов компьютера должны находиться сертификат отправителя с ключом и сертификаты получателей. Сертификат отправителя с ключом также может храниться на съемном носителе (смарт-карте, USB-токене и тд.), который должен быть подключен к компьютеру при работе с почтой, он содержит сведения об электронном адресе, для работы с которым он был выпущен.

При наличии сертификата с ключом пользователь может подписывать письма электронной подписью, но для того, чтобы зашифровать сообщение, необходимо, чтобы в хранилище сертификатов находился сертификат получателя, содержащий открытый ключ.

Самый простой способ установить сертификат в нужное хранилище – получить письмо, которое содержит электронную подпись и добавить отправителя в адресную книгу.

1. При просмотре письма нужно нажать кнопку Просмотреть действительную подпись.

OT: TECT2 <testuser1997@mail.ru></testuser1997@mail.ru>	
Кому: Иван Петров <testuser1996@mail.ru> Тема: Тестовое письмо</testuser1996@mail.ru>	
Здравствуйте, Иван.	Просмотреть ДЕЙСТВИТЕЛЬНУЮ подпись

Рисунок 161. Функция просмотра подписи в The Bat!

2. В окне проверки подписи нажмите Просмотреть свойства сертификата.

	Безопасность Windows	×
Действите У этого писы	ЛЬНАЯ ПОДПИСЬ иа действительная подпись.	
	Hanstenki Tert Center CRVPTO-PRO	
·····		
₽≡	04.10.2014	
	Просмотреть свойства	
	<u>сертификата</u>	
	ОК Отмена	

Рисунок 162. Форма просмотра подписи

3. В окне просмотра свойств сертификата нажмите Установить сертификат.

g.	Certificate Details	×
Общие	Состав Путь сертификации	
	Сведения о сертификате	
Этс	эт сертификат предназначается для: • Защищает сообщения электронной почты	
Ko	му выдан: Петр Иванов	
Ke	м выдан: Test Center CRYPTO-PRO	
	Действителен с 03.04.2014 по 04.10.2014	
	Установить сертификат Заявление поставщика	
	ОК	

Рисунок 163. Форма просмотра сертификата

4. В открывшемся мастере импорта сертификатов выберите хранилище Текущего пользователя и нажмите **Далее**.

Мастер импорта сертификатов
Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.
Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.
Расположение хранилища • Текущий пользователь О Локальный компьютер
Для продолжения нажмите кнопку "Далее".

×

Рисунок 164. Выбор расположения хранилища при импорте сертификата

5. На следующем шаге вручную выберите хранилище **Другие пользователи** и нажмите **Далее**.

з мастер импорта сертификатов	
Хранилище сертификатов Хранилища сертификатов - это системные об хранятся сертификаты.	пасти, в которых
Windows автоматически выберет хранилище, расположение сертификата вручную.	или вы можете указать
 Автоматически выбрать хранилище на Поместить все сертификаты в следующ 	основе типа сертификата цее хранилище
Хранилище сертификатов:	
	Обзор
Выбор хранилища сертификата 🛛 🗙	
Выберите хранилище сертификатов, которое вы хотите использовать.	
Сторонние корневые центры сертифи 🔨	
MSIEHistoryJournal	
Поверенные корневые сертификаты (
Показать физические хранилища	Далее Отме

Рисунок 165. Выбор хранилища при импорте сертификата

6. По завершении работы мастера нажмите **Готово**. Появится сообщение об успешном выполнении импорта.

После этого в адрес владельца сертификата можно отправлять зашифрованные письма, воспользовавшись кнопкой Зашифровать перед отправкой в окне редактирования письма.



Рисунок 166. Функция шифрования в форме редактирования письма

При этом перед отправкой предлагается сначала выбрать сертификат для шифрования письма (его можно выбрать из списка доступных или он выбирается автоматически, по е-мейлу получателя письма), а потом ввести пароль для контейнера личного сертификата, с помощью которого будет подписано письмо, если Вы указали **Подписать перед отправкой**.

8. Использование КриптоПро CSP при работе с почтовым клиентом Outlook 2013

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

8.1. Конфигурация Outlook 2013

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

¢	
Сведения	Сведения об учетной записи
Открыть и экспортировать	Microsoft Exchange
Сохранить как	🕂 Добавить учетную запись
Сохранить вложения	Параметры учетной записи и социальных сетей
Печать	Настройка учетных записей така и Измените параметры для этой учетной записе или установите больше соединений.
Учетная запись Office	 Доступ к этой учетной записи на веб- сайте. Подключение к социальным сетям.
Параметры Выход	Автоответы (нет на работе) Используйте автоответы для уведомления других пользователей о том, что вы отсутствуете на рабочем месте, находитесь в отпуске или не имеете возможности отвечать на сообщения электронной почты.
	Средства очистки ч Свободно: 24,3 Гбайт, квота: 24,4 Гбайт
	Правила и оповещения для организации входящих Управление правилами и оповещения для организации входящих сообщений электронной почты и получения обновлений при добавлении, изменении или удалении элементов.

Рисунок 167. Меню Файл Outlook

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



Рисунок 168. Центр управления безопасностью Outlook

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

Рисунок 169. Параметры защиты электронной почты

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).

ЖТЯИ.00088-01	92 01.	КриптоПро	CSP.	Инструкция	по	использованию
---------------	--------	-----------	------	------------	----	---------------

Изменение	настройки без	вопасности	×		
Настройка безопасности —— Имя конфигурации:					
Установки S/MIME ()		~		
Формат криптографии:	S/MIME		\sim		
🗌 Настройка безопасности	по умолчанию <mark>д</mark> ля	я этого формата	а		
🗌 Настройка по умолчания	о для всех сообщен	ний			
Метки безопасности	Создать	Удалить			
Сертификаты и алгоритмы					
Сертификат подписи:			Выбрать		
Алгоритм хеширования:		\sim			
Сертификат шифрования:			Выбрать		
Алгоритм шифрования;		\vee			
Передавать сертификаты с сообщением					
		ОК	Отмена		

Рисунок 170. Изменение настройки безопасности Outlook

Окно выбора сертификата:

	Безопасность Windows	×
Выбор сер	тификата	
	test Издатель: test_rut Действителен с: 22.05.2013 по 01.05.2030	
	ОК Отмена	•

Рисунок 171. Выбор сертификата

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

В закладке Защита электронной почты (E-mail Security) можно включить режимы Шифровать содержимое и вложения исходящих сообщений (Encrypt contents and attachments for outgoing messages) и Добавлять цифровую подпись к исходящим сообщениям (Add digital signature to outgoing messages) для того, чтобы шифрование и электронная цифровая подпись выполнялись автоматически для каждого сообщения. Если эти режимы не включены, опции шифрования и подписи нужно будет включать для каждого отправляемого сообщения. В этом же диалоге дополнительно можно установить опцию Отправлять подписанные сообщения открытым текстом (Send clear text signed message when sending signed messages). При включенном режиме подпись формируется в виде одного отдельного вложения для сообщения. Если режим выключен - текст сообщения и все вложения объединяются в единое целое и кодируются в соответствии с правилами кодирования BASE64, по сле чего результат кодирования подписывается.

8.2. Отправка подписанных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку Создать сообщение



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

E .	. 5 (> ^ ↓	÷		-	Тест - Сообщение (HTM	/L)	?	A	-	×
ФАЙЈ	1 COO	БЩЕНИЕ	BCTABKA	ПАРАМ	ІЕТРЫ	ΦΟΡΜΑΤ ΤΕΚCTA	РЕЦЕНЗИРОВАНИЕ				
Гемы Темы	문 СК 태 От	Разре	🔓 🔒 Ши шения 😫 По,	фровать дписать	₩Кн Уве Уве	опки голосования * едомить о доставке едомить о прочтении	Сохранить отправленн элемент *	فِيَّ Задержка до ஆ Направлять ый	оставки ответь	I B	
	Показать п	оля	Разрешение		C	Отслеживание 🖓	Дополнитель	ьные параметры		E.	^
т. Отпр	авить	Ко <u>м</u> у Копи <u>я</u>	testmail@ma	il.ru							
	<u>1</u> e	о <u>ж</u> ение		x.docx (45 K	(байт)						
test											

Рисунок 172. Создание подписанного сообщения в Outlook

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.

	H	едопустимый сертификат	×
<u> </u>	Приложению Microsoft C из-за отсутствия сертифи адреса учетной записи либо на: помощью учетной запис	Outlook не удается подписать или зашифровать соо ікатов, которые могут быть использованы для отпра ". Получите новое цифровое удостоверение / жмите кнопку "Учетные записи", чтобы отправить с и, для которой имеется сертификат.	бщение авки с для данной ообщение с
		Изменить параметры безопасности	OK

Рисунок 173. Ошибка сертификата отправителя в Outlook

8.3. 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 адр	есную книгу, нажав на значок в	нижней части области папок.
or 📰 🕤 📼	Inbox - corptest@c	ryptopro.ru - Outlook
ФАЙЛ ГЛАВНАЯ ОТ	ГПРАВКА И ПОЛУЧЕНИЕ ПАПКА ВИД	
	Сарответить всем	еместить в: ? 🔶 🍋 Пере водителю 💌 📆 Прав
сообщение элемент 🗸 🖧 🕇	Эдалить 🖳 Переслать 🛄 🗧 Сооб	бщение гр 🔻 🔊 One
Создать Уд	далить Ответить Быстры	е действия 🕞 Переі
Перетащите свои избранны	ме папки ч Поиск в папке "из текущего почто	ового ящика" (CTRL 🔎 🛛
▲ corptest@cryptopro.ru	Все Непрочитанные	По Дата т Новые ↓ .
▷ Inbox	Тест	16:45
Черновики [1]	Тест	
Sent Items	corptest	6
Deleted Items	EncryptAndSignTestMessage	5:30
News Feed	comtact	A
Outbox	EncryptAndSignTestMessage	4:53
RSS-каналы		
Нежелательная почта	corptest	
Отправленные	EncryptAndSignTestMessage	Чт 5:47
▷ Папки поиска	COrptest EncryptAndSignTestMessage	<mark>б</mark> Чт 5:19
💌 📰 🖾 🖄	•••• Corptest EncryptAndSignTestMessage	<mark>6</mark> Чт 4:48
ЭЛЕМЕНТЫ: 80	ВСЕ ПАПКИ УЖЕ ОБНОВЛЕНЫ. ПОДКЛЮ	94EHO K: MICROSOFT EXCHAI

Рисунок 174. Локальная адресная книга Outlook

- 2. В открывшейся форме выберите нужный контакт и откройте двойным кликом.
- 3. В форме, которая содержит сведения о контакте, выберите Показ (View), в открывшемся
 - выпадающем меню нажмите Сертификаты 🤗 Сертификаты (Certificates).

⊑ 🚽 Ć Ć ↑ ↓ ∓	corptest - Контакт	? 📧 —	□ ×
ФАЙЛ КОНТАКТ ВСТАВКА ФС	РМАТ ТЕКСТА РЕЦЕНЗИРОВАНИЕ		
Сохранить и создать Удалить и закрыть Сохранить и создать Ф Переслать • Ф OneNote	 Справить по электронной почте Отправить по электронной почте Собрание Дополнительно * 	Имена Параметры теги Обновить Масштаб	
Действия	Связь	Обновить Масштаб	~
Полное имя corptest Организация	Сертификаты Общие Все поля Показ	corptest corptest@cryptopro.ru	
Интернет			
Эл. почта ▼ <u>corptest@crypt</u>	<u>pro.ru</u>	2	
Отображать как corptest		заметки	
Веб-страница			
Мгн. сообщения			
Телефоны			
Рабочий 👻			
Домашний			
Факс (рабочий) 👻			
Мобильный 👻			
Адреса			
Рабочий	(Дарта) Карта		
Подробнее о corptest.		le l	^

Рисунок 175. Контакт Outlook

	з, в котором можно увидеть с	сертификат отп
🗉 🖬 🕤 🖱 🕈 🦊 🗧 corptes	st - Контакт	? 🗹 – 🗖 🗙
ФАЙЛ КОНТАКТ ВСТАВКА ФОРМАТ ТЕКСТА	РЕЦЕНЗИРОВАНИЕ	
охранить Удалить Удалить и создать удалить Удалить Опереслать В Переслать ОпеNote Действия ОпеNote Действия Показ Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Связа Св	имена имена т имена т имена т параметры т т параметры т параметры т т параметры т п параметры т п п п п п п п п п п п п п	Масштаб Масштаб
Лванов Иван Иванович(По умолчанию) corptest		Свойства По умолчанию Импорт Экспорт Удалить

Рисунок 176. Список сертификатов Outlook

После этого нажмите на кнопку Сохранить и Закрыть (Save & Close). Если абонент с таким адресом уже существует, программа предложит, либо добавить новый контакт (Add new Contact), либо обновить сведения о выделенном контакте (Update information of selected Contact). Выберите второй пункт. При этом в существующий контакт будет добавлен полученный сертификат, а резервная копия будет сохранена в Deleted Items Folder (Удаленные).

2

-

8.4. Отправка шифрованных сообщений

	оздать
Для создания и отправки шифрованного сообщения нажмите кнопку Создать 🚥	бщение: (New E-mail).
Выберите получателя сообщения (поле То) и введите тему сообщения (Subject).	Если письмо будет
содержать некоторые файлы, добавьте их в письмо, используя кнопку Вложить фа	айл (Attach File) в
закладке Вставка (Insert). Для отправки сообщения в зашифрованном виде	нажмите кнопку
Шифровать (Encrypt).	

ЖТЯИ.00088-01	92 01.	КриптоПро	CSP.	Инструкция г	10	использованию
---------------	--------	-----------	------	--------------	----	---------------

ФАЙЛ	сообщение		test - Сообщение	(HTML) PMAT TEKCTA P	? 📧 — 🗆	×
Темы Токаз	СК От Разрец ать п	ни Шифровать Цении Я Подписать Разрешение	Отслеживание •	Сохранить отправл элемент ~ Дополни	Задержка доставки «Направлять ответы в енный тельные параметры	
	Кому	korolev@cryptopro		\$		
test	Тема	test				

Рисунок 177. Создание зашифрованного сообщения Outlook

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	
1	Приложению Microsoft Outlook н сообщение, поскольку следующие сертификатов, имеют недействит поддерживают данное шифрован	е удалось зашифро е получатели не им ельные сертифика ⁻ ние:	овать іеют ты или не
	corptest		
	Сообщение может быть зашифро указанные получатели, по-видимо	вано и отправлено ому, не смогут его	о, но прочитать.

Рисунок 178. Ошибка при шифровании отозванным сертификатом

8.5. Проверка сертификата на отзыв

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



Рисунок 179. Проверка цифровой подписи

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.

000	йства безопасно	сти сообщения	×
👫 Тема: Тест			
Сообщения могут шифр слой допускает наличие	оваться и содержать нескольких подписей	слои цифровых подпи й.	сей. Каждый
Слои безопасности			
 ✓ Тема: Тест ✓ Уровень цифро ✓ Подписано: 	вых подписей		
Описание:			
Описание: ОК: подписанное сооби	цение.		
Описание: ОК: подписанное сообш Следующие кнопки позв изменения в выбранный	цение. юляют просмотреть д і слой:	ополнительные сведен	ния или внести
Описание: ОК: подписанное сообш Следующие кнопки позв изменения в выбранный Изменить доверие	цение. юляют просмотреть 4 і слой: Подробности	ополнительные сведен Доверие к центру се	ния или внести

Рисунок 180. Сведения о цифровой подписи в Outlook

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



Рисунок 181. Сообщение о недействительной цифровой подписи

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

COU	иства безопасно	сти сообщения	-
🚮 Тема: Тест			
Сообщения могут шифр слой допускает наличие Слои безопасности Выберите слой для просі	оваться и содержать нескольких подписеі мотра его описания.	слои цифровых подписей. 1.	Каждый
О Тема: Тест			
уровень цифров	вых подписеи		
подписано:			
Описание:			
Описание: Ошибка: Системе не удается пров Данной подписи сертиф Полписано	ерить, является ли и икат достоверным.	спользованный для создани спользованный для создани	ия
Описание: Ошибка: Системе не удается пров данной подписи сертиф Подписано Гледующие кнопки позв изменения в выбранный	верить, является ли и икат достоверным. оляют просмотреть д слой:	спользованный для создани спользованный для создани сполнительные сведения и	ия <u>зл 11 ол</u> У или внести
Описание: Ошибка: Системе не удается прое данной подписи сертиф Подписано Гледующие кнопки позв ізменения в выбранный Изменить доверие…	верить, является ли и икат достоверным. оляют просмотреть д слой: Подробности	спользованный для создани ополнительные сведения и Доверие к центру сертис	ия <u>зл 11 ол</u> У или внести фикации

Рисунок 182. Сведения о недействительной цифровой подписи