

# КриптоПро УЦ

программно-аппаратный комплекс УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Руководство пользователя

# АННОТАЦИЯ

Настоящий документ содержит описание эксплуатации веб-приложений Центра Регистрации программного комплекса «Удостоверяющий Центр «КриптоПро УЦ» (УЦ).

К веб-приложениям Центра Регистрации относятся:

- АРМ регистрации пользователя;
- АРМ зарегистрированного пользователя с маркерным доступом;
- АРМ зарегистрированного пользователя с ключевым доступом.

АРМы пользователя являются Web-приложениями, размещенными на Web-узле Центра Регистрации.

Приложение APM зарегистрированного пользователя с ключевым доступом предназначено для пользователя Центра Регистрации, зарегистрированного Администратором ЦР установленным порядком и имеющего как минимум один действующий сертификат. Предназначено для выполнения следующих задач:

• Генерация личных ключей ЭП и ключей проверки ЭП и запись их на ключевой носитель;

- Управление личными пользовательскими сертификатами;
- Получения сертификата Центра Сертификации УЦ;
- Получения списка отозванных сертификатов УЦ;

• Поиск и получение (импорт) сертификатов других зарегистрированных пользователей УЦ.

Приложение APM зарегистрированного пользователя с маркерным доступом предназначено для пользователя Центра Регистрации, зарегистрированного Администратором ЦР установленным порядком, имеющего маркер временного доступа и не имеющего ни одного действующего сертификата. Предназначено для выполнения следующих задач:

• Генерация личных ключей ЭП и ключей проверки ЭП и запись их на ключевой носитель;

• Получения сертификата Центра Сертификации УЦ.

Приложение APM регистрации пользователя предназначено для пользователя Центра Регистрации, проходящего процедуру регистрации в распределенном режиме установленным порядком, и предназначен для решения следующих задач:

• Формирование пользователем запроса на регистрацию и отправка его в Центр Регистрации.

# Информация о разработчике ПАК «КриптоПро УЦ»:

ООО "Крипто-Про" 127 018, Москва, улица Сущевский вал, 16 строение 5 Телефон: (495) 780 4820 Факс: (495) 780 4820 <u>http://www.CryptoPro.ru</u> E-mail: info@CryptoPro.ru

			СОДЕРЖАНИЕ	
1.	Треб	бования	для работы с приложением	5
2.	Объ	екты уп	равления	6
	2.1.	Сертиф	икат ключа проверки электронной подписи	6
	2.2.	Список	отозванных сертификатов	6
	2.3.	Запрос	на регистрацию	6
	2.4.	Запрос	на сертификат	6
	2.5.	Запрос	на отзыв сертификата	6
	2.6.	Служеб	ные ключи и сертификаты	6
	2.7.	Рабочие	е ключи и сертификаты	7
3.	Наст	гройка р	рабочего места пользователя	8
	3.1.	Установ	ка дистрибутива ПО СКЗИ КриптоПро CSP	8
	3.2.	Изменен	ние набора устройств хранения ключевой информации	8
	3.3.	Лицензи	ия и регистрация ПО СКЗИ	9
	3.4.	Настрой	і́ка КриптоПро CSP	9
	3.5.	Установ	ка Сертификата Центра Сертификации	9
	3.6.	Добавле	ение узла ЦР в зону "Надежные узлы"	11
	3.7.	Установ админио	ка личного служебного сертификата пользователя, выданного стратором ЦР	12
4.	ΑΡΜ	зареги	стрированного пользователя с ключевым доступом	16
	4.1.	Запуск	АРМ зарегистрированного пользователя с ключевым доступом	16
	4.2.	Работа і	в АРМ зарегистрированного пользователя с ключевым доступом	17
		4.2.1.	Получение списка отозванных сертификатов	19
		4.2.2.	Получение сертификата Центра Сертификации	20
		4.2.3.	Получение нового сертификата	21
		4.2.4.	Формирование запроса на сертификат	22
		4.2.5.	Установка сертификата	24
		4.2.6.	Печать сертификата	26
		4.2.7.	Приостановление действия сертификата	28
		4.2.8.	Возобновление действия сертификата	29
		4.2.9.	Отзыв сертификата	30
		4.2.10.	Поиск и импорт сертификатов других зарегистрированных пользователей Центра Регистрации	32
		4.2.11.	Формирование запроса на поиск сертификатов	33
		4.2.12.	Работа со списком отобранных сертификатов	35
		4.2.13.	Сохранение сертификатов других пользователей на локальном компьютере	37
5.	АРМ	регистр	рации пользователей	42
	5.1.	Запуск	АРМ регистрации пользователей	42
	5.2.	Процеду	ура регистрации пользователей	42
		5.2.1.	Формирование и отправка запроса на регистрацию	42

10	Перечень со		61	
9.	Перечень сокращений			
8.	Перечень те	ерминов	54	
7.	Перечень р	исунков	52	
	6.1. Запуск	АРМ зарегистрированного пользователя с маркерным доступом	51	
6.	Работа заре доступа	егистрированного пользователя, получившего маркер врем	<b>енного</b> 51	
	5.2.6.	Автоматическая обработка запроса на сертификат Центром Регистрации	49	
	5.2.5.	Обработка запроса на сертификат администратором Центра Регистрации	47	
	5.2.4.	Формирование ключей и запроса на сертификат	46	
	5.2.3.	Автоматическая обработка запроса на регистрацию Центром Регистрации	46	
	5.2.2.	Обработка запроса на регистрацию администратором Центра Регистрации	43	

# 1. Требования для работы с приложением

Для эксплуатации APM пользователя необходимо следующее программное обеспечение:

- Операционная система Microsoft Windows 2000 и выше;
- Microsoft Internet Explorer 5.0 (и выше);

• Microsoft Security Bulletin MS02-048. Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates (Q323172). August 28, 2002;

• Microsoft Security Bulletin MS02-050. Certificate Validation Flaw Could Enable Identity Spoofing (Q328145). September 09, 2002;

• Программная библиотека CAPICOM.dll версии 2.1.0.1 (http://www.microsoft.com/downloads/details.aspx?FamilyID=860ee43a-a843-462f-abb5ff88ea5896f6&DisplayLang=en);

- Сертифицированное средство криптографической защиты (СКЗИ) КриптоПро CSP;
  - Модуль поддержки сетевой аутентификации СКЗИ КриптоПро CSP КриптоПро TLS.

# 2. Объекты управления

# 2.1. Сертификат ключа проверки электронной подписи

Сертификат ключа проверки электронной подписи — электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом субъекта и информацией, которая его идентифицирует.

# 2.2. Список отозванных сертификатов

Список отозванных сертификатов (CRL – Certificate Revocation List) – это электронный документ, который содержит перечень сертификатов, являющихся отозванными из обращения в ПАК «КриптоПро УЦ». Удостоверяющий Центр поддерживает отзыв сертификатов и публикацию списков отозванных сертификатов. Абоненты могут получить эту информацию и записать ее в свое локальное хранилище, чтобы использовать для последующей проверки сертификатов.

# 2.3. Запрос на регистрацию

Запрос на регистрацию — сообщение, содержащее необходимую информацию для регистрации пользователя в ПАК «КриптоПро УЦ».

Формируется при регистрации пользователя, после чего передается на Центр Регистрации. Обработка осуществляется администратором УЦ со своего рабочего места. Результатом обработки является формирование учетной записи пользователя в Базе Данных Центра Регистрации или сообщение об ошибке.

# 2.4. Запрос на сертификат

Запрос на сертификат — сообщение, содержащее необходимую информацию для получения сертификата. Формируется в АРМ Пользователя или в АРМ Администратора, после чего передается через Центр Регистрации Удостоверяющему Центру, где и обрабатывается. Результатом обработки является выпущенный сертификат или сообщение об ошибке.

# 2.5. Запрос на отзыв сертификата

Запрос на отзыв сертификата — сообщение, содержащее необходимую информацию для выполнения процедуры отзыва сертификата пользователя из обращения в системе. Формируется в АРМ Пользователя или в АРМ Администратора, после чего передается через Центр Регистрации Удостоверяющему Центру, где и обрабатывается. Результатом обработки является занесение сертификата в список отозванных сертификатов или сообщение об ошибке.

# 2.6. Служебные ключи и сертификаты

Процесс регистрации пользователей в ПАК «КриптоПро УЦ» предусматривает централизованное изготовление служебных (закрытых) ключей и сертификатов пользователей администратором безопасности. Служебные ключи предназначены для подтверждения подлинности пользователя при формировании им рабочих закрытых ключей и передаче запроса на сертификат в Центр Регистрации ПАК «КриптоПро УЦ». Часто служебные ключи и сертификаты называют «временными». Это происходит в тех случаях, когда такой ключ действует очень короткое время, а именно до получения при помощи него первого «рабочего» ключа.

# 2.7. Рабочие ключи и сертификаты

После процесса регистрации пользователи с использованием служебных ключей и сертификатов должны сформировать рабочие ключи и получить рабочие сертификаты. Рабочие ключи предназначены для формирования ЭП, выполнения операций шифрования сообщений, аутентификации пользователя при его взаимодействии с ЦР и плановой смене ключей. Запрос на сертификат от пользователя будет обработан Центром Регистрации только в случае, если он подписан служебным ключом или действующим закрытым ключом пользователя.

**Примечание.** Разделение понятий «служебные ключи», «служебный сертификат» и соответствующих им «рабочие ключи», «рабочий сертификат» чисто условно. Наиболее частая практика регистрации новых пользователей и выдачи им первых сертификатов сводится к формированию и выдаче им временных ключей и сертификатов, действующих довольно короткое время и предназначенных лишь для того, чтобы пользователь смог с их помошью идентифицироваться в АРМ пользователя, после чего сформировать уже «рабочие» ключи и сертификат. Часто это сводится к практике централизованного изготовления ключей администратором безопасности организации и выдаче этих ключей и сертификатов пользователям на ключевых носителях. Настоящая версия Удостоверяющего центра позволяет гибко манипулировать этими понятиями, настраиваться под любые потребности конкретных организаций, эксплуатирующих УЦ. Вполне реальна ситуация, когда никаких «служебных» ключей и сертификатов не возникает. При этом сразу формируются обычные «рабочие» ключи/сертификаты, неважно, в процессе ли регистрации пользователя, или при централизованном распределении ключей. Но в целях отличия самого первого сертификата от всех последующих, полученных одним пользователем, мы в данном руководстве первоначальные ключи и сертификат будем называть «служебными» (иногда их еще называют «временными»). В результате такого сценария, после получения и установки служебного сертификата, пользователь получает статус зарегистрированного и для продолжения дальнейшей работы выполняет процедуру получения нового, рабочего сертификата самостоятельно, в АРМ пользователя.

# 3. Настройка рабочего места пользователя

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

- Получить от администратора ЦР или скачать с Web сервера ЦР дистрибутивы программного обеспечения СКЗИ «КриптоПро CSP» и «КриптоПро TLS»;
- Установить СКЗИ «КриптоПро CSP», «КриптоПро TLS»;
- Установить сертификат ЦС;
- Добавить узел ЦР в зону Надежных узлов;
- Установить личный сертификат с ключевого носителя, полученного от администратора ЦР в случае регистрации пользователя в централизованном режиме.

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

# 3.1. Установка дистрибутива ПО СКЗИ КриптоПро CSP

Установка дистрибутива должна производится пользователем, имеющим права администратора на локальном компьютере. Перед установкой дистрибутива новой версии КриптоПро CSP, удалите ранее установленную версию КриптоПро CSP. Если старая версия КриптоПро CSP не удалена, то новая версия не будет установлена. Для этого используйте пункты основного меню Windows Пуск, Настройка, Панель управления, Установка и удаление программ (см. Рисунок 1).

Рисунок 1. Окно удаления устаревших версий СКЗИ КриптоПро CSP

1	Установленные программы: Упорядочить: по имени						
Замена или удаление программ	КриптоПро СSP Щелкните здесь для получения сведений о поддержке.	Размер Используется Последний раз использован	<u>3,16 МБ</u> редко 28.10.2002	<b>^</b>			
🛃 Установка	Чтобы заменить программу или удалить ее, щелкните "Заменить/Удалить".	Заменить	/Удалить				
новой программы	🛃 КриптоПро TLS	Размер	240 КБ	-			
<b>1</b>			Закрыть				

На АРМ пользователя Удостоверяющего центра может использоваться любая сертифицированная версия СКЗИ КриптоПро CSP.

Установка СКЗИ «КриптоПро CSP» осуществляется в соответствии с эксплуатационной документацией. После установки программного обеспечения СКЗИ «КриптоПро CSP» необходимо активировать лицензию на продукт.

# 3.2. Изменение набора устройств хранения ключевой информации

СКЗИ КриптоПро CSP позволяет настроить устройства для хранения ключевой информации. Настройка для разных версий CSP производится по соответствующей

документации "КриптоПро CSP. Инструкция по использованию КриптоПро CSP и TLS" (согласно формуляру).

# 3.3. Лицензия и регистрация ПО СКЗИ

Для работы с СКЗИ КриптоПро CSP необходимо ее зарегистрировать, введя соответствующую лицензию. Ввод лицензии для разных версий CSP производится по соответствующей документации "КриптоПро CSP. Инструкция по использованию КриптоПро CSP и TLS" (согласно формуляру).

# 3.4. Настройка КриптоПро CSP

КриптоПро CSP может функционировать и хранить ключевую информацию в двух режимах:

- В памяти приложения;
- В "Службе хранения ключей", которая реализована в виде системного сервиса.

Функционирование КриптоПро CSP в "Службе хранения ключей" обеспечивает дополнительную защиту ключевой информации от других приложений, выполняющихся на компьютере, но может незначительно снизить производительность. Порядок изменения режима функционирования СКЗИ описан в соответствующей документации "КриптоПро CSP. Инструкция по использованию КриптоПро CSP и TLS" (согласно формуляру).

# 3.5. Установка Сертификата Центра Сертификации

• Для установки сертификата ЦС необходимо открыть файл, содержащий сертификат ЦС, с использованием Проводника ОС MS Windows.

# Рисунок 2. Окно просмотра сертификата Центра Сертификации

Сертификат	? >				
Общие Состав Путь сертификации					
Сведения о сертификате	-				
Этот сертификат:					
<ul> <li>Обеспечивает получение идентификации от удаленного компьютера</li> <li>Подтверждает удаленному компьютеру идентификацию вашего компьютера</li> <li>Подтверждает, что программное обеспечение получено</li> </ul>					
Кому выдан: Test Root CA on SP2					
Кем выдан: Test Root CA on SP2					
Действителен с 30.09.2002 по 30.09.2007					
Установить сертификат Заявление поставщика					
<u>ОК</u>					

 Нажать кнопку Установить сертификат и с помощью Мастера импорта сертификатов (см. Рисунок 3) произвести установку сертификата в Хранилище сертификатов.

# Рисунок 3. Окно Мастера импорта сертификатов Мастер импорта сертификатов X 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. Для продолжения нажмите кнопку "Далее". < <u>Н</u>азад Далее > Отмена

 В процессе работы Мастера, при выборе хранилища сертификатов выбрать опцию "Поместить все сертификаты в следующее хранилище" (см. Рисунок
 4) и выбрать "Доверенные корневые центры сертификации".

# Рисунок 4. Окно выбора хранилища сертификатов Мастера импорта сертификатов

Мастер импорта сертификатов	×
Хранилище сертификатов Хранилища сертификатов - это области системы в которых производится	
хранение сертификатов.	_
Выбор хранилища может быть произведен Windows автоматически, или же можно указать размещение сертификата вручную.	
💭 <u>А</u> втоматически выбрать хранилище на основе типа сертификата	
💿 Поместить все сертификаты в следующее хранилище	
Хранилище сертификатов:	
Доверенные корневые центры сертификации	
< <u>Н</u> азад Далее > Отмена	

 При появлении сообщения (см. Рисунок 5) о добавлении сертификата в корневое хранилище нажать кнопку Да. Появление данного сообщения свидетельствует об успешной установке сертификата Центра Сертификации. Отсутствие сообщения свидетельствует о том, что данный сертификат ранее был уже установлен на данный компьютер или он не является корневым сертификатом Центра Сертификации.

Рисунок 5. Окно сообщения о добавлении сертификата в корневое хранилище

Корневое	е хранилище сертификатов 🔀
1	Добавить этот сертификат в корневое хранилище? Субъект: СА, АСМЕ, RU, maslov@cryptopro.ru Поставщик: непосредственно поставщиком Действителен: с 26 января 2002 г. по 26 января 2009 г. Серийный номер : 3AF1DFBC DCFBDFAA 439DD1D4 18F32082 Отпечаток (sha1) : 215B563E B9B4EBC2 8DE395D0 8429B109 0D4B9772 Отпечаток (md5) : 35E893A0 8F703006 81499649 EB9BA05F

3.6. Добавление узла ЦР в зону "Надежные узлы"

Для добавления узла ЦР в зону "Надежные узлы" необходимо перейти в **Панель** управления, Свойства обозревателя (или зайти в меню Internet Explorer Сервис, Свойства обозревателя) и перейти на вкладку Безопасность.

Рисунок 6. Окно настройки свойства обозревателя

Свойства: Интернет 🛛 💽 🔀								
Содержан	ие	Подключен	ня	Про	граммы	Дополните	ельно	
Общие		Безопасн	юсть		Конфі	иденциальнос	ть	
Выберите	Выберите зону для настройки ее параметров безорасности.							
٢		<b>S</b>		/	C	)		
Интерн	ет	Местная интрасеть	Наде УЗ	эжные Элы	Ограни узл	1чен ПЫ		
н	адеж	ные узлы				Vane		
З л д В	она дл ричиня анным этой з	я надежных у ят вреда ваше , оне есть веб-	узлов, ему ком -узлы.	котор Ипьют	ые не еру или	75/10	,	
Уровень	безоп	асности для з	той зо	ны —				
<b>Особый</b> Особые параметры. - Чтобы изменить их, щелкните "Другой". - Для возврата к рекомендованному уровню щелкните "По умолчанию".								
Другой По умолчанию Выбрать уровень безопасности по умолчанию для всех зон								
ОК Отмена Применить								

Далее выделить **Надежные узлы,** а затем нажать кнопку **Узлы,** после этого в появившемся окне записать адрес узла ЦР <u>https://имя сервера ЦР</u> и нажать кнопку **Добавить**.

Рисунок 7. Окно добавления узла в зону надежные узлы						
Надежные узлы						
В эту зону можно добавлять веб-узлы и удал Заданные для зоны параметры безопасности использоваться для всех ее узлов.	лять их из нее. и будут					
Добавить в зону следующий узел:						
https://yura-5fb11fb62c	Добавить					
Веб-узлы:						
	Удалить					
Для всех узлов этой зоны требуется проверка се	рверов (https:)					
	Закрыть					

Для новых версий Internet Explorer (7, 8) необходимо дополнительно сделать настройку выполнения компонентов ActiveX. Для этого на той же вкладке Безопасность (см. Рисунок 6) нажать кнопку Другой и в разделе "Элементы ActiveX и модули подключения" найти настройку "Использование элементов управления ActiveX, не помеченных как безопасные для использования" – нужно поставить "Включить" (или "Предлагать").

Для выполнения на АРМах пользователей действий по: смене сертификата и закрытого ключа пользователя, приостановлению срока действия сертификата, возобновлению сертификата и отзыву сертификата на компьютере пользователя необходим компонент САРІСОМ. Его необходимо установить с правами администратора на компьютер пользователя. Дистрибутив имеется на сайте Microsoft: http://www.microsoft.com/downloads/details.aspx?FamilyID=860EE43A-A843-462F-ABB5-FF88EA5896F6&displayLang=ru

Если пользователь имеет права администратора на своём компьютере, то можно вместо этого установить версию CAPICOM, размещенную на сервере ЦР - linternet Eexplorer автоматически предложит установить её при первом подключении к ЦР.

3.7. Установка личного служебного сертификата пользователя, выданного администратором ЦР

 Для установки личного сертификата с ключевого носителя необходимо воспользоваться интерфейсом СКЗИ «КриптоПро CSP», доступного из Панели управления (см. Рисунок 8).

# Рисунок 8. Окно панели управления



- Запустите приложение КриптоПро CSP из Панели и установите сертификат с ключевого носителя. Для этого выполните следующие процедуры:
  - На вкладке Сервис окна свойств приложения КриптоПро CSP (см. Рисунок 9) нажмите кнопку Просмотреть сертификаты в контейнере;

# Рисунок 9. Вкладка Сервис окна свойств приложения КриптоПро CSP

Свойства: КриптоПро CSP							
Безопасность До	полнительно Алгоритмы ридование Сервис	ļ					
Контейнеры секретного ключа Эти мастера позволяют скопировать / удалить секретный ключ, находящийся в существующим контейнере. Скопировать контейнер							
Сертификаты в контейнере секретного ключа Этот мастер позволяет просмотреть и установить сертификаты, находящиеся в существующем контейнере секретного ключа на носителе. Просмотреть сертификаты в контейнере							
Личный сертификат Этот мастер позволяет связать существующий сертификат из файла с существующем контейнером секретного ключа на носителе. Установить личный сертификат							
Пароли на носителях секретных ключей Эти мастера предназначены для изменения / очистки запомненный паролей (ПИН-кодов) доступа к носителям секретных ключей. Изменить пароль Удалить запомненные пароли							
ОК Отмена Применить							

 В открывшемся окне нажмите кнопку Обзор для выбора ключевого контейнера (см. Рисунок 10);

# Рисунок 10. Окно выбора контейнера для установки сертификата

Сертификаты в контейнере секретного ключа 🛛 🔀					
Контейнер секретного ключа Введите или укажите контейнер секретного ключа для просмотра сертификатов в этом контейнере					
<u>И</u> мя ключевого контейнера: Обзор					
Введенное имя задает ключевой контейнер: С Пользователя С Компьютера					
Выберите CSP для поиска ключевых контейнеров: Crypto-Pro Cryptographic Service Provider					
< <u>Н</u> азад Далее> Отмена					

- В появившемся списке ключевых контейнеров установите курсор на соответствующий контейнер и нажмите кнопку **ОК**;
- Для продолжения работы нажмите кнопку Далее;
- В появившемся окне будет отражена информация из сертификата, расположенного в ключевом контейнере. Убедитесь в соответствии данной информации Вашим персональным данным. В случае, если данные совпадают, нажмите кнопку Свойства. Если данные не совпадают (выбран не тот ключевой контейнер), повторите процедуру выбора имени ключевого контейнера;
- После нажатия кнопки Свойства на экране отображается окно с полной информацией о сертификате (см. Рисунок 11);

# Рисунок 11. Окно свойств сертификата из ключевого контейнера

Property Page Select Cert	<u>?</u> ×
Общие Состав Путь сертификации	
Сведения о сертификате	
Этот сертификат:	
<ul> <li>Подтверждает удаленному компьютеру идентификации вашего компьютера</li> </ul>	
Кому выдан: аааа	
Кем выдан: СА	
Действителен с 28.02.2002 по 28.02.2003	
🌮 Есть закрытый ключ, соответствующий этому сертификат;	/.
<u>Установить сертификат</u> Ваявление поставщин	ka
	к

 Продолжая процедуру установки сертификата, нажмите кнопку Установить сертификат;

- В соответствии с работой Мастера импорта сертификатов, произведите установку данного сертификата в хранилище на рабочее место (компьютер);
- При работе Мастера рекомендуется выбирать предлагаемые им значения по умолчанию, т.е. нажимать кнопки Далее и Готово;
- Появление сообщения об успешном импорте сертификата и возврата к окну с информацией о сертификате (предыдущий рисунок), нажмите кнопку **ОК;**
- После этого на окне Сертификат для просмотра и далее последовательно нажимайте кнопки Отмена.

# 4. АРМ зарегистрированного пользователя с ключевым доступом

# 4.1. Запуск APM зарегистрированного пользователя с ключевым доступом

Для запуска и работы с APM пользователя необходимо открыть окно браузера MS IE и перейти по адресу <u>https://имя сервера UP/UI/User/User.ASP</u>, где <u>имя сервера UP</u> – имя Web-узла Центра Регистрации, или воспользоваться стартовой страничкой Webприложений Центра Регистрации (см. Рисунок 12), где выбрать режим **Вход для зарегистрированных пользователей**.

# Рисунок 12. Стартовая страница Web-приложений Центра Регистрации

🚰 Удостоверяющий центр - Microsoft Internet Explorer 📃 📃	B×
Фейл Правка Вид Избранное Сереис Справка	
(= Нарад → → → 🕼 🖉 🖄   🛞 Понкк 💼 Избранное 🛞 Медиа 🍏   🖏 - 🍠 📨 🚍 🖳	
Agpeç; 🎒 https://lord2k.cp.ru/ui/	лки »
Добро пожаловать в Удостоверяющий центр	
Программный комплекс КриптоПро УЦ (Удостоверяющий Центр) представляет собой интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих криптографическую защиту информации с сертификатами открытых ключей, а также для управления ими.	
Подсистема удаленного (Web) доступа пользователей к Центру Регистрации позволяет Вам.	
<ul> <li>Зарегистрироваться и получить свой первый сертифкат открытого ключа, с помощью которого будет осуществляться взаимодействие с Центром Регистрации.</li> </ul>	
<ul> <li>Формировать служебные ключи пользователя.</li> <li>Создавать и отправлять запросы на формирование сертификатов для различных назначений по шаблонам, установленным в нашем Удостоверяющем</li></ul>	
центрс. • Производить плановую смену ключей и сертификатов • Формировать и отправлять запросы на отзыв сертификатов	
<ul> <li>Отслеживать состояние отправленных запросов</li> <li>Получать, устанавливать, распечатывать выпущенные сертификаты</li> </ul>	
Весь обмен информацией с Центром Регистрации Удостоверяющего Центра осуществляется с использованием защищенного протокола TLS с одно и двусторонней аутентификацией.	
Установка необходимого Для работы с нашим Центром требуется установить на локальном компьютере программное обеспечение Крипто-Про. программного обеспечения Прежде всего это касается российских средств криптографической защиты информации для обеспечения конфиденциальности, авторства и целостности информации, а также аутентификации и защищенного обмена данными в Web-приложениях. Crypto Pro CSP, Crypto Pro TLS	
<u>Начать регистрацию</u> Если необходимое программное обеспечение уже установлено на Вашем компьютере и Вы собираетсь стать пользователем нашего Удостовержющего Центра, можете проиступать к регистрации.	
Вход для пользователей, обладающих маркером получения сертификата). временного доступа	
<u>Вход для зарегистрированных</u> Если Вы успешно прошли регистрацию, получили и установили свой первый сертификат, используйте данную сылку для <u>пользователей</u> продолжения работы с Центром Регистрации	
Если Вы начали, и еще не закончили регистрацию, используйте ссылку, отправленную Вам по электронной почте или сообщенную Администратором Центра Регистрации	•
🕙	

Для аутентификации пользователя на ЦР и получения доступа к АРМ пользователя необходимо в процессе запуска выбрать сертификат пользователя, по которому будет выполняться процедура аутентификации. Данный выбор происходит в окне проверки подлинности клиента приложения MS IE (см. Рисунок 13).

# Рисунок 13. Окно выбора сертификата для проверки подлинности клиента

Проверн	ка подлинности клиента	? ×
Иденти	фикация	
	Веб-узел запросил проверку подлинности. Выберите сертификат для подключения.	
		-
	Иванов Иван Иванович	-
	Подробнее Просмотр сертификата	ı
	ОК Отми	ена

В данном окне отображается список сертификатов пользователя, установленных в хранилище сертификатов текущего пользователя локального компьютера. Необходимо установить курсор на нужном сертификате и нажать кнопку **ОК**. Для просмотра информации о сертификате воспользуйтесь кнопкой **Просмотр сертификата**.

# 4.2. Работа в АРМ зарегистрированного пользователя с ключевым доступом

Основное окно Web-приложения Центра Регистрации АРМ зарегистрированного пользователя с ключевым доступом имеет следующий вид (см. Рисунок 14):

🎒 Страница зарегестирова	нного пользователя - Міс	crosoft Internet E	xplorer					
<u>Ф</u> айл Правка <u>В</u> ид <u>И</u> збр	анное Сервис <u>С</u> правка							1
Назад 🔹 🔿 🖉 👩	📸 🛛 🥘 Поиск 🛛 🔬 Избранн	юе (ФМедиа (	3   B- (	9 e · E 2				
Адрес <u>:</u> 🙆 https://lord2k.cp.ru	/ui/User/User.asp						💌 🔗 Переход	Ссылки »
				ز	(достове)	эяющий Ц	ентр Крипт	о-Про 占
Новый сертификат	Сертификат центра	Список отозв	анных					
Персональная стр	аница зарегистрир	ованного п	юльзов	ателя:				
Общее имя : Т	'est User 7							
Электронная почта: п	naslov@cryptopro.ru							
Сертификаты:								_
Серийный номер	Дата выпуска	Дата оконч	ания (	Статус сертификата	Просмотр	Отзыв П	риостановление	
61B7CDB60000000001	E 2003-08-22 13:39:00	2003-08-29 13	8:49:00 🛛	Действителен	Показать	Отозвать П	риостановить	
Запросы на сертифик	аты:							
Дата запроса	Дата рассмотрения	Комментарий	Статус	Просмотр				
2003-08-22 13:48:00	2003-08-22 13:48:00	:	Завершен	Показать				
Запросы на отзыв:								
Отсутствуют								-
🙆 Готово						🔒 🥝 Инт	ернет	

Рисунок 14. Окно АРМа зарегистрированного пользователя

В верхней части окна расположена область основных режимов работы пользователя, которая содержит три кнопки:

1. Новый сертификат – режим работы по созданию новых ключей и запроса на сертификат пользователя;

- Сертификат центра получение и установка на локальном компьютере сертификата Центра Сертификации;
- 3. Список отозванных получение списка отозванных сертификатов данного Центра Сертификации;

Ниже области режимов работы расположена информация о текущем пользователе, сформированная во время его регистрации.

Далее в виде таблиц идет информация о выпущенных сертификатах, запросах на сертификаты, запросах на отзыв сертификатов.

Таблица со списком сертификатов пользователя имеет следующие колонки:

- **Серийный номер** серийный номер сертификата, соответствующего текущей строке таблицы;
- **Дата выпуска** Дата/время выпуска сертификата. С этого момента сертификат считается действительным и может использоваться по назначению, указанному в сертификате;
- **Дата окончания** Дата/время окончания действия сертификата. После указанной даты сертификат считается недействительным и не может использоваться по назначению;
- Статус сертификата текущее состояние сертификата. Может принимать следующие значения: Действителен, Запрошен к отзыву, Отозван;
- Просмотр содержит ссылку (кнопку), по нажатию которой можно вывести содержимое сертификата в отдельное окно для просмотра и/или печати на бумажный носитель;
- Отзыв содержит ссылку (кнопку), по нажатию которой можно перейти к режиму работы по формированию запроса на отзыв соответствующего (расположенного в текущей строке таблицы) сертификата. Если же данный сертификат уже отозван, то ссылка не показывается;
- **Приостановление** содержит ссылку (кнопку), по нажатию которой можно перейти к режиму работы по формированию запроса на приостановление действия соответствующего (расположенного в текущей строке таблицы) сертификата. Если же данный сертификат уже отозван, то ссылка не показывается.

Информация о сертификате открытого ключа, который в данный момент используется для установления защищенного TLS соединения с Web сервером Центра Регистрации, показывается красным цветом.

Таблица со списком запросов на сертификаты имеет следующие колонки:

- Дата запроса дата/время формирования запроса на сертификат;
- **Дата рассмотрения** Дата/время принятия или отклонения запроса администратором Центра Регистрации;
- **Комментарий** дополнительная информация, указанная пользователем или администратором ЦР при формировании запроса на сертификат;
- Статус Текущее состояние запроса на сертификат. Может принимать значения:
  - о Обработка запрос находится в стадии рассмотрения;
  - о Отклонен запрос отклонен администратором ЦР;
  - **Завершен** запрос обработан, выпущенный сертификат получен и установлен пользователем;
  - Установить промежуточное состояние, требующее от пользователя установить выпущенный по данному запросу сертификат. В этом случае наименование состояния выполнено в виде ссылки/кнопки, по

клику на которой запускается процесс установки сертификата на локальной машине;

 Просмотр – содержит ссылку (кнопку), по нажатию которой можно вывести содержимое запроса на сертификат в отдельное окно для просмотра и/или печати на бумажный носитель.

Для каждой строки данной таблицы со статусом **Завершен** должна присутствовать строка в таблице сертификатов.

Таблица со списком запросов на отзыв сертификатов имеет следующие колонки:

- **Номер сертификата** Серийный номер отзываемого/отозванного сертификата;
- Дата запроса дата/время формирования запроса на отзыв сертификата;
- Дата отзыва Дата время рассмотрения запроса на отзыв сертификата администратором ЦР. В случае положительного решения – с данного момента сертификат считается недействительным и должен попасть в очередной список отозванных сертификатов;
- **Причина** Причина, по которой пользователь/администратор отозвал сертификат;
- Статус запроса текущее состояние запроса на отзыв сертификата. Может принимать следующие значения:
  - о **Обработка –** запрос находится в стадии рассмотрения;
  - Удовлетворен запрос принят, сертификат отозван;
  - Отклонен запрос отклонен администратором.

Если запрос на отзыв имеет статус **Удовлетворен**, то соответствующий сертификат в таблице сертификатов имеет статус **Отозван**.

Если пользователь ни разу не формировал запрос на отзыв сертификатов, то таблица со списком запросов на отзыв сертификата не показывается.

# 4.2.1. Получение списка отозванных сертификатов

Для получения и установки списка отозванных сертификатов необходимо выполнить следующие действия:

- В окне АРМ пользователя нажать ссылку Список отозванных. В результате этого действия происходит загрузка файла, содержащего список отозванных сертификатов с Центра Регистрации УЦ;
- В окне Загрузка файла (см. Рисунок 15) выберите пункт Сохранить этот файл на диске;

# Рисунок 15. Окно загрузки файла со списком отозванных сертификатов



• В окне определения имени и расположения сохраняемого файла выберите в качестве места размещения рабочий стол компьютера (см. Рисунок 16);

Рисунок 16. Окно сохранения файла со списком отозванных сертификатов

Сохранить как		<u>?</u> ×
<u>П</u> апка:	🗹 Рабочий стол	
Хурнал Курнал Рабочий стол Мои докумен Мой мотью	҈Мои документы Щ Мой компьютер ∰ Мое сетевое окружение	
Мое сетевое	Имя файла:         Сегtcrl         Сохра           Імя файла:         Список отзыва сертификатов         Отм	ена

- После этого перейдите на рабочий стол компьютера, выберите иконку данного файла, нажмите правую кнопку мышки и из появившегося списка пунктов меню выберите пункт Установить список отзыва (CRL);
- Далее в соответствии с Мастером импорта сертификатов (см. Рисунок 3), установите список отозванных сертификатов. При этом следует выбирать автоматическое определение хранилища, в соответствии с типом сертификата.

#### 4.2.2. Получение сертификата Центра Сертификации

Для получения и установки сертификата ЦС необходимо выполнить следующие действия:

- В окне АРМ пользователя нажать ссылку **Сертификат центра**. В результате этого действия происходит загрузка файла, содержащего сертификат ЦС;
- В окне Загрузка файла выберите пункт Открыть этот файл из текущего места (см. Рисунок 17);



• В появившемся окне с информацией о сертификате (см. Рисунок 18) нажмите кнопку **Установить сертификат**;

#### Рисунок 18. Окно свойств сертификата ЦС

Сертификат	? ×
Общие Состав Путь сертификации	
Сведения о сертификате	
Этот сертификат: • Обеспечивает получение идентификации от удаленного компьютера • Подтверждает удаленному компьютеру идентификацию вашего компьютера • Подтверждает, что програминое обеспечение получено от конкретного издателя	
Кому выдан: СА	_
Кем выдан: СА	
Действителен с 26.01.2002 по 26.01.2009	
Истановить сертификат	ка
	ж

• Далее следуйте указаниям Мастера импорта сертификатов.

# 4.2.3. Получение нового сертификата

Получение нового (рабочего) сертификата осуществляется в соответствии с регламентом работы, определенном Центром Регистрации (плановая смена ключей и сертификатов), или в случае внеплановой смены ключей и сертификатов (отзыв ранее действующего сертификата).

Получение нового сертификата выполняется на основании запроса на сертификат, получаемого ЦР от пользователя в электронном виде. Данный запрос формируется с использованием АРМ пользователя по ссылке **Новый сертификат**. В процессе формирования запроса производится генерация ключей и запись их на ключевой носитель.

После получения запроса на новый сертификат от пользователя, Центр Регистрации передает данный запрос на Центр Сертификации, где происходит формирование сертификата. Выпущенный сертификат устанавливается пользователем в хранилище сертификатов своего рабочего места (на компьютер). Установка сертификата также происходит с помощью программного обеспечения АРМ пользователя. В процессе установки сертификата также автоматически производится запись данного сертификата на ключевой носитель. В дальнейшем, данный сертификат может быть повторно установлен на рабочее место пользователя (в случае потери сертификата, например, в результате сбоя компьютера или операционной системы) или на другое рабочее место (в случае миграции пользователя). В этом случае установка сертификата с ключевого носителя производится с использованием интерфейса СКЗИ «КриптоПро CSP» в порядке, аналогичном порядку, определенному в соответствующем пункте раздела Установка личного служебного сертификата пользователя, выданного администратором ЦР.

Процедура получения нового сертификата:

- 4.2.4. Формирование запроса на сертификат
  - Нажмите ссылку «Новый сертификат». Рабочее окно АРМ пользователя примет, следующий вид (см. Рисунок 19);

Рисунок 19. Окно формирования запроса на новый сертификат

	Удостоверяющий Центр Крипто-Про 🖻
Запрос на сертифи	кат зарегистрированного пользователя
Общее имя : Иван Организация : ООС Город : Мос Страна/регион : RU Электронная почта: alexi	нов Иван Иванович ) 'Пупкин и сыновья' «ва @cp.ru
Пожалуйста, выберите ш	аблон запроса на новый сертификат.
Шаблон сертификата:	Временный сертификат пользователя УЦ 🔹
информация	Плановая смена ключа
<	ить >>

- В списке доступных шаблонов сертификатов выберите требуемый шаблон, определенный регламентом работы пользователя с УЦ;
- В поле дополнительной информации можете ввести небольшой комментарий, который увидит администратор Центра Регистрации;
- Нажмите кнопку Отправить для продолжения формирования запроса на сертификат. Нажмите кнопку Назад для отказа от режима формирования запроса на сертификат и возврата в главное окно АРМ пользователя.

Примечание. Шаблоны сертификатов настраиваются и формируются администратором ЦР в соответствии регламентирующими документами организации – УЦ. Пользователю необходимо выбрать нужный шаблон из представленного списка.

- После нажатия кнопки Отправить система перейдет к процедуре формирования новых ключей;
- Выберите необходимый тип ключевого носителя из списка подключенных в СКЗИ КриптоПро CSP (см. Рисунок 20);

# Рисунок 20. Окно выбора ключевого носителя для генерации ключей

🛅 КриптоПро (	CSP	<u>?</u> ×
Ber 7d3f	гавьте чистый ключевой носитель 557b-de9c-4016-8406-fd0d92e761bd.	
Устройства:	Вставленный носитель:	
	ОК Отмена Сведения <<	]

 проинициализируйте генератор случайных чисел (путем нажатия клавиш на клавиатуре или движением указателя мышки в окне инициализации) (см. Рисунок 21);

#### Рисунок 21. Окно инициализации датчика случайных чисел

Биологический датчик случайных 🗴
Нажимайте клавиши или двигайте мышью
Нет
Отказ

 при необходимости установите пароль (ПИН-код) на создаваемый ключевой контейнер (см. Рисунок 22);

Рисунок 22. Окно задания пароля на создаваемый ключевой контейнер

🧧 КриптоПро CSP		<u>? ×</u>
Чстановите ГЕЕ	пароль на создаває носитель	эмый
💿 Установить новый пар	оль	
Новый пароль:		
Подтверждение:		
🔲 Запомнить па	ароль	
OK	Отмена	Подробнее >>

- В результате успешного выполнения вышеперечисленных действий сформированный запрос будет отправлен в ЦР на рассмотрение, а в таблице запросов на сертификат появится новая строка со статусом запроса Обработка;
- После успешного принятия данного запроса уполномоченным лицом в ЦР, статус запроса изменится и появится возможность установить новый сертификат в хранилище сертификатов на локальном компьютере.

# 4.2.5. Установка сертификата

О завершении обработки запроса на сертификат и наличии возможности установить выпущенный сертификат, свидетельствует установление статуса запроса на сертификат в состояние **Установить** (см. Рисунок 23). Продолжительность обработки запроса зависит от регламента работы Центра Регистрации.

# Рисунок 23. Окно АРМ пользователя со статусом Установить запроса на сертификат

				Удостоверяюи	ций Центр І	(рипто-Про 🛌
Новый сертификат	Сертификат центра	Список отоз	ванных	<		
Персональная стран Общее имя : Иван Организация : ООС	ница зарегистрирова 108 Иван Иванович ) 'Пупкин и сыновья'	анного пользо	вателя	:		
Город : Моси	ква					
Электронная почта alexi	@ເກ.ເມ					
	@ <b>t</b> pitu					
Сертификаты:						
Серийный номер	Дата выпуска	Дата окончания		Статус сертификата	Просмотр	Отзыв
1133C166000000000A	F 2002-11-10 15:52:00	2002-11-17 16:01:00		Действителен	Показать	Отозвать
114D584D000000000	30 2002-11-10 16:20:00	2002-11-17 16:29:00		Действителен	Показать	Отозвать
Запросы на сертификаты:						
Дата запроса	Дата рассмотрения	Комментарий	Стат	тус		
2002-11-10 15:59:00 2002-11-10 16:04:00 Завершен						
2002-11-10 16:28:00 2002-11-10 16:29:00 Установить						
Запросы на отзыв:						
Отсутствуют						
						×

В случае установления статуса запроса на сертификат в состояние возможности установления сертификата в хранилище сертификатов рабочего места пользователя, выполните следующие действия:

 Нажмите ссылку Установить в соответствующей строке таблицы запросов на сертификат. При этом рабочая область АРМ пользователя примет следующий вид (см. Рисунок 24):

# Рисунок 24. Окно установки запрошенного сертификата

	Удостоверяющий Центр Крипто-Про
Установка сертификата	
	Вы получили запрошенный <u>сертификат.</u> Нажмите кнопку "Установить сертификат" чтобы установить его для дальнейшего использования. Установить сертификат Вы должны подтвердить получение и установку этого сертификата. Для этого нажмите кнопку "Подтвердить установку". В противном случае, этот сертификат будет отозван. Подтвердить установку

- В появившейся форме убедитесь в соответствии полученного сертификата отправленному запросу. Для этого нажмите на ссылку сертификат данного окна. В случае несоответствия данных обратитесь к Администратору;
- Для продолжения установки сертификата нажмите кнопку Установить сертификат;

# Рисунок 25. Информационное окно об успешной установке сертификата

VBScript:	Удостоверяющий Центр Крипто-Про	X
٩	Сертификат успешно установлен!	
	OK	

- Появление сообщения (см. Рисунок 25) свидетельствует об успешной установке данного сертификата в хранилище сертификатов;
- Для подтверждения факта установки и сообщения об этом на ЦР нажмите кнопку **Подтвердить установку**. В случае не подтверждения установки сертификат будет занесен в список отозванных сертификатов;
- После подтверждения установки запрошенного сертификата, пользователю будет отображено соответствующее окно (см. Рисунок 26), из которого он может вернуться в основное окно АРМ пользователя.

· ····································
Удостоверяющий Центр Крипто-Про 📥
становка сертификата подтверждена
ажмите <u>сюда </u> чтобы вернуться на главную страницу.
пасибо за использование нашего сервиса.
становка сертификата подтверждена ажмите <u>сюда</u> чтобы вернуться на главную страницу. пасибо за использование нашего сервиса.

# 4.2.6. Печать сертификата

Формирование печатной формы и вывод ее на бумажный носитель выполняется пользователем в порядке и в сроки, определенные регламентирующими документами УЦ.

Для печати сертификата необходимо в окне АРМ пользователя в соответствующей строке таблицы сертификатов нажать ссылку **Показать**. В результате в новом окне браузера MS IE (см. Рисунок 27) будет сформирована печатная форма сертификата пользователя.

# Рисунок 27. Окно с бланком сертификата



Для вывода бланка сертификата на печать откройте данное окно, установите указатель мыши в произвольном месте окна на тексте бланка и нажмите правую кнопку мыши. В появившемся меню (см. Рисунок 28) выберите пункт «Печать» (Print).

#### Рисунок 28. Окно меню с пунктом печати сертификата

Назад
Сохранить фон как
Сделать фоновым рисунком
Копировать фон
Сохранить как элемент рабочего стола
Выделить все
Создать ярлык Побарить в избранное
Просмотр НТМL-кода
Кодировка 🕨
Печать
Обновить
Экспорт в Microsoft Excel
Свойства

# 4.2.7. Приостановление действия сертификата

Приостановление действия сертификата, т.е. помещение его в список отозванных сертификатов на определенный срок, выполняется Центром Сертификации на основании запроса на приостановление действия сертификата, полученного от пользователя, с подтверждением данного запроса на Центре Регистрации.

Данный запрос формируется пользователем с использованием APM пользователя и посылается на Центр Регистрации в электронном виде.

Приостановленным может быть любой сертификат пользователя.

Для создания запроса на приостановление действия сертификата необходимо выполнить следующие действия:

 В таблице сертификатов нажать ссылку Приостановить соответствующей строки. Рабочая область АРМ пользователя примет следующий вид (см. Рисунок 29):

# Рисунок 29. Окно формирования запроса на приостановление действия сертификата

📲 Страница зарегистрированного пользователя - Microsoft Internet Explorer 📃 📃 🗙
Файл Правка Вид Избранное Серенс Справка
⇔Hasag • ⇒ • © 2 Δ QROUCK @Us6pannoe @Megna ③ 🖓 • 🔄 🖉 • 🗐 👷
Адрес; 🎒 https://lord2k.cp.ru/ui/User/UserMakeRevokeReq.asp7ID=22&Type=1 💌 🖉 Српреход Ссылки »
Удостоверяющий Центр Крипто-Про 🧧
Запрос на приостановление действия сертификата зарегистрированного пользователя
Пожалуйста, укажите срок, на который небходимо приостановить действие сертификата. Запрос может быть сопровожден комментарием для администратора.
лет месяцев недель дней часов минут
на срок:
комментарий:
«Назад Отправить»
🔮 Готово 🛛 🔒 🔮 Интернет 🥢

В данном окне задайте срок, на который требуется приостановить сертификат и нажмите кнопку **Отправить**.

Запрос на приостановление действия сертификата поступает на Центр Регистрации в форме запроса на отзыв и становится в очередь на обработку администратором Центра Регистрации.

В период обработки запрос на приостановление действия сертификата находится в окне АРМа в списке запросов на отзыв в состоянии **Обработка** (см. Рисунок 30).

Статус отзыва сертификата в списке сертификатов, отображаемых на APMe, находится в состоянии **Обработка** (см. Рисунок 30).

# Рисунок 30. Окно отображения состояния обработки запроса на приостановление действия сертификата

🎒 Страница зарегестирован	ного пользователя - Міс	rosoft Internet Explorer					- 🗆 ×
Файл Правка Вид Избра	нное С <u>е</u> рвис <u>С</u> правка						1
(⇔ Назад 🔹 ⇒ 🚽 🙆 🔗 🦿	🐴 🛛 🔞 Поиск 🛛 🟹 Избранн	ре 🕼 Медиа 🖽 🗔 -	<b>∌</b> ≓ • <b>■ 9</b>				
Annec: Annec: Annec: Annec:	ill kerll ker act					▼ ∂⊓enexo	и. Ссылки »
napori incipationalicipitate	arosci rosci rasp			Vacom	ocontiou		
Новый сертификат — С	ептификат центра	Список отозванных		900cm	оверяюа	цаа центр крат	no-npo 🖻
Персональная стра	аница зарегистрир	ованного пользо	вателя:				
Общее имя : Те	est User 7						
Электронная почта: т	aslov@cryptopro.ru						
Committeener							
Сертификаты.		<b>R</b>	Concerns and an and	Deserver	0		
серииный номер		Дата окончания	статус сертификата	просмотр	UT3DIB	Приостановление	
1918/CD80000000001E	2003-08-22 13:39:00	2003-08-29 13:49:00	деиствителен	і юказать —	Отозвать	і іриостановить 1	
61BB76690000000001F	2003-08-22 13:43:00	2004-11-22 13:53:00	Запрошен к отзыву	Показать	Обработка		
Запросы на сертифика	ты:						
Дата запроса	Дата рассмотрения К	омментарий Статус	Просмотр				
2003-08-22 13:48:00	2003-08-22 13:48:00	Заверше	н Показать				
2003-08-22 13:52:00	2003-08-22 13:53:00	Заверше	н Показать				
Запросы на отзыв							
Номер сертификата	Дата запроса	Дата отзыва Прич	ина Статус запроса	1			
61BB76690000000001F	2003-08-22 13:59:00	Не ука	зана Обработка	i			
				4		-	~
😂 Готово						🤣 Интернет	1.

По окончании обработки, запрос на приостановление действия сертификата переходит в состояние **Завершен** (см. Рисунок 31).

Статус сертификата в списке сертификатов, отображаемых на APMe, переходит в состояние **Отозван** (см. Рисунок 31).

# Рисунок 31. Окно отображения завершение обработки запроса на приостановление действия сертификата

🎒 Страница зарегестирован	ного пользователя - Міс	rosoft Internet	Explorer						
<u>Ф</u> айл Правка <u>В</u> ид <u>И</u> збран	нное С <u>е</u> рвис <u>С</u> правка								100 A
🕁 Назад 🔹 🔿 🖉 🙆	🖞 🔯 Поиск 🚡 Избранн	ое (Эрмедиа	3 B-	4 I - E	Q				
Адрес: 🙆 https://lord2k.cp.ru/u	ii/User/User.asp								реход Ссылки »
						Удост	поверяю	иий Центр Кр	ипто-Про 🖻
Новый сертификат Со	ертификат центра	Список отозі	ванных						
Персональная стра	аница зарегистрир	ованного	пользов	ателя:					
Общее имя : 1е	est User 7								
Электронная почта. па	asiov@cryptopro.ru								
Сертификаты:									
Серийный номер	Дата выпуска	Дата окон	чания	Статус серти	фиката	Просмотр	Отзыв	Приостановлени	e
61B7CDB60000000001E	2003-08-22 13:39:00	2003-08-29 1	3:49:00	Действителен	H	Показать	Отозвать	Приостановить	
61BB76690000000001F	2003-08-22 13:43:00	2004-11-22 1	.3:53:00	Отозван		Показать	Отозвать	Возобновить	
Запросы на сертифика	Запросы на сертификаты:							_	
Дата запроса	Дата рассмотрения 🛛 К	(омментарий	Статус	Просмотр	]				
2003-08-22 13:48:00	2003-08-22 13:48:00		Завершен	і Показать					
2003-08-22 13:52:00	2003-08-22 13:53:00		Завершен	Показать					
Запросы на отзыв:					-				
Номер сертификата	Дата запроса	Дата от	зыва	Причина	Статус з	апроса			
61BB76690000000001F	2003-08-22 13:59:00	2003-08-22	14:00:00	Не указана	Удовлета	ворен			-
é								🥶 Интернет	

# 4.2.8. Возобновление действия сертификата

Возобновление действия сертификата, т.е. удаление его из списка отозванных сертификатов, выполняется Центром Сертификации на основании запроса на возобновление действия сертификата, полученного от пользователя, с подтверждением данного запроса на Центре Регистрации.

Данный запрос формируется пользователем с использованием APM пользователя и посылается на Центр Регистрации в электронном виде.

Возобновить действие можно только для сертификата, ранее приостановленного по запросу.

Для создания запроса на возобновление действия сертификата необходимо нажать ссылку **Возобновить** соответствующей строки (см. Рисунок 31).

# 4.2.9. Отзыв сертификата

Отзыв сертификата, т.е. помещение его в список отозванных сертификатов, выполняется Центром Сертификации на основании запроса на отзыв сертификата, полученного от пользователя, с подтверждением данного запроса на Центре Регистрации.

Данный запрос формируется пользователем с использованием APM пользователя и посылается на Центр Регистрации в электронном виде.

Отозванным может быть любой сертификат пользователя, за исключением того, на котором выполнена аутентификация пользователя в текущем окне АРМ. Для отзыва данного сертификата необходимо установить соединение с Центром Регистрации на другом действующем сертификате. В случае если у пользователя имеется только один действующий сертификат, необходимо сформировать запрос на новый сертификат, получить и установить его. После этого закрыть окно АРМ и установить новое соединение с Центром Регистрации, используя новый полученный сертификат. После этого старый сертификат доступен для отзыва.

Для создания запроса на отзыв сертификата необходимо выполнить следующие действия:

• В таблице сертификатов нажать ссылку **Отозвать** соответствующей строки. Рабочая область АРМ пользователя примет следующий вид (см. Рисунок 32);

Рисунок 32. Окно формирования запроса на отзыв сертификата

Удостоверяющий Центр Крипто-Про 💆
Запрос на отзыв сертификата зарегистрированного пользователя
Пожалуйста, выберите причину отзыва сертификата. Запрос на отзыв может быть сопровожден комментарием для администратора.
причина отзыва: Не указана
<

 В появившейся форме укажите причину отзыва сертификата и, при необходимости, комментарии для Администратора. Причину отзыва можно выбрать из предложенного списка;

Не указана
Компрометация ключа
Компрометация ЦС
Изменение принадлежности
Сертификат заменен
Прекращение работы

 Нажмите кнопку Отправить для отправки запроса на отзыв в Центр Регистрации или кнопку Назад для отмены данного режима работы и возврата в основное окно АРМ пользователя.

В результате выполнения этих действий будет сформирован запрос на отзыв сертификата. В основном окне АРМ пользователя в таблице запросов на отзыв сертификатов появится соответствующая строка со статусом **Обработка**. В таблице сертификатов отзываемый сертификат примет статус **Запрошен к отзыву** (см. Рисунок 33).

# Рисунок 33. Окно АРМ пользователя со статусом сертификата "Запрошен к отзыву"

Норый сертификат	Cor		1			Удог	стовеј	эяющий Цен	нтр Крипто-	Про 🔺
повый сертификат	Cet	лификатцентра		CHRICOK OTOSBE		<b>N</b>				
Персональная стран	ница	а зарегистрирова	нн	юго пользова	теля	:				
Общее имя : <b>Иван</b> Организация : ОООО Город : Моск Страна/регион : RU Электронная почта; <b>alex</b> (	юв И 'Пу сва @ср.	Іван Иванович пкин и сыновья' ru								
Сертификаты:									]	
Серийный номер		Дата выпуска		Дата окончан	ния	Статус сертиф	иката	Просмотр	Отзыв	
1133C166000000000A	F	2002-11-10 15:52:00	52:00 2002-11-17 16:01:00 Действителен			Показать	Отозвать			
114D584D000000000E	30	2002-11-10 16:20:00	0 2002-11-17 16:29:00 Запрошен к отзыву Показат			Показать	Обработка			
Запросы на сертификаты:										
Дата запроса	Дa	та рассмотрения	Ко	мментарий	Стату	/c				
2002-11-10 15:59:00	200	02-11-10 16:04:00		3	аверц	јен				
2002-11-10 16:28:00	200	02-11-10 16:31:00		3	аверц	јен				
Запросы на отзыв:										
Номер сертификат	а	Дата запроса		Дата отзыва		Причина	Стату	ус запроса		
114D584D0000000000	BO	2002-11-10 16:35:0	0		Прен	фащение работы	Обраб	отка		
										1

Продолжительность обработки запроса на отзыв сертификата зависит от регламента работы Центра Регистрации. После подтверждения уполномоченным лицом ЦР запроса на отзыв его состояние изменится на **Удовлетворен**, а состояние соответствующего сертификата изменится на **Отозван** (см. Рисунок 34).

овый сертификат 📗	Сертификат центра	Список отозванны	Удостов к	еряющий Центр Крипто
Персональная стран	ица зарегистрирован	ного пользовател	я:	
Общее имя : Иван Эрганизация : ООО Город : Моск Страна/регион : RU Электронная почта; alex1@	ов Иван Иванович 'Пупкин и сыновья' ва Эср.ru			
Сертификаты:				
Серийный номер	Дата выпуска	Дата окончания	Статус сертификата	а Просмотр Отзыв
1133C166000000000AF	2002-11-10 15:52:00	2002-11-17 16:01:00	Действителен	Показать Отозвать
114D584D0000000000B	0 2002-11-10 16:20:00	2002-11-17 16:29:00	Отозван	Показать
Запросы на сертификаты:				
Дата запроса	Дата рассмотрения К	(омментарий Стат	ус	
2002-11-10 15:59:00	2002-11-10 16:04:00	Завер	шен	
2002-11-10 16:28:00	2002-11-10 16:31:00	Завер	шен	
2				
запросы на отзыв.		Лата отзыва	Причина	Статус запроса
Номер сертификат	а 🔰 Дата запроса	Adragiopipa		

В том случае, если запрос на отзыв будет отклонен, состояние запроса изменится на **Отклонен**.

4.2.10. Поиск и импорт сертификатов других зарегистрированных пользователей Центра Регистрации

Политикой Центра Регистрации Удостоверяющего Центра может быть разрешен доступ владельцев сертификатов к общему реестру сертификатов. Обычно это необходимо в тех случаях, когда пользователи – участники информационной системы – общаются между собой с использованием средств криптографической защиты и электронной подписи. При этом используются ключи и сертификаты, выданные в Удостоверяющем Центре.

Для подобного общения (переписка с использованием E-Mail, обмен зашифрованными и подписанными ЭП файлами, электронная подпись содержимого Web страниц) абонентам необходимо иметь у себя сертификаты других пользователей информационной системы. Данный режим Центра Регистрации позволяет зарегистрированным пользователям осуществлять удаленный поиск требуемых сертификатов в Реестре Центра Регистрации, импортировать найденные сертификаты себе на локальный компьютер в виде файлов или в специально предназначенное для этого в операционной системе Windows хранилище. В дальнейшем это позволит осуществлять проверку электронной подписи других абонентов информационной системы и шифрование информации в их адрес.

Если политикой Центра Регистрации данный режим разрешен, то основной экран интерфейса зарегистрированного пользователя будет выглядеть следующим образом (см. Рисунок 35).

			Удостоверяющи	ій Центр К	рипто-Про 🛌
новый сертификат	Сертификат центра	Список отозванных	К Поиск сертифик	атов	
Персональная стран	ица зарегистрирован	ного пользователя	:		
Общее имя : Иван Организация : ООО Город : Моск Страна/регион : RU Электронная почта: ivan@	ов Иван Иванович 'Пупкин и сыновья' ва ср.гц				
Серийный номер	Лата выпуска	Лата окончания	Статус сертификата	Просмотр	Отзыв
2254AFA000000000119	9 2002-12-26 12:33:00	2003-01-02 12:42:00	Действителен	Показать	Отозвать
Запросы на сертификаты:					
Дата запроса	Дата рассмотрения К	омментарий Статус	:		
2002-12-26 12:42:00	2002-12-26 12:42:00	Заверше	ен		
Запросы на отзыв:					

В верхней части экрана в строке меню появился новый пункт Поиск сертификатов.

Кликнув на нем указателем мыши, Вы выйдете на экран формирования запроса на поиск сертификатов (см. Рисунок 36).

4.2.11. Формирование запроса на поиск сертификатов

# Рисунок 36. Окно определения параметров поиска сертификатов

	Удостоверяющий Центр Крипто-Про
Поиск сертификатов	в Реестре
Пожалуйста, выберите пара необходимый сертификат, в укажите условия сортировкі сертификатов.	метр по которому Вы собираетесь искать ведите искомое значение, если необходимо и и параметры вывода списка отобранных
Параметр сертификата:	(Не задан) Начинается на
Значение параметра:	
Искать среди:	Всех сертификатов
Сортировать по:	Серийный номер сертификата • • по возрастанию • по убъванию
выводить по:	20 строк на странице П показывать все атрибуты имени владельца
	Найти >> Домой

Данный экран имеет три основные секции для ввода информации.

В первой секции указываются условия, по которым следует отобрать сертификаты из реестра.

Во второй секции указываются условия сортировки отобранных в результате поиска сертификатов.

В третьей – параметры отображения списка найденных сертификатов.

Поиск сертификатов в данной версии может осуществляться только по одному выбранному условию, не считая статуса сертификатов, среди которых искать (среди всех, действующих, отозванных, просроченных...).

Необходимо отметить, что если **не выбирать** параметр сертификата, по которому осуществлять поиск, то в результате будут отобраны все сертификаты из базы данных Центра Регистрации.

Для ввода условия запроса выберите из раскрывающегося списка с комментарием «Параметр сертификата» требуемый параметр.

(Не задан)
Серийный номер сертификата
Общее имя
Подразделение
Организация
Город
Область
Страна/регион
Электронная почта
Дата начала действия
Дата окончания действия

Состав параметров в каждом конкретном Центре Регистрации может варьироваться, в зависимости от «Политики Имен» Центра Регистрации, присутствующих в сертификатах. Всегда присутствуют следующие параметры: «Серийный номер сертификата», «Дата начала действия» сертификата, «Дата окончания действия» сертификата, остальные параметры формируются динамически, в зависимости от указанной политики Центра Регистрации.

После выбора параметра, по которому искать, введите в поле «Значение параметра» значение, которое искать.

Далее укажите «точность» поиска. Для этого выберите из списка условие, – каким образом осуществлять поиск введенного значения: «Начинается на ...» или «содержит...». Условие «Начинается на» означает, что будут отобраны все сертификаты, у которых указанный Вами параметр начинается на значение, введенное Вами в поле «Значение параметра». Условие «Содержит» означает, что будут отобраны все сертификаты, у которых в любом месте указанного Вами параметра содержится введенная Вами в поле «Значение параметра» подстрока.

Дополнительно, Вы можете указать подмножество сертификатов, среди которых осуществлять поиск, выраженное статусом сертификатов «Искать среди:»

Зсех сертификатов
Действующих
Отозванных
Тросроченных
Спросроченным ключом

Выберите из списка нужное подмножество. По умолчанию, поиск осуществляется среди всего множества сертификатов, находящихся в реестре Центра Регистрации.

После ввода условий поиска, Вы можете указать условия сортировки отобранного списка сертификатов. Для этого в секции сортировки выберите из списка с комментарием «Сортировать по» параметр сертификата, по которому сортировать результирующий набор:

Серийный номер сертификата Общее имя Подразделение Организация Город Область Страна/регион Электронная почта Дата начала действия Дата окончания действия

Можно указать направление сортировки – по возрастанию или по убыванию значений, выбранного параметра сертификата. Для этого установите «переключатель»:

💿 по возрастанию

<sup>О по убыванию</sup> в нужное положение.

В секции параметров отображения найденного списка можно указать количество отображаемых сертификатов результирующего списка на одной странице. Ввиду того, что списки могут быть довольно большими, разумно разбивать их на отдельные страницы (чтобы не ждать загрузки всего списка). Особенно актуально это при работе в Интернет с медленными каналами связи.

В поле «выводить по:» <u>XXX</u> «строк на странице» Вы можете указать значение от 1 до 999. Каждая страница будет содержать не более указанного количества сертификатов. Естественно, если в результате поиска будет отобрано меньше сертификатов, чем указано в данном параметре, или если на последней странице содержится не кратное данному числу количество сертификатов, то страница будет содержать меньше указанного числа строк сертификатов.

По умолчанию список сертификатов будет выдаваться в виде таблицы с ограниченным числом колонок: «Серийный номер сертификата», «Имя владельца», «Дата выпуска» сертификата, «Дата окончания» действия сертификата, «Статус» сертификата. Но вы можете указать, чтобы результирующий список содержал расширенный набор колонок, куда вошли бы все параметры Имени владельца сертификата (Адрес, Организация, Должность, город, Адрес электронной почты и др.). Состав таких параметров устанавливается «Политикой Имен» конкретного Центра Регистрации.

Для получения развернутого списка поставьте «галку» на элементе

🔲 показывать все атрибуты имени владельца

Введя все необходимые условия, нажмите кнопку «Найти >>» для запуска механизма поиска и получения списка найденных сертификатов.

Нажатие на кнопку «Домой» вернет Вас на домашнюю страницу зарегистрированного пользователя.

4.2.12. Работа со списком отобранных сертификатов

Если в результат поиска не дал положительного результата на экран будет выведено следующее сообщение (см. Рисунок 37).

# Рисунок 37. Окно сообщения об отсутствии сертификатов, удовлетворяющих условиям поиска

	Удостоверяющий Центр Крипто-Про	*
Список найденных сертификато	DB	
Сертификатов по указанным условиям не	: найдено.	
<< >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	Сохранить Новый поиск Домой	
		<b>T</b>

Если же будет найден хоть один сертификат, удовлетворяющий заданным условиям, будет отображена страница со списком найденных сертификатов (см. Рисунок 38);

# Рисунок 38. Окно сообщения со списком сертификатов, удовлетворяющих условиям поиска

				Удостоверяющи	й Центр Кр	ипто-Про 📥
Спі	исок найденных серти	фикатов				
	Серийный номер	Имя владельца	Дата выпуска	Дата окончания	Статус	Просмотр
	221A28D600000000118	Сидоров Сидор Сидорович	26.12.2002 11:29:00	02.01.2003 11:38:00	Действует	Показать
	2254AFA0000000000119	Иванов Иван Иванович	26.12.2002 12:33:00	02.01.2003 12:42:00	Действует	Показать
<< >>> Сохранить Новый поиск До					Домой	

В развернутом виде (если указано – показывать все атрибуты имени владельца) окно будет выглядеть следующим образом (см. Рисунок 39);

# Рисунок 39. Окно сообщения со списком сертификатов, удовлетворяющих условиям поиска, и полным перечнем атрибутов имени владельцев

					Удостоверян	ощий Цеі	нтр Крипг	по-Про	-
0	Спис	сок найденных сертис	фикатов						
ſ					1				
		Серийный номер	Общее имя	Подразделение	Организация	Город	Область	Страна	
		221A28D600000000118	Сидоров Сидор Сидорович	Отдел программирования	Крипто Про	Москва		RU	
		2254AFA0000000000119	Иванов Иван Иванович		ООО 'Пупкин и сыновья'	Москва		RU	
-				<<	>> Сохранить	Новый по:	иск Да	рмой	
_					,				-
•				<<	>> Сохранить	Новый пои	иск Да		мой

Примечание. На рисунке показана только левая часть списка. Воспользовавшись прокруткой можно увидеть все остальные колонки списка.

В общем случае, типовой экран со списком найденных сертификатов включает две секции:

- 1. собственно, список сертификатов;
- 2. панель кнопок с режимами работы.

На предыдущих рисунках видно, что в зависимости от указанных параметров отображения, список может содержать типовой и расширенный набор колонок.

В самой левой колонке любого списка находится колонка, позволяющая отметить требуемые сертификаты для исполнения с ними некоторых групповых операций. Элемент управления, находящийся в этой колонке в заголовке таблицы, позволяет отметить/разметить сразу все расположенные в списке сертификаты.

В самой правой колонке списка - «Просмотр» - для каждой строки содержится ссылка, по клику на которой можно просмотреть отдельный сертификат, импортировать его в локальное хранилище сертификатов для дальнейшего использования или сохранить в файле на диске.

Кнопки позволяют осуществлять следующие режимы работы:

- перейти к предыдущей странице списка (просмотреть предыдущие NNN отобранных сертификатов, где NNN – указанное Вами количество строк на странице). При этом если Вы просматриваете первую страницу, данная кнопка будет недоступна.

- перейти к следующей странице списка (просмотреть следующие NNN отобранных сертификатов, где NNN – указанное Вами количество строк на странице). При этом если Вы просматриваете последнюю (или единственную) страницу, данная кнопка будет недоступна.

Сохранить - сохранить отмеченные в списке сертификаты на своем компьютере в виде файла специального формата PKCS#7, либо импортировать их в специальное хранилище сертификатов операционной системы Windows для дальнейших криптографических операций. При этом если в списке не отмечен ни один сертификат, то данная кнопка будет недоступна.

Новый поиск - вернуться на страницу формирования условий запроса.

Домой - вернуться на домашнюю страницу зарегистрированного

пользователя.

4.2.13. Сохранение сертификатов других пользователей на локальном компьютере

Для общения между собой пользователей – участников информационной системы электронного документооборота - с использованием средств криптографической защиты и электронной подписи (переписка с использованием E-Mail, обмен зашифрованными и подписанными ЭП файлами, подпись содержимого Web страниц) необходимо, чтобы у каждого такого пользователя на локальном компьютере имелись открытые ключи других пользователей. Данные ключи в системах с открытым распределением ключей оформляются в виде сертификатов широко распространенного открытого стандарта X509. Версии операционной системы Windows имеют встроенную поддержку, обеспечивающую полноценную работу с данными сертификатами.

Web интерфейс зарегистрированного пользователя Центра Регистрации позволяет осуществлять удаленный поиск требуемых сертификатов в Реестре Центра Регистрации, импортировать найденные сертификаты себе на локальный компьютер в виде файлов или в специально предназначенное для этого в операционной системе Windows хранилище.

4.2.13.1. Сохранение группы сертификатов

Для импорта сертификатов воспользуйтесь режимом поиска, описанным в предыдущих главах. Получив список требуемых сертификатов, отметьте в нем (см. Рисунок 40) строки таблицы с сертификатами, которые Вы хотели бы иметь у себя на компьютере (для проверки ЭП пользователей-владельцев данных сертификатов или для шифрования сообщений в их адрес).

# Рисунок 40. Окно с отмеченными сертификатами для сохранения в списке найденных

					Удостоверяющий	Центр Кр	лто-Про 占
	Спи	сок найденных сертис	фикатов				
		Серийный номер	Имя владельца	Дата выпуска	Дата окончания	Статус	Просмотр
	◄	221A28D600000000118	Сидоров Сидор Сидорович	26.12.2002 11:29:00	02.01.2003 11:38:00	Действует	Показать
	◄	2254AFA0000000000119	Иванов Иван Иванович	26.12.2002 12:33:00	02.01.2003 12:42:00	Действует	Показать
4						Домой	

Если хоть одна строка списка помечена, то кнопка Сохранить станет доступна.

Нажмите кнопку **Сохранить**. При этом стандартный режим браузера MS IE предложит либо сохранить полученную от сервера информацию в файле на диске, либо открыть сообщение при помощи встроенных в операционную систему программ (см. Рисунок 41).

Рисунок 41. Окно загрузки файла с выбранными сертфиикатами

Загруз	зка файла 🛛 🕺 🗙	J
?	Выполняется загрузка следующего файла: UserSaveCertList.p7b c alexI.cp.ru	
	Открыть этот файл или сохранить его на компьютере? Открыть Сохранить Отмена Подробнее Всегда задавать этот вопрос, открывая такие файлы	

Если Вы не собираетесь сразу импортировать сертификаты в специальное хранилище OC Windows, нажмите кнопку **Сохранить** («Save»). В этом случае Вам будет предложено выбрать место в файловой директории, куда следует сохранить полученный файл.

Если вы собираетесь сразу импортировать сертификаты (или в Windows 2000 просмотреть список сертификатов, содержащихся в файле) нажмите кнопку **Открыть** («Open»).

Необходимо отметить, что при нажатии кнопки **Открыть**, разные версии операционной системы ведут себя по разному. Windows 98 при этом сразу запускает мастер импорта сертификатов, содержащихся в файле, а Windows 2000 открывает данный файл для просмотра в следующем виде (см. Рисунок 42);

# **Рисунок** 42. Окно просмотра загруженных сертификатов в MS Windows 2000

📟 Сертификаты							
] <u>Д</u> ействие <u>В</u> ид  ] 🗢 ⇒	] Действие Вид 🛛 🗢 🔿 🔁 📧 📝 🔂 😰						
Структура	Кому выдан 🔺	Кем выдан	Срок дейст				
Сертификаты - файл - С\DOCUME~1\ALEXL\LO - С\DOCUME~1\ALEXL\LO - Сертификаты	🖼 Иванов Иван Иванович 🖼 Лиманцев Алексей Конст	Test Root CA on SP2 Test Root CA on SP2	02.01.2003 02.01.2003				
•	•		Þ				
Хранилище C:\DOCUME~1\ALEXL	ранилище C:\DOCUME~1\ALEXL\LOCALS~1\TEMPOR~1\CONTENT.IE5\D						

Используя данное окно, можно просмотреть каждый сертификат, содержащийся в полученном файле (кликнув на нем дважды мышкой) и в стандартном окне просмотра сертификата выбрать кнопку **Установить сертификат** («Import certificate»), для импорта сертификата в хранилище (см. Рисунок 43).

Сертификат	? ×
Общие Состав Путь сертификации	1
Сведения о сертификате	
Этот сертификат: • Подтверждает удаленному компьютеру идентификацию вашего компьютера • Временный доступ к Центру Регистрации • Пользователь Центра Регистрации	
Кому выдан: Иванов Иван Иванович	
Кем выдан: Test Root CA on SP2	
Действителен с 26.12.2002 по 02.01.2003	
Установить сертификат Заявление поставщик	a
0	К

Рисунок 43. Окно свойств найденного сертификата

Для импорта сразу всех сертификатов в ОС Windows 2000 лучше сначала сохранить полученный файл на диске, а потом, кликнув на нем правой кнопкой мыши, из раскрывшегося меню выбрать пункт **Установить сертификат** (см. Рисунок 44).

# **Рисунок** 44. Окно меню для установки нескольких сертификатов в MS Windows 2000

Открыть
Установить сертификат
💥 Проверить DrWeb
Scan for Viruses
Открыть с помощью
🗐 Add to Zip
🗐 Add to UserViewFoundCert.zip
🗐 Zip and E-Mail UserViewFoundCert.zip
Отправить 🔸
Вырезать
Копировать
Создать ярлык
Удалить
Переименовать
Свойства

При этом запустится мастер установки (импорта) сертификатов в хранилище сертификатов пользователей. В ОС Windows 98 такой мастер запускается сразу, если Вы выберете режим «Открыть» при загрузке файла с выбранными сертификатами (см. Рисунок 3).

Далее следуйте указаниям Мастера импорта сертификатов, выбирая предлагаемые значения по умолчанию.

Примечание. Политикой безопасности Центра Регистрации может быть запрещен режим импорта чужих сертификатов. При этом загруженный с Центра Регистрации файл будет содержать только сертификаты, которые разрешены Вам для импорта политикой безопасности.

#### 4.2.13.2. Сохранение отдельного сертификата

Для импорта отдельного сертификата на странице со списком отобранных в результате поиска сертификатов в правой колонке списка кликните мышкой на ссылке **Показать** в соответствующей строке списка (см. Рисунок 45);

Рисунок 45. Окно со списком найденных сертификатов для использования
ссылки Показать

				Удостоверяющи	ій Центр К <sub>і</sub>	рипто-Про	*
Спи	сок найденных сертис	фикатов					
	Серийный номер	Имя владельца	Дата выпуска	Дата окончания	Статус	Просмотр	
	221A28D600000000118	Сидоров Сидор Сидорович	26.12.2002 11:29:00	02.01.2003 11:38:00	Действует	Показать	
	2254AFA0000000000119	Иванов Иван Иванович	26.12.2002 12:33:00	02.01.2003 12:42:00	Действует	Показать	
		<	< >>>	Сохранить Нов	ый поиск	Домой	~
• [						•	

При этом стандартный режим браузера MS IE предложит вам либо сохранить сертификат (файл с расширением .cer) в файле на диске, либо открыть его при помощи встроенного в операционную систему режима просмотра сертификатов (см. Рисунок 46).

Загру:	зка файла	×
?	Выполняется загрузка следующего файла: UserViewFoundCert.cer с alexI.cp.ru	
	Открыть этот файл или сохранить его на компьютере?	
	Открыть Сохранить Отмена Подробнее	•
	🕅 Всегда задавать этот вопрос, открывая такие файлы	

Если Вы не собираетесь просматривать или сразу импортировать полученные сертификаты в специальное хранилище ОС Windows нажмите кнопку **Сохранить** («Save»). В этом случае Вам будет предложено выбрать место в файловой директории, куда следует сохранить полученный сертификат.

Рисунок 46. Окно загрузки файла с выбранным сертификатом

Если же вы выберете режим **Открыть** («Open»), то загруженный с сервера сертификат будет отображен в стандартном окне просмотра сертификатов (см. Рисунок 43).

Для импорта сертификата в специальное хранилище операционной системы в данном окне нажмите кнопку «Установить сертификат». При этом будет запущен Мастер импорта сертификатов, описанный в предыдущей главе.

Примечание. Политикой безопасности Центра Регистрации может быть запрещен режим импорта чужих сертификатов. При этом при использовании данного режима работы (при клике на ссылке **Показать**) может быть выдано следующее сообщение (см. Рисунок 47).

# Рисунок 47. Окно с сообщением о запрещении импорта сертификатов других пользователей

Удостоверяющий Центр Крипто-Пр	• 📥
Произошла ошибка	
Невозможно получить сертификат.46: Доступ запрещен политикой ЦР. (CertRequest.GetCertificateInfo)	
Пожалуйста, обратитесь к администратору.	_

# 5. АРМ регистрации пользователей

Режим распределенной регистрации поддерживается Центром Регистрации в зависимости от его политики, определенной регламентом УЦ.

Под регистрацией пользователя в распределенном режиме понимается предоставление потенциальному пользователю возможности со своего рабочего места ввода персональных учетных данных, получения служебных ключей и служебного сертификата.

Регистрация пользователя в распределенном режиме выполняется в несколько этапов:

- Установка программного обеспечения СКЗИ «КриптоПро CSP», «КриптоПро TLS» и сертификата Центра Сертификации;
- Формирование запроса на регистрацию;
- Формирование служебных ключей и запроса на служебный сертификат;
- Получение и установка служебного сертификата.

# 5.1. Запуск АРМ регистрации пользователей

Для запуска и работы с АРМ регистрации пользователей необходимо открыть окно браузера MS IE и перейти по адресу <u>https://имя-Web-cepвepa-</u> <u>ЦP/ui/Register/RegGetSubject.asp</u>, где <u>имя сервера ЦР</u> – имя Web-узла Центра Регистрации, или воспользоваться стартовой страничкой Web-приложений Центра Регистрации (см. Рисунок 12), где выбрать режим **Начать регистрацию**.



Процесс регистрации происходит в защищенном режиме с использованием протокола TLS, поэтому обращаем внимание, что в поле **адрес** необходимо вводить именно https (а не http).

# 5.2. Процедура регистрации пользователей

# 5.2.1. Формирование и отправка запроса на регистрацию

Первой экранной формой окна браузера MS IE отображается экранная форма ввода значений атрибутов имени регистрируемого пользователя (см. Рисунок 48) для формирования запроса на регистрацию.

# Рисунок 48. Окно ввода информации по атрибутам имени регистрируемого пользователя

🚰 Страница самостоятельной регистраци	ии - Microsoft Internet Explorer	
<u>Ф</u> айл Правка <u>В</u> ид <u>И</u> збранное С <u>е</u> рвис	: <u>С</u> правка	
🗢 Назад 🔹 🔿 🖉 🙆 🔞 Поиск	📷 Избранное 🛞 Медиа 🎯 🛃 🎒 🖾 📃 🙎	
Адрес: 🝯 https://lord2k.cp.ru/ui/Register/RegG	GetSubject.asp 💽 🧭 Перехо,	д Ссылки »
	Удостоверяющий і	Центр 🗖
Добро пожаловать на стран	ицу самостоятельной регистрации!	
Вам необходимо создать запрос на предлагаемую форму (обязательнь	а регистрацию в системе. Для этого заполните, пожалуй ые поля помечены красным цветом).	:та,
Общее имя:		
Подразделение:		
Организация:		
Город:		
Область:		
Страна/регион:		
Электронная почта:		
Дополнительная информация:	<u> </u>	
	Продолжи	ть >>
🙋 Готово	📔 📄 👘 Интернет	

Данная экранная форма формируется динамически, в соответствии с политикой имен Центра Регистрации, вследствие этого, набор атрибутов имени может изменяться и не соответствовать приведенному на рисунке выше.

Обязательные для заполнения поля отображаются красным цветом букв их наименований (наименования параметров также настраиваются в Центре Регистрации).

После ввода полей экранной формы необходимо нажать кнопку Продолжить.

При этом происходит формирование запроса на регистрацию и постановка его в очередь на обработку на Центре Регистрации.

Дальнейшие действия зависят от настройки параметров работы Центра Регистрации.

5.2.2. Обработка запроса на регистрацию администратором Центра Регистрации

Если параметры работы Центра Регистрации настроены на обработку запроса, на регистрацию, стоящего в очереди, администратором/оператором Центра Регистрации, то в окне браузера отразится экранная форма, приведенная на Рисунок 49.

Рисунок 49. Окно получения маркера временного доступа регистрируемого пользователя при обработке запроса администратором Центра Регистрации

🖉 Страница самостоятельной регистрации - Microsoft Internet Explorer	- 🗆 🗵
Файл Правка Вид Избранное Сервис <u>С</u> правка	-
🖙 Назад 🔻 🔿 🗸 🙆 🚮 🔯 Поиск 📷 Избранное 🎯 Медиа 🎯 🖏 - 🎒 🗹 📃 👷	
Agpec: 🙆 https://lord2k.cp.ru/ui/Register/RegGetSubject.asp	ісылки »
Удостоверяющий Цен	imp 🖻
Для вас создан маркер временного доступа к Удостоверяющему Центру	
Убедитесь, что никто не стоит у вас за спиной, и после этого нажмите кнопку <b>"Показать мари временного доступа"</b> . Запомните (или запишите) Ш маркера доступа и пароль. Они будут ну для получения сертификата.	к <b>ер</b> жны
Показать маркер временного доступа	
Ваш запрос на регистрацию поставлен в очередь. Следить за его обработкой можно на странии пользователя, обладающего правом временного доступа к УЦ.	ie .
🖉 Готово 🛛 🔂 👹 Интернет	

Нажмите кнопку **Показать маркер временного доступа** для того, чтобы увидеть его и запомнить. Маркер временного доступа отображается в экранной форме, представленной ниже (см. Рисунок 50).

Рис	инок	50.	Окно	отоб	ражения	маркера	а врем	енного	дости	па
			• • • • •							

🚰 Страница самостоятельной регистрации - Microsoft Internet Explorer	
Файл Правка Вид Избранное Сервис Справка	1
💠 Назад 🔹 🔿 🖌 🔯 🖓 Поиск 📾 Избранное 🛞 Медиа 🧭 🛃 🚽 🎒 🗹 📃 👷	
Agpec: 🚳 https://lord2k.cp.ru/ui/Register/RegGetSubject.asp	Ссылки »
Удостоверяющий Це	нтр 🖻
Для вас создан маркер временного доступа к Удостоверяющему Центру	
Убедитесь, что никто не стоит у вас за спиной, и после этого нажмите кнопку <b>"Показать мар временного доступа"</b> . Запомните (или запишите) ID маркера доступа и пароль. Они будут ну для получения сертификата. ID маркера <b>11</b> Пароль <b>d@j\$PE</b>	кер 'жны
Ваш запрос на регистрацию поставлен в очередь. Следить за его обработкой можно на страни пользователя, обладающего правом временного доступа к УЦ.	це
	<b>v</b>

Запрос на регистрацию будет стоять в очереди Центра Регистрации до его обработки администратором/оператором Центра Регистрации.

До получения официального уведомления о завершении обработки запроса на регистрацию (как правило, уведомление рассылается по электронной почте) пользователь может получить статус обработки запроса.

Для этого надо открыть окно браузера MS IE и перейти по адресу <u>https://имя-Web-</u> <u>сервера-ЦP/ui/Register/RegTemporaryUser.asp</u>, где <u>имя сервера ЦР</u> – имя Web-узла Центра Регистрации или выбрать режим **Вход для пользователей, обладающих маркером временного доступа** со стартовой страницы Web-приложений Центра Регистрации (см. Рисунок 12).

Статус обработки отражается в экранной форме, приведенной ниже (см. Рисунок 51).

# Рисунок 51. Окно состояния обработки запроса на регистрацию

🕘 Страница самостоятел	льной регистрации - М	Microsoft Internet Explore	r	
<u>Ф</u> айл Правка <u>В</u> ид <u>И</u> з	бранное Сервис <u>С</u> г	правка		10 A
🕁 Назад 🔹 🔿 🖌 🎯 🞼	) 🖄 🔯 Поиск 👔	Избранное 🎯 Медиа 🎡	) B- <i></i>	
Адрес <u>:</u> 🕘 https://lord2k.cp.	.ru/ui/Register/RegTempo	praryUser.asp		💌 🔗 Переход Ссылки »
			Удосто	веряющий Центр 🗖
Страница пользо Здесь вы можете по установить сертифи	ователя, облад осмотреть текущее икат, после того ка	ающего правом в состояние процесса к он выпущен.	ременного доступа к вашей регистрации на УП	УЦ. (, а также загрузить и
Запрос на регистра	цию:			
ID Дата запроса	Дата рассмотрения	Комментарий пользователя	Комментарий администратора	Статус
13 06.08.2003 18:48:17				В ожидании обработки
і 🕘 Готово			🛛 🔒 🥥 Инт	ернет //

По завершению обработки запроса на регистрацию, экранная форма отображения статуса запроса принимает следующий вид (см. Рисунок 52).

# Рисунок 52. Окно подтверждения обработки запроса на регистрацию

🚰 Страница самостоятельной регистрации - Microsoft Internet Explorer 📃 🗖 🔀
Файл Правка Вид Избранное Сервис Справка
🖙 Назад 🔹 🔿 🖉 🖄 🕲 Поиск 📷 Избранное 🛞 Медиа 🧭 🛃 🗉 🛃 🖳
Адрес: 🙆 https://lord2k.cp.ru/ui/Register/RegTemporaryUser.asp
Удостоверяющий Центр 💆
Страница пользователя, обладающего правом временного доступа к УЦ.
Общее имя : user 11 Электронная почта: maslov@cryptopro.ru
Здесь вы можете посмотреть текущее состояние процесса вашей регистрации на УЦ, а также загрузить и установить сертификат, после того как он выпущен.
Запрос на регистрацию:
ID Дата Дата Комментарий Комментарий статус Статус
13         06.08.2003 18:48:17         06.08.2003 19:13:53         Завершен         Получить сертификат
🖉 Готово 🛛 🗍 🎒 👹 Интернет

После этого нажмите кнопку Получить сертификат для перехода к процедуре формирования ключей и запроса на сертификат.

5.2.3. Автоматическая обработка запроса на регистрацию Центром Регистрации

Если параметры работы Центра Регистрации настроены на автоматическую обработку запроса на регистрацию, стоящего в очереди, то в окне браузера отразиться экранная форма, приведенная на Рисунок 53.

# Рисунок 53. Окно получения маркера временного доступа регистрируемого пользователя при автоматической обработке запроса Центром Регистрации

🚰 Страница самостоятельной регистрации - Microsoft Internet Explorer 🔤 📃 🗙
Файл Правка Вид Избранное Сервис Справка
↔ Назад • → • ② Ø △ ◎ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
Адрес <u>і</u> 🍓 https://lord2k.cp.ru/ui/Register/RegGet5ubject.asp
Удостоверяющий Центр 🔼
Для вас создан маркер временного доступа к Удостоверяющему Центру
Убедитесь, что никто не стоит у вас за спиной, и после этого нажмите кнопку <b>"Показать маркер</b> временного доступа". Запомните (или запишите) Ш маркера доступа и пароль. Они будут нужны для получения сертификата.
Показать маркер временного доступа
Ваш запрос на регистрацию успешно обработан. Теперь вы можете создать запрос на сертификат. Вам понадобится ввести ID маркера и пароль.
Создать запрос на сертификат
🔄 Готово

Нажмите кнопку Показать маркер временного доступа для того, чтобы увидеть его и запомнить.

После этого нажмите кнопку Создать запрос на сертификат для перехода к процедуре формирования ключей и запроса на сертификат.

5.2.4. Формирование ключей и запроса на сертификат

В экранной форме формирования ключей и запроса на сертификат (см. Рисунок 54) необходимо выбрать шаблон сертификата, ввести дополнительную информацию (по необходимости) и нажать кнопку **Отправить**.

Рисунок 54. Окно формирования запроса на се	ертификат процедуры
удаленной регистрации пользователя	

Страница самостоятельной регистрации - Microsoft Internet Explorer
Файл Правка Вид Избранное Сервис Справка
🕁 Назад 🔹 🤿 🕫 🚰 🞯 Поиск 📾 Избранное 🞯 Медиа 🧭 🛃 - 🎒 🛃 🖳
Адрес <u>;</u> 🚳 https://lord2k.cp.ru/ui/Register/RegCreateCertRequest.asp 💽 🔗 Переход Ссылки <sup>3</sup>
Удостоверяющий Центр
Запрос на сертификат зарегистрированного пользователя
Общее имя : user 11
Электронная почта: maslov@cryptopro.ru
Выберите шаблон запроса на новый сертификат.
паслон сертификата.   Бременный сертификат пользователя эц
информация:
Отправить >>
🙆 Готово

При этом происходит генерация ключей и формирование запроса на сертификат и постановка его в очередь на обработку на Центре Регистрации.

Дальнейшие действия зависят от настройки параметров работы Центра Регистрации.

5.2.5. Обработка запроса на сертификат администратором Центра Регистрации

Если параметры работы Центра Регистрации настроены на обработку запроса на сертификат, стоящего в очереди, администратором/оператором Центра Регистрации, то в окне браузера отразиться экранная форма, приведенная на Рисунок 55.

Рисунок 55. Окно уведомления о поставке в очередь запроса на сертификат процедуры удаленной регистрации пользователя

🚰 Страница самостоятельной регистрации - Microsoft Internet Explorer	- 🗆 🗵
<u>Ф</u> айл Правка <u>В</u> ид <u>И</u> збранное С <u>е</u> рвис <u>С</u> правка	10 A
😓 Назад 🔹 🔿 🗸 🙆 🚮 🔯 Поиск 🕋 Избранное 🛞 Медиа 🧭 🛃 🚽 🛃 📃 👷	
Адрес: 🕘 https://lord2k.cp.ru/ui/Register/RegSubmitCertRequest.asp 🗾 🔗 Переход	Ссылки »
Удостоверяющий Ц	ентр 🗖
Запрос на сертификат поставлен в очередь	
Узнать о состоянии запроса на сертификат можно на странице пользователя, обладающего правом временного доступа к УЦ.	
Перейти	
	-
🙆 Готово 📃 📄 🔮 Интернет	//.

Запрос на сертификат будет стоять в очереди Центра Регистрации до его обработки администратором/оператором Центра Регистрации.

До получения официального уведомления о завершении обработки запроса на сертификат (как правило, уведомление рассылается по электронной почте) пользователь может получить статус обработки запроса.

Для этого надо открыть окно браузера MS IE и перейти по адресу <u>https://имя-Web-</u> <u>сервера-ЦP/ui/Register/RegTemporaryUser.asp</u>, где <u>имя сервера ЦР</u> – имя Web-узла Центра Регистрации, или выбрать режим **Вход для пользователей, обладающих маркером временного доступа** со стартовой страницы Web-приложений Центра Регистрации (см. Рисунок 12).

Статус обработки отражается в экранной форме, приведенной ниже (см. Рисунок 56).

# Рисунок 56. Окно просмотра состояния обработки запроса на сертификат при регистрации пользователя

🗿 Страница самостоятельной регистрации – Microsoft Internet Explorer
Файл Правка Вид Избранное Сервис Справка
Hasaд マ ⇒ マ Ø Ø ♂ Ø Ø Поиск இИзбранное இМедиа Ø В. → Э ฮ 目 Я
Адрес: The https://lord2k.co.ru/ui/Register/RegTemporaryUser.asp
Удосторараниций Центр
у оостовержощий центр
Страница пользователя, обладающего правом временного доступа к УЦ.
Оощее имя . user 11 Электронная почта: maslov@cryntonro.ru
Здесь вы можете посмотреть текущее состояние процесса вашей регистрации на УЦ, а также загрузить и установить
сертификат, после того как он выпущен.
Запрос на регистрацию:
ID Дата запроса Дата рассмотрения Комментарий пользователя Комментарий администратора Статус
13 06.08.2003 18:48:17 06.08.2003 19:13:53 Завершен
Запросы на сертификат:
ID Дата запроса Дата рассмотрения Комментарий Статус
16 06.08.2003 19:20:00 В ожидании обработки
🥙 Готово 🔰 📋 👹 Интернет

По завершению обработки запроса на сертификат администратором/оператором Центра Регистрации, экранная форма отображения статуса запроса принимает следующий вид (см. Рисунок 57).

# Рисунок 57. Окно получения сертификата при регистрации пользователя

🚰 Страница самостоятельной регистрации - Microsoft Internet Explorer	
Файл Правка Вид Избранное Сервис Справка	<b>11</b>
↓- Назад • → • ◎ Ø ▲ ◎Поиск №Избранное இМедиа Ø № • ⊕ ☑ □ ₽	
Адрес <u>:</u> 🕘 https://lord2k.cp.ru/ui/Register/RegTemporaryUser.asp	∂Переход Ссылки »
Удостоверя	ющий Центр 🗖
Страница пользователя, обладающего правом временного доступа к УЦ.	
Общее имя : <b>user 11</b> Электронная почта: <b>maslov@cryptopro.ru</b>	
- Здесь вы можете посмотреть текущее состояние процесса вашей регистрации на УЦ, а также загрузить сертификат, после того как он выпущен. 	ь и установить
Запрос на регистрацию:	
ID Дата запроса Дата рассмотрения Комментарий пользователя Комментарий администратора	Статус
13 06.08.2003 18:48:17 06.08.2003 19:13:53	Завершен
Запросы на сертификат:	
ID Дата запроса Дата рассмотрения Комментарий Статус	
16 06.08.2003 19:20:00 06.08.2003 19:24:00 Завершен Получить сертификат	
🕘 Готово	<u> </u>

Нажмите кнопку Получить сертификат для получения и установки выпущенного сертификата.

Получение и установка выпущенного сертификата выполняется в экранной форме, приведенной на Рисунок 58.

5.2.6. Автоматическая обработка запроса на сертификат Центром Регистрации

При автоматической обработке запроса на сертификат, пользователю отображается экранная форма формирования ключей и запроса на сертификат (см. Рисунок 54) в которой необходимо выбрать шаблон сертификата, ввести дополнительную информацию (по необходимости) и нажать кнопку **Отправить**.

Следующей экранной формой отображается форма получения и установки изготовленного по запросу сертификата (см. Рисунок 58).

Рисунок 58. Окно получения и уста	новки первого сертификата
пользователя	

🚰 Страница самостоятельной регис	трации - Microsoft Internet Explorer					
<u>Ф</u> айл Правка <u>В</u> ид <u>И</u> збранное С	ервис <u>С</u> правка					
🕁 Назад 👻 🔿 🚽 🚳 🥘 Г	1оиск 🝙 Избранное 🎯 Медиа 🧭 🛃 🎝 🖅 🗐 📃 🙎					
Адрес: 🚳 https://lord2k.cp.ru/ui/Register	r/RegInstallCert.asp 💽 🖉 Переход Ссылки »					
	Удостоверяющий Центр 🔤					
Установка сертификата	Поздравляем! Вы получили Ваш первый <u>сертификат.</u> Для завершения процесса регистрации Вам нужно выполнить					
следующие действия: 1. Задать ключевую фразу. Эта фраза будет использоваться в дальнейшем в процессе отзыва сертификата. ключевая фраза:						
Transit and the second	повторите фразу:					
	2. Установить сертификат >>					
Спасибо за использование нашего сервиса. Сохранить сертификат в файле <u>&gt;&gt;</u>						
🕘 Готово	🗎 🎽 🖉 Интернет 🏼 🏸					

При нажатии на кнопку **Установить сертификат**, происходит установка выпущенного сертификата в хранилище сертификатов текущего пользователя, в раздел **Личные**.

# Работа зарегистрированного пользователя, получившего маркер временного доступа

АРМ зарегистрированного пользователя с маркерным доступом предназначен для выполнения следующих задач:

- Генерация ключей;
- Формирование запроса на сертификат и постановка его в очередь на обработку на Центр Регистрации;
- Получение и установка выпущенного сертификата.

АРМ предназначен для использования следующими категориями пользователей УЦ:

- Пользователи, проходящие процедуру регистрации в распределенном режиме и разрывающие соединение с Центром Регистрации в процессе работы;
- Пользователи, в адрес которых был сформирован администратором ЦР маркер временного доступа.

Если зарегистрированный пользователь УЦ не имеет ни одного действующего сертификата, администратор/оператор Центра Регистрации может сформировать для него маркер временного доступа для получения доступа к программным средствам АРМ зарегистрированного пользователя с маркерным доступом.

# 6.1. Запуск APM зарегистрированного пользователя с маркерным доступом

Для запуска и работы с АРМ зарегистрированного пользователя с маркерным доступом необходимо открыть окно браузера MS IE и перейти по адресу <u>https://имя сервера ЦP/UI/Register/RegTemporaryUser.ASP</u>, где <u>имя сервера ЦP –</u> имя Web-узла Центра Регистрации, или воспользоваться стартовой страничкой Web-приложений Центра Регистрации (см. Рисунок 12. Стартовая страница Web-приложений Центра Регистрации), где выбрать режим **Вход для пользователей, обладающих маркером временного доступа**.

Для доступа к APM зарегистрированного пользователя с маркерным доступом требуется ввести параметры маркера временного доступа (см. Рисунок 59).

Рисунок 59.	Окно ввода	парамет	ров мар	кера в	ременного	доступа
	• · · · · • • • • • • • • •					<b>H /</b>

🚰 Страница регистрации в системе - Microsoft Internet Explorer	
Файл Правка Вид Избранное Сервис Справка	1
🗢 Назад 🔹 🤿 🖉 🚰 🔯 Поиск 📾 Избранное 🎯 Медиа 🧭 🛃 - 🍠 🖃 🖳 👷	
Адрес: 🙆 https://lord2k.cp.ru/ui/Register/RegLogin.asp?Referer=RegTemporaryUser.asp 💌 🔗 Переход	Ссылки »
	<b>A</b>
Пароль	
Войти	
	~
🙋 Готово 🛛 🔂 🙋 Интернет	

# 7. Перечень рисунков

жтяи.0	0067-02 90 10. КриптоПро УЦ. Руководство пользователя.
Рисунок	37. Окно сообщения об отсутствии сертификатов, удовлетворяющих условиям поиска
Рисунок	38. Окно сообщения со списком сертификатов, удовлетворяющих условиям поиска
Рисунок	39. Окно сообщения со списком сертификатов, удовлетворяющих условиям поиска, и полным перечнем атрибутов имени владельцев
Рисунок	40. Окно с отмеченными сертификатами для сохранения в списке найденных 38
Рисунок	41. Окно загрузки файла с выбранными сертфиикатами 38
Рисунок	42. Окно просмотра загруженных сертификатов в MS Windows 2000 39
Рисунок	43. Окно свойств найденного сертификата 39
Рисунок	44. Окно меню для установки нескольких сертификатов в MS Windows 2000 40
Рисунок	45. Окно со списком найденных сертификатов для использования ссылки Показать
Рисунок	46. Окно загрузки файла с выбранным сертификатом 41
Рисунок	47. Окно с сообщением о запрещении импорта сертификатов других пользователей
Рисунок	48. Окно ввода информации по атрибутам имени регистрируемого пользователя
Рисунок	49. Окно получения маркера временного доступа регистрируемого пользователя при обработке запроса администратором Центра Регистрации
Рисунок	50. Окно отображения маркера временного доступа 44
Рисунок	51. Окно состояния обработки запроса на регистрацию 45
Рисунок	52. Окно подтверждения обработки запроса на регистрацию
Рисунок	53. Окно получения маркера временного доступа регистрируемого пользователя при автоматической обработке запроса Центром Регистрации
Рисунок	54. Окно формирования запроса на сертификат процедуры удаленной регистрации пользователя
Рисунок	55. Окно уведомления о поставке в очередь запроса на сертификат процедуры удаленной регистрации пользователя
Рисунок	56. Окно просмотра состояния обработки запроса на сертификат при регистрации пользователя
Рисунок	57. Окно получения сертификата при регистрации пользователя 49
Рисунок	58. Окно получения и установки первого сертификата пользователя
Рисунок	59. Окно ввода параметров маркера временного доступа

# 8. Перечень терминов

# Автоматизированная Система (АС)

Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

# Администратор безопасности

Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

# Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

# Безопасность информации

Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

# Документ в электронной форме (электронный документ)

Информация, представленная в форме набора состояний элементов электронной вычислительной техники, иных электронных средств обработки, хранения и передачи информации, могущая быть преобразованной в форму, пригодную для однозначного восприятия человеком, и имеющая атрибуты для идентификации документа.

# Доступ к информации (Доступ)

Ознакомление с информацией, ее обработка, в частности, копирование и модификация.

# Закрытый ключ (ключ электронной подписи)

Криптографический ключ, который хранится пользователем системы в тайне. Он используется для формирования электронной подписи и/или шифрования данных.

# Запрос на регистрацию

Сообщение, содержащее необходимую информацию для предварительной регистрации в качестве временного пользователя на Центре Регистрации. Формируется в Web-приложении самостоятельной регистрации, после чего передается через Центр Регистрации, где и обрабатывается. Результатом обработки является сообщение по электронной почте о порядке дальнейших действий.

# Запрос на сертификат

Сообщение, содержащее необходимую информацию для получения сертификата. Формируется в АРМ Пользователя или в АРМ Администратора, после чего передается через Центр Регистрации Центру Сертификации, где и обрабатывается. Результатом обработки является выпущенный сертификат или сообщение об ошибке.

# Запрос на отзыв сертификата

Сообщение, содержащее необходимую информацию для отзыва сертификата. Формируется в АРМ Пользователя или в АРМ Администратора, после чего передается через Центр Регистрации Центру Сертификации, где и обрабатывается. Результатом обработки является отзыв сертификата или сообщение об ошибке.

# Защита от несанкционированного доступа (Защита от НСД)

Предотвращение или существенное затруднение несанкционированного доступа.

# Защищенное средство вычислительной техники (защищенная АС)

Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.

# Идентификатор доступа

Уникальный признак субъекта или объекта доступа.

### Идентификация

Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

### Информационное обеспечение (ИО)

Совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в АС при ее функционировании.

### Класс защищенности средств вычислительной техники, автоматизированной системы

Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации.

### Ключ (криптографический ключ)

Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

# Ключевая пара

Открытый и закрытый ключи (или ключ ЭП и ключ проверки ЭП).

### Ключевой носитель

Объект системы, который может содержать один или несколько ключевых контейнеров. Каждый ключевой контейнер содержит следующую информацию: только ключ подписи, только ключ шифрования, ключ подписи и ключ шифрования одновременно. Дополнительно ключевой контейнер содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей и их целостности. Каждый контейнер является полностью самостоятельным и содержит всю необходимую информацию для работы как с самим контейнером, так и с закрытыми ключами.

#### Комплекс средств защиты (КСЗ)

Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

#### Компрометация ключа

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

- 1. Потеря ключевых носителей;
- 2. Потеря ключевых носителей с их последующим обнаружением;
- 3. Увольнение сотрудников, имевших доступ к ключевой информации;
- 4. Нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;
- 5. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- 6. Нарушение печати на сейфе с ключевыми носителями;
- Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и

доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

Различают два вида компрометации секретного ключа: **явную** и **неявную**. Первые четыре события должны трактоваться как явная компрометация ключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

# Многоуровневая защита

Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

# Модель защиты

Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа.

# Модуль автоматизированной системы (модуль АС)

Часть АС, реализующая одну или более взаимосвязанных функций АС.

# Нарушитель правил разграничения доступа (Нарушитель ПРД)

Субъект доступа, осуществляющий несанкционированный доступ к информации.

### Несанкционированный доступ к информации (НСД)

Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

### Объект доступа

Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

#### Открытый ключ (ключ проверки электронной подписи)

Криптографический ключ, который связан с закрытым ключом с помощью особого математического соотношения. Открытый ключ известен другим пользователям системы и предназначен для проверки электронной подписи и шифрования. При этом открытый ключ не позволяет вычислить закрытый ключ.

### Плановая смена ключей

Смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

# Подтверждение подлинности ЭП

Положительный результат проверки правильности ЭП, выработанной правомочным лицом из исходной информации путем применения принадлежащего ему закрытого ключа ЭП, полученный с использованием зарегистрированного и сертифицированного ключа проверки ЭП.

# Показатель защищенности средств вычислительной техники (Показатель защищенности)

Характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники.

#### Пользователь автоматизированной системы (пользователь АС)

Лицо, участвующее в функционировании АС или использующее результаты ее функционирования.

# Пользователь АС зарегистрированный

Пользователь АС или системный сервис, имеющий учетную запись в АС.

# Правила разграничения доступа (ПРД)

Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

### Проверка электронной подписи документа

Проверка соотношения, связывающего хэш-функцию документа, подпись под этим документом и открытый ключ подписавшего пользователя. Если рассматриваемое соотношение оказывается выполненным, то подпись признается правильной, а сам документ - подлинным, в противном случае документ считается измененным, а подпись под ним - недействительной.

# Программное обеспечение (ПО)

Совокупность программ на носителях информации и программных документов, предназначенных для отладки, функционирования и проверки работоспособности АС. Санкционированный доступ к информации (СД)

Доступ к информации, не нарушающий правила разграничения доступа.

### Сертификат

1. Документ, выданный и заверенный удостоверяющим центром, подтверждающий принадлежность открытого ключа (ключа проверки ЭП) определенному лицу. Сертификат может содержать дополнительную информацию, необходимую для обеспечения безопасности использования открытого ключа. В случае, когда сертификат выдается в форме электронного документа, он подписывается ЭП этого центра.

2. Электронный документ, который содержит открытый ключ субъекта и подписан электронной подписью его издателя. Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом субъекта и информацией, которая его идентифицирует.

Формат сертификата определен в рекомендациях ITU-Т 1997 года X.509 [X.509] и рекомендациях IETF 2008 года RFC 5280 [RFC 5280].

#### Сертификат защиты

Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных.

#### Сертификация уровня защиты

Процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите.

# Система защиты информации от несанкционированного доступа (СЗИ НСД)

Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

#### Система защиты секретной информации (СЗСИ)

Комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах.

#### Система разграничения доступа (СРД)

Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

#### Список отзыва

Список отозванных сертификатов (CRL – Certificate Revocation List). УЦ поддерживает отзыв сертификатов и публикацию списков отозванных сертификатов.

Пользователи УЦ могут получить эту информацию и записать ее в свое локальное хранилище, чтобы использовать для последующей проверки сертификатов.

### Средство защиты от несанкционированного доступа (Средство защиты от НСД)

Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

### Средство криптографической защиты информации (СКЗИ)

Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

### Средство электронной подписи

Совокупность программных и технических средств, реализующих функцию выработки и проверки электронной подписи.

### Субъект доступа

Лицо или системный сервис (процесс), действия которого регламентируются правилами разграничения доступа.

### Техническое обеспечение (ТО)

Совокупность средств реализации управляющих воздействий, средств получения, ввода, подготовки, преобразования, обработки, хранения, регистрации, вывода, отображения, использования и передачи данных с конструкторской и эксплуатационной документацией.

### Уровень полномочий субъекта доступа

Совокупность прав доступа субъекта доступа.

# Учетная запись

Информация, хранимая в АС, служащая для идентификации, аутентификации, авторизации действий пользователей АС и системных сервисов (Login, пароль, цифровой сертификат), а также содержащая прочие, необходимые для функционирования АС характеристики пользователей и сервисов (E-mail, адрес и т.п.).

# Функция автоматизированной системы (функция АС)

Совокупность действий АС, направленная на достижение определенной цели, на выполнение определенного технологического процесса.

# Центр по удостоверению подлинности электронной подписи (удостоверяющий центр)

Юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей.

# Целостность информации

Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

# Центр Сертификации (Удостоверяющий центр)

Компонент Удостоверяющего центра. Выполняет функции службы сертификации: выпуск сертификатов, отзыв сертификатов, а также генерацию списков отзыва.

# Центр Регистрации

Компонент Удостоверяющего центра. Выполняет функции промежуточного звена, осуществляющего передачу запросов от пользователей и администраторов Центра Регистрации центру сертификации. В процессе этой передачи осуществляется аутентификация пользователя, проверка корректности передаваемой им информации, а также фиксация этой информации в базе данных ЦР.

# Шифрование

Процесс зашифрования или расшифрования.

Шифрование информации – взаимнооднозначное математическое (криптографическое) преобразование, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации, представленной в некоторой цифровой кодировке, блок шифрованной информации, также представленной в цифровой кодировке. Термин шифрование объединяет в себе два процесса: зашифрование и расшифрование информации.

Если зашифрование и расшифрование осуществляются с использованием одного и того же ключа, то такой алгоритм криптографического преобразования называется симметричным, в противном случае — асимметричным.

Прочитать зашифрованное сообщение (информацию) может только пользователь, имеющий тот же секретный ключ шифрования.

### Электронная подпись (ЭП)

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

# 9. Перечень сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
DN	Отличительное имя (Distinguished Name)
ITU-T	Международный комитет по телекоммуникациям (International Telecommunication Union)
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol.
	Упрощенный протокол доступа к справочнику
ТМ	Устройство хранения информации на таблетке touch- memory
ΡΚΙ	Public Key Infrastructure. Аналог ИОК.
RDN	Относительное отличительное имя (Relative Distinguished Name)
URI	Единый идентификатор ресурса (Uniform Resource Identifier)
URL	Единый локатор ресурса (Uniform Resource Locator)
AC	Автоматизированная система
APM	Автоматизированное рабочее место
ДСЧ	Датчик случайных чисел
ИОК	Инфраструктура Открытых Ключей
КП	Конечный пользователь
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей. Сетевой справочник
ЦP	Центр Регистрации
ЦC	Центр Сертификации
УЦ	Удостоверяющий центр
ЭП	Электронная подпись

	10.	Перечень ссылочных документов
[X.509]		ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.
[RFC 5280]		RFC 5280. D. Cooper et al., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008.
[PKCS-7]		RSA Laboratories. <i>PKCS #7: Cryptographic Message Syntax</i> Standard. Version 1.5, November 1993.
[PKCS-10]		RSA Laboratories. <i>PKCS #10:</i> Certification Request Syntax Standard.

Номера листов (страниц)			Всего листов	№ документа	Входящий №	Подпись	Дата		
Изм.	изменен- ных	заменен- ных	новых	аннули- рованных	(страниц) в докум.		тельного документа и дата		

# Лист регистрации изменений