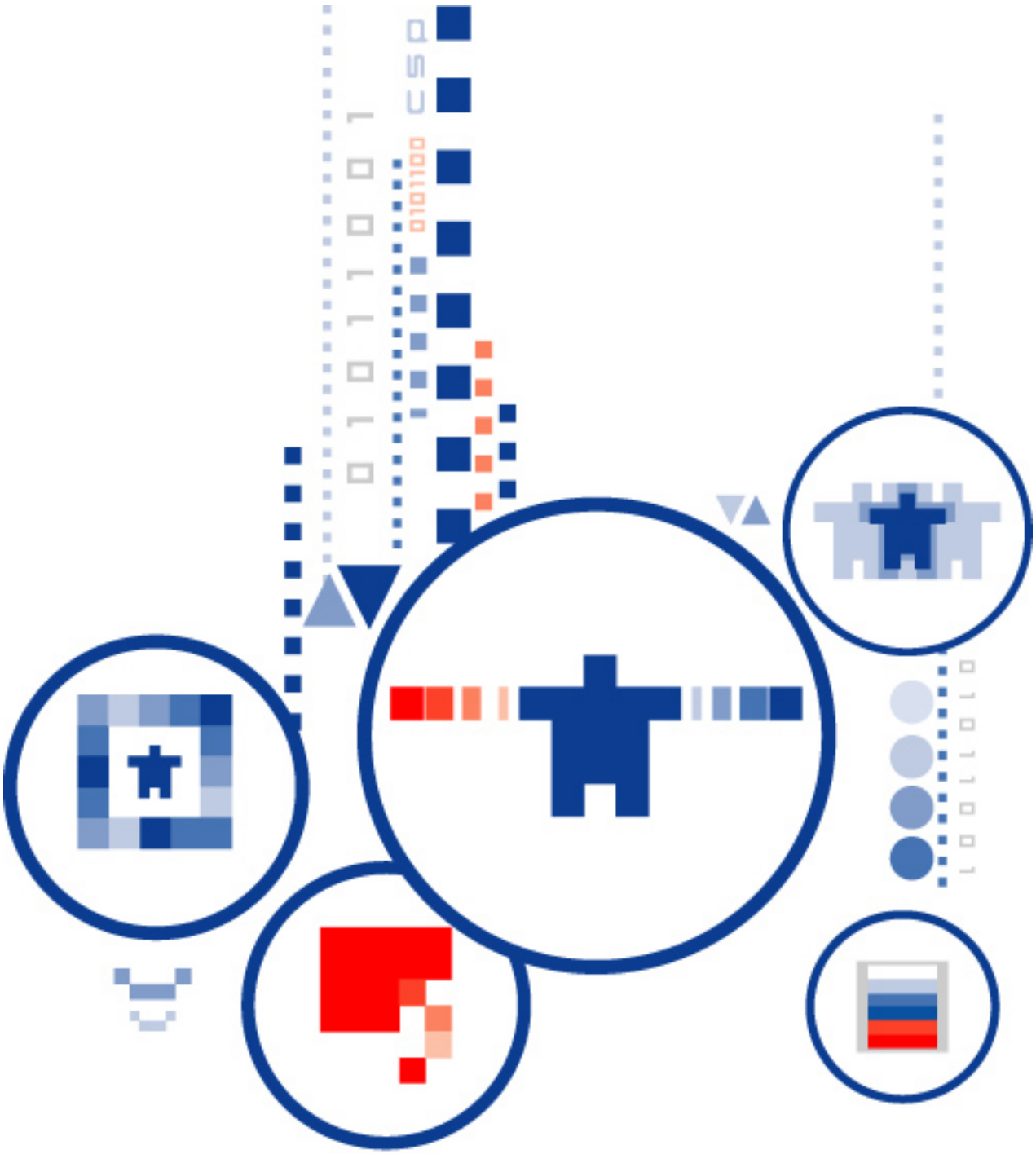
УТВЕРЖДЕН
ЖТЯИ.00035-01 90 01-ЛУ

ЖТЯИ.00035-01 90 01



КриптоПро УЦ

программно–аппаратный комплекс
удостоверяющий центр

Общее описание

АННОТАЦИЯ

Настоящий документ содержит описание программно-аппаратного комплекса «Удостоверяющий Центр «КриптоПро УЦ» (ПАК «КриптоПро УЦ»), обеспечивающего реализацию целевых функций удостоверяющего центра как организации.

Приведено назначение, характеристики, структура и функции компонентов подсистемы, а также сведения о принципах построения и функционирования ПАК «КриптоПро УЦ» на различных этапах работы - от фазы развертывания до фазы штатной работы и нештатных ситуаций.

Документ описывает основные правила пользования, связанные с установкой и эксплуатацией компонентов ПАК «КриптоПро УЦ».

Документ предназначен для администраторов как ознакомительный материал перед установкой и эксплуатацией программного обеспечения ПАК «КриптоПро УЦ».

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

http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru

Содержание

1. Термины и определения

Термин	Определение
Владелец сертификата открытого ключа	физическое лицо, на имя которого удостоверяющим центром выдан сертификат открытого ключа и которое владеет соответствующим закрытым ключом, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы)
Сертификат открытого ключа	электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра (или документ на бумажном носителе), который включает в себя открытый ключ и который выдается удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата открытого ключа
Средства электронной цифровой подписи	аппаратные и (или) программные средства криптографической защиты информации, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей
Список отозванных сертификатов (СОС, CRL)	электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были аннулированы (отозваны) или действие которых было приостановлено
Удостоверяющий Центр	субъект права, обеспечивающий выполнение целевых функций удостоверяющего центра в соответствии с №1-ФЗ от 10.01.2002г. «Об электронной цифровой подписи»
Электронная цифровая подпись	Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе
Электронный документ	документ, информация в котором представлена в электронно-цифровой форме, способной быть обработанной средствами вычислительной техники

2. Назначение ПАК «Удостоверяющий Центр «КриптоПро УЦ»

Программно-аппаратный комплекс (далее – ПАК) «Удостоверяющий Центр «КриптоПро УЦ» (далее – «КриптоПро УЦ») предназначен для:

- автоматизации деятельности удостоверяющего центра при выполнении им своих целевых функций согласно действующего законодательства Российской Федерации;
- автоматизации деятельности по управлению сертификатами открытых ключей, применяемых для шифрования, аутентификации и обеспечения достоверности информации.

ПАК «КриптоПро УЦ» применяется для выполнения организационно-технических мероприятий в целях:

- контроля целостности электронных документов, передаваемых в автоматизированных информационных системах;
- контроля целостности публичных информационных ресурсов;
- проверки подлинности взаимодействующих программных компонентов и конфиденциальности передаваемых данных при информационном взаимодействии;
- создания системы юридически значимой электронной цифровой подписи в системах электронного документооборота;
- обеспечения безопасности и разграничения доступа при взаимодействии субъектов автоматизированных информационных систем;
- аутентификации пользователей в домене MS Active Directory;
- аутентификации пользователей в локальной вычислительной сети предприятия;
- создания системы управления ключами подписи субъектов автоматизированных информационных систем.

ПАК «КриптоПро УЦ» обеспечивает:

- Реализацию многоролевой модели управлениями объектами ПАК «КриптоПро УЦ»
- Реализацию Инфраструктуры Удостоверяющих Центров, построенных как по иерархической так и по сетевой (распределенной) модели
- Аудит событий, связанных с эксплуатацией программного комплекса
- Реализацию механизма занесения в сертификат открытого ключа подписи сведений об отношениях, при которых электронный документ имеет юридическую силу, и областях применения сертификата
- Ведения реестра зарегистрированных пользователей
  - Выполнение процедуры регистрации пользователя в централизованном режиме с прибытием регистрируемого пользователя в Удостоверяющий Центр;
  - Выполнение процедуры регистрации пользователя в распределенном режиме без прибытия регистрируемого пользователя в Удостоверяющий Центр;
  - Выполнение процедуры удаления пользователей из реестра пользователей по запросам администратора Удостоверяющего Центра;
  - Выполнение процедуры удаления пользователей из реестра пользователей в автоматическом режиме;
- Генерация ключей подписи и шифрования
  - Выполнение процедуры генерации личных закрытых и открытых ключей ЭЦП и шифрования пользователя на рабочем месте пользователя;

- Выполнение процедуры генерации личных закрытых и открытых ключей ЭЦП и шифрования на рабочем месте администратора Удостоверяющего Центра;
- Выполнение процедуры генерации личных закрытых и открытых ключей ЭЦП уполномоченного лица Удостоверяющего Центра;
- Выполнение процедуры генерации личных закрытых и открытых ключей ЭЦП уполномоченного лица подчиненного Удостоверяющего Центра;

- Ведения реестра запросов и заявлений на сертификаты открытых ключей в электронном виде
  - Формирование запроса на сертификат нового открытого ключа на рабочем месте пользователя;
  - Формирование запроса на сертификат нового открытого ключа на рабочем месте администратора Удостоверяющего Центра;
  - Вывод запросов на сертификаты открытых ключей пользователей на бумажный носитель на рабочем месте пользователя;
- Ведение реестра сертификатов открытых ключей, изданных Удостоверяющим Центром в электронном виде
  - Контроль уникальности открытых ключей подписи и шифрования в формируемых сертификатах;
  - Формирование сертификатов открытых ключей пользователей в электронном виде в соответствии с рекомендациями X.509 версии 3 и RFC 2459, позволяющих с помощью криптографических методов (ЭЦП) централизованно заверять соответствие открытого ключа и атрибутов определенному пользователю;
  - Вывод сертификатов открытых ключей пользователей на бумажный носитель на рабочем месте пользователя;
  - Вывод сертификатов открытых ключей пользователей на бумажный носитель на рабочем месте администратора Удостоверяющего Центра;
- Ведение реестра запросов и заявлений на аннулирование (отзыв) и приостановление/возобновления действия сертификатов открытых ключей в электронном виде
  - Выполнение процедуры формирования запросов на отзыв сертификатов открытых ключей на рабочем месте пользователя;
  - Выполнение процедуры формирования запросов на отзыв сертификатов открытых ключей пользователей на рабочем месте администратора Удостоверяющего Центра;
  - Выполнение процедуры формирования запросов от пользователей на приостановление/возобновление действия сертификатов открытых ключей на рабочем месте пользователя;
  - Выполнение процедуры формирования запросов на приостановление/возобновление действия сертификатов открытых ключей пользователей на рабочем месте администратора Удостоверяющего Центра;
  - Формирование и доставку зарегистрированным пользователям списка отозванных сертификатов открытых ключей пользователей;
- Выполнение процедуры подтверждения подлинности ЭЦП
  - Выполнение процедуры подтверждения подлинности ЭЦП в электронных документах;
  - Выполнение процедуры подтверждения подлинности ЭЦП уполномоченного лица Удостоверяющего Центра в изданных сертификатах открытых ключей.
- Реализацию системы оповещения пользователей с использованием почтовых сообщений
  - Управление оповещением пользователей о событиях в процессе регистрации;
  - Управление оповещением пользователей о событиях в течении всего жизненного цикла сертификатов открытых ключей;
  - Оповещение пользователей об отдельных события в удостоверяющем центре (например, о смене ключей уполномоченного лица удостоверяющего центра).

3. Состав и назначение программных компонентов ПАК «КриптоПро УЦ»

3.1. Состав программных компонентов ПАК «КриптоПро УЦ»

В состав программного комплекса «Удостоверяющий Центр «КриптоПро УЦ» входят следующие программные компоненты:

- **Центр сертификации** (ЦС) в составе:
  - ПО Центра сертификации
  - Утилиты Центра Сертификации
  - СКЗИ КриптоПро CSP
  - Средство сетевой аутентификации КриптоПро TLS
- **Центр регистрации** (ЦР) в составе:
  - ПО Центра регистрации
  - Утилиты Центра Регистрации
  - ПО АРМ регистрации пользователя
  - ПО АРМ зарегистрированного пользователя с маркерным доступом
  - ПО АРМ зарегистрированного пользователя с ключевым доступом
  - СКЗИ КриптоПро CSP
  - Средство сетевой аутентификации КриптоПро TLS
- **АРМ администратора Центра Регистрации** (АРМ администратора ЦР) в составе:
  - ПО АРМ администратора
  - СКЗИ КриптоПро CSP
- **АРМ разбора конфликтных ситуаций** (АРМ РКС) в составе:
  - ПО АРМ разбора конфликтных ситуаций
  - СКЗИ КриптоПро CSP

3.2. Описание и назначение программных компонентов ПАК «КриптоПро УЦ»

3.2.1. СКЗИ КриптоПро CSP

Средство криптографической защиты информации КриптоПро CSP используется в ЦС, ЦР, АРМ администратора ЦР, АРМ разбора конфликтных ситуаций и АРМ пользователей.

На Центре сертификации используется СКЗИ КриптоПро CSP (версия 3.0) в составе согласно формуляра ЖТЯИ.00015-01 30 01, вариант исполнения 6.

На Центре регистрации используется СКЗИ КриптоПро CSP (версия 3.0) в составе согласно формуляра ЖТЯИ.00015-01 30 01, вариант исполнения 6.

На АРМ администратора ЦР с установленной ОС из следующего перечня: MS Windows 2000 Professional, MS Windows Server 2000 и MS Windows XP, используется СКЗИ КриптоПро CSP (версия 2.0) в составе согласно формуляра ЖТЯИ.00005-02 30 01, вариант исполнения 4 или СКЗИ КриптоПро CSP (версия 3.0) в составе согласно формуляра ЖТЯИ.00015-01 30 01, вариант исполнения 6.

На АРМ администратора ЦР с установленной ОС MS Windows Server 2003 используется СКЗИ КриптоПро CSP (версия 3.0) в составе согласно формуляра ЖТЯИ.00015-01 30 01, вариант исполнения 6.

На АРМ разбора конфликтных ситуаций с установленной ОС из следующего перечня: MS Windows 2000 Professional, MS Windows Server 2000 и MS Windows XP, используется СКЗИ КриптоПро CSP (версия 2.0) в составе согласно формуляра ЖТЯИ.00005-02 30 01, вариант исполнения 4 или СКЗИ КриптоПро CSP (версия 3.0) в составе согласно формуляра ЖТЯИ.00015-01 30 01, вариант исполнения 6.

На АРМ разбора конфликтных ситуаций с установленной ОС MS Windows Server 2003 используется СКЗИ КриптоПро CSP (версия 3.0) в составе согласно формуляра ЖТЯИ.00015-01 30 01, вариант исполнения 6.

Важно: С 1 января 2008 года не допускается применение алгоритма ГОСТ Р 34.10-94, реализованного СКЗИ «КриптоПро CSP» (версия 2.0) и СКЗИ «КриптоПро CSP» (версия 3.0), для формирования электронной цифровой подписи электронных документов. Применение данного алгоритма допустимо для подтверждения подлинности электронной цифровой подписи (проверки ЭЦП).

Система "Электронный замок "Соболь" (или ПАК «Аккорд-АМДЗ») предназначена для организации защиты компьютера от входа посторонних пользователей. Под посторонними пользователями понимаются все лица, не зарегистрированные в системе "**Электронный *замок***" как пользователи данного компьютера.

Система "***Электронный замок***" обеспечивает:

- регистрацию пользователей компьютера и назначение им персональных идентификаторов и паролей на вход в систему;
- запрос персонального идентификатора и пароля пользователя при загрузке компьютера;
- возможность блокирования входа в систему зарегистрированного пользователя;
- ведение системного журнала, в котором производится регистрация событий, имеющих отношение к безопасности системы;
- контроль целостности файлов на жестком диске;
- контроль целостности физических секторов жесткого диска;
- аппаратную защиту от несанкционированной загрузки операционной системы с гибкого диска и CD-ROM диска.

3.2.2. Средство сетевой аутентификации КриптоПро TLS

Модуль КриптоПро TLS разработан в соответствии с криптографическим интерфейсом корпорации Microsoft - Security Service Provider Interface (SSPI). Модуль КриптоПро TLS входит в состав СКЗИ КриптоПро CSP версии 2.0 и версии 3.0, реализующего российские криптографические алгоритмы. Он встраивается в системы Microsoft в качестве дополнения к стандартному модулю Schannel.

Основные функции, реализуемые модулем КриптоПро TLS

- Две схемы аутентификации с использованием обмена ключей по алгоритму Диффи-Хэллмана и хэширования в соответствии с ГОСТ Р 34.11-94:
  - односторонняя - анонимный клиент, аутентифицируемый сервер;
  - двухсторонняя - аутентифицируемые клиент и сервер;
- Выработка и проверка электронной цифровой подписи в соответствии с ГОСТ Р 34.10-94 или ГОСТ Р 34.10-2001;
- Шифрование соединения в соответствии с ГОСТ 28147-89 ("Системы обработки информации. Защита криптографическая.");
- Вычисление имитовставки передаваемых данных в соответствии с ГОСТ 28147-89;

3.2.3. Центр сертификации

Центр сертификации компонентов ПАК «КриптоПро УЦ» предназначен для формирования сертификатов открытых ключей пользователей и администраторов Удостоверяющего центра, списков отозванных сертификатов, хранения эталонной базы сертификатов и списков отозванных сертификатов. Центр Сертификации функционирует в операционной системе (ОС) Microsoft Windows Server 2000, Microsoft Windows Server 2003 и использует базу данных Microsoft SQL Server 2000 Desktop Engine (MSDE) и базу данных службы сертификации Microsoft Certificate Authority (CA). MSDE с пакетом обновлений SP4 устанавливается программой установки ПО Центра Сертификации и не требует ее отдельной установки.

ЦС взаимодействует только с Центром Регистрации или несколькими Центрами Регистрации по отдельному сегменту локальной сети с использованием защищенного сетевого протокола.

ЦС самостоятельно не инициирует никаких соединений с Центрами Регистрации, оставаясь пассивным слушателем. Инициирование соединения осуществляется Центрами Регистрации по протоколу TLS с двухсторонней аутентификацией. Центр Сертификации устанавливает соединение при одновременном выполнении следующих условий:

- Центр Регистрации предъявил действительный сертификат открытого ключа клиентской аутентификации;
- сертификат открытого ключа клиентской аутентификации находится в списке доверенных ЦР, который управляется с использованием приложения «Параметры Центра Сертификации».

На Центре Сертификатов находится эталонная база всех изготовленных сертификатов открытых ключей.

К функциям ЦС относятся:

- Генерация ключей и сертификата открытого ключа уполномоченного лица удостоверяющего центра.
- Смена ключей и сертификата открытого ключа уполномоченного лица удостоверяющего центра.
- Формирование сертификата открытого ключа по запросам Центра Регистрации.
- Формирование запроса на кросс-сертификат открытого ключа уполномоченного лица удостоверяющего центра;
- Ведение базы данных сертификатов с предоставлением доступа к ней ограниченному кругу компонентов системы.
- Изменение базы данных сертификатов по запросам от Центра Регистрации. Включает в себя выполнение следующих операций:

- аннулирование (отзыв) сертификата;
- приостановление действия сертификата;
- возобновление действия сертификата.

- Формирование списка аннулированных (отозванных) сертификатов открытых ключей по запросам Центра Регистрации.
- Формирование списка аннулированных (отозванных) сертификатов открытых ключей по запросам Центра Регистрации в автоматическом режиме с периодичностью, заданной в расписании.
- Ведение архива всех изданных списков аннулированных (отозванных) сертификатов открытых ключей в автоматическом режиме.
- Обеспечение уникальности следующей информации в сертификатах пользователей:
  - Открытый ключ сертификата;
  - Серийный номер сертификата.
- Взаимодействие с Центрами Регистрации:
  - Аутентификация Центров Регистрации и определение прав доступа с использованием ключей и сертификатов открытых ключей Центров Регистрации;
  - Прием от Центров Регистрации запросов;
  - Проверка наличия подписи данной информации на ключе Центров Регистрации;
  - Обработка полученных от Центров Регистрации запросов;
  - Передача на Центры Регистрации результатов обработки запросов;
  - Шифрование информации, передаваемой между ЦС и ЦР в ходе сетевого взаимодействия по протоколу TLS (КриптоПро TLS).
- Протоколирование работы Центра Сертификации.

3.2.4. Центр Регистрации

Центр Регистрации – компонент ПАК «КриптоПро УЦ», предназначенный для хранения регистрационных данных пользователей, запросов на сертификаты и сертификаты пользователей, предоставления интерфейса взаимодействия пользователей с Удостоверяющим Центром. Центр Регистрации функционирует в операционной системе (ОС) Microsoft Windows Server 2000, Microsoft Windows Server 2003 и использует базу данных Microsoft SQL Server 2000 Desktop Engine (MSDE) (по умолчанию). MSDE пакетом обновлений SP3 устанавливается программой установки ПО Центра Регистрации.

В качестве системы управления базы данных Центра Регистрации может использоваться Microsoft SQL Server 2000 (Standard Edition или Enterprise Edition).

Центр Регистрации взаимодействует с Центром Сертификации по отдельному сегменту локальной сети с использованием защищенного сетевого протокола. Взаимодействие пользователей с Удостоверяющим центром обеспечивается за счет использования приложений (АРМ зарегистрированного пользователя с ключевым доступом, АРМ зарегистрированного пользователя с маркерным доступом, АРМ регистрации пользователя), предоставляемых Центром Регистрации.

Центр Регистрации является единственной точкой входа (регистрации) пользователей в системе. Только зарегистрированный в Центре Регистрации пользователь может получить сертификат на свой открытый ключ в Удостоверяющем Центре.

База данных Центра Регистрации (Реестр) содержит полную информацию и историю обо всех изготовленных сертификатах для зарегистрированных на ЦР пользователей.

К функциям Центра Регистрации относятся:

- Обеспечение аутентификации приложений и пользователей при обращении к Центру Регистрации.
- Ведение Базы Данных (Реестра), содержащей информацию о пользователях и пользовательских сертификатах. База Данных содержит следующую информацию:
  - Данные о пользователях, включающиеся в сертификаты открытых ключей;
  - Данные о пользователях, не включаемые в сертификаты открытых ключей;
  - Ключевая фраза пользователя, необходимая для его идентификации администратором;
  - Открытые ключи пользователей, зарегистрированных в системе;
  - Сертификаты пользователей, зарегистрированных в системе:
    - действующие;
    - отозванные (аннулированные, приостановленные);
    - с истекшим сроком действия сертификата;
    - с истекшим сроком действия закрытого ключа.
  - Запросы на регистрацию пользователя:
    - поступившие;
    - отвергнутые;
    - обработанные;
  - Запросы на сертификаты открытого ключа пользователя:
    - поступившие;
    - отвергнутые;
    - обработанные;
  - Запросы на отзыв сертификатов открытого ключа пользователя:
    - поступившие;
    - отвергнутые;
    - обработанные;
- Управление шаблонами сертификатов, обеспечивающих определение области применения ключей и сертификатов открытых ключей пользователей:
  - Создание шаблонов;
  - Удаление;
  - Корректировка.
- Управление политиками:
  - Политики уведомлений администраторов и пользователей;
  - Политиками имен;
  - Политиками обработки запросов:
    - На отзыв;
    - На изготовление сертификатов;
    - Подписанными;

- Неподписанными.
  - Политиками ролевой модели и системы разграничения доступа;
- Обеспечение уникальности следующей информации в сертификатах пользователей:
  - Доменное имя пользователя.
- Взаимодействие с Центром Сертификации и внешними приложениями.
  - Прием от приложения и передача на Центр Сертификации запросов, подпись данных запросов на ключе Центра Регистрации;
  - Прием от Центра Сертификации и передача приложению результатов обработки запросов;
  - Проверка подписи Центра сертификации на принимаемой от него информации;
  - Аутентификация и шифрование информации с использованием протокола TLS (КриптоПро TLS).
- Управление режимами работы Удостоверяющего Центра по регистрации и управлению ключами и сертификатами.
- Обеспечение доступа к Базе Данных внешним приложениям через SOAP-интерфейс на базе HTTP(S).
- Обеспечение выполнения Центром Регистрации в автоматическом режиме различных задач:
  - Оповещение пользователей и администраторов по электронной почте о событиях, связанных с жизненным циклом сертификатов (о регистрации пользователя, о изготовлении сертификата, о отзыве сертификата, об истечении срока действия сертификатов, о необходимости замены ключей, и т.д.)
  - Получение списка отозванных сертификатов от соответствующего Центра Сертификации.
  - Получение списка отозванных сертификатов от Центров Регистрации вышестоящих по иерархии Удостоверяющих Центров.
  - Удаление зарегистрированных пользователей, не имеющих ни одного действующего сертификата открытого ключа.
- Протоколирование работы Центра Регистрации.

Обработанные запросы (на регистрацию, на сертификат, на отзыв сертификата) хранятся в базе данных Центра Регистрации как с ЭЦП самого пользователя, так и с ЭЦП администратора, обработавшего данный запрос.

3.2.5. АРМ администратора Центра Регистрации

Компонент АРМ Администратора ЦР предназначен для выполнения организационно-технических мероприятий, связанных с регистрацией пользователей, формированием служебных ключей и сертификатов пользователей и управления Центром регистрации. АРМ администратора функционирует в ОС Microsoft Windows 2000 Professional, Microsoft Windows Server 2000, Microsoft Windows Server 2003 или Windows XP. АРМ администратора взаимодействует только с Центром Регистрации по локальной сети с использованием защищенного сетевого протокола (TLS).

Программное обеспечение АРМа администратора является универсальным и используется для всех ролей привилегированных пользователей (администраторов, операторов и т.д.).

К основным функция АРМ администратора относятся:

- Обеспечение взаимодействия с одним или несколькими Центрами Регистрации.
- Обеспечение возможности выбора администратором сертификата, с помощью которого будет осуществляться взаимодействие с Центром Регистрации.
- Шифрование информации передаваемой Центру Регистрации с использованием протокола TLS с двусторонней аутентификацией;
- Регистрация пользователей в Центре регистрации.
- Удаление зарегистрированных пользователей из Центра Регистрации, не имеющих ни одного действующего сертификата.
- Генерация служебных и рабочих ключей пользователей.
- Организация просмотра информации из Базы Данных Центра Регистрации, относящейся к пользователю, зарегистрированному в системе.
- Создание запросов на формирование сертификатов.
- Обеспечение возможности получения пользователем нескольких сертификатов.
- Вывод сертификата открытого ключа пользователя на бумажный носитель.
- Создание запросов на отзыв сертификатов.
- Создание запросов на приостановление действия сертификатов.
- Создание запросов на возобновление действия сертификатов.
- Проверка состояния и обработка запросов на формирование сертификатов, поступающих от пользователей.
- Проверка состояния и обработка запросов на отзыв, приостановление и возобновление действия сертификатов, поступающих от пользователей.
- Просмотр протокола работы Центра Регистрации.
- Публикация списков отозванных сертификатов открытых ключей пользователей.
- Вывод сертификата открытого ключа Центра Сертификации (уполномоченного лица Удостоверяющего Центра) на бумажный носитель.
- Сохранение списка отозванных сертификатов на магнитном носителе в виде файла.
- Сохранение сертификата (цепочки сертификатов) Центра Сертификации на магнитном носителе в виде файла.

3.2.6. АРМ разбора конфликтных ситуаций

АРМ разбора конфликтных ситуаций предназначен для выполнения организационно-технических мероприятий, связанных:

- с подтверждением подлинности ЭЦП в электронных документах и определения статуса сертификатов открытых ключей пользователей;
- с подтверждением подлинности ЭЦП уполномоченного лица Удостоверяющего Центра в изготовленных им сертификатах открытых ключей.

АРМ разбора конфликтных ситуаций функционирует в ОС Microsoft Windows 2000. АРМ разбора конфликтных ситуаций не взаимодействует ни с каким другим компонентом Удостоверяющего Центра и использует в своей работе объекты, предъявляемые сторонами конфликта в качестве доказательства тех или иных фактов (электронный документ с ЭЦП, сертификаты, списки отозванных сертификатов и т.д.).

К основным функциям АРМ разбора конфликтных ситуаций относятся:

- Проверка целостности ЭЦП на электронном документе;
- Проверка целостности ЭЦП уполномоченного лица удостоверяющего центра на сертификате открытого ключа;
- Установление статуса сертификата открытого ключа подписи;
- Формирование и печать протокола проверки.

3.2.7. АРМ зарегистрированного пользователя с маркерным доступом

АРМ зарегистрированного пользователя с маркерным доступом предназначен для выполнения организационно-технических мероприятий, связанных с генерацией служебных ключей, формированием запроса на служебный сертификат открытого ключа и получением служебного сертификата открытого ключа.

Аутентификация зарегистрированного пользователя осуществляется с использованием временного маркера доступа, представляющего собой совокупность следующих сущностей:

- Идентификатор (ID);
- Пароль.

Идентификатор формируется Центром Регистрации и представляет собой целое число.

Пароль формируется Центром Регистрации и представляет собой строку символов длиной 6.

Маркер доступа, сформированный Центром Регистрации, передается пользователю либо в процессе регистрации (с использованием АРМ заочной (удаленной) регистрации) по защищенному каналу, либо сообщается пользователю администратором.

АРМ зарегистрированного пользователя с маркерным доступом, как правило, используется в двух случаях:

1. В процедуре заочной (удаленной) регистрации пользователя, после использования АРМ заочной (удаленной) регистрации;
2. В случае потери ключа аутентификации (при компрометации или в иных случаях) зарегистрированного пользователя, не имеющего возможности лично прибыть в Удостоверяющий Центр для получения ключей и сертификатов.

АРМ зарегистрированного пользователя с маркерным доступом функционирует в ОС Microsoft Windows 98 и выше (с установленным MS IE 5.0 и выше). АРМ зарегистрированного пользователя с маркерным доступом взаимодействует с Центром регистрации по протоколу HTTP(S) с односторонней (серверной) аутентификацией.

К основным функциям АРМ зарегистрированного пользователя с маркерным доступом относятся:

- Обеспечение взаимодействия с Центром Регистрации.
- Обеспечение аутентификации пользователя по паролю.
- Шифрование информации, передаваемой между пользователем и Центром Регистрации, с использованием протокола TLS с односторонней аутентификацией;
- Генерация служебных ключей пользователя.
- Создание запроса на формирование служебного сертификата пользователя.
- Печать запроса на формирование служебного сертификата пользователя.
- Обеспечение возможности получения пользователем выпущенного сертификата.

3.2.8. АРМ зарегистрированного пользователя с ключевым доступом

АРМ зарегистрированного пользователя с ключевым доступом предназначен для выполнения организационно-технических мероприятий, связанных с управлением личной ключевой информацией и сертификатами, такими как формирование рабочих ключей и сертификатов, отзыв сертификатов, установка списка отозванных сертификатов.

АРМ зарегистрированного пользователя с ключевым доступом функционирует в ОС Microsoft Windows 98 и выше (с установленным MS IE 5.0 и выше). АРМ зарегистрированного пользователя с ключевым доступом взаимодействует с Центром регистрации по протоколу HTTP(S) с двухсторонней аутентификацией.

К основным функциям АРМ пользователя относятся:

- Обеспечение взаимодействия с ЦР.
- Обеспечение возможности выбора пользователем сертификата, с помощью которого будет осуществляться взаимодействие с ЦР.
- Шифрование информации, передаваемой ЦР, с использованием протокола TLS с двусторонней аутентификацией;
- Генерация рабочих ключей пользователя.
- Создание запросов на формирование сертификатов.
- Печать запроса на формирование служебного сертификата пользователя.
- Обеспечение возможности получения пользователем выпущенных сертификатов.
- Вывод электронного сертификата открытого ключа пользователя на бумажный носитель.
- Проверка состояния запросов на формирование сертификатов.
- Создание запросов на отзыв сертификатов открытого ключа пользователя.

3.2.9. АРМ регистрации пользователей

АРМ регистрации пользователя Центра Регистрации предназначен для выполнения организационно-технических мероприятий, связанных с выполнением процедуры регистрации пользователя на Удостоверяющем Центре в режиме распределенной регистрации.

АРМ регистрации пользователя функционирует в ОС Microsoft Windows 98 и выше (с установленным MS IE 5.0 и выше). АРМ регистрации пользователя взаимодействует с Центром регистрации по протоколу HTTP(S) с односторонней аутентификацией.

К основным функциям АРМ регистрации пользователя относятся:

- Обеспечение взаимодействия с Центром Регистрации.
- Обеспечение возможности формирования и передачи запроса на регистрацию пользователя.
- Шифрование информации, передаваемой между пользователем и Центром Регистрации, с использованием протокола TLS с односторонней аутентификацией.

4. Размещение программных компонентов ПАК «КриптоПро УЦ» на технических средствах

4.1. Требования к техническим средствам компонентов ПАК «КриптоПро УЦ»

Требования к техническим средствам, на которых размещаются программные компоненты ПАК «КриптоПро УЦ», зависят от количества зарегистрированных пользователей, регламента плановой смены сертификатов открытых ключей пользователей, требований по производительности всего комплекса.

В данном документе приведены рекомендуемые минимальные требования к техническим средствам, которые обеспечивают установку и работу компонентов при 1000 пользователях.

- Центр Сертификации (выделенный сервер)
  - Процессор – Pentium IV 1 ГГц
  - Оперативная память – 512 Мбайт
  - Жесткий диск – не менее 10 Гбайт свободной памяти
- Центр Регистрации (выделенный сервер)
  - Процессор – Pentium IV 1 ГГц
  - Оперативная память – не менее 512 Мбайт
  - Жесткий диск – не менее 40 Гбайт свободной памяти
- АРМ администратора Центра Регистрации
  - Процессор – Pentium III 730 MHz
  - Оперативная память – 384 Mb
  - Жесткий диск – не менее 10 Гбайт свободной памяти
- АРМ разбора конфликтных ситуаций
  - Процессор – Pentium III 730 MHz
  - Оперативная память – 384 Mb
  - Жесткий диск – не менее 10 Гбайт свободной памяти
- Веб-приложения (АРМы пользователя) Центра Регистрации
  - Процессор – Pentium

4.2. Требования к общесистемным программным средствам компонентов ПАК «КриптоПро УЦ»

- Центр Сертификации (сервер)
  - MS Windows Server 2000 с пакетом обновлений SP4 или MS Windows Server 2003 с пакетом обновлений SP2
- Центр Регистрации (сервер)
  - MS Windows Server 2000 с пакетом обновлений SP4 или MS Windows Server 2003 с пакетом обновлений SP2
- АРМ администратора Центра Регистрации
  - Операционная система - MS Windows 2000 Professional с пакетом обновлений SP4, MS Windows Server 2000 с пакетом обновлений SP4, MS

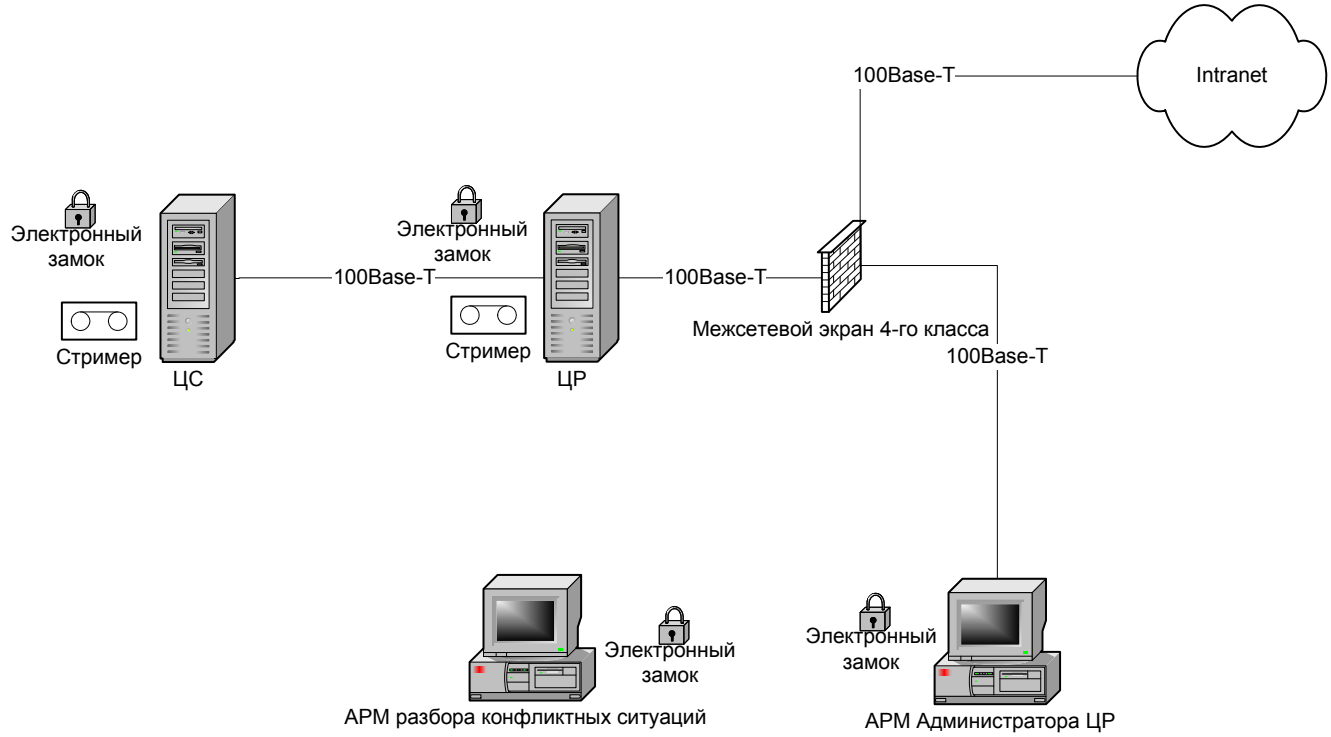
Windows Server 2003 с пакетом обновлений SP2 или MS Windows XP с пакетом обновлений SP2

- АРМ разбора конфликтных ситуаций
  - Операционная система - MS Windows 2000 Professional с пакетом обновлений SP4, MS Windows Server 2000 с пакетом обновлений SP4, MS Windows Server 2003 с пакетом обновлений SP2 или MS Windows XP с пакетом обновлений SP2
- Веб-приложения (АРМы пользователя) Центра Регистрации
  - Операционная система - MS Windows 98/Me/NT 4.0/2000/XP/2003
  - MS Internet Explorer версии 5.0 и выше

4.3. Типовая схема размещения компонентов

На Рисунок 1 приведена типовая схема размещения компонентов программного комплекса ПАК «КриптоПро УЦ» в сети предприятия.

Рисунок 1. Типовая схема размещения и взаимодействия компонентов УЦ в сети предприятия



Для защиты закрытого ключа подписи Центра сертификации Удостоверяющего центра (являющегося ключом подписи уполномоченного лица удостоверяющего центра) необходимо все непосредственно взаимодействующие с ним программно-аппаратные компоненты выделить в защищенный сегмент локальной вычислительной сети (ЛВС) предприятия.

Таким компонентом является программно-аппаратное обеспечение Центра Регистрации.

Защищенный сегмент ЛВС предприятия организуется с помощью межсетевого экрана.

4.4. Использование аппаратных криптографических модулей

Аппаратные криптографические модули (hardware security module, HSM) обеспечивают большую защищенность криптографических ключей.

В качестве указанного средства в Центре Сертификации ПАК «КриптоПро УЦ» может использоваться сертифицированный программно-аппаратный криптографический модуль. Данный модуль в первую очередь предназначен для обеспечения безопасного хранения и использования закрытого ключа уполномоченного лица удостоверяющего центра, что обеспечивается выполнением всех криптографических операций, в том числе по генерации ключа уполномоченного лица.

Защита ключа уполномоченного лица удостоверяющего центра обеспечивается в том числе с использованием "раздельных секретов", то есть для активизации закрытого ключа одновременно необходимы три из пяти дополнительных закрытых ключей, хранящихся на процессорных картах РИК (российская интеллектуальная карта). Кроме этого, взаимодействие Центра Сертификации с криптомодулем возможно только после двусторонней криптографической аутентификации.

4.5. Размещение компонентов на одном выделенном сервере

В случае, если ПАК «КриптоПро УЦ» установлен и эксплуатируется в изолированном режиме и не имеет сетевых соединений, выходящих за контролируемую зону, допускается установка компонентов Центра Сертификации и Центра Регистрации (а при необходимости и АРМ администратора ЦР) на один выделенный компьютер (сервер).

При установке компонентов на один компьютер есть ряд особенностей, а именно:

1. Установка Центра Сертификации выполняется в полном соответствии с «Руководством по установке».
2. Установка Центра Регистрации в целом осуществляется в соответствии с «Руководством по установке» за исключением того, что не должны выполняться следующие пункты:
    a. Установка СКЗИ КриптоПро CSP и КриптоПро TLS;
    b. Установка Microsoft Internet Information Services;
    c. Установка службы очереди сообщений;
    d. Выпуск и инсталляция сертификата серверной аутентификации Web-сервера ЦР.

4.6. Схема взаимодействия компонентов

Схема взаимодействия компонентов Центра Сертификации Удостоверяющего Центра приведена на Рисунок 2

Схема взаимодействия компонентов Центра Регистрации Удостоверяющего Центра приведена на Рисунок 3

Рисунок 2. Схема взаимодействия компонентов Центра Сертификации

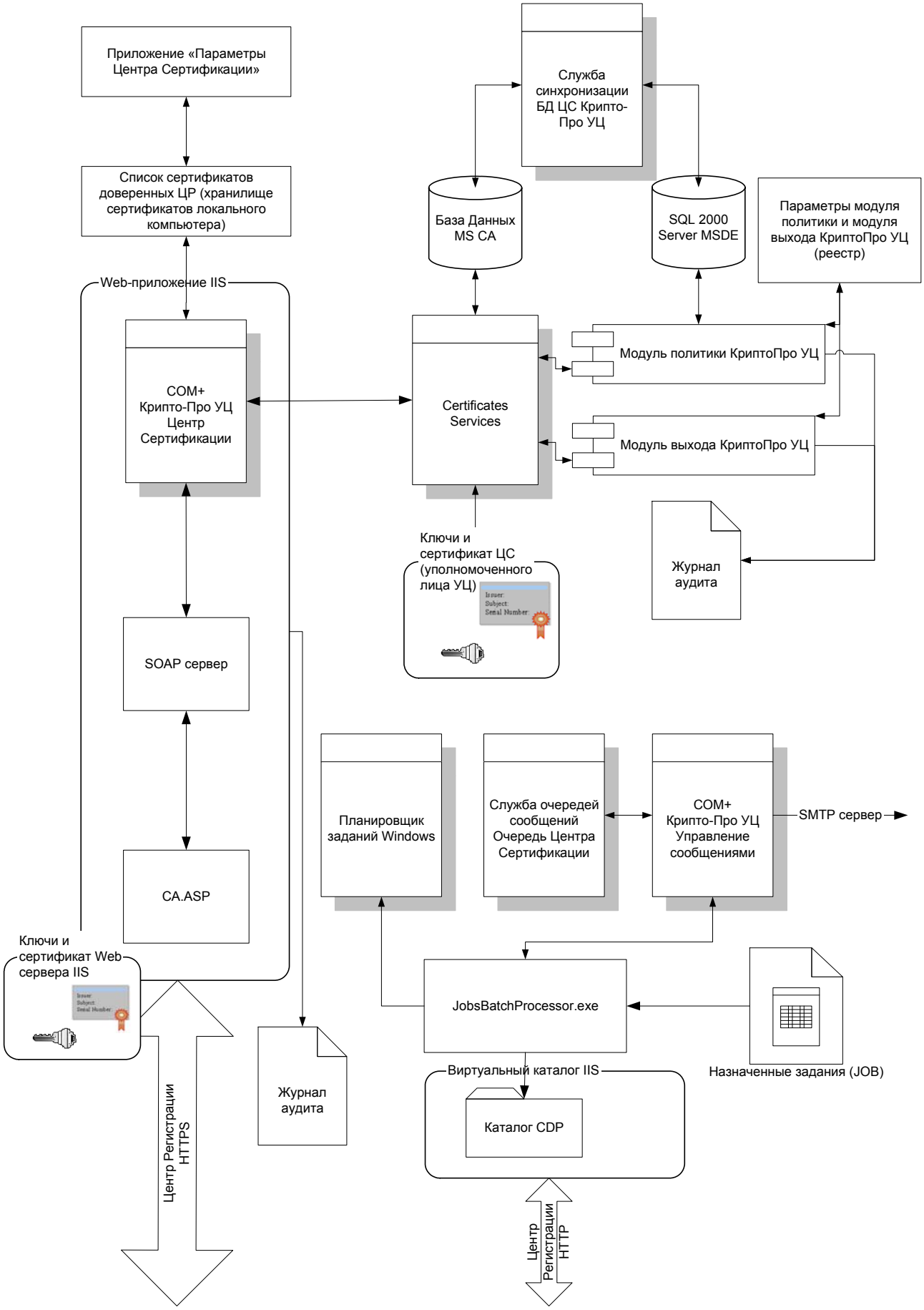
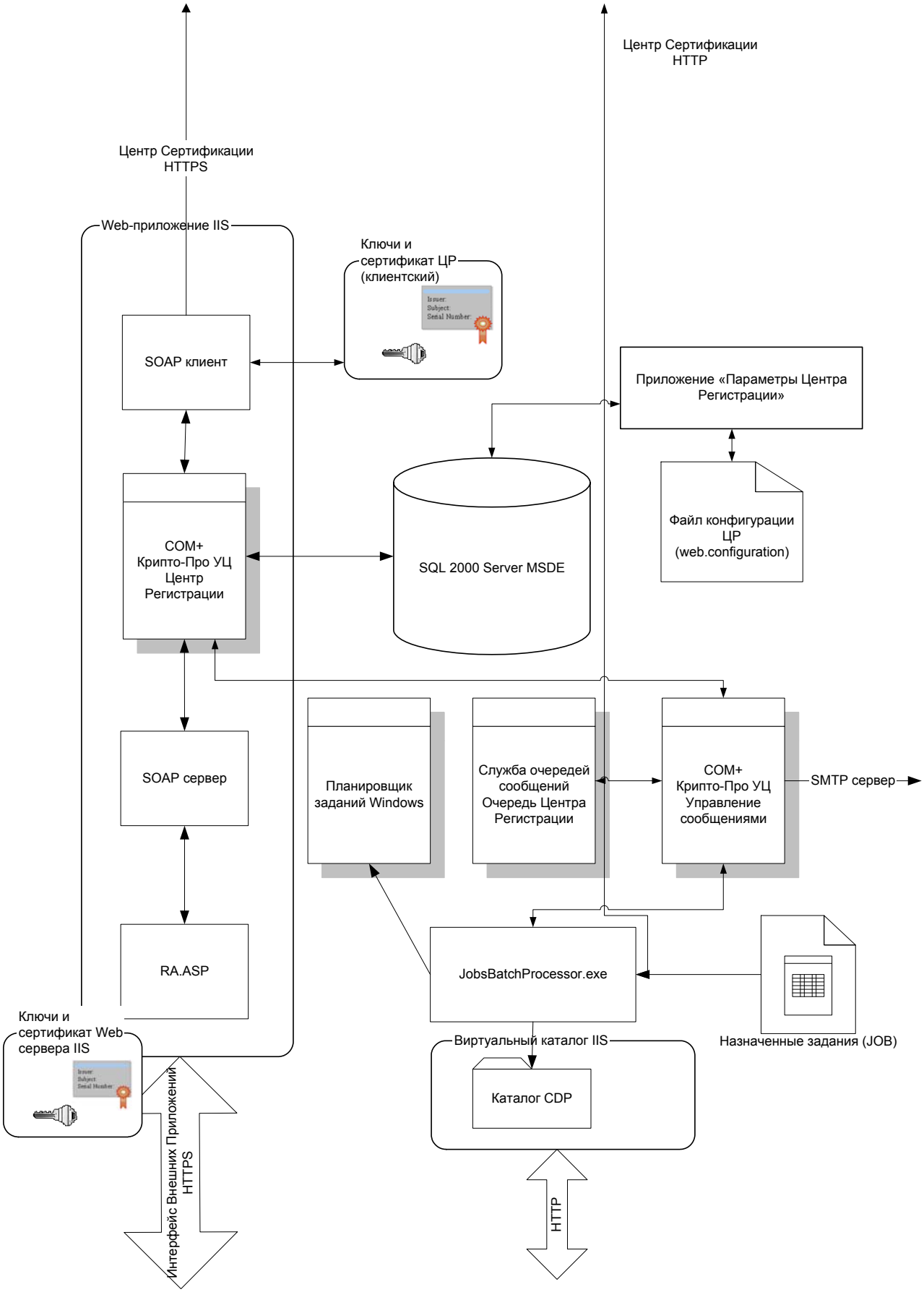


Рисунок 3. Схема взаимодействия компонентов Центра Регистрации



5. Ограничения при эксплуатации ПАК «КриптоПро УЦ»

5.1. Лицензионные ограничения на ПАК «КриптоПро УЦ»

Установка и эксплуатация компонентов ПАК «КриптоПро УЦ» должна производится на основании лицензий, выданных производителем или поставщиком продукта.

В ПАК «КриптоПро УЦ» имеется два вида лицензии на компоненты:

- лицензия на стандартную версию продукта (стандартная лицензия);
- лицензия на расширенную версию продукта (расширенная лицензия).

Стандартная лицензия предоставляет право установки и эксплуатации одной копии компонента продукта в соответствии с указанными в ней ограничениями без права изменения отдельных параметров конфигурации программного обеспечения компонента, определенного производителем по умолчанию.

Расширенная лицензия предоставляет право установки и эксплуатации одной копии компонента продукта в соответствии с указанными в ней ограничениями с правом изменения параметров конфигурации программного обеспечения компонента, определенного производителем по умолчанию.

Для рабочих мест пользователей УЦ не требуется наличие лицензий ПАК «КриптоПро УЦ». Они должны обеспечиваться лицензиями СКЗИ КриптоПро CSP, не входящих в состав ПАК «КриптоПро УЦ».

5.1.1. Лицензия Центра Сертификации

Параметры конфигурации, запрещаемые для изменения в стандартной лицензии:

- Параметры модуля политики КриптоПро УЦ:
- Параметры модуля выхода КриптоПро УЦ:

Ограничения лицензии:

- Наименование организации;
- Количество пользователей УЦ, являющихся владельцами сертификатов открытых ключей, изданных данным Центром Сертификации;
- Срок действия лицензии.

Производитель продукта в лице ООО «Крипто-Про» (г. Москва) предоставляет с каждой копией Центра Сертификации для ознакомления стандартную лицензию сроком действия 1 (один) месяц до 100 (сто) пользователей.

Учет зарегистрированных пользователей осуществляется на Центре сертификации ПАК «КриптоПро УЦ». Счетчик зарегистрированных пользователей увеличивается на единицу только в случае одновременного выполнения следующих условий:

- При изготовлении сертификата открытого ключа идентификационные данные пользователя, для которого изготавливается сертификат, отличны от идентификационных данных пользователей, для которых уже были изготовлены сертификаты;
- При изготовлении сертификата открытого ключа запрос на изготовление сертификата открытого ключа не содержит область использования - «Временный доступ к Центру регистрации» (OID 1.2.643.2.2.34.2).

Удаление пользователя средствами АРМ администратора Центра регистрации влечет удаление соответствующей учетной записи только в базе данных Центра регистрации. Соответственно, на Центре сертификации значение счетчика зарегистрированных пользователей остается прежним и не уменьшается.

При необходимости зарегистрировать нового пользователя и изготовить для него сертификат открытого ключа для проведения тестов (зарегистрировать тестового пользователя), в данный сертификат в расширение «Улучшенный ключ» (Extended Key Usage) потребуется занести область использования «Временный доступ к Центру регистрации» (OID 1.2.643.2.2.34.2) в дополнение к необходимым для выполнения тестовых задач областям. Счетчик зарегистрированных пользователей в данном случае не увеличится.

5.1.2. Лицензия Центра Регистрации

Параметры конфигурации, запрещаемые для изменения в стандартной лицензии:

- Политики обработки подписанных и неподписанных запросов;
- Политика имен;
- Системные роли;
- Шаблоны писем;
- Параметры модуля экспорта сертификатов;
- Параметры доступа к методам на вкладке **Безопасность**;
- Параметры регламентных заданий;
- Параметры веб-интерфейса.

Ограничения лицензии:

- Наименование организации;
- Срок действия лицензии.

Производитель продукта в лице ООО «Крипто-Про» (г. Москва) предоставляет с каждой копией Центра Регистрации для ознакомления стандартную лицензию сроком действия 1 (один) месяц.

5.1.3. Лицензия АРМ администратора Центра Регистрации

Для указанного компонента существуют только расширенные лицензии без ограничений.

Производитель продукта в лице ООО «Крипто-Про» (г. Москва) предоставляет с каждой копией АРМ администратора Центра Регистрации для ознакомления лицензию сроком действия 1 (один) месяц.

5.1.4. Лицензия АРМ разбора конфликтных ситуаций

Для указанного компонента существуют только расширенные лицензии без ограничений.

Производитель продукта в лице ООО «Крипто-Про» (г. Москва) предоставляет с каждой копией АРМ разбора конфликтных ситуаций для ознакомления лицензию сроком действия 1 (один) месяц.

5.2. Ограничения по конфигурации общесистемного программного обеспечения

Для обеспечения требований по безопасности эксплуатации не рекомендуется устанавливать Центр Сертификации ПАК «КриптоПро УЦ» на контроллер домена или на сервер, подключенный к домену (Active Directory).

Примечание: При установке Центра Сертификации ПАК «КриптоПро УЦ» на Windows 2003 Server, являющийся контроллером домена или подключенный к домену:

1. **В случае, если это подчинённый ЦС - по умолчанию в запрос на сертификат ЦС добавляются компоненты доменного имени компьютера, и такой запрос невозможно будет обработать и выпустить сертификат устанавливаемого подчиненного ЦС на вышестоящем ПАК «КриптоПро УЦ».**

2. В случае, если это корневой ЦС - по умолчанию в сертификат ЦС добавляются компоненты доменного имени компьютера, и в дальнейшем будет невозможно выпустить кросс-сертификат этого ЦС на другом ПАК «КриптоПро УЦ».

Сервер Центра Регистрации ПАК «КриптоПро УЦ» может являться контроллером домена или может быть подключен к домену (Active Directory).

Сервера Центра Сертификации и/или Центра Регистрации, после установки программного обеспечения ПАК «КриптоПро УЦ», категорически запрещается переименовывать, отключать или подключать к домену.

При использовании нелокализованной (International) версии операционной системы Windows 2000 в языковых параметрах операционной системы должна быть выбрана кириллица и в качестве языка системы по умолчанию должен быть выбран русский язык. Данные установки производятся в приложении **Панель управления->Язык и стандарты**.

Категорически запрещается:

- Выполнять смену сертификата аутентификации сервера веб-узла Центра Сертификации и/или Центра регистрации с отклонениями от соответствующего описания в руководствах по установке и эксплуатации указанных компонентов ПАК «КриптоПро УЦ», особенно в части выбора опции **заменить сертификат** при изменении назначения сертификата Мастера сертификатов IIS;
- Выполнять смену паролей учетных записей CPCAComPlusAcct& и/или CPRAComPlusAcct&, предварительно не ознакомившись с соответствующими разделами в руководствах по установке и эксплуатации Центра Сертификации и/или Центра регистрации ПАК «КриптоПро УЦ»;
- Включать и использовать IP-фильтрацию внутренних пакетов серверов Центра Сертификации и/или Центра регистрации;
- Изменять настройки веб-узлов Центра Сертификации и/или Центра Регистрации после установки программного обеспечения соответствующих компонентов ПАК «КриптоПро УЦ».

5.3. Ограничения при эксплуатации ПАК «КриптоПро УЦ»

ПАК «КриптоПро УЦ» не позволяет издавать сертификаты ключей подписи, содержащие более 100 областей использования сертификата в расширении EKU (сведений об отношениях при которых электронный документ имеет юридическую силу). Это связано с особенностями MS CryptoAPI 2.0 на платформах MS Windows 9x/NT/Millennium/2000. Программное обеспечение ПАК «КриптоПро УЦ» технически препятствует созданию и обработке запроса на сертификат, содержащего более 100 расширений EKU. Тем не менее рекомендуется в организационных и распорядительных документах деятельности удостоверяющего центра и информационных систем учитывать данное ограничение.

6. Режимы работы Удостоверяющего центра

6.1. Режимы регистрации пользователей Удостоверяющего Центра

ПАК «КриптоПро УЦ» обеспечивает реализацию следующих режимов регистрации пользователей:

6.1.1. Централизованный режим

При централизованном режиме регистрации, идентификация пользователя осуществляется администратором Удостоверяющего Центра на основании документов, удостоверяющих личность пользователя, при личном прибытии регистрируемого пользователя в УЦ.

Администратор с использованием ПО АРМ администратора Центра Регистрации формирует запрос на регистрацию в электронной форме от имени пользователя и принимает его.

6.1.2. Распределенный режим

Распределенный режим регистрации пользователя является опциональным режимом и используется при невозможности (по разным причинам, в том числе и по причине экономической целесообразности) регистрации пользователей в централизованном режиме.

Идентификация пользователя осуществляется нотариусом путем совершения нотариальных действий при заверении заявления на регистрацию пользователя, на основании документов, удостоверяющих личность пользователя.

С помощью ПО АРМ регистрации пользователя регистрируемые пользователи формируют запрос на регистрацию в электронной форме.

Регистрация пользователя в распределенном режиме на УЦ осуществляется администратором Удостоверяющего Центра на основании нотариально заверенного заявления на регистрацию и запроса на регистрацию в электронной форме путем принятия запроса на регистрацию в электронной форме.

При реализации распределенного режима регистрации пользователей увеличивается риск сетевой DoS-атаки (более подробно о данном виде сетевой атаки рассматривается в документе «КриптоПро УЦ. Руководство по безопасности»), заключающейся в многократном увеличении поступающих на Центр регистрации запросов на регистрацию пользователей. В данном случае необходимо обеспечить настройку выполнения Задания «Оповещение администратора о количестве необработанных запросов» (более подробное описание настроек Задания «Оповещение администратора о количестве необработанных запросов» приведено в документе «КриптоПро УЦ. Центр регистрации. Руководство по эксплуатации»), с учетом приемлемого для эксплуатирующей организации времени реакции на данную атаку. Задание «Оповещение администратора о количестве необработанных запросов» обеспечивает предоставление администратору Удостоверяющего центра (администратору безопасности) информации о количестве находящихся в очереди на обработке запросов на регистрацию, изготовление сертификата и т.д.

6.2. Управление ключами и сертификатами открытых ключей пользователей Удостоверяющего Центра

6.2.1. Централизованный режим

Пользователи УЦ получают ключи и сертификаты открытых ключей у ответственного сотрудника (администратора) УЦ.

Администратор выполняет процедуры генерации ключей и сертификатов пользователей на своем рабочем месте с использованием ПО АРМ администратора Центра Регистрации.

Управление сертификатами пользователей в течение их жизненного цикла, также осуществляется администратором УЦ.

6.2.2. Распределенный режим

Пользователи Удостоверяющего Центра самостоятельно осуществляют процедуру генерации ключей и формирование запросов на сертификат открытого ключа.

Выполнение этих процедур осуществляется с использованием АРМ зарегистрированного пользователя на рабочем месте.

Поступающие запросы на сертификаты открытых ключей пользователей обрабатываются администратором УЦ с использованием АРМ администратора Центра Регистрации.

Установку на рабочем месте выпущенных сертификатов открытых ключей пользователь осуществляет также с использованием АРМ зарегистрированного пользователя. На АРМ зарегистрированного пользователя предоставляется возможность осуществить формирование запроса на отзыв (приостановление/возобновление действия) сертификатов открытых ключей.

6.3. Режимы работы Удостоверяющего Центра

Режимы работы Удостоверяющего Центра основаны на комбинациях режимов регистрации пользователей и управления ключами и сертификатами.

6.3.1. Регистрация пользователей в централизованном режиме по «не доверенной» схеме и распределенное управление ключами и сертификатами пользователя

«Не доверенная» схема означает, что пользователь не доверяет ключам, полученным от сотрудника УЦ.

Ниже, под служебным сертификатом понимается сертификат открытого ключа, ограниченный по области использования и с коротким сроком действия. Для такого сертификата технологически в ПАК «КриптоПро УЦ» заведен идентификатор «Временный сертификат».

Общий алгоритм схемы выглядит следующим образом:

- Администратор («оператор») с использованием ПО АРМ администратора Центра Регистрации формирует запрос на регистрацию в электронной форме от имени пользователя и принимает его.
- Администратор («оператор») с использованием ПО АРМ администратора Центра Регистрации изготавливает и передает пользователю на ключевом носителе его служебные закрытый ключ и сертификат.
- С использованием служебного закрытого ключа и сертификата пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом производит со своего рабочего места двустороннюю аутентификацию при установлении соединения с сервером ЦР и формирует запрос на сертификат и ставит его в очередь на обработку в Центр Регистрации.
- Администратор («администратор») с использованием ПО АРМ администратора Центра Регистрации обрабатывает (принимает) стоящий в очереди запрос на сертификат.
- Пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом получает сертификат на рабочие ключи, изготовленные им на своем рабочем месте, и устанавливает его.
- Пользователь использует рабочие ключи и сертификат в информационной системе.

- С использованием рабочего закрытого ключа и сертификата пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом производит со своего рабочего места двустороннюю аутентификацию при установлении соединения с сервером ЦР и формирует запрос на новый рабочий сертификат и ставит его в очередь на обработку в Центр Регистрации.
- Администратор («администратор») с использованием ПО АРМ администратора Центра Регистрации обрабатывает (принимает) стоящий в очереди запрос на сертификат.
- Пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом получает сертификат на новые рабочие ключи, изготовленные им на своем рабочем месте, и устанавливает его.
- Пользователь использует новые рабочие ключи и сертификат в информационной системе.

При этом регистрация пользователей и изготовление служебного сертификата осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «оператор», а обработка запроса на сертификат осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «администратор».

Для реализации данного режима нужно выполнить следующие настройки:

На АРМ администратора:

- Настроить параметры выбора CSP (алгоритмы). Рекомендуется включить флаг пометки ключевых контейнеров как экспортируемые
- Откорректировать файл шаблона печати сертификата Cert.xsl в соответствии с корпоративными требованиями оформления внешнего вида печатной копии сертификата пользователей, при их печати через АРМ администратора ЦР

На Центре Сертификации

- Настроить срок действия служебного сертификата, путем установки нужного срока для идентификатора «Временный доступ к Центру Регистрации» в модуле политики Крипто-Про УЦ службы сертификации

На Центре Регистрации

- Выполнить полную установку ПО Центра Регистрации
- Откорректировать файл шаблона печати сертификата Cert.xsl (в каталоге UI) в соответствии с корпоративными требованиями оформления внешнего вида печатной копии сертификата пользователей, при их печати через АРМ пользователя
- Откорректировать файл шаблона печати запроса на сертификат Request.xsl (в каталоге UI) в соответствии с корпоративными требованиями оформления внешнего вида печатной копии запроса на сертификат пользователей, при их печати через АРМ пользователя
- На вкладке "Web-интерфейс" окна свойств узла Центра регистрации приложения «Параметры Центра Регистрации» настроить параметры, определяющие выбор CSP и CSP по умолчанию, а также режим возможности поиска сертификатов других пользователей. Значения данных параметров определяются владельцем УЦ.
- Отключить автоматическую обработку запросов на регистрацию и запросов на сертификат для АРМов пользователя (Веб-приложений). Для этого установить в 0 значения параметров RegReqAutoAccept и CertReqAutoAccept на вкладке "Web-интерфейс" окна свойств узла Центра регистрации приложения «Параметры Центра Регистрации»

- Настроить политику обработки подписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Временный сертификат» (определить список областей использования рабочего сертификата);
- Настроить политику обработки неподписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Оператор» (определить список областей использования служебного сертификата);
- Настроить политику обработки подписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Пользователь Центра Регистрации» (определить список областей использования рабочего сертификата);
- Настроить матрицу прав доступа на вкладке «Безопасность» окна свойств приложения «Параметры Центра Регистрации»
    - Для роли «Администратор»

№	Наименование объекта	Наименование действия	Разрешение	
			Выполнение	Делегирование
1	Admin.GetCertTemplates	Получить шаблоны сертификатов	+	
2	Admin.GetGrantedNameProperties	Получить ограничения на имена DN	+	
3	Admin.GetLogEventTypes	Получить коды событий журнала событий	+	
4	Admin.GetLogRecords	Получить список сообщений журнала событий	+	
5	Admin.PublishCRL	Отправить запрос на публикацию СОС	+	
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат	+	+
7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат	+	
8	CertRequest.ConfirmRequest	Подтвердить получение сертификата	+	+
9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу	+	+
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат	+	+
11	CertRequest.GetFirstCertRequestInfo	Получить информацию о запросе на сертификат по коду запроса на регистрацию	+	+
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат	+	+
13	CertRequest.GetRequestsList	Получить список запросов на сертификат	+	+
14	CertRequest.SetReq	Изменить информацию о	+	+

	uestInfo	запросе на сертификат		
15	CertRequest.Submit FirstCertRequest	Отправить неподписанный запрос на сертификат		
16	CertRequest.Submit Request	Отправить подписанный запрос на сертификат	+	
17	CertView.ConvertPK CS2XML	Получить сертификат в виде XML	+	
18	CertView.GetCACerti ficate	Получить сертификат Центра Сертификации	+	
19	CertView.GetCertific atesList	Получить список сертификатов	+	+
20	CertView.GetCertific ateInfo	Получить информацию о сертификате	+	+
21	CertView.GetCRL	Получить список отозванных сертификатов (СОС)	+	
22	Registration.AcceptR equest	Одобрить создание пользователя по запросу на регистрацию		
23	Registration.CreateC ertRequest	Извлечь запрос на сертификат из запроса на регистрацию		
24	Registration.CreateR equest	Отправить запрос на регистрацию пользователя самим пользователем		
25	Registration.CreateR equestByAdmin	Отправить запрос на регистрацию пользователя администратором		
26	Registration.DenyRe quest	Отклонить запрос на регистрацию		
27	Registration.GetReq uestInfo	Получить информацию о запросе на регистрацию	+	+
28	Registration.GetReq uestsList	Получить список запросов на регистрацию	+	+
29	Registration.SetReq uestInfo	Изменить информацию о запросе на регистрацию	+	
30	RevokeRequest.Acce ptRequest	Одобрить запрос на отзыв сертификата	+	+
31	RevokeRequest.Den yRequest	Отклонить запрос на отзыв сертификата	+	+
32	RevokeRequest.GetR equestInfo	Получить информацию о запросе на отзыв сертификата	+	+
33	RevokeRequest.GetR equestsList	Получить список запросов на отзыв сертификата	+	+
34	RevokeRequest.SetR equestInfo	Изменить информацию о запросе на отзыв сертификата	+	+
35	RevokeRequest.Sub mitRequest	Отправить запрос на отзыв сертификата	+	+
36	RevokeRequest.Sub	Отправить запрос на приостановление действия	+	+

	mitHoldRequest	сертификата		
37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата	+	+
38	UserView.AddDocument	Добавить документ пользователя	+	+
39	UserView.GetDocumentInfo	Получить информацию о документе пользователя	+	+
40	UserView.GetDocumentsList	Получить список документов пользователя	+	+
41	UserView.GetUserByCertificate	Найти идентификатор пользователя по сертификату	+	+
42	UserView.GetUserInfo	Получить информацию о пользователе	+	+
43	UserView.GetUsersList	Получить список пользователей	+	+
44	UserView.RemoveDocument	Удалить документ пользователя	+	+
45	UserView.SetUserInfo	Изменить информацию о пользователе	+	
46	UserView.DeleteUser	Удалить пользователя		
47	Admin.CreateTokenForUser	Создать маркер временного доступа	+	+

- Для роли «Оператор»

№	Наименование объекта	Наименование действия	Разрешение	
			Выполнение	Делегирование
1	Admin.GetCertTemplates	Получить шаблоны сертификатов	+	
2	Admin.GetGrantedNameProperties	Получить ограничения на имена DN	+	
3	Admin.GetLogEventTypes	Получить коды событий журнала событий	+	
4	Admin.GetLogRecords	Получить список сообщений журнала событий	+	
5	Admin.PublishCRL	Отправить запрос на публикацию СОС		
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат	+	
7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат	+	+
8	CertRequest.Confirm	Подтвердить получение	+	+

	Request	сертификата		
9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу		
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат	+	+
11	CertRequest.GetFirstCertRequestInfo	Получить информацию о запросе на сертификат по коду запроса на регистрацию	+	+
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат	+	+
13	CertRequest.GetRequestsList	Получить список запросов на сертификат	+	+
14	CertRequest.SetRequestInfo	Изменить информацию о запросе на сертификат	+	+
15	CertRequest.SubmitFirstCertRequest	Отправить неподписанный запрос на сертификат	+	+
16	CertRequest.SubmitRequest	Отправить подписанный запрос на сертификат	+	
17	CertView.ConvertPKCS2XML	Получить сертификат в виде XML	+	
18	CertView.GetCACertificate	Получить сертификат Центра Сертификации	+	
19	CertView.GetCertificatesList	Получить список сертификатов	+	+
20	CertView.GetCertificateInfo	Получить информацию о сертификате	+	+
21	CertView.GetCRL	Получить список отозванных сертификатов (СОС)	+	
22	Registration.AcceptRequest	Одобрить создание пользователя по запросу на регистрацию	+	+
23	Registration.CreateCertRequest	Извлечь запрос на сертификат из запроса на регистрацию	+	+
24	Registration.CreateRequest	Отправить запрос на регистрацию пользователя самим пользователем		
25	Registration.CreateRequestByAdmin	Отправить запрос на регистрацию пользователя администратором	+	
26	Registration.DenyRequest	Отклонить запрос на регистрацию	+	+
27	Registration.GetRequestInfo	Получить информацию о запросе на регистрацию	+	+
28	Registration.GetRequestsList	Получить список запросов на регистрацию	+	+
29	Registration.SetRequestInfo	Изменить информацию о запросе на регистрацию	+	+

30	RevokeRequest.AcceptRequest	Одобрить запрос на отзыв сертификата		
31	RevokeRequest.DenyRequest	Отклонить запрос на отзыв сертификата		
32	RevokeRequest.GetRequestInfo	Получить информацию о запросе на отзыв сертификата	+	+
33	RevokeRequest.GetRequestsList	Получить список запросов на отзыв сертификата	+	+
34	RevokeRequest.SetRequestInfo	Изменить информацию о запросе на отзыв сертификата	+	
35	RevokeRequest.SubmitRequest	Отправить запрос на отзыв сертификата	+	
36	RevokeRequest.SubmitHoldRequest	Отправить запрос на приостановление действия сертификата	+	
37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата	+	
38	UserView.AddDocument	Добавить документ пользователя	+	+
39	UserView.GetDocumentInfo	Получить информацию о документе пользователя	+	+
40	UserView.GetDocumentsList	Получить список документов пользователя	+	+
41	UserView.GetUserByCertificate	Найти идентификатор пользователя по сертификату	+	+
42	UserView.GetUserInfo	Получить информацию о пользователе	+	+
43	UserView.GetUsersList	Получить список пользователей	+	+
44	UserView.RemoveDocument	Удалить документ пользователя	+	+
45	UserView.SetUserInfo	Изменить информацию о пользователе	+	+
46	UserView.DeleteUser	Удалить пользователя	+	+
47	Admin.CreateTokenForUser	Создать маркер временного доступа		

- Для роли «Временный сертификат»

№	Наименование объекта	Наименование действия	Разрешение	
			Выполнение	Делегирование
1	Admin.GetCertTemplates	Получить шаблоны сертификатов	+	
2	Admin.GetGrantedN	Получить ограничения на	+	

	ameProperties	имена DN		
3	Admin.GetLogEventTypes	Получить коды событий журнала событий		
4	Admin.GetLogRecords	Получить список сообщений журнала событий		
5	Admin.PublishCRL	Отправить запрос на публикацию СОС		
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат		
7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат		
8	CertRequest.ConfirmRequest	Подтвердить получение сертификата	+	
9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу		
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат	+	
11	CertRequest.GetFirstCertRequestInfo	Получить информацию о запросе на сертификат по коду запроса на регистрацию		
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат	+	
13	CertRequest.GetRequestsList	Получить список запросов на сертификат	+	
14	CertRequest.SetRequestInfo	Изменить информацию о запросе на сертификат	+	
15	CertRequest.SubmitFirstCertRequest	Отправить неподписанный запрос на сертификат		
16	CertRequest.SubmitRequest	Отправить подписанный запрос на сертификат	+	
17	CertView.ConvertPKCS2XML	Получить сертификат в виде XML	+	
18	CertView.GetCACertificate	Получить сертификат Центра Сертификации	+	
19	CertView.GetCertificatesList	Получить список сертификатов	+	
20	CertView.GetCertificateInfo	Получить информацию о сертификате	+	
21	CertView.GetCRL	Получить список отозванных сертификатов (СОС)	+	
22	Registration.AcceptRequest	Одобрить создание пользователя по запросу на регистрацию		
23	Registration.CreateCertRequest	Извлечь запрос на сертификат из запроса на регистрацию		

24	Registration.CreateRequest	Отправить запрос на регистрацию пользователя самим пользователем		
25	Registration.CreateRequestByAdmin	Отправить запрос на регистрацию пользователя администратором		
26	Registration.DenyRequest	Отклонить запрос на регистрацию		
27	Registration.GetRequestInfo	Получить информацию о запросе на регистрацию		
28	Registration.GetRequestsList	Получить список запросов на регистрацию		
29	Registration.SetRequestInfo	Изменить информацию о запросе на регистрацию		
30	RevokeRequest.AcceptRequest	Одобрить запрос на отзыв сертификата		
31	RevokeRequest.DenyRequest	Отклонить запрос на отзыв сертификата		
32	RevokeRequest.GetRequestInfo	Получить информацию о запросе на отзыв сертификата	+	
33	RevokeRequest.GetRequestsList	Получить список запросов на отзыв сертификата	+	
34	RevokeRequest.SetRequestInfo	Изменить информацию о запросе на отзыв сертификата		
35	RevokeRequest.SubmitRequest	Отправить запрос на отзыв сертификата		
36	RevokeRequest.SubmitHoldRequest	Отправить запрос на приостановление действия сертификата		
37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата		
38	UserView.AddDocument	Добавить документ пользователя		
39	UserView.GetDocumentInfo	Получить информацию о документе пользователя		
40	UserView.GetDocumentsList	Получить список документов пользователя		
41	UserView.GetUserByCertificate	Найти идентификатор пользователя по сертификату	+	
42	UserView.GetUserInfo	Получить информацию о пользователе	+	
43	UserView.GetUsersList	Получить список пользователей		
44	UserView.RemoveDocument	Удалить документ пользователя		
45	UserView.SetUserInfo	Изменить информацию о пользователе		

46	UserView.DeleteUser	Удалить пользователя		
47	Admin.CreateTokenForUser	Создать маркер временного доступа		

- Для роли «Пользователь Центра Регистрации»

№	Наименование объекта	Наименование действия	Разрешение	
			Выполнение	Делегирование
1	Admin.GetCertTemplates	Получить шаблоны сертификатов	+	
2	Admin.GetGrantedNameProperties	Получить ограничения на имена DN	+	
3	Admin.GetLogEventTypes	Получить коды событий журнала событий		
4	Admin.GetLogRecords	Получить список сообщений журнала событий		
5	Admin.PublishCRL	Отправить запрос на публикацию СОС		
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат		
7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат		
8	CertRequest.ConfirmRequest	Подтвердить получение сертификата	+	
9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу		
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат	+	
11	CertRequest.GetFirstCertRequestInfo	Получить информацию о запросе на сертификат по коду запроса на регистрацию		
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат	+	
13	CertRequest.GetRequestsList	Получить список запросов на сертификат	+	
14	CertRequest.SetRequestInfo	Изменить информацию о запросе на сертификат	+	
15	CertRequest.SubmitFirstCertRequest	Отправить неподписанный запрос на сертификат		
16	CertRequest.SubmitRequest	Отправить подписанный запрос на сертификат	+	
17	CertView.ConvertPKCS2XML	Получить сертификат в виде XML	+	

18	CertView.GetCACertificate	Получить сертификат Центра Сертификации	+	
19	CertView.GetCertificatesList	Получить список сертификатов	+	+
20	CertView.GetCertificateInfo	Получить информацию о сертификате	+	+
21	CertView.GetCRL	Получить список отозванных сертификатов (СОС)	+	
22	Registration.AcceptRequest	Одобрить создание пользователя по запросу на регистрацию		
23	Registration.CreateCertRequest	Извлечь запрос на сертификат из запроса на регистрацию		
24	Registration.CreateRequest	Отправить запрос на регистрацию пользователя самим пользователем		
25	Registration.CreateRequestByAdmin	Отправить запрос на регистрацию пользователя администратором		
26	Registration.DenyRequest	Отклонить запрос на регистрацию		
27	Registration.GetRequestInfo	Получить информацию о запросе на регистрацию		
28	Registration.GetRequestsList	Получить список запросов на регистрацию		
29	Registration.SetRequestInfo	Изменить информацию о запросе на регистрацию		
30	RevokeRequest.AcceptRequest	Одобрить запрос на отзыв сертификата		
31	RevokeRequest.DenyRequest	Отклонить запрос на отзыв сертификата		
32	RevokeRequest.GetRequestInfo	Получить информацию о запросе на отзыв сертификата	+	
33	RevokeRequest.GetRequestsList	Получить список запросов на отзыв сертификата	+	
34	RevokeRequest.SetRequestInfo	Изменить информацию о запросе на отзыв сертификата	+	
35	RevokeRequest.SubmitRequest	Отправить запрос на отзыв сертификата	+	
36	RevokeRequest.SubmitHoldRequest	Отправить запрос на приостановление действия сертификата	+	
37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата	+	
38	UserView.AddDocument	Добавить документ пользователя		
39	UserView.GetDocum	Получить информацию о		

	entInfo	документе пользователя		
40	UserView.GetDocumentsList	Получить список документов пользователя		
41	UserView.GetUserByCertificate	Найти идентификатор пользователя по сертификату	+	
42	UserView.GetUserInfo	Получить информацию о пользователе	+	
43	UserView.GetUsersList	Получить список пользователей		
44	UserView.RemoveDocument	Удалить документ пользователя		
45	UserView.SetUserInfo	Изменить информацию о пользователе		
46	UserView.DeleteUser	Удалить пользователя		
47	Admin.CreateTokenForUser	Создать маркер временного доступа		

6.3.2. Регистрация пользователей в централизованном режиме по «доверенной» схеме и распределенное управление ключами и сертификатами пользователя

Допускается изготовление и передача пользователю рабочих ключей и сертификата открытого ключа при регистрации в централизованном режиме. Этот режим используется, когда пользователь по каким-либо причинам доверяет ключам, выданным ему сотрудником УЦ.

Т.к. схема «доверенная» то, в отличие от предыдущего режима, необходимость в служебном сертификате отпадает.

Общий алгоритм схемы выглядит следующим образом:

- Администратор («оператор») с использованием ПО АРМ администратора Центра Регистрации формирует запрос на регистрацию в электронной форме от имени пользователя и принимает его.
- Администратор («оператор») с использованием ПО АРМ администратора Центра Регистрации изготавливает и передает пользователю на ключевом носителе его рабочий закрытый ключ и сертификат.
- Пользователь использует рабочие ключи и сертификат в информационной системе.
- С использованием рабочего закрытого ключа и сертификата пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом производит со своего рабочего места двустороннюю аутентификацию при установлении соединения с сервером ЦР и формирует запрос на новый рабочий сертификат и ставит его в очередь на обработку в Центр Регистрации.
- Администратор («администратор») с использованием ПО АРМ администратора Центра Регистрации обрабатывает (принимает) стоящий в очереди запрос на сертификат.
- Пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом получает сертификат на новые рабочие ключи, изготовленные им на своем рабочем месте, и устанавливает его.
- Пользователь использует новые рабочие ключи и сертификат в информационной системе.

При этом регистрация пользователей и изготовление первого рабочего сертификата осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «оператор», а обработка запроса на новый рабочий сертификат осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «администратор».

Для реализации данного режима нужно выполнить следующие настройки:

На АРМ администратора:

- Настроить параметры выбора CSP (алгоритмы). Рекомендуется включить флаг пометки ключевых контейнеров как экспортируемые
- Откорректировать файл шаблона печати сертификата Cert.xsl в соответствии с корпоративными требованиями оформления внешнего вида печатной копии сертификата пользователей, при их печати через АРМ администратора ЦР

На Центре Сертификации

- Удалить идентификатор «Временный доступ к Центру Регистрации» в модуле политики Крипто-Про УЦ службы сертификации из списка допустимых областей использования

На Центре Регистрации

- Выполнить полную установку ПО Центра Регистрации
- Откорректировать файл шаблона печати сертификата Cert.xsl (в каталоге UI) в соответствии с корпоративными требованиями оформления внешнего вида печатной копии сертификата пользователей, при их печати через АРМ пользователя
- Откорректировать файл шаблона печати запроса на сертификат Request.xsl (в каталоге UI) в соответствии с корпоративными требованиями оформления внешнего вида печатной копии запроса на сертификат пользователей, при их печати через АРМ пользователя
- На вкладке "Web-интерфейс" окна свойств узла Центра регистрации приложения «Параметры Центра Регистрации» настроить параметры, определяющие выбор CSP и CSP по умолчанию, а также режим возможности поиска сертификатов других пользователей. Значения данных параметров определяются владельцем УЦ.
- Отключить автоматическую обработку запросов на регистрацию и запросов на сертификат для АРМов пользователя (Веб-приложений). Для этого установить в 0 значения параметров RegReqAutoAccept и CertReqAutoAccept на вкладке "Web-интерфейс" окна свойств узла Центра регистрации приложения «Параметры Центра Регистрации»
- Удалить из политики обработки неподписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» разрешения для роли «Временный сертификат»;
- Настроить политику обработки неподписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Оператор» (определить список областей использования рабочего сертификата);
- Настроить политику обработки подписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Пользователь Центра Регистрации» (определить список областей использования рабочего сертификата);
- Настроить матрицу прав доступа на вкладке «Безопасность» окна свойств приложения «Параметры Центра Регистрации»
    - Для роли «Администратор»

№	Наименование объекта	Наименование действия	Разрешение

			Выполнение	**Делегирование**
1	Admin.GetCertTemplates	Получить шаблоны сертификатов	+	
2	Admin.GetGrantedNameProperties	Получить ограничения на имена DN	+	
3	Admin.GetLogEventTypes	Получить коды событий журнала событий	+	
4	Admin.GetLogRecords	Получить список сообщений журнала событий	+	
5	Admin.PublishCRL	Отправить запрос на публикацию СОС	+	
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат	+	+
7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат	+	
8	CertRequest.ConfirmRequest	Подтвердить получение сертификата	+	+
9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу	+	+
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат	+	+
11	CertRequest.GetFirstCertRequestInfo	Получить информацию о запросе на сертификат по коду запроса на регистрацию	+	+
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат	+	+
13	CertRequest.GetRequestsList	Получить список запросов на сертификат	+	+
14	CertRequest.SetRequestInfo	Изменить информацию о запросе на сертификат	+	+
15	CertRequest.SubmitFirstCertRequest	Отправить неподписанный запрос на сертификат		
16	CertRequest.SubmitRequest	Отправить подписанный запрос на сертификат	+	
17	CertView.ConvertPKCS2XML	Получить сертификат в виде XML	+	
18	CertView.GetCACertificate	Получить сертификат Центра Сертификации	+	
19	CertView.GetCertificatesList	Получить список сертификатов	+	+
20	CertView.GetCertificateInfo	Получить информацию о сертификате	+	+
21	CertView.GetCRL	Получить список отозванных	+	

		сертификатов (СОС)		
22	Registration.AcceptRequest	Одобрить создание пользователя по запросу на регистрацию		
23	Registration.CreateCertRequest	Извлечь запрос на сертификат из запроса на регистрацию		
24	Registration.CreateRequest	Отправить запрос на регистрацию пользователя самим пользователем		
25	Registration.CreateRequestByAdmin	Отправить запрос на регистрацию пользователя администратором		
26	Registration.DenyRequest	Отклонить запрос на регистрацию		
27	Registration.GetRequestInfo	Получить информацию о запросе на регистрацию	+	+
28	Registration.GetRequestsList	Получить список запросов на регистрацию	+	+
29	Registration.SetRequestInfo	Изменить информацию о запросе на регистрацию	+	
30	RevokeRequest.AcceptRequest	Одобрить запрос на отзыв сертификата	+	+
31	RevokeRequest.DenyRequest	Отклонить запрос на отзыв сертификата	+	+
32	RevokeRequest.GetRequestInfo	Получить информацию о запросе на отзыв сертификата	+	+
33	RevokeRequest.GetRequestsList	Получить список запросов на отзыв сертификата	+	+
34	RevokeRequest.SetRequestInfo	Изменить информацию о запросе на отзыв сертификата	+	+
35	RevokeRequest.SubmitRequest	Отправить запрос на отзыв сертификата	+	+
36	RevokeRequest.SubmitHoldRequest	Отправить запрос на приостановление действия сертификата	+	+
37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата	+	+
38	UserView.AddDocument	Добавить документ пользователя	+	+
39	UserView.GetDocumentInfo	Получить информацию о документе пользователя	+	+
40	UserView.GetDocumentsList	Получить список документов пользователя	+	+
41	UserView.GetUserByCertificate	Найти идентификатор пользователя по сертификату	+	+
42	UserView.GetUserInfo	Получить информацию о пользователе	+	+

43	UserView.GetUsersList	Получить список пользователей	+	+
44	UserView.RemoveDocument	Удалить документ пользователя	+	+
45	UserView.SetUserInfo	Изменить информацию о пользователе	+	
46	UserView.DeleteUser	Удалить пользователя		
47	Admin.CreateTokenForUser	Создать маркер временного доступа	+	+

- Для роли «Оператор»

№	Наименование объекта	Наименование действия	Разрешение	
			Выполнение	Делегирование
1	Admin.GetCertTemplates	Получить шаблоны сертификатов	+	
2	Admin.GetGrantedNameProperties	Получить ограничения на имена DN	+	
3	Admin.GetLogEventTypes	Получить коды событий журнала событий	+	
4	Admin.GetLogRecords	Получить список сообщений журнала событий	+	
5	Admin.PublishCRL	Отправить запрос на публикацию СОС		
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат	+	
7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат	+	+
8	CertRequest.ConfirmRequest	Подтвердить получение сертификата	+	+
9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу		
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат	+	+
11	CertRequest.GetFirstCertRequestInfo	Получить информацию о запросе на сертификат по коду запроса на регистрацию	+	+
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат	+	+
13	CertRequest.GetRequestsList	Получить список запросов на сертификат	+	+
14	CertRequest.SetRequestInfo	Изменить информацию о запросе на сертификат	+	+

15	CertRequest.SubmitFirstCertRequest	Отправить неподписанный запрос на сертификат	+	+
16	CertRequest.SubmitRequest	Отправить подписанный запрос на сертификат	+	
17	CertView.ConvertPKCS2XML	Получить сертификат в виде XML	+	
18	CertView.GetCACertificate	Получить сертификат Центра Сертификации	+	
19	CertView.GetCertificatesList	Получить список сертификатов	+	+
20	CertView.GetCertificateInfo	Получить информацию о сертификате	+	+
21	CertView.GetCRL	Получить список отозванных сертификатов (СОС)	+	
22	Registration.AcceptRequest	Одобрить создание пользователя по запросу на регистрацию	+	+
23	Registration.CreateCertRequest	Извлечь запрос на сертификат из запроса на регистрацию	+	+
24	Registration.CreateRequest	Отправить запрос на регистрацию пользователя самим пользователем		
25	Registration.CreateRequestByAdmin	Отправить запрос на регистрацию пользователя администратором	+	
26	Registration.DenyRequest	Отклонить запрос на регистрацию	+	+
27	Registration.GetRequestInfo	Получить информацию о запросе на регистрацию	+	+
28	Registration.GetRequestsList	Получить список запросов на регистрацию	+	+
29	Registration.SetRequestInfo	Изменить информацию о запросе на регистрацию	+	+
30	RevokeRequest.AcceptRequest	Одобрить запрос на отзыв сертификата		
31	RevokeRequest.DenyRequest	Отклонить запрос на отзыв сертификата		
32	RevokeRequest.GetRequestInfo	Получить информацию о запросе на отзыв сертификата	+	+
33	RevokeRequest.GetRequestsList	Получить список запросов на отзыв сертификата	+	+
34	RevokeRequest.SetRequestInfo	Изменить информацию о запросе на отзыв сертификата	+	
35	RevokeRequest.SubmitRequest	Отправить запрос на отзыв сертификата	+	
36	RevokeRequest.SubmitHoldRequest	Отправить запрос на приостановление действия сертификата	+	

37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата	+	
38	UserView.AddDocument	Добавить документ пользователя	+	+
39	UserView.GetDocumentInfo	Получить информацию о документе пользователя	+	+
40	UserView.GetDocumentsList	Получить список документов пользователя	+	+
41	UserView.GetUserByCertificate	Найти идентификатор пользователя по сертификату	+	+
42	UserView.GetUserInfo	Получить информацию о пользователе	+	+
43	UserView.GetUsersList	Получить список пользователей	+	+
44	UserView.RemoveDocument	Удалить документ пользователя	+	+
45	UserView.SetUserInfo	Изменить информацию о пользователе	+	+
46	UserView.DeleteUser	Удалить пользователя	+	+
47	Admin.CreateTokenForUser	Создать маркер временного доступа		

- Для роли «Пользователь Центра Регистрации»

№	Наименование объекта	Наименование действия	Разрешение	
			Выполнение	Делегирование
1	Admin.GetCertTemplates	Получить шаблоны сертификатов	+	
2	Admin.GetGrantedNameProperties	Получить ограничения на имена DN	+	
3	Admin.GetLogEventTypes	Получить коды событий журнала событий		
4	Admin.GetLogRecords	Получить список сообщений журнала событий		
5	Admin.PublishCRL	Отправить запрос на публикацию СОС		
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат		
7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат		
8	CertRequest.ConfirmRequest	Подтвердить получение сертификата	+	

9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу		
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат	+	
11	CertRequest.GetFirstCertRequestInfo	Получить информацию о запросе на сертификат по коду запроса на регистрацию		
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат	+	
13	CertRequest.GetRequestsList	Получить список запросов на сертификат	+	
14	CertRequest.SetRequestInfo	Изменить информацию о запросе на сертификат	+	
15	CertRequest.SubmitFirstCertRequest	Отправить неподписанный запрос на сертификат		
16	CertRequest.SubmitRequest	Отправить подписанный запрос на сертификат	+	
17	CertView.ConvertPKCS2XML	Получить сертификат в виде XML	+	
18	CertView.GetCACertificate	Получить сертификат Центра Сертификации	+	
19	CertView.GetCertificatesList	Получить список сертификатов	+	+
20	CertView.GetCertificateInfo	Получить информацию о сертификате	+	+
21	CertView.GetCRL	Получить список отозванных сертификатов (СОС)	+	
22	Registration.AcceptRequest	Одобрить создание пользователя по запросу на регистрацию		
23	Registration.CreateCertRequest	Извлечь запрос на сертификат из запроса на регистрацию		
24	Registration.CreateRequest	Отправить запрос на регистрацию пользователя самим пользователем		
25	Registration.CreateRequestByAdmin	Отправить запрос на регистрацию пользователя администратором		
26	Registration.DenyRequest	Отклонить запрос на регистрацию		
27	Registration.GetRequestInfo	Получить информацию о запросе на регистрацию		
28	Registration.GetRequestsList	Получить список запросов на регистрацию		
29	Registration.SetRequestInfo	Изменить информацию о запросе на регистрацию		
30	RevokeRequest.Acce	Одобрить запрос на отзыв		

	ptRequest	сертификата		
31	RevokeRequest.DenyRequest	Отклонить запрос на отзыв сертификата		
32	RevokeRequest.GetRequestInfo	Получить информацию о запросе на отзыв сертификата	+	
33	RevokeRequest.GetRequestsList	Получить список запросов на отзыв сертификата	+	
34	RevokeRequest.SetRequestInfo	Изменить информацию о запросе на отзыв сертификата	+	
35	RevokeRequest.SubmitRequest	Отправить запрос на отзыв сертификата	+	
36	RevokeRequest.SubmitHoldRequest	Отправить запрос на приостановление действия сертификата	+	
37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата	+	
38	UserView.AddDocument	Добавить документ пользователя		
39	UserView.GetDocumentInfo	Получить информацию о документе пользователя		
40	UserView.GetDocumentsList	Получить список документов пользователя		
41	UserView.GetUserByCertificate	Найти идентификатор пользователя по сертификату	+	
42	UserView.GetUserInfo	Получить информацию о пользователе	+	
43	UserView.GetUsersList	Получить список пользователей		
44	UserView.RemoveDocument	Удалить документ пользователя		
45	UserView.SetUserInfo	Изменить информацию о пользователе		
46	UserView.DeleteUser	Удалить пользователя		
47	Admin.CreateTokenForUser	Создать маркер временного доступа		

6.3.3. Регистрация пользователей в централизованном режиме и централизованное управление ключами и сертификатами пользователя

Этот режим подразумевает, что пользователь не выполняет процедур управления ключами и сертификатами на своем рабочем месте и лично прибывает в УЦ при регистрации и сменах ключей и сертификатов.

Общий алгоритм схемы выглядит следующим образом:

- Администратор («оператор») с использованием ПО АРМ администратора Центра Регистрации формирует запрос на регистрацию в электронной форме от имени пользователя и принимает его.

- Администратор («оператор») с использованием ПО АРМ администратора Центра Регистрации изготавливает и передает пользователю на ключевом носителе его рабочий закрытый ключ и сертификат.
- Пользователь использует рабочие ключи и сертификат в информационной системе.
- Администратор («администратор») с использованием ПО АРМ администратора Центра Регистрации изготавливает и передает пользователю на ключевом носителе его новый рабочий закрытый ключ и сертификат.
- Пользователь использует новые рабочие ключи и сертификат в информационной системе.

При этом регистрация пользователей и изготовление первого рабочего сертификата осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «оператор», а изготовление новых рабочих ключей и сертификата осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «администратор».

Для реализации данного режима нужно выполнить следующие настройки:

На АРМ администратора:

- Настроить параметры выбора CSP (алгоритмы). Рекомендуется включить флаг пометки ключевых контейнеров как экспортируемые
- Откорректировать файл шаблона печати сертификата Cert.xsl в соответствии с корпоративными требованиями оформления внешнего вида печатной копии сертификата пользователей, при их печати через АРМ администратора ЦР

На Центре Сертификации

- Удалить идентификатор «Временный доступ к Центру Регистрации» в модуле политики Крипто-Про УЦ службы сертификации из списка допустимых областей использования
- Удалить идентификатор «пользователь Центра Регистрации» в модуле политики Крипто-Про УЦ службы сертификации из списка допустимых областей использования

На Центре Регистрации

- Выполнить выборочную установку ПО Центра Регистрации, исключив из устанавливаемых компонентов пользовательский интерфейс («Веб-интерфейс пользователя»)
- Отключить автоматическую обработку запросов на регистрацию и запросов на сертификат для АРМов пользователя (Веб-приложений). Для этого установить в 0 значения параметров RegReqAutoAccept и CertReqAutoAccept на вкладке "Web-интерфейс" окна свойств узла Центра регистрации приложения «Параметры Центра Регистрации»
- Удалить из политики обработки неподписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» разрешения для роли «Временный сертификат»;
- Удалить из политики обработки неподписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» разрешения для роли «Пользователь Центра Регистрации»;
- Настроить политику обработки неподписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Оператор» (определить список областей использования рабочего сертификата);
- Настроить политику обработки подписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли

«Администратор» (определить список областей использования рабочего сертификата);

- Настроить матрицу прав доступа на вкладке «Безопасность» окна свойств приложения «Параметры Центра Регистрации»
    - Для роли «Администратор»

№	Наименование объекта	Наименование действия	Разрешение	
			Выполнение	Делегирование
1	Admin.GetCertTemplates	Получить шаблоны сертификатов	+	
2	Admin.GetGrantedNameProperties	Получить ограничения на имена DN	+	
3	Admin.GetLogEventTypes	Получить коды событий журнала событий	+	
4	Admin.GetLogRecords	Получить список сообщений журнала событий	+	
5	Admin.PublishCRL	Отправить запрос на публикацию СОС	+	
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат	+	+
7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат	+	
8	CertRequest.ConfirmRequest	Подтвердить получение сертификата	+	+
9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу	+	+
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат	+	+
11	CertRequest.GetFirstCertRequestInfo	Получить информацию о запросе на сертификат по коду запроса на регистрацию	+	+
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат	+	+
13	CertRequest.GetRequestsList	Получить список запросов на сертификат	+	+
14	CertRequest.SetRequestInfo	Изменить информацию о запросе на сертификат	+	+
15	CertRequest.SubmitFirstCertRequest	Отправить неподписанный запрос на сертификат	+	+
16	CertRequest.SubmitRequest	Отправить подписанный запрос на сертификат	+	
17	CertView.ConvertPKCS2XML	Получить сертификат в виде XML	+	

18	CertView.GetCACertificate	Получить сертификат Центра Сертификации	+	
19	CertView.GetCertificatesList	Получить список сертификатов	+	+
20	CertView.GetCertificateInfo	Получить информацию о сертификате	+	+
21	CertView.GetCRL	Получить список отозванных сертификатов (СОС)	+	
22	Registration.AcceptRequest	Одобрить создание пользователя по запросу на регистрацию		
23	Registration.CreateCertRequest	Извлечь запрос на сертификат из запроса на регистрацию		
24	Registration.CreateRequest	Отправить запрос на регистрацию пользователя самим пользователем		
25	Registration.CreateRequestByAdmin	Отправить запрос на регистрацию пользователя администратором		
26	Registration.DenyRequest	Отклонить запрос на регистрацию		
27	Registration.GetRequestInfo	Получить информацию о запросе на регистрацию	+	+
28	Registration.GetRequestsList	Получить список запросов на регистрацию	+	+
29	Registration.SetRequestInfo	Изменить информацию о запросе на регистрацию	+	
30	RevokeRequest.AcceptRequest	Одобрить запрос на отзыв сертификата	+	+
31	RevokeRequest.DenyRequest	Отклонить запрос на отзыв сертификата	+	+
32	RevokeRequest.GetRequestInfo	Получить информацию о запросе на отзыв сертификата	+	+
33	RevokeRequest.GetRequestsList	Получить список запросов на отзыв сертификата	+	+
34	RevokeRequest.SetRequestInfo	Изменить информацию о запросе на отзыв сертификата	+	+
35	RevokeRequest.SubmitRequest	Отправить запрос на отзыв сертификата	+	+
36	RevokeRequest.SubmitHoldRequest	Отправить запрос на приостановление действия сертификата	+	+
37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата	+	+
38	UserView.AddDocument	Добавить документ пользователя	+	+
39	UserView.GetDocum	Получить информацию о	+	+

	entInfo	документе пользователя		
40	UserView.GetDocumentsList	Получить список документов пользователя	+	+
41	UserView.GetUserByCertificate	Найти идентификатор пользователя по сертификату	+	+
42	UserView.GetUserInfo	Получить информацию о пользователе	+	+
43	UserView.GetUsersList	Получить список пользователей	+	+
44	UserView.RemoveDocument	Удалить документ пользователя	+	+
45	UserView.SetUserInfo	Изменить информацию о пользователе	+	
46	UserView.DeleteUser	Удалить пользователя		
47	Admin.CreateTokenForUser	Создать маркер временного доступа	+	+

- Для роли «Оператор»

№	Наименование объекта	Наименование действия	Разрешение	
			Выполнение	Делегирование
1	Admin.GetCertTemplates	Получить шаблоны сертификатов	+	
2	Admin.GetGrantedNameProperties	Получить ограничения на имена DN	+	
3	Admin.GetLogEventTypes	Получить коды событий журнала событий	+	
4	Admin.GetLogRecords	Получить список сообщений журнала событий	+	
5	Admin.PublishCRL	Отправить запрос на публикацию СОС		
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат	+	
7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат	+	+
8	CertRequest.ConfirmRequest	Подтвердить получение сертификата	+	+
9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу		
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат	+	+
11	CertRequest.GetFirst	Получить информацию о запросе на сертификат по коду	+	+

	CertRequestInfo	запроса на регистрацию		
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат	+	+
13	CertRequest.GetRequestsList	Получить список запросов на сертификат	+	+
14	CertRequest.SetRequestInfo	Изменить информацию о запросе на сертификат	+	+
15	CertRequest.SubmitFirstCertRequest	Отправить неподписанный запрос на сертификат	+	+
16	CertRequest.SubmitRequest	Отправить подписанный запрос на сертификат	+	
17	CertView.ConvertPKCS2XML	Получить сертификат в виде XML	+	
18	CertView.GetCACertificate	Получить сертификат Центра Сертификации	+	
19	CertView.GetCertificatesList	Получить список сертификатов	+	+
20	CertView.GetCertificateInfo	Получить информацию о сертификате	+	+
21	CertView.GetCRL	Получить список отозванных сертификатов (СОС)	+	
22	Registration.AcceptRequest	Одобрить создание пользователя по запросу на регистрацию	+	+
23	Registration.CreateCertRequest	Извлечь запрос на сертификат из запроса на регистрацию	+	+
24	Registration.CreateRequest	Отправить запрос на регистрацию пользователя самим пользователем		
25	Registration.CreateRequestByAdmin	Отправить запрос на регистрацию пользователя администратором	+	
26	Registration.DenyRequest	Отклонить запрос на регистрацию	+	+
27	Registration.GetRequestInfo	Получить информацию о запросе на регистрацию	+	+
28	Registration.GetRequestsList	Получить список запросов на регистрацию	+	+
29	Registration.SetRequestInfo	Изменить информацию о запросе на регистрацию	+	+
30	RevokeRequest.AcceptRequest	Одобрить запрос на отзыв сертификата		
31	RevokeRequest.DenyRequest	Отклонить запрос на отзыв сертификата		
32	RevokeRequest.GetRequestInfo	Получить информацию о запросе на отзыв сертификата	+	+
33	RevokeRequest.GetR	Получить список запросов на	+	+

	equestsList	отзыв сертификата		
34	RevokeRequest.SetRequestInfo	Изменить информацию о запросе на отзыв сертификата	+	
35	RevokeRequest.SubmitRequest	Отправить запрос на отзыв сертификата	+	
36	RevokeRequest.SubmitHoldRequest	Отправить запрос на приостановление действия сертификата	+	
37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата	+	
38	UserView.AddDocument	Добавить документ пользователя	+	+
39	UserView.GetDocumentInfo	Получить информацию о документе пользователя	+	+
40	UserView.GetDocumentsList	Получить список документов пользователя	+	+
41	UserView.GetUserByCertificate	Найти идентификатор пользователя по сертификату	+	+
42	UserView.GetUserInfo	Получить информацию о пользователе	+	+
43	UserView.GetUsersList	Получить список пользователей	+	+
44	UserView.RemoveDocument	Удалить документ пользователя	+	+
45	UserView.SetUserInfo	Изменить информацию о пользователе	+	+
46	UserView.DeleteUser	Удалить пользователя	+	+
47	Admin.CreateTokenForUser	Создать маркер временного доступа		

6.3.4. Регистрация пользователей в распределенном режиме схемы и распределенное управление ключами и сертификатами пользователя

Распределенный режим регистрации пользователя является опциональным режимом и используется при невозможности (по разным причинам, в том числе и по причине экономической целесообразности) регистрации пользователей в централизованном режиме.

Идентификация пользователя осуществляется нотариусом путем совершения нотариальных действий при заверении заявления на регистрацию пользователя, на основании документов, удостоверяющих личность пользователя.

С помощью ПО АРМ регистрации пользователя регистрируемые пользователи формируют запрос на регистрацию в электронной форме.

Регистрация пользователя в распределенном режиме на УЦ осуществляется администратором Удостоверяющего Центра на основании нотариально заверенного заявления на регистрацию и запроса на регистрацию в электронной форме путем принятия запроса на регистрацию в электронной форме.

С помощью ПО АРМ зарегистрированного пользователя с маркерным доступом, зарегистрированные пользователи на своем рабочем месте генерируют служебные закрытый и открытый ключи, формируют и отправляют в режиме односторонней аутентификации с ЦР запрос на служебный сертификат.

Зарегистрированный пользователь должен распечатать запрос на сертификат в бумажной форме, заверить его своей собственноручной подписью и отправить в Удостоверяющий Центр.

Администратор с использованием ПО АРМ администратора Центра Регистрации, на основании поступившего запроса на сертификат в электронной форме и запроса на сертификат в бумажной форме принимает запрос на сертификат для изготовления его.

С помощью ПО АРМ зарегистрированного пользователя с маркерным доступом, зарегистрированные пользователи на своем рабочем месте получают выпущенный служебный сертификат.

Затем с использованием ПО АРМ зарегистрированного пользователя с ключевым доступом пользователь формирует рабочие ключи и запрос на рабочий сертификат и ставит его в очередь на обработку в Центр Регистрации и получает выпущенный сертификат после обработки запроса администратором УЦ.

Общий алгоритм схемы выглядит следующим образом:

- Пользователь с использованием ПО АРМ регистрации пользователя формирует запрос на регистрацию в электронной форме и по защищенному каналу (односторонний TLS) ставит в очередь на обработку в Центр Регистрации.
- Центр Регистрации формирует маркер временного доступа пользователя и также по защищенному каналу передает регистрируемому пользователю.
- Администратор («оператор») с использованием ПО АРМ администратора Центра Регистрации обрабатывает (принимает) запрос на регистрацию пользователя.
- Зарегистрированный пользователь с использованием с помощью АРМ зарегистрированного пользователя с маркерным доступом производит со своего рабочего места аутентификацию с Центром Регистрации по временному маркеру доступа, формирует ключи и запрос на служебный сертификат и ставит его (запрос) в очередь на обработку в Центр Регистрации.
- Администратор («оператор») с использованием ПО АРМ администратора Центра Регистрации обрабатывает (принимает) стоящий в очереди запрос на служебный сертификат.
- Пользователь с помощью АРМ зарегистрированного пользователя с маркерным доступом получает сертификат на служебные ключи, изготовленные им на своем рабочем месте, и устанавливает его.
- Зарегистрированный пользователь с использованием с помощью АРМ зарегистрированного пользователя с ключевым доступом производит со своего рабочего места аутентификацию с Центром Регистрации по служебному сертификату, формирует рабочие ключи и запрос на рабочий сертификат и ставит его (запрос) в очередь на обработку в Центр Регистрации.
- Администратор («администратор») с использованием ПО АРМ администратора Центра Регистрации обрабатывает (принимает) стоящий в очереди запрос на рабочий сертификат.
- Пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом получает сертификат на рабочие ключи и устанавливает его.
- Пользователь использует рабочие ключи и сертификат в информационной системе.
- С использованием рабочего закрытого ключа и сертификата пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом производит со своего рабочего места двустороннюю аутентификацию при установлении соединения с сервером ЦР и формирует запрос на новый рабочий сертификат и ставит его в очередь на обработку в Центр Регистрации.

- Администратор («администратор») с использованием ПО АРМ администратора Центра Регистрации обрабатывает (принимает) стоящий в очереди запрос на сертификат.
- Пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом получает сертификат на новые рабочие ключи, изготовленные им на своем рабочем месте, и устанавливает его.
- Пользователь использует новые рабочие ключи и сертификат в информационной системе.

При этом регистрация пользователей и обработка запроса на служебный сертификат осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «оператор», а обработка запроса на рабочий сертификат осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «администратор».

Для реализации данного режима нужно выполнить следующие настройки:

На Центре Сертификации

- Настроить срок действия служебного сертификата, путем установки нужного срока для идентификатора «Временный доступ к Центру Регистрации» в модуле политики Крипто-Про УЦ службы сертификации

На Центре Регистрации

- Выполнить полную установку ПО Центра Регистрации
- Откорректировать файл шаблона печати сертификата Cert.xsl (в каталоге UI) в соответствии с корпоративными требованиями оформления внешнего вида печатной копии сертификата пользователей, при их печати через АРМ пользователя
- Откорректировать файл шаблона печати запроса на сертификат Request.xsl (в каталоге UI) в соответствии с корпоративными требованиями оформления внешнего вида печатной копии запроса на сертификат пользователей, при их печати через АРМ пользователя
- На вкладке "Web-интерфейс" окна свойств узла Центра регистрации приложения «Параметры Центра Регистрации» настроить параметры, определяющие выбор CSP и CSP по умолчанию, а также режим возможности поиска сертификатов других пользователей. Значения данных параметров определяются владельцем УЦ.
- Отключить автоматическую обработку запросов на регистрацию и запросов на сертификат для АРМов пользователя (Веб-приложений). Для этого установить в 0 значения параметров RegReqAutoAccept и CertReqAutoAccept на вкладке "Web-интерфейс" окна свойств узла Центра регистрации приложения «Параметры Центра Регистрации»
- Настроить политику обработки неподписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Прошедший проверку» (определить список областей использования служебного сертификата);
- Настроить политику обработки подписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Временный сертификат» (определить список областей использования рабочего сертификата);
- Настроить политику обработки подписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Пользователь Центра Регистрации» (определить список областей использования рабочего сертификата);
- Настроить матрицу прав доступа на вкладке «Безопасность» окна свойств приложения «Параметры Центра Регистрации»

- Для роли «Администратор»

№	Наименование объекта	Наименование действия	Разрешение	
			Выполнение	Делегирование
1	Admin.GetCertTemplates	Получить шаблоны сертификатов	+	
2	Admin.GetGrantedNameProperties	Получить ограничения на имена DN	+	
3	Admin.GetLogEventTypes	Получить коды событий журнала событий	+	
4	Admin.GetLogRecords	Получить список сообщений журнала событий	+	
5	Admin.PublishCRL	Отправить запрос на публикацию СОС	+	
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат	+	+
7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат	+	
8	CertRequest.ConfirmRequest	Подтвердить получение сертификата	+	+
9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу	+	+
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат	+	+
11	CertRequest.GetFirstCertRequestInfo	Получить информацию о запросе на сертификат по коду запроса на регистрацию	+	+
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат	+	+
13	CertRequest.GetRequestsList	Получить список запросов на сертификат	+	+
14	CertRequest.SetRequestInfo	Изменить информацию о запросе на сертификат	+	+
15	CertRequest.SubmitFirstCertRequest	Отправить неподписанный запрос на сертификат		
16	CertRequest.SubmitRequest	Отправить подписанный запрос на сертификат	+	
17	CertView.ConvertPKCS2XML	Получить сертификат в виде XML	+	
18	CertView.GetCACertificate	Получить сертификат Центра Сертификации	+	
19	CertView.GetCertificatesList	Получить список сертификатов	+	+

20	CertView.GetCertificateInfo	Получить информацию о сертификате	+	+
21	CertView.GetCRL	Получить список отозванных сертификатов (СОС)	+	
22	Registration.AcceptRequest	Одобрить создание пользователя по запросу на регистрацию		
23	Registration.CreateCertRequest	Извлечь запрос на сертификат из запроса на регистрацию		
24	Registration.CreateRequest	Отправить запрос на регистрацию пользователя самим пользователем		
25	Registration.CreateRequestByAdmin	Отправить запрос на регистрацию пользователя администратором		
26	Registration.DenyRequest	Отклонить запрос на регистрацию		
27	Registration.GetRequestInfo	Получить информацию о запросе на регистрацию	+	+
28	Registration.GetRequestsList	Получить список запросов на регистрацию	+	+
29	Registration.SetRequestInfo	Изменить информацию о запросе на регистрацию	+	
30	RevokeRequest.AcceptRequest	Одобрить запрос на отзыв сертификата	+	+
31	RevokeRequest.DenyRequest	Отклонить запрос на отзыв сертификата	+	+
32	RevokeRequest.GetRequestInfo	Получить информацию о запросе на отзыв сертификата	+	+
33	RevokeRequest.GetRequestsList	Получить список запросов на отзыв сертификата	+	+
34	RevokeRequest.SetRequestInfo	Изменить информацию о запросе на отзыв сертификата	+	+
35	RevokeRequest.SubmitRequest	Отправить запрос на отзыв сертификата	+	+
36	RevokeRequest.SubmitHoldRequest	Отправить запрос на приостановление действия сертификата	+	+
37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата	+	+
38	UserView.AddDocument	Добавить документ пользователя	+	+
39	UserView.GetDocumentInfo	Получить информацию о документе пользователя	+	+
40	UserView.GetDocumentsList	Получить список документов пользователя	+	+
41	UserView.GetUserBy	Найти идентификатор	+	+

	Certificate	пользователя по сертификату		
42	UserView.GetUserInfo	Получить информацию о пользователе	+	+
43	UserView.GetUsersList	Получить список пользователей	+	+
44	UserView.RemoveDocument	Удалить документ пользователя	+	+
45	UserView.SetUserInfo	Изменить информацию о пользователе	+	
46	UserView.DeleteUser	Удалить пользователя		
47	Admin.CreateTokenForUser	Создать маркер временного доступа	+	+

- Для роли «Оператор»

№	Наименование объекта	Наименование действия	Разрешение	
			Выполнение	Делегирование
1	Admin.GetCertTemplates	Получить шаблоны сертификатов	+	
2	Admin.GetGrantedNameProperties	Получить ограничения на имена DN	+	
3	Admin.GetLogEventTypes	Получить коды событий журнала событий	+	
4	Admin.GetLogRecords	Получить список сообщений журнала событий	+	
5	Admin.PublishCRL	Отправить запрос на публикацию СОС		
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат	+	
7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат	+	+
8	CertRequest.ConfirmRequest	Подтвердить получение сертификата	+	+
9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу		
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат	+	+
11	CertRequest.GetFirstCertRequestInfo	Получить информацию о запросе на сертификат по коду запроса на регистрацию	+	+
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат	+	+

13	CertRequest.GetRequestsList	Получить список запросов на сертификат	+	+
14	CertRequest.SetRequestInfo	Изменить информацию о запросе на сертификат	+	+
15	CertRequest.SubmitFirstCertRequest	Отправить неподписанный запрос на сертификат		
16	CertRequest.SubmitRequest	Отправить подписанный запрос на сертификат	+	
17	CertView.ConvertPKCS2XML	Получить сертификат в виде XML	+	
18	CertView.GetCACertificate	Получить сертификат Центра Сертификации	+	
19	CertView.GetCertificatesList	Получить список сертификатов	+	+
20	CertView.GetCertificateInfo	Получить информацию о сертификате	+	+
21	CertView.GetCRL	Получить список отозванных сертификатов (СОС)	+	
22	Registration.AcceptRequest	Одобрить создание пользователя по запросу на регистрацию	+	+
23	Registration.CreateCertRequest	Извлечь запрос на сертификат из запроса на регистрацию	+	+
24	Registration.CreateRequest	Отправить запрос на регистрацию пользователя самим пользователем		
25	Registration.CreateRequestByAdmin	Отправить запрос на регистрацию пользователя администратором	+	
26	Registration.DenyRequest	Отклонить запрос на регистрацию	+	+
27	Registration.GetRequestInfo	Получить информацию о запросе на регистрацию	+	+
28	Registration.GetRequestsList	Получить список запросов на регистрацию	+	+
29	Registration.SetRequestInfo	Изменить информацию о запросе на регистрацию	+	+
30	RevokeRequest.AcceptRequest	Одобрить запрос на отзыв сертификата		
31	RevokeRequest.DenyRequest	Отклонить запрос на отзыв сертификата		
32	RevokeRequest.GetRequestInfo	Получить информацию о запросе на отзыв сертификата	+	+
33	RevokeRequest.GetRequestsList	Получить список запросов на отзыв сертификата	+	+
34	RevokeRequest.SetRequestInfo	Изменить информацию о запросе на отзыв сертификата	+	

35	RevokeRequest.SubmitRequest	Отправить запрос на отзыв сертификата	+	
36	RevokeRequest.SubmitHoldRequest	Отправить запрос на приостановление действия сертификата	+	
37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата	+	
38	UserView.AddDocument	Добавить документ пользователя	+	+
39	UserView.GetDocumentInfo	Получить информацию о документе пользователя	+	+
40	UserView.GetDocumentsList	Получить список документов пользователя	+	+
41	UserView.GetUserByCertificate	Найти идентификатор пользователя по сертификату	+	+
42	UserView.GetUserInfo	Получить информацию о пользователе	+	+
43	UserView.GetUsersList	Получить список пользователей	+	+
44	UserView.RemoveDocument	Удалить документ пользователя	+	+
45	UserView.SetUserInfo	Изменить информацию о пользователе	+	+
46	UserView.DeleteUser	Удалить пользователя	+	+
47	Admin.CreateTokenForUser	Создать маркер временного доступа		

- Для роли «Временный сертификат»

№	Наименование объекта	Наименование действия	Разрешение	
			Выполнение	Делегирование
1	Admin.GetCertTemplates	Получить шаблоны сертификатов	+	
2	Admin.GetGrantedNameProperties	Получить ограничения на имена DN	+	
3	Admin.GetLogEventTypes	Получить коды событий журнала событий		
4	Admin.GetLogRecords	Получить список сообщений журнала событий		
5	Admin.PublishCRL	Отправить запрос на публикацию СОС		
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат		

7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат		
8	CertRequest.ConfirmRequest	Подтвердить получение сертификата	+	
9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу		
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат	+	
11	CertRequest.GetFirstCertRequestInfo	Получить информацию о запросе на сертификат по коду запроса на регистрацию		
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат	+	
13	CertRequest.GetRequestsList	Получить список запросов на сертификат	+	
14	CertRequest.SetRequestInfo	Изменить информацию о запросе на сертификат	+	
15	CertRequest.SubmitFirstCertRequest	Отправить неподписанный запрос на сертификат		
16	CertRequest.SubmitRequest	Отправить подписанный запрос на сертификат	+	
17	CertView.ConvertPKCS2XML	Получить сертификат в виде XML	+	
18	CertView.GetCACertificate	Получить сертификат Центра Сертификации	+	
19	CertView.GetCertificatesList	Получить список сертификатов	+	
20	CertView.GetCertificateInfo	Получить информацию о сертификате	+	
21	CertView.GetCRL	Получить список отозванных сертификатов (СОС)	+	
22	Registration.AcceptRequest	Одобрить создание пользователя по запросу на регистрацию		
23	Registration.CreateCertRequest	Извлечь запрос на сертификат из запроса на регистрацию		
24	Registration.CreateRequest	Отправить запрос на регистрацию пользователя самим пользователем		
25	Registration.CreateRequestByAdmin	Отправить запрос на регистрацию пользователя администратором		
26	Registration.DenyRequest	Отклонить запрос на регистрацию		
27	Registration.GetRequestInfo	Получить информацию о запросе на регистрацию		

28	Registration.GetRequestsList	Получить список запросов на регистрацию		
29	Registration.SetRequestInfo	Изменить информацию о запросе на регистрацию		
30	RevokeRequest.AcceptRequest	Одобрить запрос на отзыв сертификата		
31	RevokeRequest.DenyRequest	Отклонить запрос на отзыв сертификата		
32	RevokeRequest.GetRequestInfo	Получить информацию о запросе на отзыв сертификата	+	
33	RevokeRequest.GetRequestsList	Получить список запросов на отзыв сертификата	+	
34	RevokeRequest.SetRequestInfo	Изменить информацию о запросе на отзыв сертификата		
35	RevokeRequest.SubmitRequest	Отправить запрос на отзыв сертификата		
36	RevokeRequest.SubmitHoldRequest	Отправить запрос на приостановление действия сертификата		
37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата		
38	UserView.AddDocument	Добавить документ пользователя		
39	UserView.GetDocumentInfo	Получить информацию о документе пользователя		
40	UserView.GetDocumentsList	Получить список документов пользователя		
41	UserView.GetUserByCertificate	Найти идентификатор пользователя по сертификату	+	
42	UserView.GetUserInfo	Получить информацию о пользователе	+	
43	UserView.GetUsersList	Получить список пользователей		
44	UserView.RemoveDocument	Удалить документ пользователя		
45	UserView.SetUserInfo	Изменить информацию о пользователе		
46	UserView.DeleteUser	Удалить пользователя		
47	Admin.CreateTokenForUser	Создать маркер временного доступа		

- Для роли «Пользователь Центра Регистрации»

№	Наименование объекта	Наименование действия	Разрешение

			Выполнение	**Делегирование**
1	Admin.GetCertTemplates	Получить шаблоны сертификатов	+	
2	Admin.GetGrantedNameProperties	Получить ограничения на имена DN	+	
3	Admin.GetLogEventTypes	Получить коды событий журнала событий		
4	Admin.GetLogRecords	Получить список сообщений журнала событий		
5	Admin.PublishCRL	Отправить запрос на публикацию СОС		
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат		
7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат		
8	CertRequest.ConfirmRequest	Подтвердить получение сертификата	+	
9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу		
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат	+	
11	CertRequest.GetFirstCertRequestInfo	Получить информацию о запросе на сертификат по коду запроса на регистрацию		
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат	+	
13	CertRequest.GetRequestsList	Получить список запросов на сертификат	+	
14	CertRequest.SetRequestInfo	Изменить информацию о запросе на сертификат	+	
15	CertRequest.SubmitFirstCertRequest	Отправить неподписанный запрос на сертификат		
16	CertRequest.SubmitRequest	Отправить подписанный запрос на сертификат	+	
17	CertView.ConvertPKCS2XML	Получить сертификат в виде XML	+	
18	CertView.GetCACertificate	Получить сертификат Центра Сертификации	+	
19	CertView.GetCertificatesList	Получить список сертификатов	+	+
20	CertView.GetCertificateInfo	Получить информацию о сертификате	+	+
21	CertView.GetCRL	Получить список отозванных	+	

		сертификатов (СОС)		
22	Registration.AcceptRequest	Одобрить создание пользователя по запросу на регистрацию		
23	Registration.CreateCertRequest	Извлечь запрос на сертификат из запроса на регистрацию		
24	Registration.CreateRequest	Отправить запрос на регистрацию пользователя самим пользователем		
25	Registration.CreateRequestByAdmin	Отправить запрос на регистрацию пользователя администратором		
26	Registration.DenyRequest	Отклонить запрос на регистрацию		
27	Registration.GetRequestInfo	Получить информацию о запросе на регистрацию		
28	Registration.GetRequestsList	Получить список запросов на регистрацию		
29	Registration.SetRequestInfo	Изменить информацию о запросе на регистрацию		
30	RevokeRequest.AcceptRequest	Одобрить запрос на отзыв сертификата		
31	RevokeRequest.DenyRequest	Отклонить запрос на отзыв сертификата		
32	RevokeRequest.GetRequestInfo	Получить информацию о запросе на отзыв сертификата	+	
33	RevokeRequest.GetRequestsList	Получить список запросов на отзыв сертификата	+	
34	RevokeRequest.SetRequestInfo	Изменить информацию о запросе на отзыв сертификата	+	
35	RevokeRequest.SubmitRequest	Отправить запрос на отзыв сертификата	+	
36	RevokeRequest.SubmitHoldRequest	Отправить запрос на приостановление действия сертификата	+	
37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата	+	
38	UserView.AddDocument	Добавить документ пользователя		
39	UserView.GetDocumentInfo	Получить информацию о документе пользователя		
40	UserView.GetDocumentsList	Получить список документов пользователя		
41	UserView.GetUserByCertificate	Найти идентификатор пользователя по сертификату	+	
42	UserView.GetUserInfo	Получить информацию о пользователе	+	

43	UserView.GetUsersList	Получить список пользователей		
44	UserView.RemoveDocument	Удалить документ пользователя		
45	UserView.SetUserInfo	Изменить информацию о пользователе		
46	UserView.DeleteUser	Удалить пользователя		
47	Admin.CreateTokenForUser	Создать маркер временного доступа		

6.3.5. Регистрация пользователей в распределенном режиме схемы и распределенное управление ключами и сертификатами пользователя с автоматической регистрацией

Данный режим представляет собой вариант предыдущего режима работы Удостоверяющего Центра и используется при необходимости сократить время процедуры регистрации за счет автоматизации деятельности оператора по регистрации пользователя.

Данная схема имеет уязвимость, связанную с тем, что могут появляться несанкционированно зарегистрированные пользователи.

Общий алгоритм схемы выглядит следующим образом:

- Пользователь с использованием ПО АРМ регистрации пользователя формирует запрос на регистрацию в электронной форме и по защищенному каналу (односторонний TLS) ставит в очередь на обработку в Центр Регистрации.
- Центр Регистрации формирует маркер временного доступа пользователя и также по защищенному каналу передает регистрируемому пользователю.
- Центр Регистрации автоматически обрабатывает (принимает) запрос на регистрацию пользователя.
- Зарегистрированный пользователь с использованием АРМ зарегистрированного пользователя с маркерным доступом производит со своего рабочего места аутентификацию с Центром Регистрации по временному маркеру доступа, формирует ключи и запрос на служебный сертификат и ставит его (запрос) в очередь на обработку в Центр Регистрации.
- Администратор («оператор») с использованием ПО АРМ администратора Центра Регистрации обрабатывает (принимает) стоящий в очереди запрос на служебный сертификат (и тут же он смотрит заявительные бумаги для основания действия).
- Пользователь с помощью АРМ зарегистрированного пользователя с маркерным доступом получает сертификат на служебные ключи, изготовленные им на своем рабочем месте, и устанавливает его.
- Зарегистрированный пользователь с использованием АРМ зарегистрированного пользователя с ключевым доступом производит со своего рабочего места аутентификацию с Центром Регистрации по служебному сертификату, формирует рабочие ключи и запрос на рабочий сертификат и ставит его (запрос) в очередь на обработку в Центр Регистрации.
- Администратор («администратор») с использованием ПО АРМ администратора Центра Регистрации обрабатывает (принимает) стоящий в очереди запрос на рабочий сертификат.
- Пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом получает сертификат на рабочие ключи и устанавливает его.

- Пользователь использует рабочие ключи и сертификат в информационной системе.
- С использованием рабочего закрытого ключа и сертификата пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом производит со своего рабочего места двустороннюю аутентификацию при установлении соединения с сервером ЦР и формирует запрос на новый рабочий сертификат и ставит его в очередь на обработку в Центр Регистрации.
- Администратор («администратор») с использованием ПО АРМ администратора Центра Регистрации обрабатывает (принимает) стоящий в очереди запрос на сертификат.
- Пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом получает сертификат на новые рабочие ключи, изготовленные им на своем рабочем месте, и устанавливает его.
- Пользователь использует новые рабочие ключи и сертификат в информационной системе.

При этом обработка запроса на служебный сертификат осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «оператор», а обработка запроса на рабочий сертификат осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «администратор».

Для реализации данного режима нужно выполнить следующие настройки:

На Центре Сертификации

- Настроить срок действия служебного сертификата, путем установки нужного срока для идентификатора «Временный доступ к Центру Регистрации» в модуле политики Крипто-Про УЦ службы сертификации

На Центре Регистрации

- Выполнить полную установку ПО Центра Регистрации
- Откорректировать файл шаблона печати сертификата Cert.xsl (в каталоге UI) в соответствии с корпоративными требованиями оформления внешнего вида печатной копии сертификата пользователей, при их печати через АРМ пользователя
- Откорректировать файл шаблона печати запроса на сертификат Request.xsl (в каталоге UI) в соответствии с корпоративными требованиями оформления внешнего вида печатной копии запроса на сертификат пользователей, при их печати через АРМ пользователя
- На вкладке "Web-интерфейс" окна свойств узла Центра регистрации приложения «Параметры Центра Регистрации» настроить параметры, определяющие выбор CSP и CSP по умолчанию, а также режим возможности поиска сертификатов других пользователей. Значения данных параметров определяются владельцем УЦ.
- Включить автоматическую обработку запросов на регистрацию и отключить автоматическую обработку запросов на сертификат для АРМов пользователя (Веб-приложений). Для этого установить в 1 значения параметра RegReqAutoAccept и установить в 0 значение параметра CertReqAutoAccept на вкладке "Web-интерфейс" окна свойств узла Центра регистрации приложения «Параметры Центра Регистрации»
- Настроить политику обработки неподписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Прошедший проверку» (определить список областей использования служебного сертификата);

- Настроить политику обработки подписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Временный сертификат» (определить список областей использования рабочего сертификата);
- Настроить политику обработки подписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Пользователь Центра Регистрации» (определить список областей использования рабочего сертификата);
- Настроить матрицу прав доступа на вкладке «Безопасность» окна свойств приложения «Параметры Центра Регистрации» по схеме предыдущего режима (основного распределенного)

6.3.6. Регистрация пользователей в распределенном режиме схемы и распределенное управление ключами и сертификатами пользователя с автоматической регистрацией и автоматическим выпуском служебного сертификата

Данный режим используется при необходимости сократить время процедуры регистрации и получения первого (служебного) сертификата за счет того, что регистрация пользователя и получение первого служебного сертификата не требует вмешательства оператора.

Данная схема имеет уязвимость, связанную с тем, что могут появляться несанкционированно зарегистрированные пользователи.

Общий алгоритм схемы выглядит следующим образом:

- Пользователь с использованием ПО АРМ регистрации пользователя формирует запрос на регистрацию в электронной форме и по защищенному каналу (односторонний TLS) ставит в очередь на обработку в Центр Регистрации.
- Центр Регистрации формирует маркер временного доступа пользователя и также по защищенному каналу передает регистрируемому пользователю.
- Центр Регистрации автоматически обрабатывает (принимает) запрос на регистрацию пользователя.
- Зарегистрированный пользователь с использованием АРМ зарегистрированного пользователя с маркерным доступом производит со своего рабочего места аутентификацию с Центром Регистрации по временному маркеру доступа, формирует ключи и запрос на служебный сертификат и ставит его (запрос) в очередь на обработку в Центр Регистрации.
- Центр Регистрации автоматически обрабатывает (принимает) стоящий в очереди запрос на служебный сертификат.
- Пользователь с помощью АРМ зарегистрированного пользователя с маркерным доступом получает сертификат на служебные ключи, изготовленные им на своем рабочем месте, и устанавливает его.
- Зарегистрированный пользователь с использованием АРМ зарегистрированного пользователя с ключевым доступом производит со своего рабочего места аутентификацию с Центром Регистрации по служебному сертификату, формирует рабочие ключи и запрос на рабочий сертификат и ставит его (запрос) в очередь на обработку в Центр Регистрации.
- Администратор («администратор») с использованием ПО АРМ администратора Центра Регистрации обрабатывает (принимает) стоящий в очереди запрос на рабочий сертификат (и тут же он смотрит заявительные бумаги для основания всех предыдущих действий).
- Пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом получает сертификат на рабочие ключи и устанавливает его.

- Пользователь использует рабочие ключи и сертификат в информационной системе.
- С использованием рабочего закрытого ключа и сертификата пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом производит со своего рабочего места двустороннюю аутентификацию при установлении соединения с сервером ЦР и формирует запрос на новый рабочий сертификат и ставит его в очередь на обработку в Центр Регистрации.
- Администратор («администратор») с использованием ПО АРМ администратора Центра Регистрации обрабатывает (принимает) стоящий в очереди запрос на сертификат.
- Пользователь с помощью АРМ зарегистрированного пользователя с ключевым доступом получает сертификат на новые рабочие ключи, изготовленные им на своем рабочем месте, и устанавливает его.
- Пользователь использует новые рабочие ключи и сертификат в информационной системе.

При этом обработка запроса на служебный сертификат осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «оператор», а обработка запроса на рабочий сертификат осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «администратор».

Для реализации данного режима нужно выполнить следующие настройки:

На Центре Сертификации

- Настроить срок действия служебного сертификата, путем установки нужного срока для идентификатора «Временный доступ к Центру Регистрации» в модуле политики Крипто-Про УЦ службы сертификации

На Центре Регистрации

- Выполнить полную установку ПО Центра Регистрации
- Откорректировать файл шаблона печати сертификата Cert.xsl из виртуального каталога UI в соответствии с корпоративными требованиями оформления внешнего вида печатной копии сертификата пользователей, при их печати через АРМ пользователей
- На вкладке "Web-интерфейс" окна свойств узла Центра регистрации приложения «Параметры Центра Регистрации» настроить параметры, определяющие выбор CSP по умолчанию, а также режим возможности поиска сертификатов других пользователей. Значения данных параметров определяются владельцем УЦ.
- Включить автоматическую обработку запросов на регистрацию и включить автоматическую обработку запросов на сертификат для АРМов пользователя (Веб-приложений). Для этого установить в 1 значения параметров RegReqAutoAccept и CertReqAutoAccept на вкладке "Web-интерфейс" окна свойств узла Центра регистрации приложения «Параметры Центра Регистрации»
- Настроить политику обработки неподписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Прошедший проверку» (определить список областей использования служебного сертификата);
- Настроить политику обработки подписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Временный сертификат» (определить список областей использования рабочего сертификата);
- Настроить политику обработки подписанных запросов на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации» для роли «Пользователь Центра Регистрации» (определить список областей использования рабочего сертификата);

- Настроить матрицу прав доступа на вкладке «Безопасность» окна свойств приложения «Параметры Центра Регистрации» по схеме предыдущего режима (основного распределенного)

7. Обеспечение кросс-сертификации

7.1. Основные понятия

В соответствии с рекомендациями X.509 (ITU-T Rec. X.509 (2000 E)) сертификаты Центров Сертификации могут быть:

- самоизданными (Self-issued certificate);
- кросс-сертификатами (Cross certificate).

Самоизданные сертификаты – это сертификаты в которых поля «Издатель» (Issuer) и «Субъект» (Subject) совпадают и определяют сам Центр Сертификации.

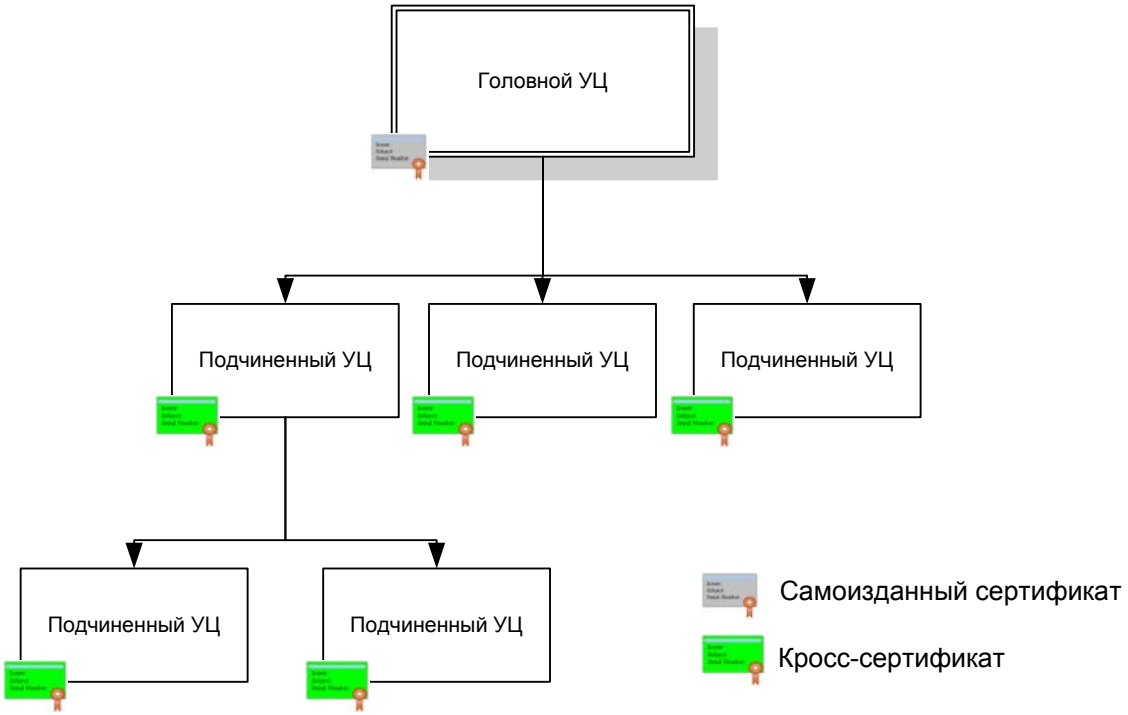
Кросс-сертификаты – это сертификаты, в которых поля «Издатель» и «Субъект» различны и определяют различные Центры Сертификации.

С помощью кросс-сертификатов устанавливаются доверительные отношения между Центрами Сертификации различных удостоверяющих центров. Установление доверительных отношений может быть основано на двух моделях:

- иерархической (strict hierarchy);
- распределенной (сетевой, мостовой, distributed trust model).

В иерархической модели доверительных отношения (см. Рисунок 4), Центр Сертификации верхнего уровня (головной УЦ) имеет самоизданный сертификат, Центры Сертификации всех подчиненных УЦ имеют кросс-сертификаты, в которых поле «Субъект» определяет Центр Сертификации подчиненного УЦ текущего уровня, поле «Издатель» определяет Центр Сертификации удостоверяющего центра вышестоящего уровня, который издал этот кросс-сертификат.

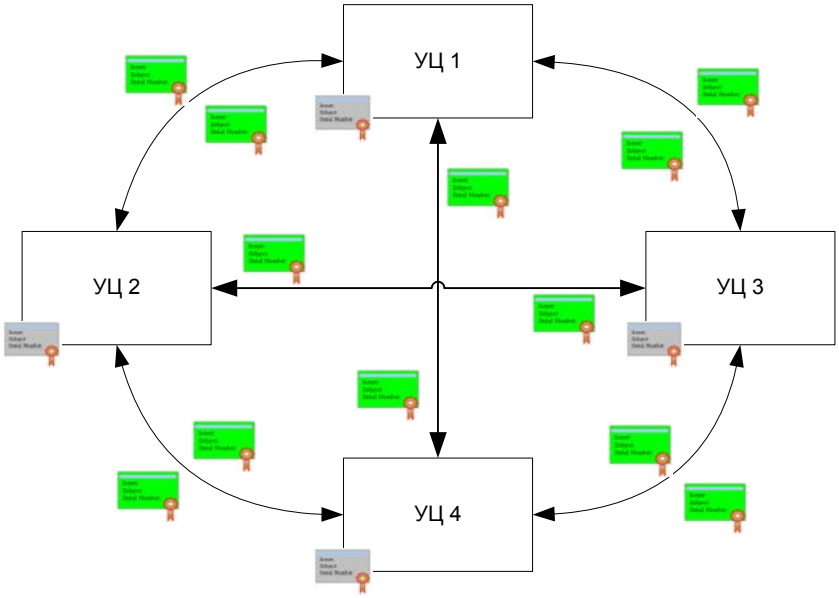
Рисунок 4. Иерархическая модель доверительных отношений УЦ



В распределенной модели доверительных отношения (см. Рисунок 5), все Центры Сертификации удостоверяющих центров имеют самоизданные сертификаты. Удостоверяющие центры устанавливают между собой доверительные отношения попарно, путем выпуска кросс-сертификатов Центров Сертификации. Таким образом, каждый Центр Сертификации помимо самоизданного сертификата является владельцем кросс-сертификатов, в количестве, равном

числу Центров Сертификации, с кем были установлены доверительные отношения. Центр Сертификации становится «подчиненным» одному или нескольким Центрам Сертификации других удостоверяющих центров.

Рисунок 5. Распределенная модель доверительных отношений УЦ



ПАК «КриптоПро УЦ» обеспечивает выполнение технологических процедур при установлении доверительных отношений между удостоверяющими центрами, с использованием кросс-сертификатов, как по иерархической модели, так и по распределенной модели. При этом в качестве технологической основы обеспечения деятельности удостоверяющих центров могут выступать не только комплексы «КриптоПро УЦ», но и комплексы других производителей, таких как: Keon RSA Security Inc., UniCERT Baltimore Technologies, «Стандарт-УЦ».

7.2. Технологические процедуры обеспечения кросс-сертификации

К технологическим процедурам обеспечения кросс-сертификации относятся:

- процедура формирования запроса на кросс-сертификат;
- процедура изготовления кросс-сертификата.

Выполнение процедур зависит от модели доверительных отношений, для которой используется кросс-сертификат.

7.2.1. Формирования запроса на кросс-сертификат в иерархической модели

Формирование запроса на кросс-сертификат для подчиненного Центра Сертификации выполняется в процессе первоначальной установки программного обеспечения Центра Сертификации ПАК «КриптоПро УЦ» и в процессе смены (плановой или неплановой) ключей Центра Сертификации.

При установке программного обеспечения Центра Сертификации данная процедура выполняется в соответствии с описанием раздела «Установка службы сертификации» (режим «Подчиненный Центр сертификации») ЖТЯИ.00035-01 90 03. КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows Server 2003 или ЖТЯИ.00035-01 90 04. КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows 2000 Server.

При плановой/неплановой смене ключей Центра Сертификации данная процедура выполняется в соответствии с описанием раздела «Смена ключей Центра Сертификации» ЖТЯИ.00035-01 90 03. КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на

платформе MS Windows Server 2003 или ЖТЯИ.00035-01 90 04. КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows 2000 Server.

7.2.2. Формирования запроса на кросс-сертификат в распределенной модели

Формирование запроса на кросс-сертификат Центра Сертификации может выполняться в любой момент в процессе эксплуатации ПАК «КриптоПро УЦ» после первоначальной установки программного обеспечения Центра Сертификации.

Данная процедура выполняется в соответствии с описанием раздела «Формирование запроса на кросс-сертификат Центра Сертификации» ЖТЯИ.00035-01 90 03. КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows Server 2003 или ЖТЯИ.00035-01 90 04. КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows 2000 Server.

7.2.3. Изготовление кросс-сертификата в иерархической модели

Изготовление кросс-сертификата в иерархической модели (сертификата подчиненного Центра Сертификации) выполняется путем выполнения штатной процедуры регистрации уполномоченного лица подчиненного удостоверяющего центра как пользователя УЦ и изготовления ему сертификата открытого ключа по запросу на сертификат.

Для обеспечения возможности издания сертификата уполномоченного лица подчиненного удостоверяющего центра необходимо предварительно выполнить настройку программного обеспечения Центра Сертификации в соответствии с разделом «Настройка Центра Сертификации для выпуска сертификатов подчиненных ЦС» ЖТЯИ.00035-01 90 03. КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows Server 2003 или ЖТЯИ.00035-01 90 04. КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows 2000 Server. и программного обеспечения Центра Регистрации в соответствии с разделом «Настройка параметров Центра Регистрации для выпуска сертификатов открытых ключей уполномоченных лиц подчиненных УЦ» ЖТЯИ.00035-01 90 05. КриптоПро УЦ. Центр Регистрации. Руководство по эксплуатации.

7.2.4. Изготовление кросс-сертификата в распределенной модели

Процедура изготовления кросс-сертификата в распределенной модели идентична по выполнению процедуре изготовления кросс-сертификата в иерархической модели. Настройки программного обпеспечения Центра Сертификации и Центра Регистрации, производимые для выполнения процедуры идентичны настройкам, осуществляемым при изготовлении кросс-сертификата в иерархической модели.

8. Публикация списков отозванных сертификатов

Одной из задач, возлагаемых на Удостоверяющий Центр, является обеспечение участников информационных систем, в которых используются сертификаты открытых ключей, информацией, необходимой для определения статуса (действительности) сертификатов открытых ключей, издаваемых Удостоверяющим Центром.

Одним из механизмов определения статуса сертификатов открытых ключей является использование списков отозванных сертификатов (СОС, CRL).

8.1. Задания публикации СОС и практика их применения

Для обеспечения автоматизации процедур распространения СОС, издаваемых Центром Сертификации, в рамках одного Удостоверяющего Центра, и по иерархии в случае использования подчиненных УЦ, на Центре регистрации используются задания публикации СОС, реализованные в программных компонентах Центра Сертификации и Центра Регистрации.

При этом задания публикации СОС на ЦР должны использоваться совместно с заданием публикации СОС и настройками модуля выхода Центра Сертификации.

Общая схема взаимодействия задания публикации СОС на Центре Сертификации и Центре Регистрации приведена на Рисунок 6.

Практика применения заданий зависит от регламента и режима работы Удостоверяющего Центра.

Режим 1: Головной удостоверяющий центр без сетевого соединения с подчиненными УЦ.

Используются следующие задания на ЦР:

- *Задание получения СОС из сетевого ресурса CDP своего ЦС в локальную папку CDP*. Это задание будет доставлять на ЦР СОС, изданные «своим» ЦС.
- *Задание копирования СОС из локальной папки CDP на дискету*. Это задание будет копировать на магнитную дискету 3,5” файлы с СОС, полученные предыдущим заданием.

Используются следующие задания на ЦС:

- *Модуль выхода Крипто-Про УЦ*. Модуль выхода будет обеспечивать формирование файла с CRL и заносить его в сетевой ресурс CDP Центра Сертификации.

Режим 2: Подчиненный УЦ, не имеющий сетевого соединения с вышестоящим УЦ (головным или вышестоящим по иерархии) и имеющий сетевое соединение с нижестоящими УЦ и/или предоставляющий сетевой доступ к файлам СОС, расположенным в сетевом ресурсе CDP Центра Регистрации, для пользователей.

Используются следующие задания на ЦР:

- *Задание публикации СОС с дискеты на сетевой ресурс incoming своего ЦС*. Это задание будет доставлять с ЦР СОС, расположенные на магнитной дискете 3,5” и полученные с вышестоящего УЦ.
- *Задание получения СОС из сетевого ресурса CDP своего ЦС в локальную папку CDP*. Это задание будет доставлять на ЦР СОС, изданные «своим» ЦС и полученные из вышестоящего УЦ.

Используются следующие задания на ЦС:

- *Модуль выхода Крипто-Про УЦ*. Модуль выхода будет обеспечивать формирование файла с CRL и заносить его в сетевой ресурс CDP Центра Сертификации.

- *Задание доставки СОС.* Задание обеспечивает репликацию файлов с CRL из папки incoming Центра Сертификации в домашний каталог папки CDP этого же Центра Сертификации.

Режим 3: Подчиненный УЦ, не имеющий сетевого соединения с вышестоящим УЦ (головным или вышестоящим по иерархии) и не имеющий сетевого соединения с нижестоящими УЦ и/или не предоставляющий сетевой доступ к файлам СОС, расположенным в сетевом ресурсе CDP Центра Регистрации, для пользователей.

Используются следующие задания на ЦР:

- *Задание публикации СОС с дискеты на сетевой ресурс incoming своего ЦС*. Это задание будет доставлять с ЦР СОС, расположенные на магнитной дискете 3,5” и полученные с вышестоящего УЦ.
- *Задание получения СОС из сетевого ресурса CDP своего ЦС в локальную папку CDP*. Это задание будет доставлять на ЦР СОС, изданные «своим» ЦС и полученные из вышестоящего УЦ.
- *Задание копирования СОС из локальной папки CDP на дискету*. Это задание будет копировать на магнитную дискету 3,5” файлы с СОС, полученные предыдущим заданием.

Используются следующие задания на ЦС:

- *Модуль выхода Крипто-Про УЦ*. Модуль выхода будет обеспечивать формирование файла с CRL и заносить его в сетевой ресурс CDP Центра Сертификации.
- *Задание доставки СОС.* Задание обеспечивает репликацию файлов с CRL из папки incoming Центра Сертификации в домашний каталог папки CDP этого же Центра Сертификации.

Режим 4: Подчиненный УЦ, имеющий сетевое соединение с вышестоящим УЦ (головным или вышестоящим по иерархии) и не имеющий сетевого соединения с нижестоящими УЦ и/или не предоставляющий сетевой доступ к файлам СОС, расположенным в сетевом ресурсе CDP Центра Регистрации, для пользователей.

Используются следующие задания на ЦР:

- *Задание публикации СОС из сетевого ресурса CDP ЦР вышестоящего ЦС на сетевой ресурс incoming своего ЦС*. Это задание будет доставлять из ЦР вышестоящего УЦ файлы с СОС и помещать их для обработки в «свой» ЦС.
- *Задание получения СОС из сетевого ресурса CDP своего ЦС в локальную папку CDP*. Это задание будет доставлять на ЦР СОС, изданные «своим» ЦС и полученные из вышестоящего УЦ.
- *Задание копирования СОС из локальной папки CDP на дискету*. Это задание будет копировать на магнитную дискету 3,5” файлы с СОС, полученные предыдущим заданием.

Используются следующие задания на ЦС:

- *Модуль выхода Крипто-Про УЦ*. Модуль выхода будет обеспечивать формирование файла с CRL и заносить его в сетевой ресурс CDP Центра Сертификации.
- *Задание доставки СОС.* Задание обеспечивает репликацию файлов с CRL из папки incoming Центра Сертификации в домашний каталог папки CDP этого же Центра Сертификации.

Режим 5: Подчиненный УЦ, имеющий сетевое соединение с вышестоящим УЦ (головным или вышестоящим по иерархии) и имеющий сетевое соединение с нижестоящими УЦ и/или

предоставляющий сетевой доступ к файлам СОС, расположенным в сетевом ресурсе CDP Центра Регистрации, для пользователей.

Используются следующие задания на ЦР:

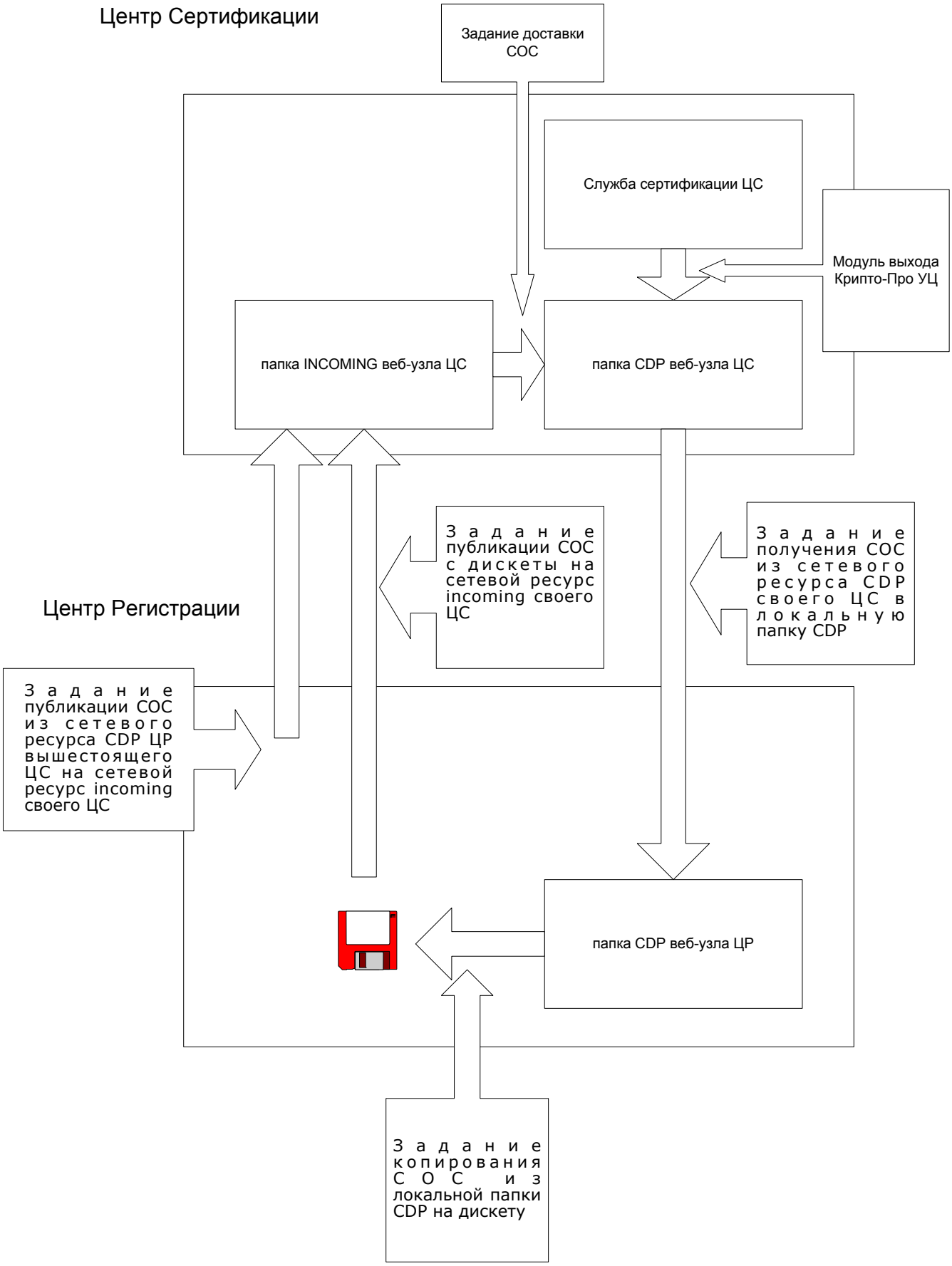
- *Задание публикации СОС из сетевого ресурса CDP ЦР вышестоящего ЦС на сетевой ресурс incoming своего ЦС*. Это задание будет доставлять из ЦР вышестоящего УЦ файлы с СОС и помещать их для обработки в «свой» ЦС.
- *Задание получения СОС из сетевого ресурса CDP своего ЦС в локальную папку CDP*. Это задание будет доставлять на ЦР СОС, изданные «своим» ЦС и полученные из вышестоящего УЦ.

Используются следующие задания на ЦС:

- *Модуль выхода Крипто-Про УЦ*. Модуль выхода будет обеспечивать формирование файла с CRL и заносить его в сетевой ресурс CDP Центра Сертификации.
- *Задание доставки СОС.* Задание обеспечивает репликацию файлов с CRL из папки incoming Центра Сертификации в домашний каталог папки CDP этого же Центра Сертификации.

8.2. Схема взаимодействия заданий публикации СОС

Рисунок 6. Схема взаимодействия заданий публикации СОС на ЦС и ЦР



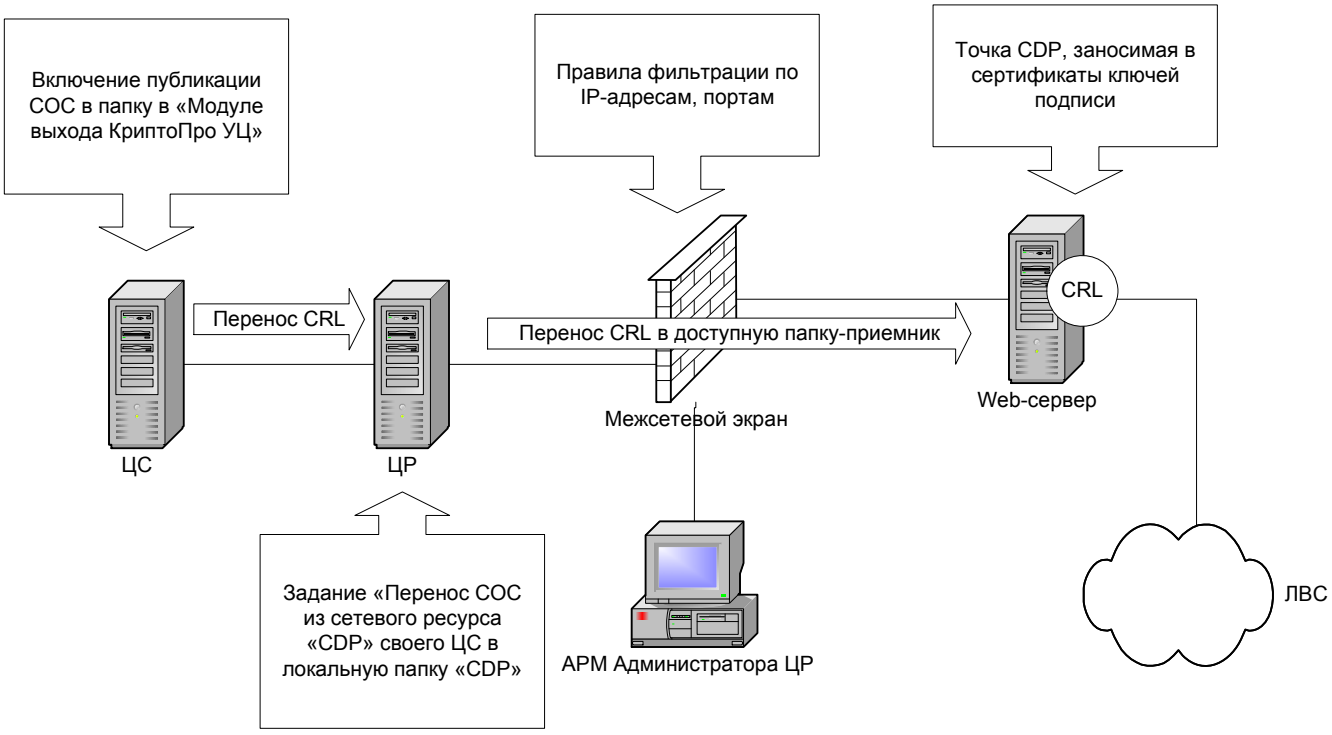
8.3. Публикация СОС в общедоступный ресурс при изолированном режиме работы

Изолированный режим работы ПАК «КриптоПро УЦ» описан в документе «ЖТЯИ.00035-01 90 10. КриптоПро УЦ. Руководство по безопасности».

Этот режим не предусматривает наличие у пользователей сетевого доступа к Центру Регистрации. В тоже время, пользователям должен быть доступен актуальный СОС, размещаемый в виде файла на ресурсе. URL этого ресурса как правило заносят в расширение CRL Distribution Point (CDP) в издаваемые сертификаты пользователей УЦ.

Для решения этой задачи применяется следующая схема подключения технических средств (см. Рисунок 7), которая предусматривает создание так называемого внешнего веб-сервера (или назначение из числа существующих), в котором будет располагаться папка с файлами СОС. При этом к данной папке должен быть предоставлен доступ командой PUT протокола HTTP с IP адреса межсетевого экрана удостоверяющего центра.

Рисунок 7. Схема подключения и настройки публикации СОС на внешний веб-сервер



Задача переноса СОС на Центре Регистрации в таком режиме настраивается так, что в качестве папки-приемника должен указываться не файловый ресурс, а URL к виртуальному каталогу размещения CRL на веб-сервере.

При такой схеме подключения необходимо выполнить дополнительную настройку (в дополнении к настройкам, приведенным в «ЖТЯИ.00035-01 90 10. КриптоПро УЦ. Руководство по безопасности») межсетевого экрана, обеспечивающую фильтрацию пакетов по следующим правилам:

- Разрешить прохождение пакетов с IP адреса ЦР на IP адрес веб-сервера в режиме сокрытия адреса источника (NAT);
- Разрешить соединение с портов с номерами больше 1024 ЦР на порт 80 веб-сервера и запретить другие порты;
- Разрешить HTTP как тип запрашиваемого сервиса и запретить другие типы запрашиваемых сервисов.

Обобщенно, указанные правила можно выразить следующей фразой: разрешить обращение с непривилегированных портов Центра Регистрации на HTTP порт WEB-сервера по протоколу HTTP в режиме сокрытия адреса источника (NAT).

8.4. Публикация СОС в Active Directory или на сервер, не входящий в состав ПАК «КриптоПро УЦ»

Если Центр Регистрации включен в домен, то публикация СОС в Active Directory настраивается в соответствии с разделом «Публикация списков отозванных сертификатов в Active Directory» документа «КриптоПро УЦ. Регламентные задания» для задачи переноса СОС на Центре Регистрации.

В том случае, когда требования безопасности не позволяют включить УЦ (Центр Регистрации) в домен, или когда требуется перенос и установка списков отзыва на отдельный сервер (например, сервер OCSP или TSP), используется приложение «КриптоПро УЦ. Регламентные задания».

Установка и настройка приложения осуществляется в соответствии с документом «КриптоПро УЦ. Регламентные задания».

9. Политики выдачи и политики применения сертификатов открытых ключей

Политики выдачи сертификатов используются для определения степени доверия к сертификатам открытых ключей. Например, политика выдачи сертификатов может определять, что сертификаты выдаются пользователям Оператором УЦ только при личной явке пользователя в УЦ (Централизованный режим работы УЦ).

Политики выдачи определяются в расширении **"Certificate Policies"** (также известном как **"Issuance Policies"**) сертификата открытого ключа и задаются объектными идентификаторами (OID). При использовании политик выдачи сертификатов необходимо зарегистрировать OID для каждой политики. Включение OID той или иной политики выдачи в расширение **"Certificate Policies"** означает, что этот сертификат был выдан в соответствии с данной политикой.

Политики применения сертификатов ограничивают область использования сертификатов. Например, политика применения сертификата может определять, что сертификат может быть использован для защиты электронной почты.

Политики применения сертификатов определяются в расширении **"Application Policies"** сертификата открытого ключа и задаются объектными идентификаторами (OID).

Политики применения сертификатов во многом аналогичны полю **"Расширенное использование ключа"** (**"Extended Key Usage"**) сертификатов, поскольку и то и другое поле содержат один или несколько объектных идентификаторов, задающих область применения сертификата. Политики применения сертификатов и Extended Key Usage являются взаимозаменяемыми на ОС Microsoft Windows XP и выше, т.е. одни и те же значения OID могут присутствовать в политике применения сертификатов или в Extended Key Usage, при этом они будут одинаково интерпретироваться. Поскольку на ОС более ранних версий, чем Windows XP, политики применения сертификатов не поддерживаются, в ПАК «КриптоПро УЦ» при создании расширения **"Application Policies"** в него включаются все объектные идентификаторы расширенного использования ключа из запроса на сертификат.

Отличием политик применения сертификатов от Extended Key Usage является возможность определения отображений политик применения или ограничений политик при кросс-сертификации различных УЦ.

Удостоверяющий Центр обязан предоставлять сведения об использовании политик выдачи и политик применения сертификатов открытых ключей. Эти сведения должны быть опубликованы в Регламенте Удостоверяющего Центра.

9.1. Настройка политик выдачи сертификатов открытых ключей

Расширение «Certificate Policies»/«Политики сертификата» (2.5.29.32) сертификата открытого ключа, выпускаемого Центром Сертификации, включает в себя компоненты, идентифицирующие политики выдачи данного сертификата открытого ключа.

Перечень политик выдачи сертификата открытого ключа и их значений, включаемых в выпускаемый сертификат, задаётся в запросе на сертификат открытого ключа (в расширении EKU - «Extended Key Usage»/«Расширенное использование ключа»), передаваемом на Центр Сертификации из Центра Регистрации.

На Центре Сертификации настраиваются правила сопоставления OID-ов EKU, которые будут включаться в выпускаемый сертификат в поле «Certificate Policies»/«Политики сертификата» – см. раздел «Использование ключа, политики выдачи и политики применения сертификатов» в документе «ЖТЯИ.00035-01 90 04. КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows 2000 Server» или «ЖТЯИ.00035-01 90 03. КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows 2003 Server».

9.2. Настройка политик применения сертификатов открытых ключей

Расширение «Application Policies»/«Политики применения» (1.3.6.1.4.1.311.21.10) сертификата открытого ключа, выпускаемого Центром Сертификации, включает в себя компоненты, идентифицирующие политики применения данного сертификата открытого ключа.

Перечень политик применения сертификата открытого ключа и их значений, включаемых в выпускаемый сертификат, задаётся в запросе на сертификат открытого ключа (в расширении EKU - «Extended Key Usage»/« Расширенное использование ключа»), передаваемом на Центр Сертификации из Центра Регистрации.

На Центре Сертификации настраиваются правила сопоставления OID-ов EKU, которые будут включаться в выпускаемый сертификат в поле «Application Policies»/«Политики применения» – см. раздел «Использование ключа, политики выдачи и политики применения сертификатов» в документе «ЖТЯИ.00035-01 90 04. КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows 2000 Server» или «ЖТЯИ.00035-01 90 03. КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows 2003 Server».

10. Описание ролей, используемых в УЦ и их реализация

Для обеспечения функционирования программно-аппаратного комплекса Удостоверяющего Центра обеспечивается реализация следующих доверенных ролей:

- системный администратор УЦ;
- администратор ЦС;
- администратор ЦР;
- администратор АРМ ЦР;
- оператор АРМ ЦР.

10.1. Описание ролей УЦ

Системный администратор УЦ – администратор общесистемного программного обеспечения, используемого для функционирования каждого компонента УЦ (ЦС, ЦР, АРМ администратора).

Системный администратор УЦ обеспечивает выполнение следующих задач:

- установку общесистемного и специального программного обеспечения компонентов УЦ;
- администрирование общесистемного программного обеспечения;
- установку и конфигурирование дополнительных программно-аппаратных средств, обеспечивающих контроль целостности программных средств;
- администрирование программно-аппаратных средств, реализующих меры защиты от НСД на компонентах УЦ.

Системный администратор работает на компонентах УЦ с учетной записью, являющейся членом группы Администраторов ОС, эксплуатируемой на ЦС, ЦР и АРМ администратора.

Администратор ЦС – уполномоченное лицо Удостоверяющего Центра, администратор специального программного обеспечения ЦС.

Администратор ЦС обеспечивает выполнение следующих задач:

- управление (формирование, эксплуатация, безопасное использование и уничтожение) секретным ключом и сертификатом ЦС;
- администрирование (установка и изменение) параметров модуля безопасности ЦС;
- управление (формирование, эксплуатация и уничтожение) секретным ключом и сертификатом Web-сервера ЦС;
- регистрацию подчиненных Центров Регистрации;
- управление (установка и изменение) параметрами публикации списка отозванных сертификатов (CRL), а также его формирование;
- архивирование и восстановление баз данных ЦС.

Администратор ЦС работает на ЦС с учетной записью, являющейся членом группы Администраторов.

Администратор ЦР – администратор специального программного обеспечения ЦР.

Администратор ЦР обеспечивает выполнение следующих задач:

- управление (формирование, эксплуатация, безопасное использование и уничтожение) закрытым ключом и сертификатом ЦР;
- администрирование (установка и изменение) параметров Центра Регистрации;

- управление (формирование, эксплуатация и уничтожение) закрытым ключом и сертификатом Web-сервера ЦР;
- регистрацию привилегированных пользователей ЦР (администраторов и операторов АРМ ЦР);
- архивирование и восстановление баз данных ЦР.

Администратор ЦР работает на ЦР с учетной записью, являющейся членом группы Администраторов.

Администратор АРМ ЦР – лицо, осуществляющее управление объектами управления Центра Регистрации.

Администратор АРМ ЦР обеспечивает выполнение следующих задач:

- идентификация и регистрация пользователей ЦР;
- генерация ключей, получение и предоставление изготовленных сертификатов открытых ключей пользователей;
- получение от пользователей системы запросов на выпуск сертификата в электронном виде с подтверждением на бумажном бланке;
- верификация запросов на выпуск сертификата;
- отзыв сертификатов открытых ключей пользователей системы;
- публикация списка отозванных сертификатов;
- получение и обработка сообщений о компрометации ключей пользователями.

Администратор АРМ ЦР работает на рабочем месте с учетной записью, являющейся членом группы Администраторов.

Оператор АРМ ЦР – лицо, осуществляющее выполнение следующих функций:

- регистрация пользователей в Базе Данных Центра Регистрации;
- генерация служебных ключей и сертификатов открытых ключей при выполнении процедуры регистрации пользователей в централизованном режиме;
- обработка запросов на регистрацию пользователей.

10.2. Реализация ролей

Системный администратор УЦ реализует свои задачи с использованием программных средств, предоставляемых операционной системой (ОС) Windows 2000, SQL Server 2000.

Администратор ЦС реализует свои задачи с использованием программных средств, предоставляемых ПО ЦС и ОС Windows 2000, а именно:

- утилиты ПО ЦС: CaCliMak.exe, CaWebMak.exe, CaWebReq.exe;
- приложение настройки параметров ЦС: CAConfig.exe;
- компонент «Служба сертификации»;
- компонент «Диспетчер Служб Интернет».

Администратор ЦР реализует свои задачи с использованием программных средств, предоставляемых ПО ЦР и ОС Windows 2000, а именно:

- утилиты ПО ЦР: RaCliReq.exe, RaCliSet.exe, RaWebReq.exe, RaWebSet.exe;
- приложение настройки параметров ЦР: RaConfig.msc;
- компонентом «Диспетчер Служб Интернет».

Администратор и оператор АРМ ЦР реализуют свои задачи с использованием программных средств, предоставляемых ПО АРМ администратора ЦР и Web-браузера MS Internet Explorer в части печати бумажных форм сертификатов открытых ключей.

11. Формат и состав сертификатов открытых ключей пользователей

11.1. Требования законодательства РФ по составу сертификатов открытых ключей подписи

В соответствии со статьей 6 Федерального Закона Российской Федерации от 10 января 2002 года № 1-ФЗ «ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ» Сертификат ключа подписи должен содержать следующие сведения:

- уникальный регистрационный номер сертификата ключа подписи;
- даты начала и окончания срока действия сертификата ключа подписи;
- фамилию, имя и отчество владельца сертификата ключа подписи или псевдоним владельца;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
- наименование и место нахождения Удостоверяющего Центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

На основании этой же статьи Закона сертификат открытого ключа может содержать следующие сведения:

- должность владельца сертификата открытого ключа;
- наименование организации, в которой данная должность занимается;
- местонахождение организации;
- квалификацию владельца сертификата открытого ключа;
- иные сведения, подтверждаемые соответствующими документами.

11.2. Состав сертификатов открытых ключей пользователей

Формат сертификата, выпускаемого Центром Сертификации, определен в рекомендациях IETF RFC 3280, которые описывают профиль международного стандарта ISO/IEC 9594-8:1998 (также опубликован как рекомендации ITU-T X.509 в 1997 году). В настоящее время основным принятым форматом является формат версии 3, позволяющий определить дополнения (**extensions**), с помощью которых реализуется определенная политика безопасности в системе.

Наименование поля	Описание	Применение в соответствии с Законом «Об ЭЦП»
CertificateSerialNumber	Серийный номер является целым числом, устанавливаемым ЦС для каждого сертификата. Значение серийного номера является уникальным для каждого сертификата, выпущенного данным ЦС	Уникальный регистрационный номер сертификата ключа подписи

Validity	Срок действия (в виде временного интервала) в течение которого УЦ управляет сертификатом (отслеживает состояние). Данное поле представляет последовательность двух дат: дата начала действия сертификата (**notBefore**) и дата окончания срока действия сертификата (**notAfter**).	Даты начала и окончания срока действия сертификата ключа подписи
Subject	Поле **Владелец** идентифицирует физическое лицо, являющееся обладателем закрытого ключа, соответствующего открытому ключу в сертификате.	Фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца, иные сведения о владельце сертификата ключа подписи
SubjectPublicKeyInfo	Поле содержит информацию об открытом ключе (subjectPublicKey), идентификатор и параметры алгоритма открытого ключа (algorithm)	Открытый ключ электронной цифровой подписи и наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи
Issuer	Поле **Издатель** идентифицирует уполномоченное лицо УЦ, с использованием закрытого ключа которого сформирована ЭЦП сертификата.	Наименование и место нахождения Удостоверяющего Центра, выдавшего сертификат ключа подписи
ExtendedKeyUsage	Поле **Расширенная область применения ключа** идентифицирует области применения сертификата	Сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение

11.3. Настройка имени владельцев сертификатов открытых ключей

Поле **Subject** сертификата открытого ключа, выпускаемого Центром Сертификации, включает в себя компоненты, идентифицирующие владельца сертификата открытого ключа.

Центр Сертификации поддерживает следующие компоненты имени:

Обозначение	Наименование	Описание
CommonName	Общее имя	Для сертификатов пользователей: полное имя владельца сертификата открытого ключа; Для сертификатов серверных компонентов: полное доменное имя в DNS
Country	Страна/регион	Страна проживания владельца сертификата открытого ключа (в

		кодировке в соответствии со стандартом ISO 3166)
DeviceSerialNumber	Серийный номер устройства	Идентифицирует серийный номер устройства, на котором работает серверный компонент, использующий сертификат открытого ключа (сертификаты серверных компонентов)
DomainComponent	Компонент доменного имени	Компонент DNS имени владельца сертификата открытого ключа
Email	Электронная почта	Адрес электронной почты владельца сертификата открытого ключа
GivenName	Имя	Имя (первое имя) владельца сертификата открытого ключа
Initials	Инициалы	Инициалы владельца сертификата открытого ключа
Locality	Город	Наименование города местонахождения/проживания владельца сертификата открытого ключа
Organization	Организация	Наименование организации, в которой занимает должность владелец сертификата открытого ключа
OrgUnit	Подразделение	Наименование подразделения организации, в которой занимает должность владелец сертификата открытого ключа
State	Область	Наименование области (субъекта Федерации) местонахождения/проживания владельца сертификата открытого ключа
StreetAddress	Адрес	Почтовый код, наименование улицы, номер дома и т.д., определяющие местонахождение/проживание владельца сертификата открытого ключа
SurName	Фамилия	Фамилия владельца сертификата открытого ключа
Title	Должность	Должность, занимаемая владельцем сертификата открытого ключа
UnstructuredAddress	Неструктурированный адрес	Полный почтовый или юридический адрес владельца сертификата открытого ключа
UnstructuredName	Неструктурированное имя	Полное имя или псевдоним владельца сертификата открытого ключа

Перечень полей имени владельца сертификата открытого ключа и их значений, включаемые в выпускаемый сертификат, задаются в запросе на сертификат открытого ключа, передаваемый на Центр Сертификации из Центра Регистрации. На Центре Регистрации перечень полей имени, которые могут (или должны) включать пользователи в свои запросы на

сертификат открытого ключа, определяются **Политикой имен** приложения **Параметры Центра Регистрации**. Необходимо обеспечить (организационными мерами) синхронизацию политики имен на Центре Сертификации, задаваемой на вкладке **Политика имен** в настройке **Модуля политики КриптоПро УЦ** с политиками имен всех Центров Регистрации (включая дополнительные модули доступа к Центру Регистрации), работающих с данным Центром Сертификации, таким образом, чтобы политика имен на Центре Сертификации представляла собой объединение политик имен, заданных на Центрах Регистрации, работающих с этим Центром Сертификации.

11.4. Дополнения (extensions) сертификатов открытых ключей

Сертификаты открытых ключей, формируемые Центром Сертификации УЦ, могут содержать дополнения формата версии 3.

Дополнения, используемые в сертификатах версии 3, определены рекомендациями X.509 версии 3 ITU-T и рекомендациями IETF RFC 3280.

Перечень дополнений, которые поддерживаются Центром Сертификации УЦ, приведен в таблицах 1 и 2.

Таблица 1. Дополнения, включаемые в сертификат Центром Сертификации

№ п/п	Наименование дополнения	Предназначение	Точка настройки
1.	cRLDistributionPoint	Точка распространения СОС	Модуль политики КриптоПро УЦ
2.	authorityAccessInfo	Способ доступа к информации ЦС	Модуль политики КриптоПро УЦ
3.	CertificatesPolicies	Политики выдачи сертификата	Модуль политики КриптоПро УЦ (на основе данных запроса), см. п. 9.1
4.	ApplicationPolicies	Политики применения сертификата	Модуль политики КриптоПро УЦ (на основе данных запроса), см. п. 9.2
5.	basicConstraints	Базовые ограничения	Модуль политики КриптоПро УЦ

Таблица 2. Дополнения, включаемые в сертификат Центром Сертификации на основе данных запроса

№ п/п	Наименование дополнения	Предназначение	Поддержка в ПО УЦ
1.	keyUsage	применение ключа	АРМ
2.	extendedKeyUsage	Расширенная область применения ключа	АРМ
3.	NameConstraints	Ограничения имен	ПП
4.	SubjectAltName	Альтернативные имена	АРМ*, ПП
5.	CertificateTemplate	Имя шаблона сертификата	АРМ*, ПП
6.	PrivateKeyUsagePeriod	Срок действия закрытого ключа	ПП

Графа «Поддержка в ПО УЦ» содержит информацию о том, какие дополнения сертификата включаются в запрос на сертификат открытого ключа в клиентских компонентах программного комплекса УЦ.

Сокращение **АРМ** означает, что данное дополнение включается в запрос на сертификат, формируемый программным обеспечением АРМ администратора ЦР, АРМ зарегистрированного пользователя, АРМ сетевой (удаленной) регистрации.

Сокращение **АРМ*** означает, что данное дополнение включается в запрос на сертификат, формируемый программным обеспечением АРМ администратора ЦР для сертификатов, используемых для входа в домен Windows (WinLogon).

Сокращение **ПП** означает, что данное дополнение может включаться в запрос на сертификат, формируемым программным обеспечением другого производителя. В этом случае, запрос на сертификат должен быть передан администратору/оператору, работающему с использованием АРМ администратора ЦР для дальнейшей обработки. Запрос на сертификат также может быть передан на обработку в ЦР посредством использования программного Интерфейса Внешних Приложений (см. Руководство программиста).

Для обработки дополнений, помеченных в таблице 1 сокращением **ПП**, при формировании сертификата Центром Сертификации необходимо выполнить настройку модуля политики КриптоПро УЦ на Центре Сертификации, разрешающую включение данных дополнений в сертификат открытого ключа.

Идентификаторы дополнений сертификата приведены в таблице 3.

Таблица 3. Идентификаторы дополнений (расширений)

№ п/п	Наименование дополнения	Идентификатор
1.	NameConstraints	2.5.29.30
2.	SubjectAltName	2.5.29.17
3.	PrivateKeyUsagePeriod	2.5.29.16
4.	KeyUsage	2.5.29.15
5.	extendedKeyUsage	2.5.29.37

12. Формат и состав запросов на сертификаты открытых ключей

Запрос на сертификат представляет собой структурированную двоичную запись в формате ASN.1, состоящую из:

- имени пользователя системы;
- открытого ключа пользователя;
- дополнительных атрибутов, которые могут быть включены в сертификат;
- ЭЦП пользователя, сформированную с использованием закрытого ключа, соответствующего открытому ключу в запросе, заверяющую совокупность этих данных.

В соответствии с международной практикой, запрос на сертификат оформляется по стандарту RSA PKCS#10.

Запрос на сертификат представляет собой последовательность следующего синтаксиса:

```
CertificationRequest ::= SEQUENCE {
  certificationRequestInfo   CertificationRequestInfo,
  signatureAlgorithm         SignatureAlgorithmIdentifier,
  signature                  Signature }

SignatureAlgorithmIdentifier ::= AlgorithmIdentifier

Signature ::= BIT STRING
```

Поля **signatureAlgorithm** и **signature** имеют то же значение, что и аналогичные поля в сертификате.

Информация в запросе на сертификат представлена в виде последовательности:

```
CertificationRequestInfo ::= SEQUENCE {
  version                  Version,
  subject                  Name,
  subjectPublicKeyInfo     SubjectPublicKeyInfo,
  attributes           [0] IMPLICIT Attributes }

Version ::= INTEGER

Attributes ::= SET OF Attribute
```

Поля последовательности **CertificationRequestInfo** имеют следующее значение:

- **version** – номер версии. Используется значение 0;
- **subject** – X.500 DN владельца сертификата (субъекта или объекта, чей открытый ключ должен быть сертифицирован);
- **subjectPublicKeyInfo** – информация об открытом ключе, который должен быть сертифицирован. Описание поля приведено в разделе описания сертификата.
- **attributes** – набор дополнительной информации (атрибутов), которую субъект намерен поместить в издаваемый сертификат.

13. Формат и состав списка аннулированных (отозванных) сертификатов (СОС)

Список отозванных сертификатов (СОС) представляет собой структурированную двоичную запись в формате ASN.1, состоящую из:

- имени Издателя (Удостоверяющего центра), выпустившего СОС;
- даты выпуска СОС и даты обновления СОС;
- дополнительных атрибутов, которые могут быть включены в СОС;
- списка элементов, каждый из которых включает ссылку на отзываемый сертификат и дополнительной информации о нем и причинах его отзыва;
- ЭЦП Издателя, заверяющую совокупность этих данных.

Формат СОС определен в рекомендациях ITU-T 1997 года и рекомендациях IETF 1999 года. В настоящее время основным принятым форматом является формат СОС версии 2.

СОС имеет следующий синтаксис.

```
CertificateList  ::=  SEQUENCE  {
     tbsCertList          TBSCertList,
     signatureAlgorithm   AlgorithmIdentifier,
     signatureValue       BIT STRING  }

TBSCertList  ::=  SEQUENCE  {
     version                 Version OPTIONAL,
                                  -- if present, shall be v2
     signature               AlgorithmIdentifier,
     issuer                  Name,
     thisUpdate              Time,
     nextUpdate              Time OPTIONAL,
     revokedCertificates     SEQUENCE OF SEQUENCE  {
          userCertificate         CertificateSerialNumber,
          revocationDate          Time,
          crlEntryExtensions      Extensions OPTIONAL
                                        -- if present, shall be v2
                                }  OPTIONAL,
     crlExtensions           [0]  EXPLICIT Extensions OPTIONAL
                                        -- if present, shall be v2
                                }
```

Поля **Version**, **Time**, **CertificateSerialNumber** и **Extensions** определены и описаны в разделе описания сертификата.

Список отозванных сертификатов (СОС) представляет собой последовательность из трех обязательных полей:

- tbsCertList;
- signatureAlgorithm;
- signatureValue.

Первое поле **tbsCertList** является последовательностью, содержащей информацию об имени Издателя, дату издания данного списка и дату издания следующего списка, список отозванных сертификатов и опциональные дополнения. Каждый элемент из списка отозванных сертификатов в свою очередь тоже является последовательностью, содержащей серийный номер отозванного сертификата, дату отзыва и опциональные дополнения элемента списка.

Поле **signatureAlgorithm** содержит идентификатор алгоритма, использованный ЦС при формировании ЭЦП СОС. Данное поле содержит тот же идентификатор алгоритма, что и поле **signature** в последовательности **tbsCertList**.

Поле **signatureValue** содержит ЭЦП, сформированную на последовательность **tbsCertList**, которая представлена в кодировке DER ASN.1.

13.1.1. Версия

version

Данное поле опционально и идентифицирует версию СОС. При использовании дополнений в СОС используется версия 2.

13.1.2. ЭЦП

signature

Данное поле содержит идентификатор алгоритма, используемого ЦС при формировании ЭЦП СОС. Идентификатор алгоритма в данном поле аналогичен идентификатору в поле **Алгоритм ЭЦП (signatureAlgorithm)** в последовательности сертификата.

13.1.3. Издатель

issuer

Данное поле идентифицирует издателя, выпустившего и подписавшего СОС. Для дополнительной идентификации издателя может быть использовано дополнение **Альтернативное имя Издателя.** Поле содержит имя издателя в виде X.500 DN.

Подробное описание значения поля приведено в разделе **Издатель** сертификата.

13.1.4. Дата издания СОС

thisUpdate

Данное поле указывает дату издания данного СОС. Дата может быть представлена в виде типа **UTCTime** или **GeneralizedTime**. Описание типов **UTCTime** и **GeneralizedTime** представлено в разделе описания сертификата.

13.1.5. Дата следующего издания СОС

nextUpdate

Данное поле указывает дату следующего издания (обновления) СОС. Следующий СОС может быть издан ранее, но не позже указанной даты. ЦС при издании СОС должен устанавливать значение **nextUpdate** равным или большим, чем в во всех предыдущих СОС. Дата может быть представлена в виде типа **UTCTime** или **GeneralizedTime**. Согласно рекомендациям RFC 2459, УЦ при издании СОС включает поле **nextUpdate** во все издаваемые СОС, хотя данное поле и является опциональным.

13.1.6. Отозванные сертификаты

revokedCertificates

Данное поле содержит последовательность отозванных сертификатов. Каждый сертификат идентифицируется серийным номером. Для каждого сертификата указывается дата отзыва **revocationDate**. Для каждого сертификата может присутствовать список дополнений.

13.1.7. Дополнения

Extensions

Данное поле содержит список дополнений, описанных в разделе Дополнения.

14. Учетная информация по пользователям Удостоверяющего Центра

14.1. Персональная информация пользователя, заносимая в сертификат открытого ключа

Учетная информация о пользователе, заносимая в сертификат, определяет имя владельца сертификата открытого ключа. Удостоверяющий Центр обеспечивает уникальность имен владельцев сертификатов.

Перечень учетной информации по пользователям Удостоверяющего Центра, определяется настройками Центра Сертификации и Центра Регистрации.

Полный возможный набор компонентов имени владельцев сертификатов приведен в таблице (см. Таблица 4).

Таблица 4. Информация о владельцах сертификатов

Наименование компоненты имени	**Описание**
SurName	Фамилия
GivenName	Отчество
Initials	Инициалы
Title	Должность
UnstructuredName	Неструктурированное имя.
StreetAddress	Адрес
UnstructuredAddress	Неструктурированный адрес
DeviceSerialNumber	Серийный номер устройства
DomainComponent	Компонента доменного имени
CommonName	Общее имя/псевдоним
OrganizationalUnit	Наименование подразделения
Organization	Наименование организации
Locality	Город
State	Область/субъект Федерации
Country	Страна
Email	Адрес электронной почты

Учетная информация по зарегистрированному пользователю не может изменяться администратором Центра Регистрации в процессе работы.

14.2. Персональная информация пользователя, не заносимая в сертификат открытого ключа

Для более надежной идентификации пользователя на Удостоверяющем Центре при регистрации пользователя возможно занесение дополнительной информации. Данная информация не включается в выпускаемые сертификаты открытого ключа пользователя.

К этой информации относятся:

- ключевая фраза пользователя;
- неструктурированное поле длины 8000 байт;

Данная учетная информация может изменяться администратором Центра Регистрации в процессе работы.

15. Нештатные ситуации при эксплуатации УЦ

Ниже приведен основной перечень нештатных ситуаций и соответствующие действия персонала при их возникновении, который может служить для создания соответствующих инструкций пользователям системы.

Таблица 5. Действия персонала в нештатных ситуациях.

№ п/п	Нештатная ситуация	Действия персонала
1.	Эвакуация, угроза нападения, взрыва и т.п., стихийные бедствия, аварии общего характера в Удостоверяющем центре.	Остановить все ЭВМ. Персонал, имеющий доступ к ключам, обязан сдать все имеющиеся у него в наличии ключевые носители администратору безопасности. Администратор безопасности упаковывает все ключевые носители, регистрационные карточки сертификатов открытых ключей пользователей в опечатываемый контейнер, который выносит в безопасное помещение или здание. Опечатанный контейнер должен находиться под охраной до окончания действия нештатной ситуации и восстановления нормальной работы аппаратных и программных средств СКЗИ. Администратор безопасности оповещает по телефонным каналам общего пользования всех пользователей о приостановке работы системы. В случае наступления события, повлекшего за собой долговременный выход из строя аппаратных средств СКЗИ, администратор безопасности уничтожает всю ключевую информацию с носителей, находящихся в контейнере.
2.	Компрометация одного из личных ключевых носителей.	Порядок действий при компрометации ключей определяется регламентом Удостоверяющего Центра
3.	Выход из строя личного ключевого носителя.	Необходимо сообщить по телефону администратору о факте выхода из строя личного ключевого носителя и обеспечить его доставку для выяснения причин выхода из строя.
4.	Отказы и сбои в работе аппаратной части АРМ со встроенной СКЗИ.	При отказах и сбоях в работе аппаратной части АРМ со встроенной СКЗИ необходимо остановить работу, по возможности локализовать неисправность и в дальнейшем произвести ремонт в установленном порядке и, при необходимости, переустановку СКЗИ.
5.	Отказы и сбои в работе средств защиты от НСД.	При отказах и сбоях в работе средств защиты от НСД администратор безопасности должен восстановить работоспособность средств НСД. При необходимости переустановить программно-аппаратные средства НСД.
6.	Утеря личного ключевого носителя.	Утеря личного ключевого носителя приводит к компрометации ключей.
7.	Отказы и сбои в работе программных средств,	При отказах и сбоях в работе программных средств, вследствие не выявленных ранее ошибок в

№ п/п	Нештатная ситуация	Действия персонала
	вследствие не выявленных ранее ошибок в программном обеспечении.	программном обеспечении, необходимо остановить работу, локализовать по возможности причину отказов и сбоев и сообщить разработчику данного ПО для устранения причин, вызывающих отказы и сбои.
9.	Отказы в работе программных средств вследствие случайного или умышленного их повреждения.	При отказах в работе программных средств, вследствие случайного или умышленного их повреждения, лицо, ответственное за безопасность функционирования программных и аппаратных средств, обязано произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы программных средств в установленном порядке.
10.	Отказы в работе программных средств вследствие ошибок оператора.	При отказах в работе программных средств, вследствие ошибок оператора, оператор сообщает о данном факте лицу, ответственному за безопасность функционирования программных и аппаратных средств. Ответственный за безопасность функционирования программных и аппаратных средств дает соответствующие указания обслуживающему персоналу по восстановлению правильной работы программных средств в установленном порядке.

Типовые нештатные ситуации и их причины при отказе в работе программных средств в процессе эксплуатации.

№ п/п	Наименование приложения ПАК «КриптоПро УЦ»	Выполняемое действие	Описание ошибки программных средств	Перечень возможных причин
1.	АРМ администратора ЦР	Установка сертификата администратора с помощью **Мастера установки сертификата администратора**	Ошибка при установке сертификата	- capicom.dll или xenroll.dll не той версии или не установлен - ключевой контейнер не доступен - запрос на сертификат администратора делался не на этом экземпляре ОС - сертификат администратора уже устанавливался на этом экземпляре ОС
2.	Параметры Центра Регистрации	Протестировать соединение	Ошибка при установлении соединения с центром сертификации. Описание: Доступ запрещен	Сертификат Центра Регистрации не добавлен в список сертификатов Центров Регистрации в приложении **Параметры Центра Сертификации**.

3.	Параметры Центра Регистрации	Протестировать соединение	Ошибка при установлении соединения с центром сертификации. Описание ошибки содержит описание неопределенной ошибки клиента	- сбой в настройках SSL/TLS параметров к содержимому виртуального каталога CA на ЦС - на ЦР не установлен сертификат ЦС и/или актуальный CRL в хранилище сертификатов локального компьютера - веб-сервер ЦС не имеет доступа к ключевому контейнеру, соответствующего серверному сертификату - ПО ЦР не имеет доступа к ключевому контейнеру, соответствующего сертификату Центра Регистрации
4.	Параметры Центра Регистрации	Создать привилегированного пользователя	Некорректный запрос. Неверное имя DN	- перечень атрибутов имени субъекта в запросе не удовлетворяет политике имен ЦР - атрибуты имени субъекта в запросе расположены в порядке, не соответствующему порядку, определенном в политике имен ЦР
5.	АРМ администратора ЦР	Протестировать соединение	Описание ошибки содержит описание неопределенной ошибки клиента	- не установлен сертификат ЦС и/или актуальный CRL в хранилище сертификатов локального компьютера на ЦР и/или на рабочем месте администратора - сбой в настройках SSL/TLS параметров к содержимому виртуального каталога RA на ЦР - веб-сервер ЦР не имеет доступа к ключевому контейнеру, соответствующего серверному сертификату - ПО АРМ администратора не имеет доступа к ключевому контейнеру, соответствующего сертификату администратора
6.	АРМ администратора ЦР	Отзыв сертификата пользователя	Описание ошибки: Запрос находится в неподходящем состоянии	- не выполнена задача **Подтвердить** для данного сертификата

16. Приложения

16.1. Приложение 1. Запрос на сертификат

Имя владельца открытого ключа:

CN = Sidorov Alexander/OU = Management/O = ACME/C=RU/E = ASidorov@ACME.RU

```
SEQUENCE {
  SEQUENCE {
    INTEGER 0
    SEQUENCE {
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER countryName (2 5 4 6)
            (X.520 id-at (2 5 4))
          PrintableString 'RU'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER commonName (2 5 4 3)
            (X.520 id-at (2 5 4))
          PrintableString 'Sidorov Alexander'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
            (X.520 id-at (2 5 4))
          PrintableString 'Management'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER organizationName (2 5 4 10)
            (X.520 id-at (2 5 4))
          PrintableString 'ACME'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER emailAddress (1 2 840 113549 1 9 1)
            (PKCS #9 (1 2 840 113549 1 9).
          IA5String 'ASidorov@ACME.RU'
          }
        }
      }
    SEQUENCE {
      SEQUENCE {
        OBJECT IDENTIFIER GOST R 34.10-94 (1 2 643 2 2 20)
          (Crypto Pro Algorithm)
        SEQUENCE {
          OBJECT IDENTIFIER '1 2 643 2 2 32 2'
          OBJECT IDENTIFIER '1 2 643 2 2 30 1'
          }
        }
      BIT STRING 0 unused bits, encapsulates {
          OCTET STRING
            AB 2F A6 9F 61 F6 1A 8A 07 2D D7 3F BF 59 97 10
            5F AF 69 62 CC 30 13 3D 4A BB 47 04 B3 4D DF B7
```

```
            46 B8 CD E8 97 2F 93 DF E7 C7 95 B4 B7 3E 2E 64
            B4 89 4A E8 41 83 5C B1 65 07 D1 08 5E BA B1 1F
            39 4C 22 EA F0 1A E7 5E F6 17 68 D5 B0 DC D9 8A
            C8 1C 07 F3 15 59 D6 D7 73 E9 31 70 FC 60 EF 25
            64 6C 23 33 EB 40 C2 D5 5C D8 15 16 51 29 E3 27
            0E 6F 29 8F 9E F3 1B DE 5D D4 E3 7B 41 F6 E7 A4
          }
      }
    [0] {
      SEQUENCE {
        OBJECT IDENTIFIER '1 3 6 1 4 1 311 13 2 3'
        SET {
          IA5String '5.0.2195.2'
          }
        }
      SEQUENCE {
        OBJECT IDENTIFIER
          certReqExtensions (1 3 6 1 4 1 311 2 1 14)
          (Microsoft)
        SET {
          SEQUENCE {
            SEQUENCE {
              OBJECT IDENTIFIER keyUsage (2 5 29 15)
                (X.509 id-ce (2 5 29))
              BOOLEAN TRUE
              OCTET STRING, encapsulates {
                  BIT STRING 6 unused bits
                    '11'B
                  }
              }
            SEQUENCE {
              OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
                (X.509 id-ce (2 5 29))
              OCTET STRING, encapsulates {
                  SEQUENCE {
                    OBJECT IDENTIFIER
                      clientAuth (1 3 6 1 5 5 7 3 2)
                      (PKIX key purpose)
                    }
                  }
              }
            }
          }
        }
      SEQUENCE {
        OBJECT IDENTIFIER
          MS CryptoAPI-related extension (1 3 6 1 4 1 311 13 2 2)
          (Microsoft attribute)
        SET {
          SEQUENCE {
            INTEGER 2
            BMPString
              'Crypto-Pro Cryptographic Service Provider'
            BIT STRING 0 unused bits
              '101001100111011011110110011101 10'B
            }
          }
        }
      }
    }
  SEQUENCE {
    OBJECT IDENTIFIER GOST R 34.11/34.10-94 (1 2 643 2 2 4)
      (Crypto Pro Algorithm)
    NULL
```

```
    }
  BIT STRING 0 unused bits
    42 65 19 D1 06 17 03 97 78 2C 4B 2D 5B 38 A1 05
    AD 98 23 19 C9 20 7B 05 6D 5E D0 F5 98 55 DD FB
    60 D6 D6 85 D2 51 16 A5 54 B7 EF 3D 9F 62 DD 42
    B9 E9 26 7F A4 E2 CE AF 88 C2 E2 9C 15 72 28 18
  }
```

16.2. Приложение 2. Сертификат открытого ключа.

Имя владельца открытого ключа:

CN = Sidorov Alexander/OU = Management/O = ACME/C = RU/E = ASidorov@ACME.RU

Имя издателя сертификата открытого ключа:

CN = CPDUALDD/O = CryptoPro/L = Moscow/C = RU

Серийный номер сертификата:

0500C3B7000000000010

Срок действия сертификата

10 ноября 2001 г. 13:24:12 - 10 ноября 2002 г. 13:34:12

```
SEQUENCE {
  SEQUENCE {
    [0] {
      INTEGER 2
      }
    INTEGER
      05 00 C3 B7 00 00 00 00 00 10
    SEQUENCE {
      OBJECT IDENTIFIER GOST R 34.11/34.10-94 (1 2 643 2 2 4)
        (Crypto Pro Algorithm)
      NULL
      }
    SEQUENCE {
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER countryName (2 5 4 6)
            (X.520 id-at (2 5 4))
          PrintableString 'RU'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER localityName (2 5 4 7)
            (X.520 id-at (2 5 4))
          PrintableString 'Moscow'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER organizationName (2 5 4 10)
            (X.520 id-at (2 5 4))
          PrintableString 'CryptoPro'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER commonName (2 5 4 3)
            (X.520 id-at (2 5 4))
          PrintableString 'CPDUALDD'
          }
```

```
      }
    }
  SEQUENCE {
    UTCTime '011110102412Z'
    UTCTime '021110103412Z'
    }
  SEQUENCE {
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER countryName (2 5 4 6)
          (X.520 id-at (2 5 4))
        PrintableString 'RU'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER emailAddress (1 2 840 113549 1 9 1)
          (PKCS #9 (1 2 840 113549 1 9).
        IA5String 'ASidorov@ACME.RU'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER organizationName (2 5 4 10)
          (X.520 id-at (2 5 4))
        PrintableString 'ACME'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
          (X.520 id-at (2 5 4))
        PrintableString 'Management'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER commonName (2 5 4 3)
          (X.520 id-at (2 5 4))
        PrintableString 'Sidorov Alexander'
        }
      }
    }
  SEQUENCE {
    SEQUENCE {
      OBJECT IDENTIFIER GOST R 34.10-94 (1 2 643 2 2 20)
        (Crypto Pro Algorithm)
      SEQUENCE {
        OBJECT IDENTIFIER '1 2 643 2 2 32 2'
        OBJECT IDENTIFIER '1 2 643 2 2 30 1'
        }
      }
    BIT STRING 0 unused bits, encapsulates {
        OCTET STRING
          AB 2F A6 9F 61 F6 1A 8A 07 2D D7 3F BF 59 97 10
          5F AF 69 62 CC 30 13 3D 4A BB 47 04 B3 4D DF B7
          46 B8 CD E8 97 2F 93 DF E7 C7 95 B4 B7 3E 2E 64
          B4 89 4A E8 41 83 5C B1 65 07 D1 08 5E BA B1 1F
          39 4C 22 EA F0 1A E7 5E F6 17 68 D5 B0 DC D9 8A
          C8 1C 07 F3 15 59 D6 D7 73 E9 31 70 FC 60 EF 25
          64 6C 23 33 EB 40 C2 D5 5C D8 15 16 51 29 E3 27
          0E 6F 29 8F 9E F3 1B DE 5D D4 E3 7B 41 F6 E7 A4
        }
    }
```

```
[3] {
  SEQUENCE {
    SEQUENCE {
      OBJECT IDENTIFIER keyUsage (2 5 29 15)
        (X.509 id-ce (2 5 29))
      BOOLEAN TRUE
      OCTET STRING, encapsulates {
          BIT STRING 6 unused bits
            '11'B
          }
      }
    SEQUENCE {
      OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
        (X.509 id-ce (2 5 29))
      OCTET STRING, encapsulates {
          SEQUENCE {
            OBJECT IDENTIFIER clientAuth (1 3 6 1 5 5 7 3 2)
              (PKIX key purpose)
            }
          }
      }
    SEQUENCE {
      OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
        (X.509 id-ce (2 5 29))
      OCTET STRING, encapsulates {
          OCTET STRING
            14 7F 19 CE 08 94 2F 11 CE 3E BD A7 5B 0A D8 2A
            CD BC E9 40
          }
      }
    SEQUENCE {
      OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
        (X.509 id-ce (2 5 29))
      OCTET STRING, encapsulates {
          SEQUENCE {
            [0]
              35 D5 3E 11 8B 91 A8 1D D6 E1 71 E1 BE CB C8 FC
              F8 74 3A 20
            [1] {
              [4] {
                SEQUENCE {
                  SET {
                    SEQUENCE {
                      OBJECT IDENTIFIER countryName (2 5 4 6)
                        (X.520 id-at (2 5 4))
                      PrintableString 'RU'
                      }
                    }
                  SET {
                    SEQUENCE {
                      OBJECT IDENTIFIER
                        localityName (2 5 4 7)
                        (X.520 id-at (2 5 4))
                      PrintableString 'Moscow'
                      }
                    }
                  SET {
                    SEQUENCE {
                      OBJECT IDENTIFIER
                        organizationName (2 5 4 10)
                        (X.520 id-at (2 5 4))
                      PrintableString 'CryptoPro'
                      }
                    }
```

```
                    SET {
                      SEQUENCE {
                        OBJECT IDENTIFIER commonName (2 5 4 3)
                          (X.520 id-at (2 5 4))
                        PrintableString 'CPDUALDD'
                        }
                      }
                    }
                  }
                }
              [2]
                06 85 DE 6E F6 E4 ED A0 4E D3 C6 B7 8F FF 46 ED
              }
            }
          }
        SEQUENCE {
          OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
            (X.509 id-ce (2 5 29))
          OCTET STRING, encapsulates {
              SEQUENCE {
                SEQUENCE {
                  [0] {
                    [0] {
                      [6]
                  'http://cpdualdd.cp.ru/CertEnroll/CPDUALDD.crl'
                      }
                    }
                  }
                }
              }
          }
        SEQUENCE {
          OBJECT IDENTIFIER
            authorityInfoAccess (1 3 6 1 5 5 7 1 1)
            (PKIX private extension)
          OCTET STRING, encapsulates {
              SEQUENCE {
                SEQUENCE {
                  OBJECT IDENTIFIER
                    caIssuers (1 3 6 1 5 5 7 48 2)
                    (PKIX authority info access descriptor)
                  [6]
                  'http://cpdualdd.cp.ru/CertEnroll/cpdualdd.cp.ru_'
                  'CPDUALDD.crt'
                  }
                }
              }
          }
        }
      }
    }
  SEQUENCE {
    OBJECT IDENTIFIER GOST R 34.11/34.10-94 (1 2 643 2 2 4)
      (Crypto Pro Algorithm)
    NULL
    }
  BIT STRING 0 unused bits
    57 C7 79 6D E3 72 AD E6 27 7A E5 BC F8 C1 D3 3F
    5B 42 0C 43 F3 A5 6C 04 C5 4E 6B EE FF A4 23 15
    37 7C 41 18 E4 8B D3 9D 20 34 05 F7 35 F0 3B A8
    50 C4 81 8A 9B 5E 84 BA 2B B5 B3 F7 C8 54 F0 2F
  }
```

16.3. Приложение 3. Список отозванных сертификатов.

Имя издателя списка отозванных сертификатов:

CN = CPDUALDD/O = CryptoPro/L = Moscow/C = RU

Серийный номер сертификата:

0500C3B7000000000010

Срок действия:

9 ноября 2001 г. 14:57:19 - 10 декабря 2001 г. 6:17:19

Отозванные сертификаты:

Серийный номер: 615EDD45000000000005

Дата отзыва: 5 ноября 2001 г. 17:38:39

Причина отзыва: Приостановка действия(6)

```
SEQUENCE {
  SEQUENCE {
    INTEGER 1
    SEQUENCE {
      OBJECT IDENTIFIER GOST R 34.11/34.10-94 (1 2 643 2 2 4)
        (Crypto Pro Algorithm)
      NULL
      }
    SEQUENCE {
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER countryName (2 5 4 6)
            (X.520 id-at (2 5 4))
          PrintableString 'RU'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER localityName (2 5 4 7)
            (X.520 id-at (2 5 4))
          PrintableString 'Moscow'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER organizationName (2 5 4 10)
            (X.520 id-at (2 5 4))
          PrintableString 'CryptoPro'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER commonName (2 5 4 3)
            (X.520 id-at (2 5 4))
          PrintableString 'CPDUALDD'
          }
        }
      }
    UTCTime '011109115719Z'
    UTCTime '011210031719Z'
    SEQUENCE {
      SEQUENCE {
        INTEGER
          61 5E DD 45 00 00 00 00 00 05
        UTCTime '011105143839Z'
```

```
        SEQUENCE {
          SEQUENCE {
            OBJECT IDENTIFIER cRLReason (2 5 29 21)
              (X.509 id-ce (2 5 29))
            OCTET STRING, encapsulates {
                ENUMERATED 6
                }
            }
          }
        }
      }
    [0] {
      SEQUENCE {
        SEQUENCE {
          OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
            (X.509 id-ce (2 5 29))
          OCTET STRING, encapsulates {
              SEQUENCE {
                [0]
                  35 D5 3E 11 8B 91 A8 1D D6 E1 71 E1 BE CB C8 FC
                  F8 74 3A 20
                }
              }
          }
        SEQUENCE {
          OBJECT IDENTIFIER
            cAKeyCertIndexPair (1 3 6 1 4 1 311 21 1)
            (Microsoft attribute)
          OCTET STRING, encapsulates {
              INTEGER 0
              }
          }
        }
      }
    }
  SEQUENCE {
    OBJECT IDENTIFIER GOST R 34.11/34.10-94 (1 2 643 2 2 4)
      (Crypto Pro Algorithm)
    NULL
    }
  BIT STRING 0 unused bits
    26 87 8C E8 ED 94 FB 06 9C A5 EE 21 8F 1A 07 59
    D0 4D 38 6E 30 33 87 F5 0C 48 55 B4 6E D1 46 2A
    71 0A D7 3B C2 12 07 A5 DE FA F9 CF 8D F4 F1 5D
    3C D9 50 C4 0E DC 05 8E 83 F8 94 9D FD 8C 2E DB
  }
```

17. 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
TM	Устройство хранения информации на таблетке touch-memory
PKI	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)
АС	Автоматизированная система
АРМ	Автоматизированное рабочее место
ДСЧ	Датчик случайных чисел
ИОК	Инфраструктура Открытых Ключей
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
СЗИ	Средство защиты информации
ЦР	Центр Регистрации
ЦС	Центр Сертификации
УЦ	Удостоверяющий центр
ЭЦП	Электронная цифровая подпись

18. Перечень рисунков

19. Перечень таблиц