



# КриптоПро УЦ

программно-аппаратный комплекс  
удостоверяющий центр

версии 2.0

Типовой регламент

## АННОТАЦИЯ

Настоящий документ содержит типовой Регламент Удостоверяющего центра (УЦ) организации, эксплуатирующей Программно-аппаратный комплекс (ПАК) «Удостоверяющий центр «КриптоПро УЦ» версии 2.0 (далее «КриптоПро УЦ»).

Регламент УЦ эксплуатирующей организации должен создаваться с учётом положений настоящего документа, действующего законодательства Российской Федерации (N 63-ФЗ), и международных рекомендаций (RFC 3647).

Информация о разработчике программно-аппаратного комплекса «КриптоПро УЦ» версии 2.0:

ООО "КРИПТО-ПРО"

127 018, г. Москва, ул. Сущевский вал, 18

Телефон: +7 (495) 995 4820

Факс: +7 (495) 995 4820

<http://www.cryptopro.ru>

E-mail: [info@cryptopro.ru](mailto:info@cryptopro.ru)

# Содержание

<b>Термины и определения .....</b>	<b>7</b>
<b>Перечень сокращений.....</b>	<b>9</b>
<b>1. Введение .....</b>	<b>10</b>
1.1. Обзорная информация .....	10
1.2. Идентификация Регламента .....	10
1.3. Публикация Регламента.....	10
1.4. Область применения Регламента .....	10
1.5. Срок действия Регламента .....	11
1.6. Контактная информация.....	11
<b>2. Общие положения .....</b>	<b>12</b>
2.1. Назначение УЦ .....	12
2.2. Услуги УЦ.....	12
2.3. Структура УЦ.....	12
2.3.1. Административная служба УЦ.....	12
2.3.2. Служба регистрации УЦ .....	13
2.3.3. Служба безопасности УЦ .....	13
2.3.4. Техническая служба УЦ.....	13
2.4. Пользователи УЦ .....	13
2.5. Разрешение споров .....	14
2.6. Платность услуг.....	14
2.7. Ответственность .....	14
2.8. Прекращение деятельности .....	15
2.9. Порядок утверждения и внесения изменений в Регламент .....	15
<b>3. Права.....</b>	<b>16</b>
3.1. Права УЦ .....	16
3.2. Права Пользователей УЦ .....	16
3.2.1. Права лиц, не зарегистрированных в УЦ.....	16
3.2.2. Права лиц, зарегистрированных в УЦ.....	17
3.2.3. Права лиц, которые проходят процедуру регистрации в УЦ.....	17
<b>4. Обязанности .....</b>	<b>18</b>
4.1. Обязанности УЦ.....	18
4.1.1. Ключи электронной подписи Уполномоченных лиц УЦ .....	18
4.1.2. Синхронизация времени.....	18
4.1.3. Регистрация пользователей УЦ .....	18
4.1.4. Изготовление ключей ЭП и ключей проверки ЭП пользователей УЦ .....	18
4.1.5. Изготовление сертификатов ключей проверки ЭП .....	19
4.1.6. Аннулирование сертификатов ключей проверки ЭП.....	19
4.1.7. Приостановление действия сертификатов ключей проверки ЭП.....	19
4.1.8. Возобновление действия сертификатов ключей проверки ЭП .....	19
4.1.9. Уведомления .....	19
4.1.9.1. Уведомление о факте изготовлении сертификата ключа проверки ЭП19	
4.1.9.2. Уведомление о факте аннулирования сертификата ключа проверки ЭП20	
4.1.9.3. Уведомление о факте приостановления действия сертификата ключа проверки ЭП.....	20
4.1.9.4. Уведомление о факте возобновления действия сертификата ключа проверки ЭП.....	20
4.1.10. Реестр сертификатов ключей проверки ЭП.....	20
4.1.11. Восстановление работоспособности УЦ после сбоев.....	21
4.1.12. Прочие обязанности.....	21
4.2. Обязанности Пользователей УЦ.....	21

4.2.1.	Обязанности лиц, не зарегистрированных в УЦ .....	21
4.2.2.	Обязанности лиц, зарегистрированных в УЦ .....	21
4.2.3.	Обязанности лиц, которые проходят процедуру регистрации в УЦ .....	22
<b>5.</b>	<b>Политика конфиденциальности .....</b>	<b>23</b>
5.1.	Типы конфиденциальной информации .....	23
5.2.	Типы информации, не являющейся конфиденциальной .....	23
5.3.	Исключительные полномочия официальных лиц .....	23
<b>6.</b>	<b>Процедуры и механизмы .....</b>	<b>24</b>
6.1.	Процедура регистрации пользователей УЦ .....	24
6.1.1.	Заявление на регистрацию .....	24
6.1.2.	Идентификация Пользователя УЦ .....	24
6.1.3.	Регистрация Пользователя УЦ в централизованном режиме .....	24
6.1.4.	Регистрация Пользователя УЦ в распределённом режиме .....	25
6.2.	Идентификация зарегистрированного пользователя .....	26
6.3.	Аутентификация зарегистрированного пользователя .....	26
6.3.1.	Очная аутентификация зарегистрированного пользователя .....	26
6.3.2.	Удалённая аутентификация зарегистрированного пользователя .....	26
6.3.3.	Аутентификация зарегистрированного пользователя по сертификату ключа проверки ЭП .....	26
6.3.4.	Аутентификация зарегистрированного пользователя по паролю .....	27
6.4.	Изготовление ключей .....	27
6.4.1.	Заявление на изготовление ключей .....	27
6.4.2.	Изготовление и выдача ключей владельцу .....	27
6.5.	Изготовление сертификата ключа проверки ЭП и предоставление его владельцу .....	27
6.5.1.	Заявление на изготовление сертификата ключа проверки ЭП в электронной форме .....	28
6.5.2.	Заявление на изготовление сертификата ключа проверки ЭП в бумажной форме .....	28
6.5.3.	Идентификация владельца сертификата ключа проверки ЭП .....	29
6.6.	Аннулирование (отзыв) сертификата ключа проверки ЭП .....	29
6.6.1.	Заявление на отзыв сертификата ключа проверки ЭП в электронной форме .....	29
6.6.2.	Заявление на отзыв сертификата ключа проверки ЭП в бумажной форме .....	29
6.7.	Приостановление действия сертификата ключа проверки ЭП .....	29
6.7.1.	Заявление на приостановление действия сертификата ключа проверки ЭП в электронной форме .....	30
6.7.2.	Заявление на приостановление действия сертификата ключа проверки ЭП в бумажной форме .....	30
6.7.3.	Заявление на приостановление действия сертификата ключа проверки ЭП в устной форме .....	30
6.8.	Возобновление действия сертификата ключа проверки ЭП .....	30
6.8.1.	Заявление на возобновление действия сертификата ключа проверки ЭП в электронной форме .....	31
6.8.2.	Заявление на возобновление действия сертификата ключа проверки ЭП в бумажной форме .....	31
6.9.	Срок хранения сертификата ключа проверки ЭП .....	31
6.10.	Процедура подтверждения электронной подписи с использованием сертификата ключа проверки ЭП .....	31
6.11.	Процедура подтверждения электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки ЭП .....	32
6.12.	Механизм доказательства обладания ключом ЭП, соответствующим ключу проверки ЭП .....	34
6.13.	Порядок проведения разбора конфликтной ситуации, связанной с применением электронной подписи в электронном документе .....	34

<b>7. Дополнительные положения.....</b>	<b>37</b>
7.1. Идентифицирующие данные Уполномоченного лица УЦ.....	37
7.2. Сроки действия ключей Уполномоченных лиц УЦ.....	37
7.3. Требования к средствам электронной подписи, используемым в составе Удостоверяющего центра и требования к средствам электронной подписи пользователей УЦ.....	37
7.4. Сроки действия ключей ЭП и сертификатов ключей проверки ЭП пользователей УЦ.....	38
7.5. Служебные ключи и служебный сертификат ключа проверки ЭП.....	39
7.6. Рабочие ключи и рабочий сертификат ключа проверки ЭП.....	39
7.7. Меры защиты ключей ЭП.....	39
7.8. Информация из сертификата ключа проверки ЭП на бумажном носителе.....	39
7.9. Архивное хранение документированной информации.....	40
7.9.1. Состав архивируемых документов.....	40
7.9.2. Источник комплектования архивного фонда.....	40
7.9.3. Архивохранилище.....	40
7.9.4. Срок архивного хранения.....	40
7.9.5. Уничтожение архивных документов.....	40
7.10. Смена ключей Уполномоченного лица УЦ.....	40
7.10.1. Плановая смена ключей Уполномоченного лица УЦ.....	40
7.10.2. Внеплановая смена ключей Уполномоченных лиц УЦ.....	41
<b>8. Структуры сертификатов и списков отозванных сертификатов.....</b>	<b>42</b>
8.1. Структура квалифицированного сертификата.....	42
8.2. Структура списка отозванных сертификатов, изготавливаемого УЦ в электронной форме.....	45
8.2.1. Расширения списка отозванных сертификатов.....	45
<b>9. Программные и технические средства обеспечения деятельности УЦ.....</b>	<b>46</b>
9.1. Программный комплекс обеспечения реализации целевых функций УЦ.....	46
9.2. Технические средства обеспечения работы ПК УЦ.....	48
9.3. Программные и программно-аппаратные средства защиты информации.....	48
9.4. Перечень событий, регистрируемых программным комплексом обеспечения реализации целевых функций УЦ.....	48
9.5. Перечень данных программного комплекса обеспечения реализации целевых функций УЦ, подлежащих резервному копированию.....	49
9.6. Порядок технического обслуживания средств обеспечения деятельности УЦ..	49
9.6.1. Техническое обслуживание вычислительной техники и периферийного оборудования.....	49
9.6.2. Техническое обслуживание общесистемного и специализированного программного обеспечения.....	51
<b>10. Роли обслуживающего персонала средств обеспечения деятельности УЦ</b>	<b>54</b>
<b>11. Обеспечение безопасности.....</b>	<b>56</b>
11.1. Инженерно-технические меры защиты информации.....	56
11.1.1. Размещение технических средств УЦ.....	56
11.1.2. Физический доступ в помещения.....	56
11.1.3. Электроснабжение и кондиционирование воздуха.....	56
11.1.4. Подверженность воздействию влаги.....	57
11.1.5. Предупреждение и защита от возгорания.....	57
11.1.6. Хранение документированной информации.....	57
11.1.7. Уничтожение документированной информации.....	57
11.2. Программно-аппаратные меры защиты информации.....	57
11.2.1. Организация доступа к техническим средствам УЦ.....	57
11.2.2. Организация доступа к программным средствам УЦ.....	57
11.2.2.1. Общий перечень объектов доступа УЦ.....	58

11.2.2.2.	Перечень объектов доступа, предоставляемых сотрудникам УЦ .....	58
11.2.2.3.	Перечень объектов доступа, предоставляемых аутентифицированным пользователям УЦ при осуществлении сетевого взаимодействия с программными средствами УЦ .....	58
11.2.3.	Контроль целостности программного обеспечения .....	59
11.2.4.	Контроль целостности технических средств .....	59
11.2.5.	Защита внешних сетевых соединений .....	60
11.2.5.1.	Перечень информации, подлежащей защите .....	60
11.3.	Организационные меры защиты информации .....	61
11.3.1.	Предъявляемые требования к персоналу УЦ .....	61
11.3.2.	Профессиональная переподготовка и повышение квалификации персонала	61
11.3.3.	Организация сменной работы .....	61
11.3.4.	Организация доступа персонала к документам и документации .....	61
11.3.5.	Охрана здания и помещений .....	61
11.4.	Юридические меры защиты информации .....	61
<b>12.</b>	<b>Взаимодействие Удостоверяющего центра с федеральными органами исполнительной власти в сфере использования электронной подписи .....</b>	<b>63</b>
	<b>Перечень таблиц .....</b>	<b>64</b>
	<b>Список литературы.....</b>	<b>65</b>

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Используемые в настоящем документе термины описаны в таблице ниже.

**Таблица 1. Список терминов**

<b>Термин</b>	<b>Определение</b>
<b>Владелец сертификата ключа проверки электронной подписи</b>	Лицо, которому в установленном Федеральным законом (N 63-ФЗ) порядке выдан сертификат ключа проверки электронной подписи.
<b>Демилитаризованная зона</b>	Технология обеспечения защиты информационного периметра сети предприятия, при которой серверы, отвечающие на запросы из внешней сети, находятся в особом сегменте сети, называемом демилитаризованной зоной (ДМЗ). Компьютеры в ДМЗ ограничены в доступе к основным сегментам сети предприятия с помощью межсетевого экрана (МЭ) с целью минимизировать ущерб при взломе одного из общедоступных сервисов, находящихся в ДМЗ.
<b>Межсетевой экран</b>	Комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.
<b>Сертификат ключа проверки электронной подписи</b>	Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.
<b>Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат)</b>	Сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.
<b>Средства электронной подписи</b>	Шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.
<b>Список отозванных сертификатов</b>	Электронный документ с электронной подписью уполномоченного лица удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые были аннулированы до окончания срока их действия или действие которых было приостановлено.
<b>Удостоверяющий центр</b>	Юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом (N 63-ФЗ).

<b>Электронная подпись</b>	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
<b>Электронный документ</b>	Документ, информация в котором представлена в электронной форме, способной быть обработанной средствами вычислительной техники

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Устойчивые русскоязычные сокращения, используемые в этом документе, описаны в таблице ниже.

**Таблица 2. Список сокращений**

<b>Сокращение</b>	<b>Значение</b>
<b>АРМ</b>	Автоматизированное рабочее место
<b>ДМЗ</b>	Демилитаризованная зона
<b>МЭ</b>	Межсетевой экран
<b>НСД</b>	Несанкционированный доступ
<b>ОС</b>	Операционная система
<b>ПАК</b>	Программно-аппаратный комплекс
<b>ПО</b>	Программное обеспечение
<b>СКЗИ</b>	Средство криптографической защиты информации
<b>СКПЭП</b>	Сертификат ключа проверки электронной подписи
<b>СУБД</b>	Системы управления базами данных
<b>УЦ</b>	Удостоверяющий центр
<b>ЭП</b>	Электронная подпись

Используемые иностранные сокращения, как правило, англоязычные, приведены в таблице ниже.

**Таблица 3. Список иностранных сокращений**

<b>Сокращение</b>	<b>Значение</b>	<b>Перевод</b>
<b>AIA</b>	Authority Info Access	Доступ к информации о Центре сертификации
<b>CRL</b>	Certificate Revocation List	Список отозванных сертификатов, СОС
<b>CDP</b>	CRL Distribution Point	Пункт распространения CRL
<b>DN</b>	Distinguished Name	Отличительное имя
<b>IETF</b>	Internet Engineering Task Force	Специальная комиссия интернет разработок
<b>ITU</b>	International Telecommunication Union	Международный союз электросвязи, МСЭ
<b>ITU-T</b>	Telecommunication Standardization Sector (ITU's)	Сектор стандартизации электросвязи (в МСЭ), МСЭ-Т
<b>LDAP</b>	Lightweight Directory Access Protocol	Облегченный протокол доступа к Справочнику
<b>PKI</b>	Public Key Infrastructure	Инфраструктура ключей проверки ЭП
<b>RDN</b>	Relative Distinguished Name	Относительное отличительное имя

# 1. Введение

## 1.1. Обзорная информация

Настоящий Регламент определяет механизмы и условия предоставления и использования услуг УЦ (далее по тексту — «Владелец УЦ»)

---

(полное наименование юридического лица)

включая обязанности пользователей (владельцев ключей проверки ЭП) и членов группы администрирования УЦ, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, необходимые для безопасной работы УЦ.

## 1.2. Идентификация Регламента

Наименование документа: «Регламент работы УЦ».

Версия: 1.0

Дата: \_\_\_\_ . \_\_\_\_ . 20 \_\_\_\_

Объектный идентификатор: \_\_\_\_\_

## 1.3. Публикация Регламента

Настоящий Регламент распространяется:

- в электронной форме
  - по протоколу HTTPS из репозитория Владельца УЦ по адресу URL

---

(URL с указанием протокола)

- по электронной почте E-mail от отправителя

---

(адрес электронной почты отправителя)

- в бумажной форме
  - через Почту России

---

(почтовый адрес Владельца УЦ)

Копии Регламента, предназначенные для распространения в электронной форме по протоколу HTTPS из репозитория Владельца УЦ, состоят из двух файлов, один из которых содержит электронный образ Регламента в формате RTF, а другой — электронную подпись Руководителя УЦ на файл электронного образа Регламента. Файл, содержащий электронную подпись Руководителя УЦ, имеет формат PKCS#7 Signed в кодировке Base64 и не содержит самих данных, т.е. является отсоединённой (detached) подписью.

Копии Регламента, предназначенные для распространения в электронной форме через электронную почту E-mail, являются электронным письмом E-mail, защищённым электронной подписью Руководителя УЦ по технологии S/MIME. Подписанное письмо имеет вложение, содержащее электронный образ Регламента в формате RTF.

## 1.4. Область применения Регламента

Настоящий Регламент предназначен служить соглашением, налагающим обязанности по всем вовлечённым сторонам, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

## 1.5. Срок действия Регламента

Настоящий Регламент вступает в силу со дня его публикации.

Срок действия Регламента — 6 лет.

Если УЦ официально не уведомит своих пользователей о прекращении действия Регламента, то Регламент автоматически пролонгируется на следующий срок.

Официальное уведомление о прекращении действия Регламента осуществляется способами, определёнными в разделе публикации Регламента:

- Копии уведомлений, предназначенные для распространения в электронной форме из репозитория Владельца УЦ, распространяются с использованием протокола HTTPS.
- Копии уведомления, предназначенные для распространения в электронной форме через E-mail, защищены электронной подписью с использованием S/MIME.

## 1.6. Контактная информация

---

(полное наименование юридического лица)

---

(почтовый адрес)

---

(адрес электронной почты)

---

(факс)

Контактный телефон Административной службы УЦ \_\_\_\_\_

E-mail Административной службы УЦ \_\_\_\_\_

Контактный телефон Службы регистрации УЦ \_\_\_\_\_

E-mail Службы регистрации УЦ \_\_\_\_\_

Контактный телефон Службы безопасности УЦ \_\_\_\_\_

E-mail Службы безопасности УЦ \_\_\_\_\_

Контактный телефон Технической службы УЦ \_\_\_\_\_

E-mail Технической службы УЦ \_\_\_\_\_

## 2. Общие положения

### 2.1. Назначение УЦ

УЦ предназначен для обеспечения участников корпоративных информационных систем средствами и спецификациями для использования сертификатов ключей проверки ЭП в целях обеспечения:

- применения электронной подписи;
- контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем;
- аутентификации участников информационных систем в процессе взаимодействия;
- конфиденциальности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем.

### 2.2. Услуги УЦ

В процессе своей деятельности УЦ предоставляет потребителям или Пользователям УЦ следующие виды услуг:

- внесение в Реестр УЦ регистрационной информации о Пользователях УЦ;
- изготовление сертификатов ключей проверки ЭП Пользователей УЦ в электронной форме;
- изготовление копий сертификатов ключей проверки ЭП Пользователей УЦ на бумажных носителях;
- формирование ключей ЭП и ключей проверки ЭП по обращениям Пользователей УЦ с записью их на ключевой носитель;
- ведение Реестра изготовленных сертификатов ключей проверки ЭП Пользователей УЦ;
- предоставление сертификатов ключей проверки ЭП в электронной форме, находящихся в Реестре изготовленных сертификатов, по запросам Пользователей УЦ;
- аннулирование (отзыв) сертификатов ключей проверки ЭП по обращениям владельцев сертификатов ключей проверки ЭП;
- приостановление и возобновление действия сертификатов ключей проверки ЭП по обращениям владельцев сертификатов ключей проверки ЭП;
- предоставление Пользователям УЦ сведений об аннулированных и приостановленных сертификатах ключей проверки ЭП;
- подтверждение подлинности электронных подписей в документах, представленных в электронной форме, по обращениям Пользователей УЦ;
- подтверждение подлинности электронных подписей Уполномоченных лиц УЦ в изготовленных ими сертификатах ключей проверки ЭП по обращениям Пользователей УЦ;
- распространение средств электронной подписи по обращениям Пользователей УЦ.

### 2.3. Структура УЦ

Структура УЦ включает в себя следующие организационные подразделения (службы):

- Административная служба УЦ;
- Служба регистрации УЦ;
- Служба безопасности УЦ;
- Техническая служба УЦ.

#### 2.3.1. Административная служба УЦ

Административная служба УЦ предназначена для решения следующих задач:

- управление деятельностью УЦ;
- координация деятельности других Служб УЦ;
- взаимодействие с Пользователями УЦ в части разрешения вопросов, связанных с применением средств ЭП, ключей и сертификатов ключей проверки ЭП, изготавливаемых и/или распространяемых УЦ;
- взаимодействие с Пользователями УЦ в части разрешения вопросов, связанных с подтверждением электронной подписи Уполномоченного лица УЦ в сертификатах ключей проверки ЭП, изготовленных УЦ в электронной форме, или подтверждения собственноручной подписи Уполномоченного лица УЦ в копиях сертификатов ключей проверки ЭП, изготовленных УЦ на бумажном носителе.

### 2.3.2. Служба регистрации УЦ

Служба регистрации УЦ предназначена для решения следующих задач:

- регистрация Пользователей УЦ;
- ведение Реестра зарегистрированных Пользователей УЦ;
- предоставление служебных ключей ЭП и сертификатов служебных ключей проверки ЭП по обращению Пользователей УЦ;
- распространение средств электронной подписи и шифрования.

### 2.3.3. Служба безопасности УЦ

Служба безопасности УЦ предназначена для решения следующих задач:

- организация и выполнение мероприятий по защите ресурсов УЦ;
- изготовление и предоставление ключей по обращению Пользователей УЦ;
- изготовление и предоставление изготовленных сертификатов ключей проверки ЭП в электронной форме по обращению Пользователей УЦ;
- изготовление и предоставление копий сертификатов ключей проверки ЭП на бумажном носителе по обращению их владельцев;
- аннулирование (отзыв) сертификатов ключей проверки ЭП по обращениям владельцев сертификатов ключей проверки ЭП;
- приостановление и возобновление действия сертификатов ключей проверки ЭП по обращению владельцев сертификатов ключей проверки ЭП;
- предоставление Пользователям УЦ сведений об аннулированных и приостановленных сертификатах ключей проверки ЭП;
- предоставление копий сертификатов ключей проверки ЭП из Реестра сертификатов УЦ, по запросам Пользователей УЦ;
- техническое обеспечение процедуры подтверждения электронной подписи в документах, представленных в электронной форме, по обращениям Пользователей УЦ;
- техническое обеспечение процедуры подтверждения подлинности электронных подписей Уполномоченного лица УЦ в изготовленных сертификатах ключей проверки ЭП по обращениям Пользователей УЦ.

### 2.3.4. Техническая служба УЦ

Техническая служба УЦ предназначена для решения следующих задач:

- организация и выполнение мероприятий по эксплуатации программных и технических средств обеспечения деятельности УЦ;
- организация и выполнение мероприятий по техническому сопровождению распространяемых средств электронной подписи и шифрования.

## 2.4. Пользователи УЦ

Потребителями или пользователями услуг УЦ (далее по тексту — «Пользователи УЦ») называются лица, которые входят в одну из следующих групп:

- **Лица, не зарегистрированные в УЦ** — лица, не прошедшие процедуру регистрации в УЦ, использующие сертификаты других зарегистрированных Пользователей УЦ для каких-либо целей, например, для проверки электронных подписей;
- **Лица, зарегистрированные в УЦ** — лица, прошедшие полную процедуру регистрации в УЦ и являющиеся полноценными Пользователями УЦ;
- **Лица, которые проходят процедуру регистрации в УЦ** — лица, ещё не прошедшие полную процедуру регистрации в УЦ, но уже отправившие в УЦ запрос на регистрацию, который ещё не был одобрен оператором УЦ;

Проходить регистрацию в УЦ и стать зарегистрированным Пользователем УЦ может только физическое лицо.

Владельцем сертификата может быть только зарегистрированный Пользователь УЦ, физическое лицо.

Физическое лицо может представлять юридическое лицо при наличии доверенности, которая даёт данному физическому лицу право пользоваться услугами УЦ от имени юридического лица.

В случае если физическое лицо действует от имени юридического лица на основании уставных документов, то в УЦ предоставляется нотариально заверенная копия уставных документов, подтверждающих заявленные полномочия физического лица.

В тех случаях, когда сертификаты ключей проверки ЭП требуются для работы каких-либо устройств или программ, назначается ответственное лицо, которое регистрируется в УЦ и на имя которого УЦ изготавливает сертификаты.

Пользователем сертификата может быть любое лицо, устройство или программа.

Зарегистрированные Пользователи УЦ могут являться:

- владельцами ключей ЭП,
- владельцами сертификатов ключей проверки ЭП,
- пользователями сертификатов ключей проверки ЭП (владельцами которых являются другие пользователи).

Незарегистрированные пользователи могут являться:

- пользователями сертификатов ключей проверки ЭП (владельцами которых являются другие пользователи),
- пользователями, проходящими процедуру регистрации в УЦ

## 2.5. Разрешение споров

Сторонами в споре, в случае его возникновения, считаются УЦ и Пользователь УЦ.

Стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путём переговоров.

Споры между сторонами, связанные с действием настоящего Регламента, не урегулированные в процессе переговоров, должны рассматриваться в Арбитражном суде в соответствии с действующим законодательством Российской Федерации.

## 2.6. Платность услуг

Услуга УЦ по предоставлению копий сертификатов ключей проверки ЭП в электронной форме, находящихся в Реестре изготовленных сертификатов, предоставляется на безвозмездной основе.

Примечание. Состав и стоимость предоставляемых дополнительных услуг определяется Владельцем УЦ.

## 2.7. Ответственность

УЦ не несёт никакой ответственности в случае нарушения Пользователями УЦ положений настоящего Регламента.

Претензии к УЦ ограничиваются указанием на несоответствие его действий настоящему Регламенту.

## 2.8. Прекращение деятельности

Деятельность УЦ может быть прекращена в порядке, установленном законодательством Российской Федерации.

В случае принятия решения о прекращении своей деятельности аккредитованный удостоверяющий центр обязан:

- 1) сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;
- 2) передать в уполномоченный федеральный орган в установленном порядке реестр квалифицированных сертификатов;
- 3) передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

## 2.9. Порядок утверждения и внесения изменений в Регламент

Настоящий Регламент составляется в письменной форме и заверяется собственноручной подписью Руководителя УЦ и печатью УЦ.

Изменения в Регламент вносятся путём составления дополнительного соглашения к Регламенту.

Изменению не подлежат положения настоящего Регламента, прямо или косвенно ущемляющие права пользователей услуг УЦ.

Утверждение и публикация дополнительных соглашений к Регламенту осуществляется в порядке, соответствующем порядку утверждения и публикации Регламента.

## 3. Права

### 3.1. Права УЦ

УЦ имеет право:

1. Предоставлять сертификаты ключей проверки ЭП в электронной форме, находящихся в Реестре УЦ, всем лицам, обратившимся в УЦ;
2. Не проводить регистрацию лиц, обратившихся по вопросу представления сертификатов ключей проверки ЭП в электронной форме, находящихся в Реестре УЦ;
3. Отказать в предоставлении услуг по регистрации пользователям УЦ, подавшим заявление на регистрацию, без предоставления информации о причинах отказа;
4. Отказать в изготовлении ключей не зарегистрированным пользователям УЦ, подавшим заявление на изготовление ключей, без предоставления информации о причинах отказа;
5. Отказать в изготовлении сертификата ключа проверки ЭП зарегистрированным пользователям УЦ, подавшим заявление на изготовление сертификата ключа проверки ЭП, с указанием причин отказа;
6. Отказать в аннулировании (отзыве) сертификата ключа проверки ЭП владельцу сертификата, подавшему заявление на аннулирование (отзыв) сертификата, в случае если истёк установленный срок действия ключа ЭП, соответствующего ключу проверки ЭП в сертификате;
7. Отказать в приостановлении или возобновлении действия сертификата ключа проверки ЭП владельцу сертификата, подавшему заявление на приостановление или возобновление действия сертификата, в случае если истёк установленный срок действия ключа ЭП, соответствующего ключу проверки ЭП в сертификате;
8. Аннулировать сертификат ключа проверки ЭП Пользователя УЦ в случае установленного факта компрометации соответствующего ключа ЭП, с уведомлением владельца аннулированного сертификата ключа проверки ЭП и указанием обоснованных причин;
9. Приостановить действие сертификата ключа проверки ЭП Пользователя УЦ, с уведомлением владельца приостановленного сертификата ключа проверки ЭП и указанием обоснованных причин.

### 3.2. Права Пользователей УЦ

В этом разделе описаны права Пользователей УЦ для каждой группы, перечисленной в разделе 2.4 на стр. 13.

#### 3.2.1. Права лиц, не зарегистрированных в УЦ

Эту группу Пользователей УЦ составляют лица, не прошедшие регистрацию в УЦ, использующие сертификаты других зарегистрированных пользователей УЦ для каких-либо целей, например, для проверки электронных подписей.

Лица, не зарегистрированные в УЦ, имеют следующие права:

- Получать в электронной форме списки отозванных сертификатов ключей проверки ЭП, изготовленные УЦ;
- Получать в электронной форме сертификаты ключа проверки ЭП Уполномоченных лиц УЦ;
- Получать в электронной форме сертификаты ключа проверки ЭП Пользователей УЦ, находящиеся в Реестре сертификатов ключей проверки ЭП УЦ;
- Применять сертификаты ключа проверки ЭП Уполномоченных лиц УЦ для проверки электронных подписей Уполномоченных лиц УЦ в сертификатах ключа проверки ЭП пользователей, изготовленных УЦ.
- Применять сертификаты ключа проверки ЭП Пользователей УЦ для проверки электронных подписей в электронных документах в соответствии со сведениями, указанными в сертификатах ключа проверки ЭП.

- Применять список отозванных сертификатов ключей проверки ЭП, изготовленный УЦ, для проверки статуса сертификатов ключей проверки ЭП.
- Обращаться в УЦ для внесения в Реестр УЦ регистрационной информации о пользователе;
- Обращаться в УЦ за подтверждением подлинности электронных подписей в электронных документах;
- Обращаться в УЦ за подтверждением подлинности электронных подписей Уполномоченных лиц УЦ в изготовленных УЦ сертификатах ключей проверки ЭП пользователей;
- Обращаться в УЦ с целью получения (приобретения) средств электронной подписи;

### 3.2.2. Права лиц, зарегистрированных в УЦ

Эту группу Пользователей УЦ составляют лица, прошедшие полную регистрацию в УЦ.

Лица, составляющие группу зарегистрированных пользователей УЦ, имеют все права группы незарегистрированных пользователей и, дополнительно к ним, следующие права:

- Формировать ключи ЭП и ключи проверки ЭП на своём рабочем месте с использованием средства ЭП и программных средств, предоставляемых УЦ;
- Обращаться в УЦ для изготовления сертификатов ключа проверки ЭП;
- Пользоваться предоставляемыми УЦ программными средствами для получения и установки на своё рабочее место изготовленных сертификатов ключа проверки ЭП;
- Обращаться в УЦ для аннулирования (отзыва), приостановления действия, возобновления действия своих сертификатов ключей проверки ЭП в течение срока действия соответствующих ключей ЭП.

### 3.2.3. Права лиц, которые проходят процедуру регистрации в УЦ

Эту группу пользователей услуг УЦ составляют лица, не прошедшие полную регистрацию в УЦ, но уже отправившие запрос на регистрацию, который ещё не одобрен оператором УЦ.

Лица, составляющие группу подавших запрос на регистрацию в УЦ пользователей, имеют все права группы незарегистрированных пользователей и, дополнительно к ним, следующие права:

- Обращаться в УЦ за проверкой состояния отправленного ранее запроса на регистрацию.

## 4. Обязанности

### 4.1. Обязанности УЦ

#### 4.1.1. Ключи электронной подписи Уполномоченных лиц УЦ

УЦ обязан использовать для изготовления ключей ЭП Уполномоченных лиц УЦ и формирования электронных подписей только средства криптографической защиты информации (средства электронной подписи), входящие в состав выбранной комплектации «КриптоПро УЦ» согласно (ЖТЯИ.00078-01 30 01).

При использовании в соответствии с положениями формуляра (ЖТЯИ.00078-01 30 01), ПАК «КриптоПро УЦ 2.0» удовлетворяет «Требованиям к средствам удостоверяющего центра» ФСБ России:

- варианты исполнения 1, 4 и 5 – классу КС2 (используются СКЗИ/средства ЭП класса КС2);
- варианты исполнения 2 и 6 – классу КС3 (используются СКЗИ/средства ЭП класса КС3);
- вариант исполнения 3 – классу КС1 (используются СКЗИ/средства ЭП класса КС1).

УЦ обязан использовать ключи ЭП Уполномоченных лиц УЦ только для подписи издаваемых им сертификатов ключей проверки ЭП и списков отозванных сертификатов.

УЦ обязан принять меры по защите ключей ЭП Уполномоченных лиц УЦ в соответствии с положениями настоящего Регламента.

#### 4.1.2. Синхронизация времени

УЦ организует работу своих Служб по Всемирному координированному времени (UTC) с учётом часового пояса места расположения УЦ.

УЦ обязан синхронизировать по времени все программные и технические средства обеспечения деятельности по предназначению.

#### 4.1.3. Регистрация пользователей УЦ

УЦ обеспечивает регистрацию Пользователей УЦ по заявлениям на регистрацию в соответствии с порядком регистрации, изложенным в настоящем Регламенте.

УЦ обязан обеспечить уникальность информации, используемой для идентификации и аутентификации Пользователей УЦ в УЦ.

УЦ обязан не разглашать (публиковать) регистрационную информацию пользователей УЦ, за исключением информации, заносимой в изготавливаемые сертификаты.

#### 4.1.4. Изготовление ключей ЭП и ключей проверки ЭП пользователей УЦ

УЦ обязан изготовить ключ ЭП и ключ проверки ЭП зарегистрированному Пользователю УЦ по заявлению с использованием средств электронной подписи, сертифицированных в соответствии с действующим законодательством Российской Федерации.

УЦ обязан обеспечить сохранение в тайне изготовленного ключа ЭП.

УЦ обязан записать ключ на отчуждаемый магнитный носитель, в соответствии с требованиями по эксплуатации программного и/или аппаратного средства, выполняющего процедуру генерации ключей.

УЦ обязан выполнять процедуру генерации ключей и запись ключей на отчуждаемый носитель только с использованием программного и/или аппаратного средства, сертифицированного в соответствии с законодательством Российской Федерации.

УЦ обязан обеспечить защиту ключевого носителя от копирования.

#### 4.1.5. Изготовление сертификатов ключей проверки ЭП

УЦ обеспечивает изготовление сертификата ключа проверки ЭП зарегистрированному Пользователю УЦ по заявлению, в соответствии с форматом и порядком идентификации владельца сертификата ключа проверки ЭП, определённым в настоящем Регламенте.

В том случае, если на Центре сертификации УЦ осуществляется автоматическое создание сертификатов ключей проверки электронной подписи, то руководством организации, являющейся удостоверяющим центром, должно быть назначено лицо, ответственное за автоматическое создание и проверку ЭП в УЦ. Также должно быть назначено лицо, ответственное за аннулирование, приостановление действия, возобновление действия сертификатов ключей проверки электронной подписи.

Условия, в которых может использоваться автоматический режим работы УЦ, и требования, вытекающие из федерального закона (N 63-ФЗ) «Об электронной подписи», должны быть отражены в Регламенте УЦ, подготавливаемым на основании настоящего документа и являющимся юридически значимым.

УЦ обязан обеспечить уникальность регистрационных (серийных) номеров изготавливаемых сертификатов ключей проверки ЭП Пользователей УЦ.

УЦ обязан обеспечить уникальность значений ключей проверки ЭП в изготовленных сертификатах ключей проверки ЭП пользователей УЦ.

#### 4.1.6. Аннулирование сертификатов ключей проверки ЭП

УЦ обязан аннулировать сертификат ключа проверки ЭП по заявлению его владельца.

УЦ обязан в течение 12 часов занести сведения об аннулированном сертификате в список отозванных сертификатов с указанием даты, времени, причины аннулирования.

#### 4.1.7. Приостановление действия сертификатов ключей проверки ЭП

УЦ обязан приостановить действие сертификат ключа проверки ЭП по заявлению его владельца.

УЦ обязан в течение 12 часов занести сведения о приостановленном сертификате в список отозванных сертификатов с указанием даты, времени и признака приостановления.

#### 4.1.8. Возобновление действия сертификатов ключей проверки ЭП

УЦ обязан возобновить действие сертификат ключа проверки ЭП по заявлению его владельца.

УЦ обязан в течение 12 часов исключить сведения о приостановленном сертификате из списка отозванных сертификатов.

#### 4.1.9. Уведомления

##### 4.1.9.1. Уведомление о факте изготовлении сертификата ключа проверки ЭП

УЦ обязан официально уведомить о факте изготовления сертификата ключа проверки ЭП его владельца.

Срок уведомления — не позднее 24 часов с момента изготовления сертификата ключа проверки ЭП.

Официальным уведомлением о факте изготовлении сертификата является отправка почтового сообщения по электронной почте с прикрепленным сертификатом ключа проверки ЭП с адреса отправителя \_\_\_\_\_.

Временем отправки почтового сообщения признается время отправки почтового сообщения с почтового сервера \_\_\_\_\_, осуществляющего отправку почтовых сообщений УЦ, и включённое в заголовок почтового сообщения.

#### 4.1.9.2. Уведомление о факте аннулирования сертификата ключа проверки ЭП

УЦ обязан официально уведомить о факте аннулирования сертификата ключа проверки ЭП его владельца.

Срок уведомления — не позднее 24 часов с момента занесения сведений об аннулированном сертификате в список отозванных сертификатов.

Официальным уведомлением о факте аннулирования сертификата является опубликование списка отозванных сертификатов, который содержит сведения об аннулированном сертификате, в репозитории Владельца УЦ по адресу \_\_\_\_\_.

Временем аннулирования сертификата ключа проверки ЭП признается время занесения сведений об аннулированном сертификате в список отозванных сертификатов, указанное в списке отозванных сертификатов.

Временем опубликования списка отозванных сертификатов признается время изготовления списка отозванных сертификатов, указанное в списке отозванных сертификатов.

УЦ обязан включать полный адрес (URL) списка отозванных сертификатов из репозитория УЦ в издаваемые сертификаты ключей проверки ЭП пользователей УЦ.

#### 4.1.9.3. Уведомление о факте приостановления действия сертификата ключа проверки ЭП

УЦ обязан официально уведомить о факте приостановления действия сертификата его владельца.

Срок уведомления – не позднее 24 часов с момента занесения сведений о приостановленном сертификате в список отозванных сертификатов.

Официальным уведомлением о факте приостановления действия сертификата является опубликование списка отозванных сертификатов, содержащим сведения о приостановленном сертификате, в репозитории Владельца УЦ по адресу \_\_\_\_\_.

Временем приостановления действия сертификата ключа проверки ЭП признается время занесения сведений о приостановленном сертификате в список отозванных сертификатов, включённое в его структуру.

Временем опубликование списка отозванных сертификатов признается время изготовления списка отозванных сертификатов, включённое в его структуру.

#### 4.1.9.4. Уведомление о факте возобновления действия сертификата ключа проверки ЭП

УЦ обязан официально уведомить о факте возобновления действия сертификата его владельца.

Срок уведомления – не позднее 24 часов с момента исключения сведений о приостановленном сертификате из списка отозванных сертификатов.

Официальным уведомлением о факте возобновления действия сертификата является опубликование списка отозванных сертификатов, не содержащим сведения о приостановленном сертификате, в репозитории Владельца УЦ по адресу \_\_\_\_\_. Список отозванных сертификатов должен иметь более позднее, чем приостановление действия сертификата, время изготовления списка отозванных сертификатов, включённое в его структуру

Временем возобновления действия сертификата ключа проверки ЭП признается время официального уведомления о факте возобновления действия сертификата.

#### 4.1.10. Реестр сертификатов ключей проверки ЭП

УЦ обязан вести Реестр всех изготовленных сертификатов ключей проверки ЭП пользователей УЦ в течение установленного срока хранения.

Реестр сертификатов ключей проверки ЭП ведётся в электронном виде.

УЦ обязан осуществлять выдачу сертификатов ключей проверки ЭП в электронной форме по обращениям пользователей УЦ.

УЦ обязан публиковать выписки из Реестра, позволяющие определить действительность сертификатов ключей проверки ЭП пользователей УЦ.

Выписка из Реестра УЦ предоставляется в виде списка отозванных сертификатов в электронной форме и формате, определённом настоящим Регламентом.

#### 4.1.11. Восстановление работоспособности УЦ после сбоев

В целях недопущения технических сбоев Удостоверяющий центр обязан обеспечить выполнение мероприятий, направленных на их предотвращение и оперативное восстановление работоспособности средств УЦ, руководствуясь «Порядком технического обслуживания средств обеспечения деятельности УЦ», изложенным в п. 9.6. настоящего Регламента. В случае возникновения технического сбоя Удостоверяющий центр должен обеспечить информирование участников информационных систем о статусе сертификатов не позднее 2-х часов с момента наступления сбоя (обеспечить публикацию списков отозванных сертификатов), а полное восстановление работоспособности УЦ – не позднее суток с момента наступления сбоя.

#### 4.1.12. Прочие обязанности

УЦ обязан уведомлять владельца сертификата ключа проверки ЭП о фактах, которые стали известны УЦ и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа проверки ЭП.

УЦ обязан обеспечивать передачу пароля от рабочего места Пользователя УЦ, проходящего процедуру регистрации в распределённом режиме, посредством защищённого канала связи, реализуемого сертифицированными шифровальными (криптографическими) средствами.

### 4.2. Обязанности Пользователей УЦ

#### 4.2.1. Обязанности лиц, не зарегистрированных в УЦ

Лица, не зарегистрированные в УЦ, если являются пользователями сертификатов ключей проверки ЭП, изготовленных этим УЦ, обязаны:

- перед использованием сертификата ключа проверки ЭП, изготовленного этим УЦ, удостовериться, что назначения ключа и назначения сертификата, указанные в сертификате, соответствуют предполагаемому использованию сертификата, согласно настоящему Регламенту.

#### 4.2.2. Обязанности лиц, зарегистрированных в УЦ

Лица, зарегистрированные в УЦ, если являются владельцами ключей ЭП, на соответствующие ключи проверки ЭП которых в этом УЦ изготовлены сертификаты, обязаны:

- хранить в тайне свой ключ ЭП, принимать всевозможные меры для предотвращения его потери, раскрытия, изменения или несанкционированного использования;
- не использовать для электронной подписи ключи электронной подписи, если ему известно, что эти ключи используются или использовались ранее другими лицами;
- использовать ключи ЭП только для целей, разрешённых назначениями ключа и назначениями сертификата, согласно настоящему Регламенту.

Лица, зарегистрированные в УЦ, если являются владельцами сертификатов ключей проверки ЭП, изготовленных этим УЦ, обязаны:

- использовать сертификаты своих ключей проверки ЭП только для целей, разрешённых назначениями ключа и назначениями сертификата, которые указаны в сертификате, согласно настоящему Регламенту;

- немедленно обращаться в УЦ с заявлением на аннулирование (отзыв) сертификата ключа проверки ЭП в случае, если стало известно, что эти ключи используются или использовались ранее другими лицами.

Лица, зарегистрированные в УЦ, если им предоставлены имя и пароль временного доступа к УЦ, обязаны:

- хранить в тайне пароль временного доступа к УЦ в течение срока действия пароля.

#### 4.2.3. Обязанности лиц, которые проходят процедуру регистрации в УЦ

Лица, которые проходят процедуру регистрации в УЦ, обязаны:

- предоставлять регистрационную и идентифицирующую информацию в объёме, определённом положениями настоящего Регламента.

Лица, которые проходят процедуру регистрации в УЦ, если им предоставлены имя и пароль временного доступа к УЦ, обязаны:

- хранить в тайне предоставленный пароль временного доступа в течение срока действия пароля.

## 5. Политика конфиденциальности

### 5.1. Типы конфиденциальной информации

Ключ ЭП владельца сертификата ключа проверки ЭП является конфиденциальной информацией данного Пользователя УЦ. УЦ не депонирует и не архивирует ключи ЭП.

Пароль, предоставляемый пользователю УЦ в процессе прохождения процедуры регистрации в распределённом режиме, считается конфиденциальной информацией (имя временного доступа конфиденциальной информацией не считается).

Персональная и корпоративная информация пользователей УЦ, содержащаяся в УЦ, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки ЭП, списка отозванных сертификатов, считается конфиденциальной и не публикуется.

Информация, хранящаяся в журналах аудита УЦ, считается конфиденциальной и не подлежит разглашению.

Отчётные материалы по выполненным проверкам деятельности УЦ являются конфиденциальными, за исключением заключения по результатам проверок, публикуемого в соответствии с настоящим Регламентом.

### 5.2. Типы информации, не являющейся конфиденциальной

Информация, не являющейся конфиденциальной информацией, является открытой информацией.

Открытая информация может публиковаться по решению УЦ. Место, способ и время публикации также определяется решением УЦ.

Информация, включаемая в сертификаты ключей проверки ЭП пользователей УЦ и списки отозванных сертификатов, издаваемые УЦ, не считается конфиденциальной.

Также не считается конфиденциальной информация о настоящем Регламенте.

### 5.3. Исключительные полномочия официальных лиц

УЦ не должен раскрывать информацию, относящуюся к типу конфиденциальной информации, каким бы то ни было третьим лицам, за исключением:

- случаев, определённых в настоящем Регламенте;
- случаев, требующих раскрытия в соответствии с действующим законодательством или при наличии судебного постановления.

## 6. Процедуры и механизмы

### 6.1. Процедура регистрации пользователей УЦ

Под регистрацией пользователей УЦ понимается внесение регистрационной информации о пользователях УЦ в Реестр УЦ.

Процедура регистрации пользователей УЦ применяется в отношении физических лиц, обращающихся к услугам УЦ в части изготовления сертификатов ключей проверки ЭП пользователей УЦ и/или формирования ключей ЭП и ключей проверки ЭП пользователей УЦ с записью их на ключевой носитель.

#### 6.1.1. Заявление на регистрацию

Лицо (заявитель), желающее пройти процедуру регистрации в УЦ, должно подать заявление на регистрацию в простой письменной форме в Службу регистрации УЦ. Для регистрации лица – будущего владельца квалифицированного сертификата Заявление должно содержать данные, установленные Статьёй 17 63-ФЗ «Об электронной подписи».

К данному заявлению должны прилагаться все необходимые документы, которые подтверждают заносимые в квалифицированный сертификат данные.

Дополнительно (определяется заявителем по согласованию с УЦ) заявление может содержать иную идентифицирующую пользователя информацию.

#### 6.1.2. Идентификация Пользователя УЦ

Идентификация пользователя выполняется в процессе его регистрации в качестве зарегистрированного Пользователя УЦ.

Результатом идентификации является присвоение пользователю УЦ идентификатора и занесение идентификатора в Реестр зарегистрированных пользователей УЦ.

#### 6.1.3. Регистрация Пользователя УЦ в централизованном режиме

Регистрация Пользователя УЦ (владельца сертификата ключа проверки ЭП) в централизованном режиме осуществляется сотрудником Службы регистрации УЦ на основе заявления на регистрацию при личном прибытии лица, проходящего процедуру регистрации, в офис УЦ, расположенный по адресу \_\_\_\_\_.

Сотрудник Службы регистрации УЦ выполняет процедуру идентификации лица, проходящего процедуру регистрации, путём установления личности по паспорту или иному документу, удостоверяющему личность.

После положительной идентификации лица, проходящего процедуру регистрации, сотрудник Службы регистрации УЦ подготавливает бланк заявления на регистрацию и передаёт его заявителю.

Заявитель заверяет заявление на регистрацию собственноручной подписью и передаёт заявление вместе с необходимыми приложениями сотруднику Службы регистрации УЦ.

Заявление на регистрацию рассматривается Службой регистрации УЦ в течение 2 рабочих дней с момента поступления.

В случае отказа в регистрации заявление на регистрацию вместе с приложениями возвращается заявителю.

При принятии положительного решения, сотрудник Службы регистрации УЦ выполняет регистрационные действия по занесению регистрационной информации в Реестр УЦ и изготавливает служебные ключи и служебный сертификат ключа проверки ЭП (в соответствии с пунктом 7.5 настоящего Регламента).

Заявление на изготовление служебных ключей и сертификата ключа проверки ЭП подаётся заявителем в соответствии с дополнительным соглашением или устно.

По окончании процедуры регистрации, зарегистрированному пользователю УЦ выдаются:

- ключи, записанные на ключевой носитель;
- сертификат ключа проверки ЭП в электронной форме, соответствующий ключу ЭП;
- копия сертификата ключа проверки ЭП на бумажном носителе, заверенная собственноручной подписью уполномоченного лица УЦ;
- сертификаты ключа проверки ЭП в электронной форме Уполномоченных лиц УЦ и вышестоящих УЦ по иерархии;
- списки отозванных сертификатов в электронной форме УЦ и вышестоящих УЦ по иерархии.

По необходимости (в случае его отсутствия у пользователя), регистрируемый Пользователь УЦ должен приобрести (получить) средство электронной подписи и шифрования, распространяемое УЦ.

#### 6.1.4. Регистрация Пользователя УЦ в распределённом режиме

Регистрация Пользователя УЦ в распределённом режиме осуществляется сотрудником Службы регистрации УЦ на основании нотариально заверенного заявления на регистрацию лица, проходящего процедуру регистрации, поступившего в офис УЦ, расположенный по адресу \_\_\_\_\_, и на основании запроса на регистрацию в электронной форме, поступившего в УЦ.

Идентификация лица, проходящего процедуру регистрации, выполняется нотариусом в процессе совершения нотариальных действий по заверению заявления на регистрацию.

Сотрудник Службы регистрации УЦ выполняет процедуру проверки соответствия идентификационных данных, поступивших в запросе на регистрацию в электронной форме и в заявлении на регистрацию в бумажной форме.

Регистрация Пользователя УЦ в распределённом режиме осуществляется с использованием программных средств, предоставляемых УЦ.

Перед началом процедуры регистрации в распределённом режиме, пользователь должен получить средство электронной подписи и шифрования, распространяемое УЦ.

В комплект средства электронной подписи и шифрования должны входить сертификаты в электронной форме УЦ и вышестоящих УЦ по иерархии, а также списки отозванных сертификатов в электронной форме УЦ и вышестоящих УЦ по иерархии.

Лицо, проходящее процедуру регистрации в распределённом режиме, должно с использованием программного обеспечения регистрации Пользователя УЦ, предоставляемого УЦ, сформировать и отправить в УЦ запрос на регистрацию в электронном виде.

В процессе формирования и отправки запроса на регистрацию в электронном виде, лицо, проходящее процедуру регистрации, получает имя и пароль, сформированный УЦ, для аутентификации Пользователя УЦ по паролю.

После отправки запроса на регистрацию в электронном виде, лицо, проходящее процедуру регистрации, должно выслать почтовым сообщением с уведомлением о вручении в Службу регистрации УЦ нотариально заверенное заявление на регистрацию (в соответствии с пунктом 6.1.1 настоящего Регламента).

Заявление на регистрацию рассматривается Службой регистрации УЦ в течение 2 рабочих дней с его момента поступления в Службу.

В случае отказа в регистрации заявление на регистрацию вместе с приложениями заявителю не возвращается.

Официальным уведомлением Пользователя УЦ об отказе в регистрации является отправка почтового сообщения через E-mail от отправителя \_\_\_\_\_ (адрес электронной почты отправителя).

При принятии положительного решения, сотрудник Службы регистрации УЦ выполняет регистрационные действия по занесению регистрационной информации в Реестр УЦ.

Официальным уведомлением Пользователя УЦ о регистрации является отправка почтового сообщения через E-mail от отправителя \_\_\_\_\_ (адрес электронной почты отправителя).

Зарегистрированный Пользователь УЦ должен с использованием программного обеспечения регистрации Пользователя УЦ, предоставляемого УЦ, выполнить процедуру генерации рабочих ключей, сформировать и отправить в УЦ запрос на рабочий сертификат ключа проверки ЭП в электронном виде и заявление на рабочий сертификат ключа проверки ЭП в бумажном виде.

Заявление на рабочий сертификат ключа проверки ЭП в бумажном виде рассматривается Службой регистрации УЦ в течение 3 рабочих дней с его момента поступления в Службу.

Официальным уведомлением Пользователя УЦ о выпуске рабочего сертификата ключа проверки ЭП является отправка почтового сообщения через E-mail от отправителя \_\_\_\_\_ (адрес электронной почты отправителя).

Зарегистрированный Пользователь УЦ должен с использованием программного обеспечения регистрации Пользователя УЦ, предоставляемого УЦ, выполнить процедуру установки выпущенного сертификата ключа проверки ЭП на рабочее место.

Отсутствие в течение 3 рабочих дней официального уведомления Пользователя УЦ о выпуске рабочего сертификата ключа проверки ЭП является официальным отказом в изготовлении рабочего сертификата ключа проверки ЭП.

## 6.2. Идентификация зарегистрированного пользователя

Идентификация зарегистрированного Пользователя УЦ осуществляется по идентификатору зарегистрированного пользователя, занесённому в Реестр УЦ.

Также идентификация зарегистрированного Пользователя УЦ может осуществляться по сертификату ключа проверки ЭП, которым владеет этот пользователь.

## 6.3. Аутентификация зарегистрированного пользователя

### 6.3.1. Очная аутентификация зарегистрированного пользователя

Очная аутентификация зарегистрированного Пользователя УЦ выполняется по паспорту или другому документу, удостоверяющему личность, предъявляемому лично.

### 6.3.2. Удалённая аутентификация зарегистрированного пользователя

Удалённая аутентификация зарегистрированного Пользователя УЦ предназначена для идентификации зарегистрированного Пользователя УЦ по средствам телефонной связи.

Удалённая аутентификация зарегистрированного Пользователя УЦ выполняется по ключевой фразе, определённой пользователем в заявлении на регистрацию.

Лицо, проходящее процедуру удалённой аутентификации, должно сообщить свои идентификационные данные и, по запросу сотрудника УЦ, назвать ключевую фразу.

Этот тип аутентификации применяется только для отзыва или приостановления сертификата.

### 6.3.3. Аутентификация зарегистрированного пользователя по сертификату ключа проверки ЭП

Аутентификация зарегистрированного Пользователя УЦ по сертификату ключа проверки ЭП выполняется по протоколу аутентификации TLS.

#### 6.3.4. Аутентификация зарегистрированного пользователя по паролю

Аутентификация зарегистрированного Пользователя УЦ по паролю выполняется путём сопоставления предъявленного зарегистрированным пользователем УЦ пароля с учётной информацией, хранимой в Реестре зарегистрированных пользователей УЦ.

Действие пароля начинается с момента его предоставления пользователю УЦ.

Срок действия пароля составляет 30 календарных суток. Действие пароля может быть прекращено досрочно ответственным сотрудником УЦ.

#### 6.4. Изготовление ключей

Изготовление ключей ЭП осуществляется УЦ по обращению граждан. Обращение граждан оформляется в форме заявления на изготовление ключей. Прием заявлений, изготовление и выдача ключей осуществляется Службой безопасности УЦ при личном присутствии лица, обратившегося с заявлением.

##### 6.4.1. Заявление на изготовление ключей

Заявление на изготовление ключей подаётся заявителем в простой письменной форме на бумажном носителе и заверяется собственноручной подписью заявителя.

Заявление на изготовление ключей оформляется заявителем либо по образцу, предоставляемому Службой безопасности УЦ, либо по бланку, подготавливаемому сотрудником Службы безопасности УЦ.

Заявление на изготовление ключей рассматривается Службой безопасности УЦ в течение 30 минут с момента поступления.

##### 6.4.2. Изготовление и выдача ключей владельцу

Изготовление ключей выполняется ответственным сотрудником Службы безопасности УЦ на специализированном рабочем месте, на основании принятого заявления в присутствии заявителя.

Изготовление ключей осуществляется в присутствии заявителя.

Изготовленные ключи записываются на ключевой носитель, предоставляемый заявителем.

Предоставляемый заявителем ключевой носитель должен удовлетворять следующим требованиям:

- иметь тип устройства, входящий в перечень, определяемый Службой безопасности УЦ;
- быть проинициализированным (отформатированным);
- не содержать никакой информации, за исключением данных инициализации.

Ключевые носители, не удовлетворяющие указанным требованиям, для записи ключевой информации не принимаются.

Ключевой носитель, содержащий изготовленные ключи, передаётся владельцу (заявителю). Факт выдачи ключей заносится в Журнал учёта изготовления и выдачи ключей под роспись владельца.

#### 6.5. Изготовление сертификата ключа проверки ЭП и предоставление его владельцу

Изготовление сертификата ключа проверки ЭП осуществляется УЦ на основании заявления на изготовление сертификата ключа проверки ЭП зарегистрированного Пользователя УЦ.

В том случае, если на Центре сертификации УЦ настроено автоматическое создание сертификата ключа проверки электронной подписи, то ответственность за создание сертификата ключа проверки электронной подписи, содержащего актуальные и действительные сведения о владельце сертификата, полностью возлагаются на сотруд-

ника Службы безопасности УЦ, принимающего решение о создании и выдаче сертификата ключа проверки электронной подписи.

Заявление на изготовление сертификата ключа проверки ЭП подаётся заявителем в электронной или бумажной форме в Службу безопасности УЦ.

Заявление на изготовление сертификата ключа проверки ЭП в электронной форме подаётся зарегистрированным пользователем УЦ с использованием программно-го обеспечения зарегистрированного пользователя, предоставляемого УЦ.

Заявление на изготовление сертификата ключа проверки ЭП в бумажной форме подаётся зарегистрированным пользователем УЦ в офис Службы безопасности УЦ лично.

Срок рассмотрения заявления на изготовление сертификата ключа проверки ЭП составляет 3 рабочих дня с момента его поступления в Службу безопасности УЦ.

После изготовления сертификата ключа проверки ЭП его владельцу направляется официальное уведомление (см. раздел 4.1.9 настоящего Регламента).

Изготовленный сертификат ключа проверки ЭП в электронной форме, подписанный электронной подписью одного из Уполномоченных лиц УЦ, предоставляется его владельцу путём отправки с официальным уведомлением в виде прикрепленного файла, содержащего изготовленный сертификат в электронной форме.

Копия сертификата ключа проверки ЭП на бумажном носителе, заверенная собственноручной подписью уполномоченного лица УЦ, предоставляется его владельцу при личном обращении в Службу безопасности УЦ.

#### 6.5.1. Заявление на изготовление сертификата ключа проверки ЭП в электронной форме

Заявление на изготовление сертификата ключа проверки ЭП в электронной форме представляет собой электронный документ формата PKCS#7 или CMC, содержащий в подписываемых данных запрос на сертификат в формате PKCS#10, подписанный электронной подписью с использованием ключа ЭП и сертификата ключа проверки ЭП, владельцем которых заявитель является.

В качестве ключа ЭП должен использоваться ключ ЭП, до окончания срока действия которого, на момент поступления заявления в Службу безопасности УЦ, остаётся не менее 1 календарного месяца.

#### 6.5.2. Заявление на изготовление сертификата ключа проверки ЭП в бумажной форме

Заявление на изготовление сертификата ключа проверки ЭП в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление должно содержать данные, установленные Статьей 17 63-ФЗ «Об электронной подписи».

К данному заявлению должны прилагаться все необходимые документы, которые подтверждают заносимые в квалифицированный сертификат данные.

Дополнительно (определяется заявителем по согласованию с УЦ) заявление может содержать иную идентифицирующую пользователя информацию.

Заявление должно содержать текст запроса на сертификат в формате PKCS#10 в кодировке Base64.

Обязательным приложением к заявлению на изготовление сертификата в бумажной форме является файл, содержащий запрос на сертификат в формате PKCS#10 в кодировке Base64, размещенный на сменном носителе (например, на флеш-накопителе).

### 6.5.3. Идентификация владельца сертификата ключа проверки ЭП

Владелец сертификата ключа проверки ЭП идентифицируется по сертификату ключа проверки ЭП после прохождения процедуры аутентификации TLS. Процедура аутентификации TLS доказывает Удостоверяющему центру, что владелец сертификата обладает ключом ЭП, соответствующим сертификату и что владелец использовал его в настоящее время для выполнения протокола аутентификации TLS.

### 6.6. Аннулирование (отзыв) сертификата ключа проверки ЭП

Аннулирование (отзыв) сертификата ключа проверки ЭП, изготовленного УЦ, осуществляется УЦ по заявлению на отзыв сертификата ключа проверки ЭП его владельца (далее по тексту раздела — заявитель).

Заявление на отзыв сертификата ключа проверки ЭП подаётся заявителем в электронной или бумажной форме в Службу безопасности УЦ.

Заявление на отзыв сертификата ключа проверки ЭП в электронной форме подаётся зарегистрированным пользователем УЦ с использованием программного обеспечения зарегистрированного пользователя, предоставляемого УЦ.

Заявление на отзыв сертификата ключа проверки ЭП в бумажной форме подаётся заявителем в офис Службы безопасности УЦ лично.

Срок рассмотрения заявления на отзыв сертификата ключа проверки ЭП составляет 1 рабочий день с момента его поступления в Службу безопасности УЦ.

После аннулирования (отзыва) сертификата ключа проверки ЭП его владельцу направляется официальное уведомление (см. раздел 4.1.9 настоящего Регламента).

#### 6.6.1. Заявление на отзыв сертификата ключа проверки ЭП в электронной форме

Заявление на отзыв сертификата ключа проверки ЭП в электронной форме представляет собой электронный документ формата PKCS#7 или СМС, содержащий в подписываемых данных сведения, необходимые для отзыва сертификата, подписанный электронной подписью с использованием ключа ЭП и сертификата ключа проверки ЭП, владельцем которых заявитель является.

#### 6.6.2. Заявление на отзыв сертификата ключа проверки ЭП в бумажной форме

Заявление на отзыв сертификата ключа проверки ЭП в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление включает в себя следующие обязательные реквизиты:

- Идентификационные данные заявителя;
- Идентификационные данные отзываемого сертификата (включая его серийный номер);
- Причину отзыва сертификата;
- Дату и подпись заявителя.

### 6.7. Приостановление действия сертификата ключа проверки ЭП

Приостановление действия сертификата ключа проверки ЭП, изготовленного УЦ, осуществляется УЦ по заявлению на приостановление сертификата ключа проверки ЭП его владельца (далее по тексту раздела — заявитель).

Заявление на приостановление действия сертификата ключа проверки ЭП подаётся заявителем в электронной, бумажной или устной форме в Службу безопасности УЦ.

Заявление на приостановление действия сертификата ключа проверки ЭП в электронной форме подаётся зарегистрированным пользователем УЦ с использованием программного обеспечения зарегистрированного пользователя, предоставляемого УЦ.

Заявление на приостановление действия сертификата ключа проверки ЭП в бумажной форме подаётся заявителем в офис Службы безопасности УЦ лично.

Заявление на приостановление действия сертификата ключа проверки ЭП в устной форме подаётся заявителем в офис Службы безопасности УЦ по средствам телефонной связи.

Срок рассмотрения заявления на приостановление действия сертификата ключа проверки ЭП составляет 1 рабочий день с момента его поступления в Службу безопасности УЦ.

После приостановления действия сертификата ключа проверки ЭП его владельцу направляется официальное уведомление (см. раздел 4.1.9 настоящего Регламента).

#### 6.7.1. Заявление на приостановление действия сертификата ключа проверки ЭП в электронной форме

Заявление на приостановление действия сертификата ключа проверки ЭП в электронной форме представляет собой электронный документ формата PKCS#7 или СМС, содержащий в подписываемых данных сведения, необходимые для приостановления действия сертификата, подписанный электронной подписью с использованием ключа ЭП и сертификата ключа проверки ЭП, владельцем которых заявитель является.

#### 6.7.2. Заявление на приостановление действия сертификата ключа проверки ЭП в бумажной форме

Заявление на приостановление действия сертификата ключа проверки ЭП в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление включает в себя следующие обязательные реквизиты:

- Идентификационные данные заявителя;
- Идентификационные данные приостанавливаемого сертификата (включая его серийный номер);
- Срок, на который приостанавливается действие сертификата;
- Причина приостановки действия сертификата;
- Дата и подпись заявителя.

#### 6.7.3. Заявление на приостановление действия сертификата ключа проверки ЭП в устной форме

Заявление на приостановление действия сертификата ключа проверки ЭП в устной форме подаётся заявителем с прохождением процедуры удалённой аутентификации зарегистрированного Пользователя УЦ (см. раздел 6.3.2 настоящего Регламента).

После успешного прохождения процедуры удалённой аутентификации, зарегистрированный Пользователь УЦ должен по запросу сотрудника Службы безопасности УЦ представить следующие сведения:

- Идентификационные данные приостанавливаемого сертификата (включая его серийный номер);
- Срок, на который приостанавливается действие сертификата;
- Причина приостановки действия сертификата.

### 6.8. Возобновление действия сертификата ключа проверки ЭП

Возобновление действия сертификата ключа проверки ЭП, изготовленного УЦ, осуществляется УЦ по заявлению на возобновление действия сертификата ключа проверки ЭП его владельца (далее по тексту раздела — заявитель).

Заявление на возобновление действия сертификата ключа проверки ЭП подаётся заявителем в электронной или бумажной форме в Службу безопасности УЦ.

Заявление на возобновление действия сертификата ключа проверки ЭП в электронной форме подаётся зарегистрированным пользователем УЦ с использованием программного обеспечения зарегистрированного пользователя, предоставляемого УЦ.

Заявление на возобновление действия сертификата ключа проверки ЭП в бумажной форме подаётся заявителем в офис Службы безопасности УЦ лично.

Срок рассмотрения заявления на возобновление действия сертификата ключа проверки ЭП составляет 3 рабочих дня с момента его поступления в Службу безопасности УЦ.

После возобновления действия сертификата ключа проверки ЭП его владельцу направляется официальное уведомление (см. раздел 4.1.9 настоящего Регламента).

#### 6.8.1. Заявление на возобновление действия сертификата ключа проверки ЭП в электронной форме

Заявление на возобновление действия сертификата ключа проверки ЭП в электронной форме представляет собой электронный документ формата PKCS#7 или СМС, содержащий в подписываемых данных сведения, необходимые для возобновления действия сертификата, подписанный электронной подписью с использованием ключа ЭП и сертификата ключа проверки ЭП, владельцем которых заявитель является.

#### 6.8.2. Заявление на возобновление действия сертификата ключа проверки ЭП в бумажной форме

Заявление на возобновление действия сертификата ключа проверки ЭП в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление включает в себя следующие обязательные реквизиты:

- Идентификационные данные заявителя;
- Идентификационные данные возобновляемого сертификата (включая его серийный номер);
- Причина возобновления действия сертификата;
- Дата и подпись заявителя.

#### 6.9. Срок хранения сертификата ключа проверки ЭП

Хранение сертификата ключа проверки ЭП пользователей УЦ в Реестре сертификатов ключей проверки ЭП УЦ, осуществляется в течение установленного срока действия сертификата ключа проверки ЭП.

Срок архивного хранения сертификата ключа проверки ЭП устанавливается в соответствии со сроком, определённым разделом 7.9 настоящего Регламента.

#### 6.10. Процедура подтверждения электронной подписи с использованием сертификата ключа проверки ЭП

Подтверждение электронной подписи в электронном документе осуществляется УЦ по обращению граждан (далее по тексту раздела — заявитель), на основании заявления на подтверждение электронной подписи в электронном документе в простой письменной форме.

Заявление на подтверждение электронной подписи в электронном документе подаётся заявителем в офис Административной службы УЦ лично.

Заявление на подтверждение электронной подписи в электронном документе должно содержать информацию от заявителя о дате и времени формирования электронной подписи в электронном документе.

Бремя доказывания достоверности даты и времени формирования электронной подписи в электронном документе возлагается на заявителя.

Обязательным приложением к заявлению на подтверждение электронной подписи в электронном документе является магнитный носитель (дискета 3'5"), содержащий следующие файлы:

- Файл, содержащий электронный документ, к которому применена электронная подпись;
- Файл, содержащий электронную подпись формата PKCS#7 электронного документа, к которому применена электронная подпись;
- Файл, содержащий сертификат ключа проверки ЭП электронного документа вместе с цепочкой сертификатов издателей, заканчивающейся корневым сертификатом;
- Файл, содержащий список отозванных сертификатов УЦ, являющегося издателем сертификата ключа проверки ЭП электронного документа, и использовавшийся для проверки ЭП электронного документа заявителем.

Срок рассмотрения заявления на подтверждение электронной подписи в электронном документе составляет 5 рабочих дней с момента его поступления в Административную службу УЦ.

В случае отказа от подтверждения электронной подписи в электронном документе заявителю возвращается заявление на подтверждение электронной подписи в электронном документе с резолюцией ответственного сотрудника Административной службы УЦ.

В случае принятия положительного решения по заявлению на подтверждение электронной подписи в электронном документе заявителю предоставляется ответ в письменной форме, заверенный собственноручной подписью ответственного сотрудника Административной службы УЦ и печатью УЦ.

Ответ содержит:

- результат проверки соответствующим сертифицированным средством электронной подписи с использованием сертификата ключа проверки ЭП в электронном документе владельцу сертификата ключа проверки ЭП и отсутствия искажений в подписанном данной электронной подписью электронном документе;
- детальный отчёт по выполненной проверке (экспертизе).

Детальный отчёт по выполненной проверке включает следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основания для проведения проверки (экспертизы);
- сведения об эксперте или комиссии экспертов, которым поручено проведение проверки, включая фамилию, имя, отчество, образование, специальность, стаж работы, учёную степень, учёное звание, занимаемую должность;
- вопросы, поставленные перед экспертом или комиссией экспертов;
- объекты исследований и материалы по заявлению, представленные эксперту для проведения проверки (экспертизы);
- содержание и результаты исследований с указанием применённых методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения в соответствии с федеральным законом.

Материалы и документы, иллюстрирующие заключение эксперта или комиссии экспертов, прилагаются к детальному отчёту и служат его составной частью.

Детальный отчёт составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами комиссии экспертов.

#### 6.11. Процедура подтверждения электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки ЭП

Подтверждение электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки ЭП осуществляется УЦ по обращению граждан (далее по тексту раздела — заявителей), на основании заявления на подтверждение электронной подписи

Уполномоченного лица УЦ в сертификате ключа проверки ЭП в простой письменной форме.

Заявление на подтверждение электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки ЭП подаётся заявителем в офис Административной службы УЦ лично.

Обязательным приложением к заявлению на подтверждение электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки ЭП является носитель информации, содержащий следующие файлы:

- Файл, содержащий сертификат ключа проверки ЭП зарегистрированного Пользователя УЦ, подвергающийся процедуре проверки;
- Файл, содержащий сертификат ключа проверки ЭП Уполномоченного лица УЦ, являющегося издателем сертификата ключа проверки ЭП Пользователя УЦ, подвергающегося процедуре проверки;
- Файл, содержащий список отозванных сертификатов УЦ, являющегося издателем сертификата ключа проверки ЭП, и использовавшийся для проверки электронной подписи Уполномоченного лица УЦ заявителем.

Срок рассмотрения заявления на подтверждение электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки ЭП составляет 5 рабочих дней с момента его поступления в Административную службу УЦ.

В случае отказа от подтверждения электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки ЭП заявителю возвращается заявление на подтверждение электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки ЭП с резолюцией ответственного сотрудника Административной службы УЦ.

В случае принятия положительного решения по заявлению на подтверждение электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки ЭП заявителю предоставляется ответ в письменной форме, заверенный собственноручной подписью ответственного сотрудника Административной службы УЦ и печатью УЦ.

Ответ содержит:

- результат проверки соответствующим сертифицированным средством электронной подписи Уполномоченного лица УЦ на сертификате ключа проверки ЭП и отсутствия искажений в подписанном данной электронной подписью сертификате ключа проверки ЭП;
- детальный отчёт по выполненной проверке.

Детальный отчёт по выполненной проверке включает следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основания для проведения проверки (экспертизы);
- сведения об эксперте или комиссии экспертов, которым поручено проведение проверки, включая фамилию, имя, отчество, образование, специальность, стаж работы, учёную степень, учёное звание, занимаемую должность;
- вопросы, поставленные перед экспертом или комиссией экспертов;
- объекты исследований и материалы по заявлению, представленные эксперту для проведения проверки (экспертизы);
- содержание и результаты исследований с указанием применённых методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения в соответствии с федеральным законом.

Материалы и документы, иллюстрирующие заключение эксперта или комиссии экспертов, прилагаются к детальному отчёту и служат его составной частью.

Детальный отчёт составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами комиссии экспертов.

## 6.12. Механизм доказательства обладания ключом ЭП, соответствующим ключу проверки ЭП

Заявления на изготовление сертификата ключа проверки ЭП, поступающие в УЦ от владельцев ключей ЭП и ключей проверки ЭП, должны содержать собственноручную подпись заявителя и, в качестве реквизита документа, сам запрос на сертификат, в формате криптографических сообщений PKCS#10 Base-64.

Электронная подпись запроса на сертификат из заявления на изготовление сертификата ключа проверки ЭП и наличие собственноручной подписи заявителя подтверждают, что заявитель является владельцем ключа ЭП, соответствующего ключу проверки ЭП из заявления на изготовление сертификата ключа проверки ЭП (так как только владелец ключа ЭП может поставить такую электронную подпись).

## 6.13. Порядок проведения разбора конфликтной ситуации, связанной с применением электронной подписи в электронном документе

Настоящий раздел описывает порядок разбора конфликтной ситуации на основе работы согласительной комиссии, формируемой из числа участников информационной системы и сотрудников удостоверяющего центра, как третьей стороны, обеспечивающей подтверждение подлинности электронной подписи в электронных документах в отношении сертификатов ключей проверки электронной подписи, созданных удостоверяющим центром. Удостоверяющий центр в описанном случае является организатором работы согласительной комиссии.

В общем случае порядок разбора конфликтной ситуации устанавливается оператором информационной системы, либо соглашением между участниками информационной системы и может отличаться от приведенного.

Разрешение конфликтных ситуаций, возникающих в информационной системе и связанных с применением электронной подписи, осуществляется согласительной комиссией. Согласительная комиссия создается с целью разрешения конфликтных ситуаций при обмене (в связи с обменом) и применении электронных документов, подписанных электронной подписью.

Конфликтная ситуация может возникнуть между участниками информационной системы. При возникновении разногласий участник информационной системы (сторона-инициатор), обязан направить в удостоверяющий центр заявление о разногласиях, возникших при обмене (в связи с обменом) и применением электронных документов с другим участником информационной системы (сторона-ответчик), подписанное собственноручной подписью уполномоченного на данное действие лицом, с подробным изложением причин разногласий и предложением создать комиссию по ее разрешению.

По заявлению о разногласиях удостоверяющий центр формирует согласительную комиссию, в которую входят:

- представитель удостоверяющего центра – председатель комиссии.
- Пользователь информационной системы – представитель участника информационной системы (сторона-инициатор), который непосредственно участвовал в информационном обмене электронными документами, по которым возникли разногласия;
- Пользователь информационной системы - представитель участника информационной системы (сторона-ответчик), который непосредственно участвовал в информационном обмене электронными документами, по которым возникли разногласия.

Комиссия осуществляет свою деятельность по месторасположению удостоверяющего центра. Язык работы согласительной комиссии – русский.

Сторона-инициатор представляет заявление о разногласии (уведомление о возникших разногласиях) с указанием:

- даты подачи заявления (уведомления);
- информации, идентифицирующей инициатора и ответчика;
- обстоятельств, на которых основаны заявленные требования;

- обоснованного расчета заявленных требований;
- нормы законодательных и иных нормативных правовых актов, на основании которых заявляется требование;
- прилагаемые к заявлению (уведомлению) о разногласии документы, составляющие доказательную базу.

До начала работы согласительной комиссии стороне - инициатору рекомендуется убедиться в целостности установленных на его технических средствах программного обеспечения, в том числе средства электронной подписи, а также отсутствии несанкционированных действий со стороны третьих лиц.

Сторона-ответчик обязана в период работы комиссии представить стороне-инициатору и комиссии возражения по каждому требованию, изложенному в заявлении о разногласиях, либо согласиться с предъявляемыми требованиями.

В возражениях ответчика на каждое требование должны содержаться документально обоснованные ответы или сделана ссылка на доказательства, которые могут быть представлены в ходе работы комиссии.

Любая сторона в ходе работы комиссии может внести ходатайства об изменении или дополнении своих требований или возражений.

Комиссия в ходе разбирательства в любой момент может затребовать от сторон предоставления документов, вещественных или иных доказательств в устанавливаемый комиссией срок.

Рассмотрение конфликтной ситуации производится на основании всех представленных документов, доказательств.

В том случае, если обстоятельства, имеющие значение для принятия решения по делу, могут быть исследованы только на основе применения специальных научных знаний, комиссия вправе назначить экспертизу по подтверждению подлинности электронной подписи в электронном документе.

Проведение экспертизы возлагается на удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, с использованием которого была сформирована электронная подпись электронного документа, являющегося предметом разногласий. Запрос на проведение экспертизы оформляется заявлением на подтверждение подлинности электронной подписи в электронном документе, подаваемом в удостоверяющий центр от лица участника информационной системы - владельца сертификата ключа проверки электронной подписи (см. пункт 6.10 и 6.11 настоящего Регламента). Порядок проведения экспертных работ Удостоверяющим центром по подтверждению подлинности электронной подписи в электронном документе устанавливается Удостоверяющим центром. Для проведения удостоверяющим центром указанных работ электронные документы и их электронная подпись экспортируются из информационной системы в соответствующие файлы и предоставляются вместе с заявлением на подтверждение подлинности электронной подписи в удостоверяющий центр. Результатом проведения экспертных работ удостоверяющего центра является заключение удостоверяющего центра.

Экспертиза может быть назначена комиссией по обоснованному ходатайству любой из сторон или по ее собственной инициативе.

По итогам работы согласительной комиссии составляется акт, в котором содержится краткое изложение выводов комиссии и решение комиссии по рассматриваемому разногласию.

Помимо изложения выводов согласительной комиссии и решения комиссии акт должен содержать следующие данные:

- состав комиссии;
- дату и место составления акта;
- дату и время начала и окончания работы комиссии;
- краткий перечень мероприятий, проведенных комиссией;
- выводы комиссии;
- собственноручные подписи членов комиссии;

– указание на особое мнение члена (или членов комиссии), в случае наличия такового.

Акт составляется в 3-х экземплярах и предоставляется по одному экземпляру для каждой из сторон конфликтной ситуации, а также удостоверяющему центру.

## 7. Дополнительные положения

### 7.1. Идентифицирующие данные Уполномоченного лица УЦ

Каждое Уполномоченное лицо УЦ обычно идентифицируется следующими данными:

- Фамилия, имя, отчество: \_\_\_\_\_
- Организация: \_\_\_\_\_
- Подразделение: \_\_\_\_\_
- Адрес электронной почты: \_\_\_\_\_
- Субъект Федерации: \_\_\_\_\_

### 7.2. Сроки действия ключей Уполномоченных лиц УЦ

Максимальный срок действия ключа ЭП и сертификата ключа проверки ЭП Уполномоченного лица УЦ определяются требованиями применяемого средства криптографической защиты информации.

Для «КриптоПро УЦ» установлены следующие максимальные сроки действия ключей ЭП и ключей проверки ЭП Уполномоченного лица УЦ.

При использовании СКЗИ "КриптоПро CSP" максимальные сроки действия ключа ЭП УЦ составляют 3 года (при условии, что общее время использования ключа ЭП для выполнения целевых функций в течении трех лет его действия ограничено 1 годом и 3 месяцами, остальное время ключ ЭП используется только для подписи списков аннулированных сертификатов); максимальный срок действия сертификата ключа проверки ЭП - 16 лет.

При использовании ПАКМ "КриптоПро HSM" версии 1.0 для хранения ключа ЭП Удостоверяющего центра максимальные сроки действия ключа ЭП УЦ составляют 5 лет (при условии, что общее время использования ключа ЭП для выполнения целевых функций в течении пяти лет его действия ограничено 3 годами, остальное время ключ ЭП используется только для подписи списков аннулированных сертификатов); максимальный срок действия сертификата ключа проверки ЭП 18 лет.

При использовании ПАКМ "КриптоПро HSM" версии 2.0 для хранения ключа ЭП Удостоверяющего центра в неэкспортируемом виде максимальный срок действия ключа ЭП УЦ составляет 5 лет (при условии, что общее время использования ключа ЭП для выполнения целевых функций в течении пяти лет его действия ограничено 2 годами, остальное время ключ ЭП используется только для подписи списков аннулированных сертификатов; в случае, если регламентом УЦ установлено, что срок действия ключа пользователя УЦ не превышает 1 год и 3 месяца, общее время использования ключа ЭП УЦ для выполнения целевых функций в течении пяти лет его действия ограничено 3 годами, остальное время ключ ЭП используется только для подписи списков аннулированных сертификатов); максимальный срок действия сертификата ключа проверки ЭП - 18 лет.

Начало периода действия ключа ЭП Уполномоченного лица УЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки ЭП.

### 7.3. Требования к средствам электронной подписи, используемым в составе Удостоверяющего центра и требования к средствам электронной подписи пользователей УЦ

Средства электронной подписи аккредитованного Удостоверяющего центра и средства электронной подписи пользователя Удостоверяющего центра должны удовлетворять требованиям Федерального закона №63-ФЗ «Об электронной подписи» и требованиям Приказа ФСБ РФ от 27.12.2011 г. №796.

Формирование и проверка электронной подписи на серверных компонентах Удостоверяющего центра, а именно на Центре сертификации и Центре регистрации (или Центрах Регистрации, если таковых в Удостоверяющем центре более одного) осуществ-

ляется Администратором УЦ или в автоматическом режиме, под контролем лица, ответственного за создание и проверку ЭП в ЦС (п. 4.1.5).

На Автоматизированном рабочем месте Администратора Центра регистрации выполнение операции создания электронной подписи под запросами на регистрацию, запросами на сертификат, запросами на управление статусом сертификата осуществляется только после того, как привилегированный пользователь (Администратор, Оператор, Администратора Аудита) ознакомится с содержимым подписываемого документа. После ознакомления - привилегированный пользователь подтверждает создание электронной подписи. Выполнение операции создания электронной подписи заканчивается уведомлением о выполнении операции, связанной с созданием электронной подписи (положительный результат свидетельствует об успешном создании ЭП, отрицательный – ЭП не создана).

На Автоматизированных рабочих местах Администратора Центра регистрации и разбора конфликтных ситуаций выполнение операции проверки электронной подписи сопровождается ознакомлением с электронным документом, информированием о внесении изменений в электронный документ (при изменении электронного документа появляется сообщение – электронная подпись – «Не верна»), отображением сертификата ключа проверки ЭП подписчика данного электронного документа.

#### 7.4. Сроки действия ключей ЭП и сертификатов ключей проверки ЭП пользователей УЦ

Максимальный срок действия ключа ЭП Пользователя УЦ, соответствующего сертификату ключа проверки ЭП, владельцем которого он является, определяется требованиями средства криптографической защиты информации, использующим данный ключ ЭП.

Начало периода действия ключа ЭП Пользователя УЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки ЭП Пользователя УЦ.

Срок действия ключа проверки ЭП устанавливается равным сроку действия сертификата ключа проверки ЭП.

Максимальный срок действия сертификата ключа проверки ЭП Пользователя УЦ определяется требованиями средства криптографической защиты информации, использующим ключ ЭП пользователя, соответствующий указанному сертификату.

Для «КриптоПро УЦ» установлены следующие максимальные сроки действия ключей ЭП и ключей проверки ЭП Пользователей УЦ.

Максимальный срок действия ключа пользователя УЦ составляет 3 года (но не более сроков действия ключей ЭП, указанных в эксплуатационной документации на используемые пользователями средства ЭП), максимальный срок действия сертификата - 18 лет, но не более сроков действия соответствующих ключей проверки ЭП, обеспечиваемых используемыми пользователями средствами ЭП и средствами УЦ при выполнении следующих условий: а) ключ ЭП Уполномоченного лица УЦ с помощью которого подписан сертификат пользователя создаётся и хранится в ПАКМ "КриптоПро HSM" версии 2.0 в неэкспортируемом виде, б) ключ пользователя создаётся и хранится в неэкспортируемом виде. В остальных случаях максимальный срок действия ключа пользователя УЦ (владельца сертификата ключа проверки ЭП) составляет 1 год и 3 месяца (но не более сроков действия ключей ЭП, указанных в эксплуатационной документации на используемые пользователями средства ЭП), максимальный срок действия сертификата - 16 лет, но не более сроков действия соответствующих ключей проверки ЭП, обеспечиваемых используемыми пользователями средствами ЭП и средствами УЦ. Срок действия сертификата ключа подписи пользователя УЦ не может превышать срок действия соответствующего ключа подписи более, чем на 15 лет.

Конкретный срок действия сертификата ключа проверки ЭП устанавливается УЦ в момент его изготовления.

Максимальные сроки действия ключа ЭП и ключа проверки ЭП Пользователя УЦ определяются типом запрашиваемого сертификата. Тип сертификата задаётся пользователем в заявлении на изготовление сертификата или назначается Оператором УЦ. При назначении сроков действия УЦ учитывает пожелания пользователей из запроса на

сертификат, которые, однако, не могут вывести назначенные сроки из интервала времени, ограниченного максимальными сроками действия.

Приложение №1 к настоящему регламенту содержит описание всех шаблонов сертификатов, поддерживаемых УЦ, с указанием сроков действия ключа ЭП и ключа проверки ЭП.

## 7.5. Служебные ключи и служебный сертификат ключа проверки ЭП

Служебные ключи и служебный сертификат ключа проверки ЭП используются, когда политика безопасности прикладной системы не допускает использование пользователем ключей, созданных не им лично. Служебные ключи создаются в УЦ и передаются пользователю. Пользователь использует их только для первоначальной аутентификации, и для проведения смены временных ключей и получения рабочих ключей. Временные ключи отличаются от рабочих только ограниченным сроком действия и отсутствием другой специфичной информации.

Служебные ключи и служебный сертификат ключа проверки ЭП предназначены для:

- обеспечения аутентификации и авторизации зарегистрированного Пользователя УЦ при использовании программного обеспечения зарегистрированного Пользователя УЦ, предоставляемого УЦ;
- формирования электронной подписи в заявлении на рабочий сертификат ключа проверки ЭП в электронном виде.

## 7.6. Рабочие ключи и рабочий сертификат ключа проверки ЭП

Рабочие ключи и рабочий сертификат ключа проверки ЭП предназначены для:

- обеспечения аутентификации и авторизации зарегистрированного Пользователя УЦ при использовании программного обеспечения зарегистрированного Пользователя УЦ, предоставляемого УЦ;
- формирования электронной подписи в заявлении на рабочий сертификат ключа проверки ЭП в электронном виде;
- использования в соответствии со сведениями, указанными в сертификате в областях использования.

## 7.7. Меры защиты ключей ЭП

Ключи ЭП пользователей УЦ должны записываться при их генерации на типы ключевых носителей, которые поддерживаются используемым средством криптографической защиты информации.

Ключи ЭП на ключевом носителе защищаются паролем (ПИН-кодом). Пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство криптографической защиты информации.

Если процедуру генерации ключей Пользователя УЦ выполняет сотрудник УЦ, то он должен сообщить сформированный пароль (ПИН-код) владельцу ключей ЭП.

Ответственность за сохранение пароля (ПИН-кода) в тайне возлагается на владельца ключей ЭП.

Сотрудники УЦ, являющиеся владельцами ключей ЭП, также выполняют указанные в разделе меры защиты ключей ЭП.

## 7.8. Информация из сертификата ключа проверки ЭП на бумажном носителе

При получении квалифицированного сертификата заявителем он должен быть под расписку ознакомлен аккредитованным удостоверяющим центром с информацией, содержащейся в квалифицированном сертификате.

Оператор обязан осуществить проверку соответствия сертификата ключа проверки электронной подписи в электронном виде распечатанной копии этого сертификата. Только после успешного проведения указанной проверки сведения предоставляются на подпись владельцу сертификата.

При оформлении данной расписки в бумажной форме указанная информация должна включать сведения, установленные Статьей 17 Федерального закона №63-ФЗ «Об электронной подписи».

## 7.9. Архивное хранение документированной информации

### 7.9.1. Состав архивируемых документов

Архивированию подлежат следующая документированная информация:

- Реестр сертификатов ключей проверки ЭП пользователей УЦ;
- сертификаты ключей проверки ЭП Уполномоченного лица УЦ;
- журналы аудита программно-аппаратных средств обеспечения деятельности УЦ;
- Реестр зарегистрированных пользователей УЦ;
- заявления на изготовление ключей пользователей УЦ;
- заявления на изготовление сертификатов ключей проверки ЭП пользователей УЦ;
- заявления на аннулирование (отзыв) сертификатов ключей проверки ЭП;
- заявления на приостановление действия сертификатов ключей проверки ЭП;
- заявления на возобновление действия сертификатов ключей проверки ЭП;
- служебные документы УЦ.

### 7.9.2. Источник комплектования архивного фонда

Источником комплектования архивного фонда УЦ являются подразделения (Службы) УЦ, обеспечивающие документирование.

### 7.9.3. Архивохранилище

Архивные документы хранятся в специально оборудованном помещении-архивохранилище, обеспечивающим режим хранения архивных документов, устанавливаемый законодательством Российской Федерации.

### 7.9.4. Срок архивного хранения

Документы, подлежащие архивному хранению, являются документами временно-го хранения.

Срок хранения архивных документов устанавливается \_\_\_\_ лет.

### 7.9.5. Уничтожение архивных документов

Выделение архивных документов к уничтожению и уничтожение осуществляется постоянно действующей комиссией, формируемой из числа сотрудников Службы безопасности УЦ и назначаемой приказом руководителя УЦ.

## 7.10. Смена ключей Уполномоченного лица УЦ

### 7.10.1. Плановая смена ключей Уполномоченного лица УЦ

Плановая смена ключей (ключа ЭП и соответствующего ему ключа проверки ЭП) каждого Уполномоченного лица УЦ должна выполняться в течение срока действия ключа ЭП Уполномоченного лица УЦ.

При использовании СКЗИ «КриптоПро CSP» плановая смена ключей Уполномоченного лица УЦ выполняется не ранее, чем через 1 год, и не позднее, чем через 1 год и 3 месяца после начала действия ключа ЭП Уполномоченного лица УЦ.

Процедура плановой смены ключей Уполномоченного лица УЦ осуществляется в следующем порядке:

- Уполномоченное лицо УЦ формирует новый ключ ЭП и соответствующий ему ключ проверки ЭП;
- Уполномоченное лицо УЦ изготавливает сертификат нового ключа проверки ЭП и подписывает его электронной подписью с использованием нового ключа ЭП.

Старые ключи ЭП Уполномоченных лиц УЦ используются в течение своего срока действия для формирования списков отозванных сертификатов в электронной форме, изданных УЦ в период действия старых ключей ЭП Уполномоченных лиц УЦ.

#### 7.10.2. Внеплановая смена ключей Уполномоченных лиц УЦ

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации ключа ЭП Уполномоченного лица УЦ.

Процедура внеплановой смены ключей Уполномоченного лица УЦ выполняется в порядке, определённом процедурой плановой смены ключей Уполномоченного лица УЦ.

## 8. Структуры сертификатов и списков отозванных сертификатов

### 8.1. Структура квалифицированного сертификата

Квалифицированный сертификат ключа проверки электронной подписи в электронной форме создается в формате X.509 версии 3, структура квалифицированного сертификата ключа проверки ЭП должна удовлетворять требованиям Федерального закона №63-ФЗ «Об электронной подписи» (с учетом изменений, вносимых Федеральным законом №445-ФЗ) и Приказа ФСБ России от 27.12.2011 г. №795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Структура квалифицированного сертификата ключа проверки электронной подписи:

Название	Описание	Содержание
<b>Базовые поля сертификата</b>		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001 или ГОСТ Р 34.11/34.10-2012
Issuer	УЦ - Издатель сертификата	Согласно Таблицы заполнения поля Субъект (для ЮЛ, авторматическое создание/проверка ЭП)
Validity Period	Срок действия сертификата	Действителен с (not Before): дд.мм.гггг чч:мм:сс UTC Действителен по (not After): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	Согласно Таблицы заполнения поля Субъект
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001 или ГОСТ Р 34.11/34.10-2012
Issuer Signature	ЭП УЦ - издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 или ГОСТ Р 34.11/34.10-2012
<b>Дополнения сертификата</b>		
Authority Key Identifier	Идентификатор ключа УЦ - издателя сертификата	Идентификатор ключа подписи Удостоверяющего центра, на котором подписан данный сертификат; УЦ – издатель сертификата, заполняется Согласно Таблицы заполнения поля Субъект (для ЮЛ, авторматическое создание/проверка ЭП); Серийный номер сертификата УЦ
Key Usage (critical)	Область использования ключа	Набор областей использования ключа (реализуется установкой соответствующих битов в значение «1»).
Certificate Policies	Политика сертификации	Идентификатор политики – класс средства ЭП Например: Для средства ЭП класса КС1: [1] Политика сертификата Идентификатор политики=Класс средства ЭП КС1 Для средства ЭП класса КС2: [1] Политика сертификата Идентификатор политики=Класс средства ЭП КС1 [2] Политика сертификата Идентификатор политики=Класс средства ЭП КС2 Для средства ЭП класса КС3: [1] Политика сертификата Идентификатор политики=Класс средства ЭП КС1 [2] Политика сертификата

		Идентификатор политики=Класс средства ЭП КС2 [3] Политика сертификата Идентификатор политики=Класс средства ЭП КС3
Subject Sign Tool	Средство ЭП владельца сертификата	Наименование средства ЭП владельца сертификата Например: КриптоПро CSP
Issuer Sign Tool	Средство ЭП и средство УЦ, использующиеся для создания сертификатов	Наименование средства ЭП и средства УЦ, а также реквизитов документа, подтверждающего соответствие указанных средств требованиям, установленным законодательством РФ (в случае отсутствия действующего сертификата соответствия на средство ЭП или средство УЦ допускается указывать номер положительного заключения) Например: Средство электронной подписи: "СКЗИ "КриптоПро CSP" версии 3.9, вариант исполнения 2 Заключение на средство ЭП: Сертификат соответствия № СФ/___-___ от __.__.____ Г." Средство УЦ: "ПАК "КриптоПро УЦ" версии 2.0, вариант исполнения 1 Заключение на средство УЦ: Сертификат соответствия № СФ/___-___ от __.__.____ Г."
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор ключа подписи владельца сертификата
Extended Key Usage (необязательное дополнение)	Расширенная область использования ключа	Набор расширенных областей использования ключа - объектных идентификаторов
CRL Distribution Point (необязательное дополнение)	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/Name.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, Name – наименование файла списка отозванных сертификатов
Authority Information Access (необязательное дополнение)	Адрес Службы актуальных статусов сертификатов, Адрес размещения информации о сертификате УЦ	URL адреса Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP URL адреса размещения файла сертификата УЦ
Private Key Period (необязательное дополнение)	Период использования ключа подписи	Действителен с (not Before): дд.мм.гггг чч:мм:сс UTC Действителен по (not After): дд.мм.гггг чч:мм:сс UTC
		В сертификат могут быть добавлены дополнительные поля и дополнения согласно RFC 5280

Таблица заполнения поля Субъект квалифицированного сертификата ключа проверки электронной подписи

Физическое лицо	Физическое лицо – индивидуальный предприниматель	Юридическое лицо с информацией о представителе (российское юрлицо)	Юридическое лицо без информации о представителе (автоматическое создание и/или проверка ЭП) (российское юрлицо)	Юридическое лицо с информацией о представителе (иностранное юрлицо)	Юридическое лицо без информации о представителе (автоматическое создание и/или проверка ЭП) (иностранное юрлицо)
commonName (общее имя) - ФИО	commonName (общее имя) - ФИО	commonName (общее имя) – полное или сокращенное наименование юридического лица в соответствии с учредительными документами	commonName (общее имя) - полное или сокращенное наименование юридического лица в соответствии с учредительными документами	commonName (общее имя) – полное или сокращенное наименование юридического лица в соответствии с учредительными документами	commonName (общее имя) – полное или сокращенное наименование юридического лица в соответствии с учредительными документами
surname (фамилия) – фамилия	surname (фамилия) – фамилия	surname (фамилия) – фамилия представителя		surname (фамилия) – фамилия представителя	
givenName (приобретенное имя) – имя и отчество	givenName (приобретенное имя) – имя и отчество	givenName (приобретенное имя) – имя и отчество представителя		givenName (приобретенное имя) – имя и отчество представителя	
countryName (наименование страны) – двухсимвольный код	countryName (наименование страны) – двухсимвольный код	countryName (наименование страны) – двухсимвольный код - RU	countryName (наименование страны) – двухсимвольный код - RU	countryName (наименование страны) – двухсимвольный код	countryName (наименование страны) – двухсимвольный код
stateOrProvinceName (наименование штата или области) - наименование субъекта РФ	stateOrProvinceName (наименование штата или области) - наименование субъекта РФ	stateOrProvinceName (наименование штата или области) - наименование субъекта РФ	stateOrProvinceName (наименование штата или области) - наименование субъекта РФ		
localityName (наименование населенного пункта)	localityName (наименование населенного пункта)	localityName (наименование населенного пункта)	localityName (наименование населенного пункта)	localityName (наименование населенного пункта)	localityName (наименование населенного пункта)
streetAddress (название улицы, номер дома) - опционально	streetAddress (название улицы, номер дома) - опционально	streetAddress (название улицы, номер дома)			
		organizationName (наименование организации)	organizationName (наименование организации)	organizationName (наименование организации)	organizationName (наименование организации)
		organizationUnitName (подразделение)	organizationUnitName (подразделение) - опционально	organizationUnitName (подразделение)	organizationUnitName (подразделение) - опционально
		title (должность) – должность представителя		title (должность) – должность представителя	
E-mail (адрес электронной почты) - опционально	E-mail (адрес электронной почты) - опционально	E-mail (адрес электронной почты) - опционально	E-mail (адрес электронной почты) - опционально	E-mail (адрес электронной почты) - опционально	E-mail (адрес электронной почты) - опционально
		OGRN (ОГРН)	OGRN (ОГРН)		
SNILS (СНИЛС)	SNILS (СНИЛС)	SNILS (СНИЛС) - представителя			
INN (ИНН)	INN (ИНН)	INN (ИНН) – юридического лица			
	OGRNIP (ОГРНИП)				

## 8.2. Структура списка отозванных сертификатов, изготавливаемого УЦ в электронной форме

УЦ изготавливает списки отозванных сертификатов ключей проверки ЭП пользователей УЦ и Уполномоченного лица УЦ в электронной форме (далее по тексту раздела — СОС) формата X.509 версии 2.

### 8.2.1. Расширения списка отозванных сертификатов.

При изготовлении списка отозванных сертификатов УЦ использует следующие расширения:

- Расширение «Authority Key Identifier» содержит идентификатор ключа Уполномоченного лица УЦ;
- Расширение «Reason Code» содержит код причины отзыва сертификата ключа проверки ЭП;
- Расширение «Microsoft CA Version» содержит номер сертификата службы сертификатов.

## 9. Программные и технические средства обеспечения деятельности УЦ

Для реализации своих услуг и обеспечения жизнедеятельности УЦ использует следующие программные и технические средства:

- Программный комплекс обеспечения реализации целевых функций УЦ (ЖТЯИ.00078-01 99 01), далее по тексту — ПК УЦ;
- Технические средства обеспечения работы ПК УЦ, далее по тексту — ТС УЦ;
- Программные и программно-аппаратные средства защиты информации, далее по тексту — СЗИ УЦ.

### 9.1. Программный комплекс обеспечения реализации целевых функций УЦ

Каждый логический компонент «КриптоПро УЦ» должен оснащаться необходимым набором программных компонент «КриптоПро УЦ», которые поставляются в виде единого пакета установки «КриптоПро УЦ. Комплекс программ» (ЖТЯИ.00078-01 99 01).

Пакет установки «КриптоПро УЦ» устанавливает следующие программы:

- Программный компонент УЦ «Диспетчер УЦ»
- Роль УЦ «Сервер центров сертификации»
- Роль УЦ «Сервер центров регистрации»
- Роль УЦ «Сервер CDP»
- Программный компонент УЦ «Консоль управления ЦР»
- Программный компонент УЦ «Консоль экспертизы ЭП»

Роль УЦ — это набор программ, которые при правильной установке и настройке позволяют компьютеру выполнять определённую функцию УЦ. Роли УЦ определяют основную функцию, назначение или цель использования компьютера. Можно назначить компьютер для выполнения одной роли, которая интенсивно используется в УЦ, или для выполнения нескольких ролей, если каждая из них применяется лишь изредка.

Логические компоненты УЦ могут разворачиваться не только на серверных, но и на клиентских операционных системах (в отличие от Windows, где «Диспетчер сервера» доступен только на серверных операционных системах и все Роли могут быть добавлены только на серверах).

Роли УЦ позволяют настроить сервер или рабочую станцию в качестве одной или нескольких логических структурных элементов УЦ. Они обычно имеют собственные базы данных, в которых создаются очереди запросов. После правильной установки и настройки Роли УЦ функционируют автоматически. Это позволяет компьютерам, на которых они установлены, выполнять назначенные задачи при ограниченном участии пользователя.

Набор программных компонент «КриптоПро УЦ», которые необходимо установить на компьютерной системе для разворачивания на ней определённого логического структурного компонента, приведён в таблице ниже.

**Таблица 4. Программные компоненты УЦ, требуемые для разворачивания логических структурных компонент УЦ**

Логический компонент УЦ	Требуемые программные компоненты «КриптоПро УЦ»
<b>Центр сертификации</b>	Программный компонент УЦ «Диспетчер УЦ», Роль УЦ «Сервер центров сертификации»
<b>Центр регистрации</b>	Программный компонент УЦ «Диспетчер УЦ», Роль УЦ «Сервер центров регистрации»
<b>АРМ обслуживающего персонала</b>	Программный компонент УЦ «Консоль управления ЦР»

<b>АРМ разбора конфликтных ситуаций</b>	Программный компонент УЦ «Консоль экспертизы ЭП»
<b>АРМ пользователя</b>	Специальные программные компоненты «КриптоПро УЦ» не требуются

Центр сертификации является логическим компонентом УЦ и предназначен для обеспечения реализации следующих целевых функций УЦ:

- Формирования сертификатов ключей проверки ЭП пользователей УЦ в электронной форме с использованием ключа ЭП и сертификата ключа проверки ЭП Уполномоченного лица УЦ;
- Формирования списков отозванных сертификатов ключей проверки ЭП пользователей УЦ в электронной форме с использованием ключей ЭП и сертификатов ключей проверки ЭП Уполномоченных лиц УЦ на основе эталонной копии списка отозванных сертификатов ключей проверки ЭП пользователей УЦ;
- Ведения эталонной копии Реестра сертификатов ключей проверки ЭП УЦ;
- Ведения эталонной копии списка отозванных сертификатов ключей проверки ЭП пользователей УЦ;
- Обеспечения уникальности ключей проверки ЭП в изданных сертификатах ключей проверки ЭП пользователей УЦ.

Ответственность за эксплуатацию Центра сертификации возлагается на Уполномоченных лиц УЦ.

Центр регистрации является логическим компонентом УЦ и предназначен для обеспечения реализации следующих целевых функций УЦ:

- Ведения Реестра зарегистрированных пользователей УЦ;
- Ведения Реестра сертификатов ключей проверки ЭП УЦ;
- Ведения Реестра заявлений на изготовление сертификатов ключей проверки ЭП пользователей УЦ в электронной форме;
- Ведения Реестра заявлений на аннулирование (отзыв) сертификатов ключей проверки ЭП пользователей УЦ в электронной форме;
- Ведения Реестра заявлений на приостановление действия сертификатов ключей проверки ЭП пользователей УЦ в электронной форме;
- Ведения Реестра запросов на регистрацию пользователей УЦ в электронной форме;
- Ведения Реестра заявлений на возобновление действия сертификатов ключей проверки ЭП пользователей УЦ в электронной форме;
- Предоставления программных средств для незарегистрированных пользователей УЦ для обеспечения реализации их права передать по сети в УЦ запрос на регистрацию в электронной форме;
- Предоставления программных средств для зарегистрированных пользователей УЦ для обеспечения реализации их прав в части пользования предоставляемыми программными средствами.

Ответственность за эксплуатацию Центра регистрации возлагается на Службу регистрации УЦ.

АРМ обслуживающего персонала ЦР предназначен для обеспечения реализации своих функциональных обязанностей сотрудникам Службы регистрации и Службы безопасности УЦ.

АРМ разбора конфликтных ситуаций предназначен для обеспечения своих функциональных обязанностей сотрудникам Административной службы УЦ в части взаимодействия с пользователями УЦ при разрешении вопросов, связанных с подтверждением электронной подписи Уполномоченного лица УЦ в сертификатах ключей проверки ЭП, изготовленных УЦ в электронной форме.

## 9.2. Технические средства обеспечения работы ПК УЦ

Технические средства обеспечения работы ПК УЦ включают в себя:

- Выделенный сервер Центра сертификации;
- Выделенный сервер Центра регистрации;
- Телекоммуникационное оборудование;
- Компьютеры рабочих мест сотрудников Служб УЦ;
- Устройства печати на бумажных носителях (принтеры).

Ответственность за эксплуатацию технических средств и общесистемного программного обеспечения возлагается на Техническую службу УЦ.

## 9.3. Программные и программно-аппаратные средства защиты информации

Программные и программно-аппаратные средства защиты информации включают в себя:

- Средства криптографической защиты информации;
- Межсетевой экран для обеспечения защиты информации при сетевом взаимодействии с Центром регистрации;
- Программно-аппаратные комплексы защиты от несанкционированного доступа типа «электронный замок»;
- Устройства для обеспечения бесперебойного питания серверов Центра сертификации и Центра регистрации;
- Устройства обеспечения температурно-влажностного режима и кондиционирования служебных и рабочих помещений УЦ;
- Устройства обеспечения противопожарной безопасности помещений УЦ.

На компонентах УЦ должны использоваться средства криптографической защиты информации (средства электронной подписи), входящие в состав комплектации «КриптоПро УЦ».

Ответственность за эксплуатацию программных и программно-аппаратных средств защиты информации возлагается на Техническую службу УЦ.

## 9.4. Перечень событий, регистрируемых программным комплексом обеспечения реализации целевых функций УЦ

Основные типы событий, регистрируемые программными компонентами УЦ:

- Центром Сертификации:
  - Поступление запроса на сертификат;
  - Издание сертификата;
  - Издан СОС;
  - Невыполнение внутренней операции программной компоненты;
  - Системные события общесистемного программного обеспечения.
- Центром Регистрации:
  - Помещен запрос на регистрацию;
  - Принят запрос на регистрацию;
  - Отклонен запрос на регистрацию;
  - Помещен запрос на сертификат;
  - Принят запрос на сертификат;
  - Отклонен запрос на сертификат;
  - Установка сертификата подтверждена пользователем;
  - Помещен запрос на отзыв сертификата;
  - Принят запрос на отзыв сертификата;
  - Отклонен запрос на отзыв сертификата;

- Помещен запрос на первый сертификат;
- Запрошен список отозванных сертификатов;
- Опубликован список отозванных сертификатов;
- Невыполнение внутренней операции программной компоненты;
- Установлено сетевое соединение с внешней программной компонентой;
- Системные события общесистемного программного обеспечения.

Структуры записей событий приведены в эксплуатационной документации ПК УЦ и общесистемного программного обеспечения.

## 9.5. Перечень данных программного комплекса обеспечения реализации целевых функций УЦ, подлежащих резервному копированию

При эксплуатации программного комплекса обеспечения реализации целевых функций УЦ ежедневно выполняется резервное копирование данных компонент ПК УЦ.

Перечень данных ПК УЦ, подлежащих резервному копированию, включает в себя:

- Базу данных Службы сертификатов ПК УЦ, включающую журнал выданных сертификатов, очередь запросов, сертификаты ключей проверки ЭП Уполномоченных лиц УЦ;
- Базу данных Службы регистрации ПК УЦ;
- Журналы аудита компонент ПК УЦ в составе, определенном эксплуатационной документацией ПК УЦ.

## 9.6. Порядок технического обслуживания средств обеспечения деятельности УЦ

Порядок технического обслуживания средств обеспечения деятельности удостоверяющего центра, построенного на базе программно-аппаратного комплекса «Удостоверяющий Центр «КриптоПро УЦ» содержит описание и правила выполнения работ по техническому обслуживанию средств удостоверяющего центра.

Техническое обслуживание средств обеспечения деятельности удостоверяющего центра направлено на обеспечение постоянной готовности указанных средств к использованию по прямому назначению и предотвращению выхода их из строя.

Техническое обслуживание средств обеспечения деятельности удостоверяющего центра включает:

- техническое обслуживание вычислительной техники и периферийного оборудования;
- техническое обслуживание общесистемного и специализированного программного обеспечения.

### 9.6.1. Техническое обслуживание вычислительной техники и периферийного оборудования

К средствам вычислительной техники и периферийному оборудованию удостоверяющего центра относятся:

- Сервер Центра сертификации;
- Сервер Центра регистрации;
- Автоматизированные рабочие места привилегированных пользователей Удостоверяющего центра (администраторов и операторов удостоверяющего центра);
- Автоматизированное рабочее место разбора конфликтных ситуаций;
- Межсетевой экран;

- Программно-аппаратный криптографический модуль (ПАКМ) «КриптоПро HSM» (может отсутствовать в случае использования на Центре сертификации СКЗИ «КриптоПро CSP»);
- Источник бесперебойного питания (может отсутствовать в случае использования в эксплуатирующей организации единой централизованной системы бесперебойного питания);
- Сетевое и коммутационное оборудование.

Все виды работ по техническому обслуживанию вычислительной техники и периферийного оборудования проводятся по установленному графику, вне зависимости от технического состояния изделия. Уменьшать установленный объем и изменять периодичность технического обслуживания не рекомендуется.

Для поддержания работоспособности удостоверяющего центра необходимо производить периодические осмотры входящего в него оборудования.

Техническое обслуживание вычислительной техники и периферийного оборудования должно включать в себя следующие виды работ:

№ п/п	Наименование работы	Периодичность выполнения работы	Порядок проведения	Примечание
1	2	3	4	5
1.	Проверка внешнего вида корпусов оборудования, сетевого и соединительного шнуров на отсутствие повреждений	Ежедневно	Проводится визуально	Допускается проводить внешний осмотр оборудования без выключения напряжения питания. Эксплуатация оборудования с повреждениями категорически запрещается.
2.	Проверка работоспособности	Ежедневно	Проверяется исправность оборудования посредством выполнения штатных задач, запускаемых в связи с основной деятельностью удостоверяющего центра (по назначению)	Проводится с учётом местных условий эксплуатации
3.	Проверка пломбировки, маркировки, целостности корпусов оборудования	Ежедневно	Проводится визуально	При нарушении пломбировки, маркировки, целостности корпуса оборудования дальнейшая эксплуатация изделия запрещена до установления причин нарушения пломбировки, маркировки, целостности корпуса
4.	Очистка от пыли и грязи	Один раз в месяц	Отключить изделие от сети переменного тока. Удалить с поверхности изделия пыль, грязь и влагу. Для очистки изделия от пыли и грязи допускается использование мягкой ветоши (легкая безворсовая ткань, например, марля хлопчатобумажная ГОСТ 11109 – 74) и неагрессивных моющих растворов.	Очистку выполнять путем последовательной протирки поверхностей: 1) влажной салфеткой, смоченной в 5 % растворе бытовых моющих средств; 2) влажной салфеткой, смоченной в чистой воде; 3) сухой салфеткой. При протирке не допускать попадания влаги на разъемные соединения и токоведущие цепи
5.	Контрольная проверка работоспособности оборудования	Один раз в год	Проверку оборудования необходимо выполнять путем прогона контрольной задачи	Контрольная проверка оборудования необходима в случае его устойчивой работоспособности по назначению

№ п/п	Наименование работы	Периодичность выполнения работы	Порядок проведения	Примечание
1	2	3	4	5
6.	Текущий ремонт	По мере необходимости	Оборудование может быть отремонтировано у эксплуатирующей организации. В случае выхода из строя подлежит замене или ремонту в условиях предприятия-изготовителя.	
7.	Дополнительные работы	Согласно руководства по эксплуатации на конкретное оборудование	В том случае, если требованиями эксплуатационной документации на конкретное оборудование предусмотрено обязательное выполнение определенных работ по его техническому обслуживанию, то данные работы должны быть включены в указанный перечень проводимых работ	

Оборудование рекомендуется периодически (один раз в год) подвергать техническому осмотру с участием специалистов предприятия-изготовителя или специалистов рекомендуемого предприятием-изготовителем сервисного центра.

По истечении срока гарантии оборудования рекомендуется заключение с предприятием-изготовителем или соответствующим сервисным центром договора на техническое обслуживание оборудования.

Запрещается осуществлять самовольную регулировку, ремонт, переустановку или вносить какие-либо изменения в конструкцию оборудования.

Техническое обслуживание оборудования, входящего в состав удостоверяющего центра, производится в соответствии с инструкциями по эксплуатации каждого аппарата в него входящего.

Все неисправности оборудования, обнаруженные при периодических осмотрах, должны устраняться по мере их выявления и регистрироваться в соответствующем журнале.

#### 9.6.2. Техническое обслуживание общесистемного и специализированного программного обеспечения

Общесистемное программное обеспечение включает в себя структурные компоненты операционной системы, средства управления базами данных, а также стандартные средства администрирования операционной системы.

К специализированному программному обеспечению относятся:

- Средства криптографической защиты информации (СКЗИ «КриптоПро CSP», ПАКМ «КриптоПро HSM»);
- Средства обеспечения деятельности удостоверяющего центра (ПАК «Удостоверяющий центр «КриптоПро УЦ»);
- Антивирусные средства;
- Средства резервного хранения данных.

Техническое обслуживание общесистемного программного обеспечения включает в себя выполнение следующих видов работ:

№ п/п	Наименование работы	Периодичность выполнения работы	Порядок проведения	Примечание
1	2	3	4	5
1.	Проверка целостности загрузочных секторов диска и общесистемных файлов	При включении серверов Центра сертификации, Центра регистрации, АРМ привилегированных	Проводится средствами аппаратно-программного модуля доверенной загрузки типа «Электронный замок» до загрузки операционной си-	

№ п/п	Наименование работы	Периодичность выполнения работы	Порядок проведения	Примечание
1	2	3	4	5
		пользователей, АРМ разбора конфликтных ситуаций, ПАКМ «КриптоПро HSM»	стемы	
2.	Проверка работоспособности операционной системы	Ежедневно	Проверяется исправность системы посредством выполнения общесистемных задач, запускаемых в связи с основной деятельностью удостоверяющего центра (по назначению)	Проводится с учётом местных условий эксплуатации
3.	Проверка на наличие вирусов	Ежедневно	Осуществляется с использованием специализированных средств антивирусного контроля. Рекомендуется использовать в автоматическом режиме	
4.	Обновление операционной системы	По мере выхода критических обновлений операционной системы	Осуществляется с использованием стандартных средств администрирования операционной системы (Windows Update)	
5.	Создание резервного образа диска	Один раз в неделю	Осуществляется с использованием специализированных средств резервного хранения данных	
6.	Проверка наличия свободного дискового пространства на системном диске и удаление ненужных файлов	Один раз в месяц	Проводится с использованием стандартных средств администрирования операционной системы	
7.	Проверка состояния файловой системы	Один раз в три месяца	Проводится с использованием стандартных средств администрирования операционной системы	
8.	Восстановление работоспособности операционной системы	По мере необходимости	Осуществляется посредством восстановления или переустановки операционной системы, а также восстановления образа всего диска	

Техническое обслуживание специализированного программного обеспечения включает в себя выполнение следующих видов работ:

№ п/п	Наименование работы	Периодичность выполнения работы	Порядок проведения	Примечание
1	2	3	4	5
•	Проверка целостности программных модулей СКЗИ и ПАК «КриптоПро УЦ»	При включении серверов Центра регистрации, АРМ привилегированных пользователей, АРМ разбора конфликтных ситуаций, ПАКМ «КриптоПро HSM»	Проводится средствами аппаратно-программного модуля доверенной загрузки типа «Электронный замок» до загрузки операционной системы	
•	Проверка работоспособности СКЗИ и ПАК «КриптоПро УЦ»	Ежедневно	Проверяется исправность средств в связи с основной деятельностью удостоверяющего центра (по назначению)	Проводится с учётом местных условий эксплуатации
•	Обновление антивирусных баз	Ежедневно	Осуществляется с использованием специализированных средств антивирусного контроля. Рекомендуется использовать в автоматическом режиме	
•	Создание резервных копий баз дан-	Ежедневно	Осуществляется с использованием специализированных	

№ п/п	Наименование работы	Периодичность выполнения работы	Порядок проведения	Примечание
1	2	3	4	5
	ных удостоверяющего центра		средств резервного хранения данных. Рекомендуется выполнять в автоматическом режиме	
•	Создание резервного образа диска	Один раз в неделю	Осуществляется с использованием специализированных средств резервного хранения данных	
•	Контрольная проверка работоспособности СКЗИ «КриптоПро CSP» и ПАК «КриптоПро УЦ»	Один раз в 6 месяцев	Проверку работоспособности средств обеспечения деятельности удостоверяющего центра необходимо выполнять путем выполнения тестовых задач, связанных с основной деятельностью удостоверяющего центра.	
•	Восстановление работоспособности удостоверяющего центра	По мере необходимости	Осуществляется посредством восстановления или переустановки программных компонент удостоверяющего центра, а также восстановления образа всего диска	

В части технического обслуживания средств криптографической защиты информации и средств обеспечения деятельности удостоверяющего центра рекомендуется заключение соответствующего договора с организацией разработчиком указанных средств, либо с организацией – лицензиатом ФСБ России, имеющей соответствующую лицензию на техническое обслуживание шифровальных (криптографических) средств. Помимо этого, сотрудники указанной организации, которых планируется привлечь к проведению данных работ, должны иметь документ (сертификат), подтверждающий прохождение обучения сотрудника на специализированных курсах.

В указанный договор рекомендуется включать следующие обязательства Исполнителя по выполнению услуг по техническому обслуживанию и сопровождению деятельности удостоверяющего центра:

№	Уровень	Наименование услуги	
		Описание	
1.	формализованный	Консультации по выбору конфигурации оборудования и общесистемного программного обеспечения серверов УЦ	
2.	не формализованный	Консультации по установке компонент УЦ	
3.	не формализованный	Консультации по администрированию компонент УЦ	
4.	формализованный	Восстановление комплекта поставки УЦ (в случае его разрушения)	
5.	не формализованный	Консультация по переносу информационных баз данных компонент УЦ	
6.	формализованный	Консультация по организации резервного копирования баз данных компонент УЦ	
7.	не формализованный	Консультация по восстановлению поврежденных баз данных компонент УЦ с резервных копий	
8.	не формализованный	Консультации по восстановлению работоспособности компонент УЦ (в случае ее потери)	
9.	не формализованный	Дистанционное выполнение работ по восстановлению работоспособности компонент УЦ (в случае ее потери)	
10.	формализованный	Информирование о появлении новых сборок версии УЦ, находящейся в эксплуатации у Заказчика	
11.	формализованный	Информирование о появлении новых версий УЦ	
12.	формализованный	Предоставление новых сборок версии УЦ, находящейся в эксплуатации у Заказчика	
13.	не формализованный	Консультирование по обновлению сборок версии УЦ, находящейся в эксплуатации у Заказчика	

## 10. Роли обслуживающего персонала средств обеспечения деятельности УЦ

Удостоверяющий Центр осуществляет разделение ролей обслуживающего персонала средств обеспечения деятельности УЦ. Каждая роль имеет свой набор задач, возможность осуществления которых задаётся параметрами безопасности, сопоставленными данной роли.

Перечень и описание обязанностей ролей, выполняемых обслуживающим персоналом УЦ на сервере ЦС и на сервере ЦР приведён в таблицах ниже.

### Ролевое администрирование сервера ЦС

Роли и группы	Разрешение безопасности Службы сертификатов	Описание
<b>Локальный администратор (Сервера ЦС)</b>		Установка и разворачивание ЦС, формирование и уничтожение ключа ЭП и сертификатом ключа проверки ЭП ЦС (совместно с Администратором ЦС), управление ключом шифрования и сертификатом Веб-сервера ЦС, регистрация ЦР, архивирование и восстановление баз ЦР. Это роль операционной системы. Определяется членством в группе локальных администраторов операционной системы.
<b>Администратор ЦС</b>	Управление ЦС	Настройка и обслуживание ЦС, загрузка ключа ЭП ЦС. Это роль ЦС, которая включает в себя возможность назначать все остальные роли. Эта роль также называется Уполномоченное лицо УЦ. Данные разрешения назначаются с помощью Диспетчера УЦ.
<b>Аудитор (Сервера ЦС)</b>	Управление аудитом и журналом безопасности	Настройка, просмотр и обслуживание журналов аудита. Аудит — это функциональная возможность операционной системы. Аудитор — это роль операционной системы.

### Ролевое администрирование сервера ЦР

Роли и группы	Разрешение безопасности Сервера ЦР	Описание
<b>Локальный администратор (Сервера ЦР)</b>		Установка и разворачивание ЦР, управление ключом ЭП и сертификатом ЦР, управление ключом шифрования и сертификатом Веб-сервера ЦР, регистрация администраторов службы регистрации, архивирование и восстановление баз ЦР. Это роль операционной системы. Определяется членством в группе локальных администраторов операционной системы.
<b>Администратор службы регистрации</b>	Администратор службы регистрации	Настройка и обслуживание всей службы регистрации. Это роль клиента ЦР, которая включает в себя возможность назначать все остальные роли ЦР и настраивать Центр регистрации. Данные разрешения назначаются с помощью Диспетчера УЦ и Консоли управления ЦР. Администраторы службы регистрации выполняют

<b>Роли и группы</b>	<b>Разрешение безопасности Сервера ЦР</b>	<b>Описание</b>
		свои функции через Консоль управления ЦР.
<b>Аудитор (Сервера ЦР)</b>	Управление аудитом и журналом безопасности	Настройка, просмотр и обслуживание журналов аудита. Аудит — это функциональная возможность операционной системы. Аудитор — это роль операционной системы.
<b>Администратор ЦР</b>	Чтение, Подача запросов, Одобрение запросов, Настройка параметров, Настройка безопасности	Администратор ЦР — это клиенты ЦР, которым разрешено регистрировать пользователей и запрашивать сертификаты в ЦС. Настраивается в Консоли Управления ЦР. Администратор ЦР отличается от Оператора ЦР возможностью создавать других Операторов ЦР и настраивать ЦР, в том числе параметры безопасности. Администраторы ЦР выполняют свои функции через Консоль управления ЦР.
<b>Оператор ЦР</b>	Чтение, Подача запросов, Одобрение запросов	Оператор ЦР — это клиенты ЦР, которым разрешено регистрировать пользователей и запрашивать сертификаты в ЦС. Операторы ЦР выполняют свои функции через Консоль управления ЦР.

## 11. Обеспечение безопасности

### 11.1. Инженерно-технические меры защиты информации

#### 11.1.1. Размещение технических средств УЦ

Сервера Центра сертификации, Центра регистрации и телекоммуникационное оборудование должны быть размещены в серверном помещении.

Сервера Центра сертификации, Центра регистрации и телекоммуникационное оборудование размещаются в шкафу-стойке (cabinet).

Остальные технические средства УЦ размещаются в рабочих помещениях УЦ по схеме организации рабочих мест персонала.

#### 11.1.2. Физический доступ в помещения

Серверное помещение УЦ оборудовано системой контроля доступа с идентификацией по карте.

Серверное помещение оборудовано исполнительным устройством системы контроля доступа электромеханического типа.

Рабочие и служебные помещения УЦ не подключены к системе контроля доступа и оборудованы механическими замками

Идентификационные карты для доступа в серверное помещение выдаются сотрудникам из состава Службы безопасности и Технической службы УЦ по приказу руководителя УЦ.

Ключи механических замков рабочих помещений УЦ выдаются сотрудникам УЦ по распоряжению руководителя Административной службы УЦ на основании схемы организации рабочих мест персонала.

#### 11.1.3. Электроснабжение и кондиционирование воздуха

Технические средства УЦ подключены к общегородской сети электроснабжения.

Электрические сети и электрооборудование, используемые в УЦ, отвечают требованиям действующих «Правил устройства электроустановок», «Правил технической эксплуатации электроустановок потребителей», «Правил техники безопасности при эксплуатации электроустановок потребителей».

Сервера Центра сертификации и Центра регистрации, телекоммуникационное оборудование подключены к источникам бесперебойного питания, обеспечивающие их работу в течение не менее 1 часа после прекращения основного электроснабжения.

Технические средства, эксплуатируемые на рабочих местах сотрудников УЦ, источниками бесперебойного питания не оборудуются.

Серверное помещение оборудовано средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

Служебные помещения УЦ, используемые для архивного хранения документов на бумажных, магнитных и оптических носителях оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

Рабочие и прочие служебные помещения УЦ оборудованы средствами вентиляции и кондиционирования воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством Российской Федерации.

#### 11.1.4. Подверженность воздействию влаги

Защита серверов Центра сертификации и Центра регистрации и телекоммуникационного оборудования от воздействия влаги обеспечивается их размещением в шкафу-стойке (cabinet).

#### 11.1.5. Предупреждение и защита от возгорания

Серверное помещение УЦ оборудовано системой автоматического пожаротушения, пожарной сигнализации и дымоудаления.

Пожарная безопасность помещений УЦ обеспечивается в соответствии с нормами и требованиями СНиП по классу Ф3.5, устанавливаемыми законодательством Российской Федерации.

#### 11.1.6. Хранение документированной информации

Документальный фонд УЦ, как фондообразователя, подлежит хранению в соответствии с действующим законодательством Российской Федерации по делопроизводству и архивному делу.

#### 11.1.7. Уничтожение документированной информации

Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется сотрудниками УЦ, обеспечивающими документирование.

### 11.2. Программно-аппаратные меры защиты информации

#### 11.2.1. Организация доступа к техническим средствам УЦ

Доступ к техническим средствам УЦ, размещённым в серверном помещении, осуществляется с использованием системы контроля доступа.

Идентификационные карты доступа в серверное помещение выдаются сотрудникам на основании приказа руководителя УЦ.

Организация доступа к техническим средствам УЦ, размещённых на рабочих местах сотрудников УЦ, возлагается на сотрудников УЦ, ответственных за эксплуатацию данных технических средств.

#### 11.2.2. Организация доступа к программным средствам УЦ

Сервера Центра сертификации и Центра регистрации оснащены сертифицированными программно-аппаратными комплексами защиты от несанкционированного доступа типа «Электронный замок».

Рабочие места сотрудников УЦ, на которых эксплуатируются программные приложения «АРМ администратора ЦР» и «АРМ разбора конфликтных ситуаций» также оснащены сертифицированными программно-аппаратными комплексами защиты от несанкционированного доступа типа «Электронный замок».

Устройство типа «Электронный замок» при локальной аутентификации администраторов на технических компонентах УЦ должно ограничивать количество подряд следующих неудачных попыток доступа числом не более 3.

Доступ системных администраторов общесистемного программного обеспечения серверов Центра сертификации и Центра регистрации для выполнения регламентных работ осуществляется в присутствии сотрудников Службы безопасности УЦ, отвечающих за эксплуатацию соответствующего прикладного программного обеспечения (Цentra сертификации и/или Центра регистрации).

#### 11.2.2.1. Общий перечень объектов доступа УЦ

К объектам доступа УЦ относятся:

- технические средства компонент УЦ;
- программное обеспечение компонент УЦ: ПО центра сертификации, ПО Центра регистрации, ПО АРМ администратора Центра регистрации, ПО АРМ разбора конфликтных ситуаций, ПО, предназначенное для регистрации и управления сертификатами пользователей УЦ;
- базы данных компонент УЦ: база данных ЦС, база данных ЦР;
- ключи ЭП и сертификаты ключей проверки ЭП;
- списки отозванных сертификатов УЦ.

#### 11.2.2.2. Перечень объектов доступа, предоставляемых сотрудникам УЦ

Сотрудникам Административной службы УЦ:

- технические средства Центра сертификации и Центра регистрации УЦ;
- технические средства АРМ разбора конфликтных ситуаций;
- программное обеспечение Центра сертификации и Центра регистрации УЦ;
- база данных Центра сертификации и Центра регистрации УЦ;
- ключи ЭП и сертификаты ключей проверки ЭП, использующиеся для эксплуатации Центра сертификации и Центра регистрации;
- списки отозванных сертификатов УЦ.

Сотрудникам Службы регистрации УЦ:

- технические средства АРМ администратора Центра регистрации;
- программное обеспечение АРМ администратора Центра регистрации;
- база данных Центра регистрации;
- личные ключи ЭП и сертификаты ключей проверки ЭП сотрудников Службы регистрации;
- служебные ключи и служебные сертификаты ключей проверки ЭП пользователей УЦ;
- рабочие сертификаты ключей проверки ЭП пользователей УЦ;
- списки отозванных сертификатов.

Сотрудникам Службы безопасности УЦ:

- технические средства АРМ администратора Центра регистрации;
- программное обеспечение АРМ администратора Центра регистрации;
- база данных Центра регистрации;
- личные ключи ЭП и сертификаты ключей проверки ЭП сотрудников Службы безопасности;
- служебные сертификаты ключей проверки ЭП пользователей УЦ;
- рабочие ключи и рабочие сертификаты ключей проверки ЭП пользователей УЦ;
- списки отозванных сертификатов.

Сотрудникам технической службы УЦ:

- технические средства компонент УЦ;
- программное обеспечение компонент УЦ;
- базы данных Центра сертификации и Центра регистрации.

#### 11.2.2.3. Перечень объектов доступа, предоставляемых аутентифицированным пользователям УЦ при осуществлении сетевого взаимодействия с программными средствами УЦ

Незарегистрированным пользователям УЦ, проходящим процедуру регистрации в УЦ:

- программное обеспечение формирования запроса на регистрацию Пользователя УЦ в электронном виде;
- программное обеспечение формирования запроса на регистрацию Пользователя УЦ в бумажном виде;

Зарегистрированным пользователям УЦ:

- сертификат ключа проверки ЭП Уполномоченного лица УЦ в электронной форме;
- список отозванных сертификатов ключей проверки ЭП в электронной форме;
- сертификат ключа проверки ЭП пользователей УЦ в электронной форме;
- программное обеспечение предоставления учётной информации о сертификатах ключей проверки ЭП аутентифицированного Пользователя УЦ и их статусе;
- программное обеспечение предоставления учётной информации о запросах (заявлениях) в электронной форме, поступивших в УЦ от аутентифицированного Пользователя УЦ и статусе их обработки;
- программное обеспечение формирования ключей и заявления на изготовление сертификата ключа проверки ЭП в электронной форме аутентифицированного Пользователя УЦ;
- программное обеспечение получения и установки на рабочем месте изготовленного сертификата ключа проверки ЭП Пользователя УЦ;
- программное обеспечение формирования электронного бланка копии сертификата ключа проверки ЭП Пользователя УЦ в бумажной форме;
- программное обеспечение формирования заявления на аннулирование (отзыв) сертификата ключа проверки ЭП в электронной форме Пользователя УЦ;
- программное обеспечение формирования заявления на приостановление действия сертификата ключа проверки ЭП в электронной форме Пользователя УЦ;
- программное обеспечение формирования заявления на возобновление действия сертификата ключа проверки ЭП в электронной форме Пользователя УЦ;
- программное обеспечение предоставления учётной информации о сертификатах ключей проверки ЭП пользователей УЦ и самих сертификатов ключей проверки ЭП пользователей УЦ в электронной форме.
- личные ключи и сертификаты ключей проверки ЭП Пользователя УЦ.

### 11.2.3. Контроль целостности программного обеспечения

Контролю целостности подлежат следующие программные компоненты из состава программного обеспечения, эксплуатируемого УЦ:

- Программные модули средств электронной подписи и криптографической защиты информации;
- Программные модули Комплекса программ Удостоверяющего центра.

Состав программных модулей, подлежащих контролю целостности, определяется внутренним документом УЦ, утверждаемый руководителем УЦ.

Система контроля целостности программных модулей, подлежащих контролю целостности, основывается на аппаратном контроле целостности и общесистемного программного обеспечения до загрузки операционной системы.

Данная система контроля целостности обеспечивается использованием сертифицированного устройства типа «электронный замок».

Контроль целостности программных модулей средств электронной подписи и криптографической защиты информации осуществляется средствами средств электронной подписи и криптографической защиты информации.

Периодичность выполнения мероприятий по контролю целостности — ежедневно.

Ответственность за выполнение мероприятий по контролю целостности программных средств возложена на Службу безопасности УЦ.

### 11.2.4. Контроль целостности технических средств

Контроль целостности технических средств УЦ обеспечивается опечатыванием корпусов устройств, препятствующим их неконтролируемому вскрытию.

Опечатывание устройств выполняется перед вводом технических средств в эксплуатацию и после выполнения регламентных работ.

Контроль целостности печатей осуществляется в начале каждой рабочей смены.

Ответственность за выполнение мероприятий по контролю целостности технических средств возложена на Службу безопасности УЦ.

#### 11.2.5. Защита внешних сетевых соединений

Защита конфиденциальной информации, передаваемой между программно-техническими средствами обеспечения деятельности УЦ и программными средствами, предоставляемыми УЦ пользователям УЦ, в процессе обмена документами в электронной форме, осуществляется путём шифрования информации с использованием шифровальных (криптографических) средств, сертифицированных в соответствии с действующим законодательством Российской Федерации.

В качестве шифровальных (криптографических) средств пользователей УЦ, используемых для защиты конфиденциальной информации, используется средство электронной подписи Пользователя УЦ.

Защита программно-технических средств обеспечения деятельности Удостоверяющего Центра от несанкционированного доступа по внешним сетевым соединениям осуществляется путем использования межсетевого экрана сертифицированного ФСБ России не ниже 4-го класса защиты.

При организации сетевого взаимодействия компонентов ПАК «КриптоПро УЦ 2.0» между собой в случае их размещения в разных контролируемых зонах, каналы связи (сети связи) между этими компонентами должны быть защищены с использованием СКЗИ, сертифицированных ФСБ России по классу не ниже КВ2, либо быть выделенными в соответствии с ФЗ «О связи» №126-ФЗ от 07.07.2003 года.

Технические средства с установленным ПАК «КриптоПро УЦ 2.0» не должны подключаться к техническим средствам общедоступных сетей связи, в том числе, сети Интернет.

##### 11.2.5.1. Перечень информации, подлежащей защите

Поступающая в УЦ информация:

- Заявление на регистрацию в электронной форме;
- Заявление на изготовление сертификата ключа проверки ЭП в электронной форме;
- Заявление на аннулирование (отзыв) сертификата ключа проверки ЭП в электронной форме;
- Заявление на приостановление действия сертификата ключа проверки ЭП в электронной форме;
- Заявление на возобновление действия сертификата ключа проверки ЭП в электронной форме;
- Имя и пароль, передаваемые пользователем для аутентификации по паролю;
- Ключевая фраза пользователя.

Передаваемая из УЦ информация:

- Имя и пароль, передаваемый пользователю для аутентификации по паролю;
- Бланк копии сертификата ключа проверки ЭП для вывода на бумажный носитель;
- Список сертификатов ключа проверки ЭП Пользователя УЦ и их статус;
- Список запросов на сертификаты ключей проверки ЭП Пользователя УЦ и их статус;
- Список запросов на аннулирование (отзыв), приостановление и возобновление действия сертификатов ключей проверки ЭП Пользователя УЦ и их статус.

### 11.3. Организационные меры защиты информации

#### 11.3.1. Предъявляемые требования к персоналу УЦ

Уполномоченное лицо УЦ имеет высшее профессиональное образование и профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области более 2 лет.

Сотрудники Службы безопасности УЦ имеют высшее профессиональное образование и прошли курсы повышения квалификации в области информационной безопасности с получением специализации в области систем с открытым распределением ключей.

#### 11.3.2. Профессиональная переподготовка и повышение квалификации персонала

Профессиональная переподготовка персонала УЦ не осуществляется.

Сотрудники УЦ осуществляют повышение квалификации в областях знаний согласно занимаемым должностям не реже одного раза в 2 года.

#### 11.3.3. Организация сменной работы

Деятельность УЦ по работе с пользователями УЦ в части приёма заявлений в бумажной форме и изготовления сертификатов ключей проверки ЭП организована в одну рабочую смену с 9.00 до 18.00 в будние дни.

Выходными днями являются: суббота, воскресенье, а также дни общенациональных праздников.

#### 11.3.4. Организация доступа персонала к документам и документации

Доступ сотрудников УЦ к документам и документации, составляющей документальный фонд организации, организован в соответствии с должностными инструкциями и функциональными обязанностями.

#### 11.3.5. Охрана здания и помещений

УЦ имеет собственную (привлекаемую) службу охраны здания и помещений, обеспечивающую:

- Обнаружение и задержание нарушителей, пытающихся проникнуть в здание (помещения) УЦ;
- Сохранность материальных ценностей и документов;
- Предупреждение происшествий и ликвидацию их последствий.

### 11.4. Юридические меры защиты информации

УЦ имеет разрешение (лицензии) по всем видам деятельности, связанных с предоставлением услуг (см. 2.2).

Системы безопасности УЦ и защиты информации созданы и поддерживаются на договорной основе с юридическими лицами, осуществляющими свою деятельность на основании лицензий, полученных в соответствии с действующим законодательством Российской Федерации.

Все меры по защите информации в УЦ введены в действие приказами руководителя УЦ.

Для обеспечения деятельности УЦ использует средства электронной подписи и криптографической защиты информации, сертифицированные в соответствии с действующим законодательством Российской Федерации.

Исключительные имущественные права на информационные ресурсы УЦ находятся в собственности УЦ.

Пользователям УЦ предоставляются неисключительные имущественные права на копии сертификатов и списков отозванных сертификатов, изготавливаемые УЦ в объеме прав согласно разделу 3.2 настоящего Регламента.

## 12. Взаимодействие Удостоверяющего центра с федеральными органами исполнительной власти в сфере использования электронной подписи

Для использования пользователями Удостоверяющего центра квалифицированной электронной подписи и изготовления квалифицированных сертификатов ключей проверки ЭП Удостоверяющий центр должен быть аккредитован Уполномоченным федеральным органом исполнительной власти в области применения электронной подписи (Статья 6, пункт 2, ФЗ №63-ФЗ «Об электронной подписи»).

Порядок и требования к аккредитации устанавливаются ФЗ №63-ФЗ «Об электронной подписи» (Статья 16) и Правилами аккредитации Удостоверяющих центров, устанавливаемых федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий.

## ПЕРЕЧЕНЬ ТАБЛИЦ

Таблица 1. Список терминов .....	7
Таблица 2. Список сокращений .....	9
Таблица 3. Список иностранных сокращений .....	9
Таблица 4. Программные компоненты УЦ, требуемые для разворачивания логических структурных компонент УЦ.....	46

## СПИСОК ЛИТЕРАТУРЫ

- N 63-ФЗ. «Об электронной подписи.» *Федеральный закон*. Москва, 6 Апреля 2011 г.
- PKCS #9. «Selected Object Classes and Attribute Types Version 2.0.» Ноябрь 2000 г. *RFC 2985*.  
<<http://tools.ietf.org/html/rfc2985>>.
- RFC 3647. «Certificate Policy and Certification Practices Framework.» Ноябрь 2003 г. *Internet X.509 Public Key Infrastructure*. <<http://tools.ietf.org/html/rfc3647>>.
- RFC 4519. «Schema for User Applications.» Июнь 2006 г. *Lightweight Directory Access Protocol (LDAP)*. <<http://tools.ietf.org/html/rfc4519>>.
- RFC 5280. «Certificate and Certificate Revocation List (CRL) Profile.» Май 2008 г. *Internet X.509 Public Key Infrastructure*. <<http://tools.ietf.org/html/rfc5280>>.
- ЖТЯИ.00078-01 30 01. ПАК КриптоПро УЦ 2.0. *Формуляр*. 2013.
- ЖТЯИ.00078-01 90 02. ПАК КриптоПро УЦ 2.0. *Руководство по установке*. 2013.
- МСЭ-Т X.509. «Структуры сертификатов открытых ключей и атрибутов.» Август 2008 г. *Информационные технологии – Взаимосвязь открытых систем – Справочник*.  
<<http://www.itu.int/rec/T-REC-X.509-200508-I/en>>.
- МСЭ-Т X.520. «Избранные типы атрибутов.» Август 2005 г. *Информационные технологии – Взаимосвязь открытых систем – Справочник*. <<http://www.itu.int/rec/T-REC-X.520-200508-I/en>>.
- Приказ ФНС N ММ-7-6/353@. «Об утверждении требований к сертификату ключа подписи и списку отозванных сертификатов для обеспечения единого пространства доверия сертификатам ключей электронной цифровой подписи.» *Приказ ФНС РФ*. 2 Июля 2009 г.
- Приказ ФСС №19. «О внедрении защищенного обмена документами в электронном виде с применением электронной цифровой подписи для целей обязательного социального страхования.» *Приказ ФСС РФ*. 12 Февраля 2010 г.