Приложение № 16 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю

Директор по информационным технологиям

АО «Гринатом»

_____/ А.Н. Киселёв /

М.П.

Заместитель директора по ИТ,
Нач. управл. И.П. Тарасов
Доверенность от 18.06.2021
22/306/2021-ДОВ

Регламент Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом»)

Москва 2021 г.

Оглавление

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Используемые в настоящем документе термины описаны в таблице ниже.

Таблица 1. Список терминов

Термин	Определение
Владелец сертификата ключа проверки электронной подписи	Лицо, которому в установленном Федеральным законом (N 63-ФЗ) порядке выдан сертификат ключа проверки электронной подписи.
Межсетевой экран	Комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.
Сертификат ключа проверки электронной подписи	Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.
Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат)	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.
Средства электронной подписи	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.
Список отозванных сертификатов	Электронный документ с электронной подписью удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые были аннулированы до окончания срока их действия.
Удостоверяющий центр	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).
Электронная подпись	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.
Электронный документ	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

Сокращен	Значение
АРМ	Автоматизированное рабочее место
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СКПЭП	Сертификат ключа проверки электронной подписи
СУБД	Системы управления базами данных
КУЦ	Корпоративный удостоверяющий центр Госкорпорации «Росатом»
ЭП	Электронная подпись

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

Таблица 3. Список иностранных сокращений

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

1. Общие положения

1.1. Предмет регулирования Порядка

Настоящий Регламент Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом») (Далее – Регламент) определяет механизмы и условия предоставления и использования услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом») (Далее – КУЦ), включая обязанности КУЦ и сотрудников КУЦ, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, необходимые для безопасной работы КУЦ.

1.2. Сведения о КУЦ

Акционерное общество «Гринатом»

(полное наименование юридического лица)

115230, Москва, 1-й Нагатинский проезд., д. 10, стр. 1

(почтовый адрес)

ca@rosatom.ru

(адрес электронной почты)

Контактный телефон +7 (499) 949-49-19 доб. 54-54

Деятельность КУЦ в том числе его обособленных подразделений (филиалов) по работе с пользователями КУЦ и созданию сертификатов ключей проверки ЭП организована в одну рабочую смену с 9.00 до 18.00 в будние дни.

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

1.3. Справочные телефоны КУЦ, его обособленных подразделений (филиалов)

адрес: 665816, Россия, Иркутская обл., г. Ангарск, ул.14 декабря, д.22

Телефон: 8(3955)54-32-47

адрес: 600007, Владимирская область, г.Владимир ул.Северная, д. 1а

Телефон: +7 (4922) 47-38-26

адрес: 427620, Удмуртская респ., г.Глазов ул.Белова д.7

Телефон: 8 (34141) 96346 ; 8 (34141) 96349

адрес: 663690 Красноярский край г.Зеленогорск ул.Первая Промышленная, д.1

Телефон: 8(39169) 9-39-36; 8(39169) 9-43-23

адрес: 601909, Владимирская область, г.Ковров, ул.Социалистическая д.26

Телефон: 8(49232) 9-40-04 (доб. 11-67); 8(49232) 9-40-04 (доб. 11-66)

адрес: 603064, Нижегородская область, г. Нижний Новгород, пр. Ленина, д.93 каб. 634

Телефон: +7 (499) 949-49-19 доб. 7887; +7 (831) 268-15-68 доб. 7887

адрес: 630110, Новосибирская область, г. Новосибирск, ул.Б.Хмельницкого, д.94

Телефон: +7 (038)274-89-33

адрес: 624130, Свердловская обл., г. Новоуральск, ул. Мичурина, д.29, ОПС а/я 10 Филиал АО «Гринатом» в г. Новоуральске.

Телефон: +7 (34370) 5-69-51; +7 (34370) 5-31-33

адрес: 191036, г. Санкт-Петербург, ул. 2-ая Советская, д. 7

Телефон для связи с оператором КУЦ: 8(499)949-49-19 доб.(030) 5-42-29

адрес: 607328, Нижегородская обл., Дивеевский р-н, п. Сатис, ул. Парковая д.3. стр.5-1

Телефон:7 (83130) 70-9-70 доб. 603

адрес: 636039, г. Северск Томской обл., ул. Ленина 90

Телефон:8(3823) 52-46-41; 8(3823) 52-71-63

адрес: 144001, Россия, Московская обл., г.Электросталь, ул.Карла Маркса, д.12

Телефон: 8 496 577 31 74, вн. 31 74; 8 496 577 31 74, вн. 43 93

1.4. Порядок информирования о предоставлении услуг КУЦ

Настоящий Регламент распространяется:

- В электронной форме на официальном сайте: http://crypto.rosatom.ru

Порядок получения информации заявителями по вопросам предоставления услуг КУЦ доступен по телефонному обращению на справочный телефон +7 (499) 949-49-19 доб. 54-54

Телефон для справок: +7 (499) 949-29-99 доб.: 0; с КТС: внутренний 1111

Телефон для связи с оператором КУЦ: +7 (499) 949-49-19 доб: 5454

1.5. Стоимость услуг

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

Состав и стоимость предоставляемых иных услуг определяется КУЦ

Порядок информирования заинтересованных лиц о стоимости услуг КУЦ определён Договором присоединения и опубликован на сайте КУЦ https://crypto.rosatom.ru/dokumentatsiya/dogovor/.

Срок и порядок расчетов за оказание услуг КУЦ определён Договором присоединения и опубликован на сайте КУЦ https://crypto.rosatom.ru/dokumentatsiya/dogovor/

1.6. Область применения Регламента

Настоящий Регламент является средством официального уведомления и

информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг КУЦ.

1.7. Срок действия Регламента

Настоящий Регламент вступает в силу со дня его публикации. Срок действия Регламента — 10 лет.

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

Официальное уведомление о прекращении действия Регламента осуществляется путём публикации об этом сведений на официальном сайте КУЦ.

1.8. Структура КУЦ

Структура КУЦ включает в себя Отдел криптографической защиты АО «Гринатом». Отдел криптографической защиты обеспечивает решение следующих задач:

Администратор КУЦ:

- управление деятельностью КУЦ;
- координация деятельности КУЦ;
- взаимодействие с Пользователями КУЦ в части разрешения вопросов, связанных с применением средств ЭП, ключей и сертификатов ключей проверки ЭП, создаваемых КУЦ;
- взаимодействие с Пользователями КУЦ в части разрешения вопросов, связанных с подтверждением электронной подписи КУЦ в сертификатах ключей проверки ЭП, созданных КУЦ;
- организация и выполнение мероприятий по защите ресурсов КУЦ;

создание 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;
- предоставление Пользователям КУЦ сведений об аннулированных сертификатах ключей проверки ЭП;
- техническое обеспечение процедуры подтверждения электронной подписи в документах, по обращениям Пользователей КУЦ;
- техническое обеспечение процедуры подтверждения подлинности электронных подписей КУЦ в созданных сертификатах ключей проверки ЭП по обращениям Пользователей КУЦ.
- организация и выполнение мероприятий по эксплуатации программных и технических средств обеспечения деятельности КУЦ;

Оператор КУЦ:

- регистрация Пользователей КУЦ;
- ведение Реестра зарегистрированных Пользователей КУЦ;
- предоставление служебных ключей ЭП и сертификатов служебных ключей проверки ЭП по обращению Пользователей КУЦ;
- распространение средств электронной подписи и шифрования.
- создание и вручение ключей Пользователей КУЦ;
- предоставление сертификатов ключей проверки ЭП в электронной форме Пользователей КУЦ;

1.9. Пользователи КУЦ

Пользователями КУЦ называются лица, зарегистрированные в КУЦ — лица, прошедшие полную процедуру идентификации и аутентификации в КУЦ;

Стать зарегистрированным Пользователем КУЦ может только физическое лицо, являющееся представителем юридического лица, при наличии доверенности, которая даёт данному физическому лицу право пользоваться услугами КУЦ от имени юридического лица.

Владельцем сертификата и ключа ЭП может быть только зарегистрированный Пользователь КУЦ, физическое лицо.

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

1.10. Разрешение споров

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

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.

1.11. Ответственность

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

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

1.12. Прекращение деятельности

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

В случае принятия решения о прекращении своей деятельности КУЦ:

1) сообщает об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;

2) передаёт в уполномоченный федеральный орган в установленном порядке реестр квалифицированных сертификатов установленным порядком;

3) передает на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

1.13. Порядок утверждения и внесения изменений в Регламент

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

КУЦ в одностороннем порядке вносит изменения в Регламент.

Внесение изменений (дополнений) в Регламент, а также в Приложения к нему, производится посредством утверждения новой редакции Регламента. Новая версия Регламента вступает в силу через 30 (тридцать) дней после публикации на сайте КУЦ.

Все Приложения, изменения и дополнения к настоящему Регламенту являются его составной и неотъемлемой частью.

2. Перечень реализуемых КУЦ функций (Оказываемых услуг)

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

1) создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата с учетом требований, установленных в соответствии с пунктом 4 части 4 статьи 8 Федерального закона № 63-ФЗ;

1.1) осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;

2) устанавливает сроки действия сертификатов ключей проверки электронных подписей;

3) аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;

4) выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

5) ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

6) устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";

7) создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;

8) проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

9) осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

10) осуществляет иную связанную с использованием электронной подписи деятельность.

3. Права и обязанности

3.1. Права КУЦ

КУЦ имеет право:

- Предоставлять сертификаты ключей проверки ЭП в электронной форме, находящихся в Реестре КУЦ, всем лицам, обратившимся в КУЦ;
- Не проводить регистрацию лиц, обратившихся по вопросу представления сертификатов ключей проверки ЭП в электронной форме, находящихся в Реестре КУЦ;

- Отказать в создании сертификата ключа проверки ЭП зарегистрированным пользователям КУЦ, без указания причин отказа;
- Отказать в аннулировании (отзыве) сертификата ключа проверки ЭП владельцу сертификата, в случае если истёк установленный срок действия ключа ЭП, соответствующего ключу проверки ЭП в сертификате;

3.2. Права Пользователей КУЦ

Пользователи КУЦ, имеют следующие права:

- Получать в электронной форме списки отозванных сертификатов ключей проверки ЭП, созданные КУЦ;
- Получать в электронной форме сертификаты ключа проверки ЭП КУЦ;
- Получать в электронной форме сертификаты ключа проверки ЭП Пользователей КУЦ, находящиеся в Реестре сертификатов ключей проверки ЭП КУЦ;
- Применять сертификаты ключа проверки ЭП КУЦ для проверки электронных подписей КУЦ в сертификатах ключа проверки ЭП пользователей, созданных КУЦ.
- Применять сертификаты ключа проверки ЭП Пользователей КУЦ для проверки электронных подписей в электронных документах в соответствии со сведениями, указанными в сертификатах ключа проверки ЭП.
- Применять список отозванных сертификатов ключей проверки ЭП для проверки статуса сертификатов ключей проверки ЭП.
- Обращаться в КУЦ за подтверждением подлинности электронных подписей в электронных документах;
- Обращаться в КУЦ за подтверждением подлинности электронных подписей КУЦ в созданных КУЦ сертификатах ключей проверки ЭП пользователей;
- Обращаться в КУЦ для аннулирования (отзыва) своих сертификатов ключей проверки ЭП в течение срока действия соответствующих ключей ЭП.

3.3. Обязанности КУЦ

3.3.1. Ключи электронной подписи КУЦ

КУЦ обязан выполнять порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, установленных КУЦ в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения обязанностей.

КУЦ обязан использовать для создания ключей ЭП КУЦ 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 вариант исполнения 5 – классу КС2 (используются СКЗИ/средства ЭП класса КС2).

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

КУЦ обязан принять меры по защите ключей ЭП КУЦ в соответствии с положениями настоящего Регламента.

КУЦ обязан обеспечивать конфиденциальность созданных ключей электронных подписей до момента вручения владельцам.

3.3.2. Синхронизация времени

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

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

3.3.3. Создание ключей ЭП и ключей проверки ЭП

КУЦ обязан отказать Пользователю КУЦ в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что Пользователь КУЦ владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи.

КУЦ для подписания от своего имени квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган.

КУЦ запрещается использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами.

КУЦ обязан отказать заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи

КУЦ обязан создать ключ ЭП и ключ проверки ЭП зарегистрированному Пользователю КУЦ с использованием средств электронной подписи, сертифицированных в соответствии с действующим законодательством Российской Федерации.

КУЦ обязан обеспечить сохранение в тайне созданного ключа ЭП.

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

КУЦ 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.

КУЦ обязан обеспечить защиту ключевого носителя от копирования.

КУЦ обязан обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей проверки ЭП Пользователей КУЦ.

КУЦ обязан обеспечить уникальность значений ключей проверки ЭП в созданных сертификатах ключей проверки ЭП пользователей КУЦ.

КУЦ запрещается указывать в создаваемом им сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном этому удостоверяющему центру любым другим удостоверяющим центром.

КУЦ обязан хранить следующую информацию:

1) реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;

2) сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;

3) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать от имени юридических лиц, государственных органов, органов местного самоуправления, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.

КУЦ должен хранить указанную информацию в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации. Хранение информации должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

3.3.4. Выдача сертификатов

При выдаче квалифицированного сертификата КУЦ обязан в порядке, установленном законодательством, идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата.

Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата либо посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", КУЦ обязан отказать такому лицу в проведении указанной идентификации.

Устанавливаются - наименование, организационно-правовая форма, идентификационный номер налогоплательщика, а также основной государственный регистрационный номер и адрес юридического лица

При выдаче квалифицированного сертификата КУЦ обязан получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата

При выдаче квалифицированного сертификата аккредитованный КУЦ обязан в установленном порядке идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата (в целях получения от заявителя, выступающего от имени юридического лица, подтверждения правомочия обращаться за получением квалифицированного сертификата).

При получении квалифицированного сертификата Пользователем УЦ ознакомить с информацией, содержащейся в квалифицированном сертификате. Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования заявителем квалифицированной

электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы. Указанное согласие, подписанное электронной подписью, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица. КУЦ обязан хранить информацию, подтверждающую ознакомление заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности.

КУЦ одновременно с выдачей квалифицированного сертификата должен предоставить владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

При выдаче квалифицированного сертификата КУЦ направляет в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате. Требования к порядку предоставления владельцам квалифицированных сертификатов сведений о выданных им квалифицированных сертификатах с использованием единого портала государственных и муниципальных услуг устанавливаются Правительством Российской Федерации. При выдаче квалифицированного сертификата КУЦ по желанию владельца квалифицированного сертификата безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии.

3.3.5. Уведомления

КУЦ обязан предложить использовать шифровальные (криптографические) средства, указанные в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", физическим лицам, обратившимся к нему в целях проведения идентификации без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы (для предоставления биометрических персональных данных физического лица в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством сети "Интернет"), и указать страницу сайта в информационно-телекоммуникационной сети "Интернет", с которой безвозмездно предоставляются эти средства.

При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством информационно-телекоммуникационной сети "Интернет" при выдаче сертификата ключа проверки электронной подписи отказывается от использования шифровальных (криптографических) средств, аккредитованный удостоверяющий центр обязан отказать такому лицу в проведении идентификации и выдаче сертификата ключа проверки электронной подписи.

Страница для скачивания шифровальных (криптографических) средств –

https://www.cryptopro.ru/downloads

Уведомление о факте создания сертификата ключа проверки ЭП

КУЦ обязан информировать пользователей КУЦ об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных

с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки

КУЦ обязан официально уведомить о факте создания сертификата ключа проверки ЭП его владельца.

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

Официальным уведомлением о факте создании сертификата является отправка почтового сообщения по электронной почте с прикреплённым сертификатом ключа проверки ЭП с адреса отправителя ca@rosatom.ru.

Временем отправки почтового сообщения признается время отправки почтового

сообщения с почтового сервера ca@rosatom.ru, осуществляющего отправку почтовых сообщений КУЦ, и включённое в заголовок почтового сообщения.

Уведомление о факте аннулирования сертификата ключа проверки ЭП

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

Срок уведомления — не позднее 12 часов с момента занесения сведений о факте аннулирования сертификата в список отозванных сертификатов.

Официальным уведомлением о факте аннулирования сертификата является опубликование списка отозванных сертификатов, который содержит сведения об сертификате, в репозитории КУЦ по адресам:

http://crl1.rosatom.ru
http://crl1.rosatom.local
http://crl2.rosatom.ru
http://crl2.rosatom.local

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

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

КУЦ обязан включать полный адрес (URL) списка отозванных сертификатов в издаваемые сертификаты.

3.3.6. Реестр сертификатов ключей проверки ЭП

КУЦ обязан вести Реестр всех созданных сертификатов ключей проверки ЭП пользователей КУЦ в течение установленного срока хранения.

КУЦ обязан обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий

КУЦ обязан обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", к реестру квалифицированных сертификатов КУЦ в любое время в течение срока деятельности этого удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

КУЦ обязан предоставлять безвозмездно любому лицу по его обращению в соответствии с порядком доступа к реестру сертификатов, определённом в п.4.13. информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи.

КУЦ обязан публиковать выписки из Реестра, позволяющие определить

действительность сертификатов ключей проверки ЭП пользователей КУЦ.

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

3.3.7. Восстановление работоспособности КУЦ после сбоев

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

3.3.8. Прекращение деятельности

В случае принятия решения о прекращении своей деятельности:

КУЦ обязан сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;

КУЦ обязан передать в уполномоченный федеральный орган в установленном порядке реестр выданных квалифицированных сертификатов;

КУЦ обязан передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

3.4. Обязанности Пользователей КУЦ

Пользователи КУЦ, обязаны:

- не использовать ключ электронной подписи и немедленно обратиться в КУЦ для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена
- перед использованием сертификата ключа проверки ЭП, созданного этим КУЦ, удостовериться, что назначения ключа и назначения сертификата, указанные в сертификате, соответствуют предполагаемому использованию сертификата, согласно настоящему Регламенту.
- 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.
- использовать сертификаты своих ключей проверки ЭП только для целей, разрешённых назначениями ключа и назначениями сертификата, которые указаны в сертификате, согласно настоящему Регламенту;
- предоставлять идентифицирующую информацию в объёме, определённом положениями настоящего Регламента.

4. Процедуры и механизмы

4.1. Процедура Идентификации и аутентификации пользователей КУЦ

Первичная идентификация и аутентификация зарегистрированного Пользователя КУЦ выполняется по документу, удостоверяющему личность, предъявляемому лично.

Идентификация Пользователя проводится при его личном присутствии или посредством идентификации Пользователя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата либо посредством идентификации Пользователя с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации". При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации. Создание сертификатов ключей проверки электронных подписей и выдача таких сертификатов Пользователем в отношении усиленных неквалифицированных электронных подписей также могут осуществляться при определении лица, подающего заявление в электронной форме без личного присутствия с использованием простой электронной подписи, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации, и при условии организации взаимодействия удостоверяющего центра с единой системой идентификации и аутентификации, гражданами (физическими лицами) и организациями с применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации

Удалённая аутентификация зарегистрированного Пользователя КУЦ при доступе к Информационной системе органа криптографической защиты и Информационной системе «Платформа доверенных сервисов» выполняется в соответствии с приказом Госкорпорации «Росатом» №1517 «Об утверждении Единых отраслевых методических указании по предоставлению пользователям доступа к централизованным ИТ-ресурсам Госкорпорации «Росатом» и организаций Госкорпорации «Росатом»

4.2. Процедура создания ключей электронных подписей и ключей проверки электронных подписей

Пользователь КУЦ создает ключ электронной подписи и ключ проверки электронной подписи в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" (зарегистрирован Министерством юстиции Российской Федерации 3 марта 2005 г., регистрационный N 6382), с изменениями, внесенными приказом ФСБ России 12 апреля 2010 г. N 173 "О внесении изменений в некоторые нормативные правовые акты ФСБ России" (зарегистрирован Министерством юстиции Российской Федерации 25 мая 2010 г., регистрационный N 17350);

КУЦ создает ключ электронной подписи и ключ проверки электронной подписи для заявителя в соответствии с правилами пользования средствами криптографической защиты

информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09 февраля 2005 г. №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона «Об электронной подписи» создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности

Создание ключа электронной подписи и ключа проверки электронной подписи на автоматизированном рабочем месте КУЦ производится после выполнения требований, установленных постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 (Собрание законодательства Российской Федерации, 2012, № 7, ст. 863; 2016, № 26, ст. 4049),

4.3. Порядок смены ключей КУЦ

Плановая смена ключей КУЦ

Плановая смена ключей (ключа ЭП и соответствующего ему ключа проверки ЭП) КУЦ выполняется в течение срока действия ключа ЭП КУЦ.

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

Процедура плановой смены ключей КУЦ осуществляется в следующем порядке:

КУЦ формирует новый ключ ЭП и соответствующий ему ключ проверки ЭП;

КУЦ направляет запрос на создание нового сертификата ЭП КУЦ в Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации изготавливает сертификат нового ключа проверки ЭП и подписывает его электронной подписью с использованием ключа ЭП Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации направляет в КУЦ новый сертификат КУЦ

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

Доверенным способом получения нового квалифицированного сертификата КУЦ Пользователям КУЦ является скачивание нового квалифицированного сертификата КУЦ с официального сайта по защищённому протоколу HTTPS - https://crypto.rosatom.ru/ca/tsepochka-sertifikatov/ исключающее уничтожение, модифицирование, блокирование при передаче.

Внеплановая смена ключей КУЦ

Внеплановая смена ключа электронной подписи КУЦ осуществляется в случае нарушения конфиденциальности ключа электронной подписи или угрозы нарушения конфиденциальности такого ключа электронной подписи

Процедура внеплановой смены ключей КУЦ выполняется в порядке, определённом процедурой плановой смены ключей КУЦ.

Одновременно с внеплановой сменой ключа электронной подписи производится

прекращается действие всех квалифицированных сертификатов, созданных с использованием этого ключа электронной подписи, с занесением сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов.

Виды угроз нарушения конфиденциальности ключа электронной подписи КУЦ:

- Оставление ключа электронной подписи КУЦ без контроля
- Разглашение ключа электронной подписи КУЦ администратором КУЦ.

4.4. Порядок осуществления смены ключа электронной подписи владельца квалифицированного сертификата

Смена ключа электронной подписи владельца квалифицированного сертификата осуществляется в случаях, указанных в пунктах 1, 2, 4 части 6 и части 6.1 статьи 14 Федерального закона «Об электронной подписи»;

Требования к заявлению на смену ключа электронной подписи владельца квалифицированного сертификата аналогичны заявлению на создание ключа электронной подписи и содержатся в п.4.5. настоящего регламента

Заявление на смену ключа электронной подписи владельца квалифицированного сертификата может быть создано в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца квалифицированного сертификата, при этом в случае, если смена ключа электронной подписи владельца квалифицированного сертификата связана с нарушением его конфиденциальности или угрозой нарушения конфиденциальности, соответствующее заявление подписывается иной усиленной квалифицированной электронной подписью владельца квалифицированного сертификата.

Процедура выдачи квалифицированного сертификата и ключа электронной подписи владельцу описана в п.4.5.

4.5. Процедура создания и выдачи квалифицированных сертификатов

В зависимости от выбранного Пользователем КУЦ способа, порядок подачи заявления на создание и выдачу квалифицированных сертификатов определён в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)
- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)
- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

В зависимости от выбранного Пользователем КУЦ способа, форма заявления на создание и выдачу квалифицированных сертификатов Приведена в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)
- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)
- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации

«Росатом» (Приложение №12 к договору присоединения)

Заявление на создание и выдачу квалифицированного сертификата может быть оформлено как на бумажном носителе (в соответствии с Порядком Предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»), так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью Пользователя КУЦ (в соответствии с Порядком Предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Платформа доверенных сервисов»)

Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность;

Личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства;

Личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц;

Порядок установления личности заявителя определён в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)
- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)
- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

Перечень документов, запрашиваемых КУЦ у заявителя для создания и выдачи квалифицированного сертификата, в том числе для удостоверения личности заявителя, в соответствии с частью 2 статьи 17 и частью 2 статьи 18 Федерального закона №63-ФЗ определён в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)
- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)
- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

В случае если для подтверждения сведений, вносимых в квалифицированный сертификат, законодательством Российской Федерации установлена определенная форма документа, заявитель представляет в КУЦ документ соответствующей формы

Порядок проверки достоверности документов и сведений, представленных заявителем определён в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)
- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

Для заполнения квалифицированного сертификата в соответствии с частью 2 статьи 17 Федерального закона «Об электронной подписи» КУЦ запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные частью 2.2 статьи 18 Федерального закона «Об электронной подписи»;

В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и КУЦ установлена личность заявителя – физического лица или получено подтверждение правомочий лица, выступающего от имени заявителя – юридического лица, на обращение за получением квалифицированного сертификата, КУЦ осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В противном случае КУЦ отказывает заявителю в выдаче квалифицированного сертификата;

Порядок создания квалифицированного сертификата определён в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

После создания квалифицированного сертификата КУЦ осуществляет регистрацию квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи»

По желанию лица, которому выдан квалифицированный сертификат, КУЦ на безвозмездной основе производит регистрацию указанного лица в единой системе идентификации и аутентификации

Порядок выдачи квалифицированного сертификата определён в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

При выдаче квалифицированного сертификата КУЦ производит информирование заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки путём предоставления руководства по обеспечению безопасности.

Срок создания и выдачи квалифицированного сертификата с момента получения КУЦ соответствующего заявления составляет не более 10 рабочих дней.

4.6. Процедура подтверждения действительности электронной подписи, использованной для подписания электронных документов

Требования к заявлению на подтверждение действительности электронной подписи, в том числе перечень прилагаемых к такому заявлению документов; срок предоставления услуги по подтверждению действительности электронной подписи в электронном документе; а так же порядок оказания услуги определены в документе:

– Порядок подтверждения подлинности электронной подписи в электронном документе (утвержденный приказом АО «Гринатом» от 19.11.2012 №22/284-П)

Порядок оказания услуги содержит процедуру проверки действительности всех квалифицированных сертификатов, включенных в последовательность проверки от проверяемого квалифицированного сертификата до квалифицированного сертификата КУЦ, выданного ему головным удостоверяющим центром.

4.7. Процедура прекращении действия и аннулировании квалифицированного сертификата

Квалифицированный сертификат прекращает свое действие в случаях, установленных статьей 14 Федерального закона «Об электронной подписи».

КУЦ признает квалифицированный сертификат аннулированным, если:

не подтверждено, что владелец квалифицированного сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате;

установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате;

вступило в силу решение суда, которым установлено, что квалифицированный сертификат содержит недостоверную информацию;

Порядок подачи и приема заявления о прекращении действия квалифицированного сертификата, в том числе порядок подтверждения полномочий владельца квалифицированного сертификата, а так же порядок внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов и требования к заявлению определены в документах:

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Приложение №2 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» и использованием информационной системы Органа криптографической защиты» (Приложение №8 к договору присоединения)

- Порядок предоставления услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом» с выпуском квалифицированного сертификата ключа проверки электронной подписи с использованием Платформы доверенных сервисов Госкорпорации «Росатом» (Приложение №12 к договору присоединения)

Заявления о прекращении действия квалифицированного сертификата могут быть направлены в КУЦ как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью.

Срок внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов не превышает двенадцать часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона «Об электронной подписи», или в течение двенадцати часов с момента получения КУЦ соответствующих сведений.

4.8. Порядок ведения реестра квалифицированных сертификатов;

Обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов производится путём внесения сведений в реестр Оператором КУЦ

Обеспечение защиты информации, содержащейся в реестре квалифицированных сертификатов от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий производится путём применения сертифицированных средств КУЦ в качестве реестра сертификатов КУЦ.

Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов, производится за счёт применения средств отказоустойчивости и проведения организационно-технических мероприятий по поддержанию доступности.

Реестр квалифицированных сертификатов КУЦ ведётся в форме ПАК «Центр регистрации» и предназначен для обеспечения реализации следующих функций КУЦ:

- Ведения Реестра зарегистрированных пользователей КУЦ;
- Ведения Реестра сертификатов ключей проверки ЭП КУЦ;
- Ведения Реестра запросов на создание сертификатов ключей проверки ЭП пользователей КУЦ;
- Ведения Реестра запросов на аннулирование (отзыв) сертификатов ключей проверки ЭП пользователей КУЦ;

Информация о прекращении действия или аннулировании квалифицированного сертификата вносится в реестр квалифицированных сертификатов в срок не более 12 часов после поступления заявления о прекращении действия или аннулировании квалифицированного сертификата.

УЦ определяет следующий порядок доступа к реестру сертификатов - предоставление сведений из реестра квалифицированных сертификатов КУЦ производится по запросам пользователей через форму размещённую на сайте: https://crypto.rosatom.ru/ca/reestr-sertifikatov/

КУЦ предоставляет по запросу информацию о выпущенных сертификатах, путем заполнения формы с указанием (серийного номера квалифицированного сертификата, ФИО владельца квалифицированного сертификата, Email на который необходимо получить информации о выпущенном квалицированном сертификате АО «Гринатом»).

Доступ любому лицу к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата осуществляется безвозмездно.

Публикации перечня прекративших свое действие (аннулированных) квалифицированных сертификатов производится путём публикации действующего списка отозванных сертификатов.

Предоставление информации о сертификате осуществляется в течении 24 часов после подачи заявки в электронном виде.

4.9. Порядок технического обслуживания реестра квалифицированных сертификатов.

Максимальный срок проведения технического обслуживания реестра квалифицированных сертификатов составляет 12 часов;

В случае проведения технического обслуживания реестра квалифицированных

сертификатов Администратор КУЦ производит уведомление участников информационного взаимодействия о проведении технического обслуживания путём публикации сведений о проведений технического обслуживания на сайте КУЦ: https://crypto.rosatom.ru/ca/reestr-sertifikatov/

4.10. 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 КУЦ, как третьей стороны, обеспечивающей подтверждение подлинности электронной подписи в электронных документах в отношении сертификатов ключей проверки электронной подписи, созданных КУЦ. КУЦ 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 КУЦ 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 КУЦ формирует согласительную комиссию, в которую входят:

- представитель КУЦ – 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 КУЦ. 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 КУЦ, 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, подающемся в КУЦ от лица участника информационной системы - владельца сертификата ключа проверки электронной подписи (см. пункт 6.10 и 6.11 настоящего Регламента).

Порядок проведения экспертных работ КУЦ по подтверждению подлинности электронной подписи в электронном документе устанавливается КУЦ. Для проведения 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 КУЦ. Результатом проведения экспертных работ является заключение КУЦ.

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 содержит 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.

5. Порядок исполнения обязанностей Удостоверяющего центра

5.1. информирование заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

При выдаче квалифицированного сертификата КУЦ производит информирование заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки путём предоставления руководства по обеспечению безопасности.

5.2. выдача по обращению заявителя средств электронной подписи.

Порядок выдачи и учёта средств электронной подписи определён в документе: «Регламент процесса «Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну Госкорпорации «Росатом»

Средства электронной подписи в соответствии с частью 4 статьи 6 Федерального закона «Об электронной подписи» обеспечивают возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями;

5.3. обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

Обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов производится путём внесения сведений в реестр Оператором КУЦ

Обеспечение защиты информации, содержащейся в реестре квалифицированных сертификатов от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий производится путём применения сертифицированных средств КУЦ в качестве реестра сертификатов КУЦ.

5.4. обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети "Интернет" в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов;

Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов, производится за счёт применения средств отказоустойчивости и проведения организационно-технических мероприятий по поддержанию доступности.

5.5. порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей.

Ключи ЭП пользователей КУЦ записываются при их генерации на типы ключевых носителей, которые поддерживаются используемым средством криптографической защиты информации.

В качестве ключевых носителей используются сертифицированные ключевые носителю Рутокен.

Ключи ЭП на ключевом носителе защищаются паролем (ПИН-кодом). Пароль (ПИН-код) формирует сотрудник КУЦ в соответствии с требованиями на используемое средство криптографической защиты информации.

Для обеспечения конфиденциальности Ключи ЭП создаются в не экспортируемом формате. По запросу пользователя с обоснованием причин и по согласованию Администратора КУЦ ключи ЭП могут быть созданы в экспортируемом формате.

Сотрудник КУЦ сообщает сформированный пароль (ПИН-код) владельцу ключей ЭП.

Ключи ЭП до момента передачи владельцу находятся на временном хранении ключей электронных подписей у Сотрудника КУЦ или доверенного лица КУЦ. Срок временного хранения не может превышать срок действия сертификата ключа проверки электронной подписи, соответствующего данному ключу ЭП. В случае истечения срока временного хранения ключи ЭП подлежат уничтожению в десятидневный срок.

Ответственность за сохранение пароля (ПИН-кода) в тайне до момента передачи владельцу возлагаются на сотрудника КУЦ, ответственного за создание данного ключа. Для вручения ключа ЭП владельцу Оператор КУЦ имеет право передать ключ уполномоченному доверенному лицу КУЦ. Созданные ключи и ПИН-коды к ним хранятся исключительно в специальных помещениях КУЦ с ограничением доступа посторонних лиц в данные помещения.

После вручения квалифицированного сертификата ответственность за сохранение пароля (ПИН-кода) в тайне возлагается на владельца ключей ЭП.

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

5.6. осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона "Об электронной подписи";

После создания квалифицированного сертификата КУЦ осуществляет регистрацию квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи»

5.7. осуществление по желанию лица, которому выдан квалифицированный сертификат, безвозмездной регистрации указанного лица в единой системе идентификации и аутентификации;

По желанию лица, которому выдан квалифицированный сертификат, КУЦ на безвозмездной основе производит регистрацию указанного лица в единой системе идентификации и аутентификации

5.8. предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, в том числе путем публикации перечня

прекративших свое действие (аннулированных) квалифицированных сертификатов.

Предоставление сведений из реестра квалифицированных сертификатов КУЦ производится по запросам пользователей через форму размещённую на сайте: https://crypto.rosatom.ru/ca/reestr-sertifikatov/

Доступ любому лицу к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата осуществляется безвозмездно.

6. Политика конфиденциальности

6.1. Типы конфиденциальной информации

Ключ ЭП владельца сертификата ключа проверки ЭП является конфиденциальной информацией данного Пользователя КУЦ.

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

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

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

6.2. Типы информации, не являющейся конфиденциальной

Информация, не являющейся конфиденциальной информацией, является открытой информацией.

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

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

Также не считается конфиденциальной информация о настоящем Регламенте.

6.3. Исключительные полномочия официальных лиц

УЦ не раскрывает 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.

7. Дополнительные положения

7.1. Сроки действия ключей КУЦ

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

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

При использовании СКЗИ «КриптоПро CSP» 1 год и 3 месяца или 3 года (при условии, что общее время использования ключа ЭП для выполнения целевых функций в течение 3-х лет его действия ограничено 1 годом и 3 месяцами, остальное время ключ ЭП используется только для подписи списков отозванных сертификатов). Сроки действия сертификата ключа проверки ЭП составляют 16 и 18 лет соответственно.

При создании и хранении ключа ЭП посредством ПАКМ «КриптоПро HSM» – 3 года или 5 лет (при условии, что общее время использования ключа ЭП для выполнения целевых функций в течение пяти лет его действия ограничено 3 годами, остальное время ключ ЭП используется только для подписи списков отозванных сертификатов). Сроки действия сертификата ключа проверки ЭП составляют 18 и 20 лет соответственно.

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

7.2. Требования к средствам электронной подписи, использующимся в составе КУЦ и требования к средствам электронной подписи пользователей КУЦ

Средства электронной подписи КУЦ и средства электронной подписи пользователя КУЦ должны удовлетворять требованиям Федерального закона №63-ФЗ «Об электронной подписи» и требованиям Приказа ФСБ Российской Федерации от 27.12.2011 г. №796.

Формирование и проверка электронной подписи на серверных компонентах КУЦ, а именно на Центре сертификации и Центре регистрации осуществляется Администратором КУЦ или в автоматическом режиме, под контролем лица, ответственного за создание и проверку ЭП в ЦС.

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 Администратор КУЦ ознакомится с содержимым подписываемого документа. После ознакомления Администратор КУЦ 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.

7.3. Сроки действия ключей ЭП и сертификатов ключей проверки ЭП пользователей КУЦ

Максимальный срок действия ключа ЭП Пользователя КУЦ, 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 КУЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки ЭП Пользователя КУЦ.

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

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

Установлены следующие максимальные сроки действия ключей ЭП и ключей проверки ЭП Пользователей КУЦ:

- Срок действия ключа ЭП — 1 год 3 месяца; При этом устанавливается, что срок действия ключа для планового использования составляет 1 год. Срок действия сертификата на период смены ключа составляет 3 месяца)
- Срок действия ключа проверки ЭП — 1 год 3 месяца, но не более сроков действия соответствующих ключей проверки ЭП, обеспечиваемых используемыми пользователями ПАК «КриптоПро УЦ 2.0» средствами ЭП и средствами КУЦ.

Конкретный срок действия сертификата ключа проверки ЭП устанавливается КУЦ в момент его создания.

Максимальные сроки действия ключа ЭП и ключа проверки ЭП Пользователя КУЦ определяются типом запрашиваемого сертификата. Тип сертификата назначается Оператором КУЦ. При назначении сроков действия КУЦ 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 КУЦ, с указанием сроков действия ключа ЭП и ключа проверки ЭП.

7.4. Архивное хранение документированной информации

Архивированию подлежат следующая документированная информация:

- Реестр сертификатов ключей проверки ЭП пользователей КУЦ;
- сертификаты ключей проверки ЭП КУЦ;
- журналы аудита программно-аппаратных средств обеспечения деятельности КУЦ;
- заявления на аннулирование (отзыв) сертификатов ключей проверки ЭП;

Источником комплектования архивного фонда КУЦ являются подразделения КУЦ, обеспечивающие документирование.

Архивные документы хранятся в специально оборудованном помещении-архивохранилище.

Документы, подлежащие архивному хранению, являются документами временного хранения.

Срок хранения архивных документов устанавливается 5 лет.

Выделение архивных документов к уничтожению и уничтожение осуществляется постоянно действующей комиссией, формируемой из числа сотрудников Отдела криптографической защиты и назначаемой приказом руководителя КУЦ.

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 №63ФЗ «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
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer	УЦ Издатель сертификата	Согласно Таблицы заполнения поля Субъект (для ЮЛ, автоматическое 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 34.11/34.10-2012
Issuer Signature	ЭП КУЦ издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Дополнения сертификата		
Authority Key Identifier	Идентификатор ключа КУЦ 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 КУЦ
Key Usage (critical)	Область использования ключа	Набор областей использования ключа (реализуется установкой соответствующих битов в значение «1»).
Certificate Policies	Политика сертификации	[1]Политика сертификата: Идентификатор политики=Класс средства ЭП КС1
Subject Sign Tool	Средство ЭП владельца сертификата	Средство электронной подписи: СКЗИ "КриптоПро CSP" (версия 4.0)
Issuer Sign Tool	Средство ЭП и средство К У Ц , использующиеся для создания сертификатов	Средство электронной подписи: СКЗИ "КриптоПро CSP" (версия 4.0) Заключение на средство ЭП: Сертификат соответствия № СФ/124-3380 от 11.05.2018 Средство КУЦ: ПАК "КриптоПро УЦ" версии 2.0 Заключение на средство КУЦ: Сертификат соответствия № СФ/128-3592 от 17.10.2018
Subject Key Idendifier	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 КУЦ	URL адреса Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP URL адреса размещения файла сертификата КУЦ
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)	streetAddress (название улицы, номер дома)	streetAddress (название улицы, номер дома)	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	INN (ИНН) – юридического лица	INN (ИНН) – юридического лица	INN (ИНН) – юридического лица
	OGRNIP (ОГРНИП)				

8.2. Структура списка отозванных сертификатов, изготавливаемого КУЦ в электронной форме

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

При создании списка отозванных сертификатов КУЦ использует следующие расширения:

- Расширение «Authority Key Identifier» содержит идентификатор ключа КУЦ;
- Расширение «Reason Code» содержит код причины отзыва сертификата ключа проверки ЭП;
- Расширение «Microsoft CA Version» содержит номер сертификата Центра сертификации.

9. Программные и технические средства обеспечения деятельности КУЦ

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

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

9.1. Программный комплекс обеспечения реализации целевых функций КУЦ

Каждый логический компонент «КриптоПро УЦ» оснащается 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:

- ПАК «Сервер центр сертификации»
- ПАК «Сервер центр регистрации»
- Программный компонент КУЦ «Консоль управления ЦР»
- Программный компонент КУЦ «Консоль экспертизы ЭП»

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

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

Программные компоненты КУЦ, требуемые для разворачивания логических структурных компонент КУЦ

Логический компонент КУЦ	Требуемые программные компоненты «КриптоПро УЦ»
Центр сертификации	Программный компонент КУЦ «Диспетчер УЦ», Роль УЦ «Сервер центров сертификации»
Центр регистрации	Программный компонент КУЦ «Диспетчер УЦ», Роль УЦ «Сервер центров регистрации»
АРМ обслуживающего персонала	Программный компонент УЦ «Консоль управления ЦР»
АРМ разбора конфликтных ситуаций	Программный компонент УЦ «Консоль экспертизы ЭП»
АРМ пользователя	Специальные программные компоненты «КриптоПро УЦ» не требуются

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

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

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

- Ведения Реестра зарегистрированных пользователей КУЦ;
- Ведения Реестра сертификатов ключей проверки ЭП КУЦ;
- Ведения Реестра заявлений на создание сертификатов ключей проверки ЭП пользователей КУЦ;
- Ведения Реестра заявлений на аннулирование (отзыв) сертификатов ключей проверки ЭП пользователей КУЦ;
- Предоставления программных средств для зарегистрированных пользователей КУЦ для обеспечения реализации их прав в части пользования предоставляемыми программными средствами.

АРМ обслуживающего персонала ЦР предназначен для обеспечения реализации своих функциональных обязанностей сотрудникам КУЦ.

АРМ разбора конфликтных ситуаций предназначен для обеспечения своих функциональных обязанностей сотрудникам КУЦ в части взаимодействия с пользователями КУЦ при разрешении вопросов, связанных с подтверждением электронной подписи КУЦ в сертификатах ключей проверки ЭП, созданых КУЦ в электронной форме.

9.2. Технические средства обеспечения работы ПК КУЦ

Технические средства обеспечения работы ПК КУЦ включают в себя:

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

9.3. Программные и программно-аппаратные средства защиты информации

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

- Средства криптографической защиты информации;
- 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 КУЦ;
- Устройства обеспечения противопожарной безопасности помещений КУЦ.

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

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

Основные типы событий, регистрируемые программными компонентами КУЦ:

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 КУЦ и общесистемного программного обеспечения.

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

При эксплуатации программного комплекса обеспечения реализации целевых функций КУЦ ежесуточно выполняется резервное копирование данных компонент ПК КУЦ.

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

- Базу данных КУЦ, включающую журнал выданных сертификатов, очередь запросов, сертификаты ключей проверки ЭП КУЦ;
- Журналы аудита компонент ПК КУЦ в составе, определённом эксплуатационной документацией ПК КУЦ.

9.6. Порядок технического обслуживания средств обеспечения деятельности КУЦ

Порядок технического обслуживания средств обеспечения деятельности КУЦ, 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 КУЦ направлено на обеспечение постоянной готовности указанных средств к использованию по прямому назначению и предотвращению выхода их из строя.

Техническое обслуживание средств обеспечения деятельности КУЦ 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 КУЦ относятся:

- Сервер Центра сертификации;
- Сервер Центра регистрации;
- Автоматизированные рабочие места привилегированных пользователей Удостоверяющего центра (администраторов КУЦ и операторов КУЦ);
- Автоматизированное рабочее место разбора конфликтных ситуаций;
- 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 КУЦ производятся периодические осмотры входящего в него оборудования.

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

№	Наименование работы	Периодичность выполнения работы	Порядок проведения	Примечание
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 необязательна в случае его устойчивой работоспособности по назначению
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	В том случае, если требованиями эксплуатационной документации на конкретное оборудование	

		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 КУЦ, 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 КУЦ (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.	Проверка целостности загрузочных секторов диска и общесистемных файлов	При включении серверов Центра сертификации, Центра регистрации, АРМ привилегированных пользователей, АРМ разбора конфликтных ситуаций,	Проводится средствами аппаратно-программного модуля доверенной загрузки типа «Электронный замок» до загрузки операционной системы	
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	По мере выхода критических	Осуществляется с использованием стандартных средств	

	системы	обновлений операционной системы	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:

№	Наименовани работы	Периодичность выполнения работы	Порядок проведения	Примечание
1.	Проверка целостности программных модулей СКЗИ и ПАК «КриптоПро УЦ»	При включении серверов Центра сертификации, 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	
2.	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
3.	Обновление антивирусных баз	Ежедневно	Осуществляется с использованием специализированных средств антивирусного контроля. Рекомендуется использовать в автоматическом режиме	
4.	Создание резервных копий баз данных удостоверяющего центра	Ежедневно	Осуществляется с использованием специализированных средств резервного хранения данных. Рекомендуется выполнять в автоматическом режиме	
5.	Создание резервного образа диска	Один раз в неделю	Осуществляется с использованием специализированных средств резервного хранения данных	
6.	Контрольная проверка работоспособности СКЗИ «КриптоПро CSP» и ПАК	Один раз в 6 месяцев	Проверку работоспособности средств обеспечения деятельности удостоверяющего центра необходимо выполнять путем выполнения тестовых задач, связанных с основной	

	«КриптоПро УЦ»		деятельностью удостоверяющего центра.	
7.	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 КУЦ является организацией – лицензиатом ФСБ России, имеющей соответствующую лицензию на техническое обслуживание шифровальных (криптографических) средств. Сотрудники КУЦ привлекаемые к проведению данных работ, имеют документ (сертификат), подтверждающий прохождение обучения сотрудника на специализированных курсах.

10. Роли обслуживающего персонала средств обеспечения деятельности КУЦ

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

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

Ролевое администрирование сервера ЦС

Роли и группы	Разрешение безопасности	Описание
Администратор ЦС	Управление ЦС	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. Настройка и обслуживание ЦС, загрузка ключа ЭП ЦС. Это роль ЦС, которая включает в себя возможность назначать все остальные роли. Эта роль также называется КУЦ. Данные разрешения назначаются с помощью Диспетчера КУЦ.
Администратор безопасности ЦС	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

	Администратор центра регистрации Чтение, Подача запросов, Одобрение запросов, Настройка параметров, Настройка безопасности	Установка и разворачивание ЦР, управление ключом ЭП и сертификатом ЦР, управление ключом шифрования и сертификатом Вебсервера ЦР, регистрация администраторов КУЦ, архивирование и восстановление баз ЦР. Это роль операционной системы. Определяется членством в группе локальных администраторов операционной системы. Это роль клиента ЦР, которая включает в себя возможность назначать все остальные роли ЦР и настраивать Центр регистрации. Данные разрешения назначаются с помощью Диспетчера КУЦ и Консоли управления ЦР. 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.
Администратор безопасности ЦР	Управление аудитом и журналом безопасности	Настройка, просмотр и обслуживание журналов аудита. Аудит — это функциональная возможность операционной системы. Аудитор — это роль операционной системы.
Оператор ЦР	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 КУЦ

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

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

Остальные технические средства КУЦ размещаются в рабочих помещения КУЦ по схеме организации рабочих мест персонала.

11.1.2. Физический доступ в помещения

Серверное помещение КУЦ оборудовано системой контроля доступа с идентификацией по карте. Серверное помещение оборудовано исполнительным устройством системы контроля доступа электромеханического типа.

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

Идентификационные карты для доступа в помещения КУЦ, подключенные к системе

контроля доступа, выдаются сотрудникам КУЦ по распоряжению руководителя КУЦ.

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

11.1.3. Электроснабжение и кондиционирование воздуха

Технические средства КУЦ подключены к общегородской сети электроснабжения.

Электрические сети и электрооборудование, используемые в КУЦ, 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 КУЦ, 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 КУЦ, используемые для архивного хранения документов на бумажных, магнитных и оптических носителях оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурновлажностного режима, вентиляции и очистки воздуха.

Рабочие и прочие служебные помещения КУЦ 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 КУЦ оборудовано системой автоматического пожаротушения, пожарной сигнализации и дымоудаления.

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

11.1.6. Хранение документированной информации

Документальный фонд КУЦ, 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 КУЦ, обеспечивающими документирование.

11.2. Программно-аппаратные меры защиты информации

11.2.1. Организация доступа к техническим средствам КУЦ

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

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

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

11.2.2. Организация доступа к программным средствам КУЦ

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

Рабочие места сотрудников КУЦ, 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».

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

11.2.2.1. Общий перечень объектов доступа КУЦ

К объектам доступа КУЦ относятся:

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

11.2.2.2. Перечень объектов доступа, предоставляемых сотрудникам КУЦ

Операторам КУЦ:

- технические средства АРМ администратора Центра регистрации;
- программное обеспечение АРМ администратора Центра регистрации;
- база данных Центра регистрации;
- рабочие сертификаты ключей проверки ЭП пользователей КУЦ;
- ключи ЭП и сертификаты ключей проверки ЭП, использующиеся для эксплуатации Центра сертификации и Центра регистрации;
- списки отозванных сертификатов.

Администраторам КУЦ:

- списки отозванных сертификатов КУЦ.
- база данных Центра сертификации и Центра регистрации КУЦ;

- программное обеспечение Центра сертификации и Центра регистрации КУЦ;
- технические средства АРМ разбора конфликтных ситуаций;
- технические средства Центра сертификации и Центра регистрации КУЦ;
- технические средства АРМ администратора Центра регистрации;
- программное обеспечение АРМ администратора Центра регистрации;
- база данных Центра регистрации;
- технические сертификаты ключей проверки ПАК КУЦ
- рабочие ключи и рабочие сертификаты ключей проверки ЭП пользователей КУЦ;
- списки отозванных сертификатов.
- технические средства компонент КУЦ;
- программное обеспечение компонент КУЦ;
- базы данных Центра сертификации и Центра регистрации.

11.2.3. Контроль целостности программного обеспечения

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

- Программные модули средств электронной подписи и криптографической защиты информации;
- Программные модули Комплекса программ Удостоверяющего центра.
- Состав программных модулей, подлежащих контролю целостности, определяется внутренним документом КУЦ, утверждаемый руководителем КУЦ.

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 — ежесуточно.

11.2.4. Контроль целостности технических средств

Контроль целостности технических средств технических средств КУЦ 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.

11.2.5. Защита внешних сетевых соединений

Защита конфиденциальной информации, передаваемой между программно-техническими средствами обеспечения деятельности КУЦ осуществляется путём шифрования информации с использованием шифровальных (криптографических) средств, сертифицированных в соответствии с действующим законодательством Российской Федерации.

Защита программно-технических средств обеспечения деятельности КУЦ 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 пределах одой контролируемой зоны используются шифровальные (криптографических) средства сертифицированные по классу КВ.

Технические средства аккредитованного удостоверяющего центра - Центр регистрации и Центр сертификации ПАК «КриптоПро УЦ 2.0» не подключены к техническим средствам общедоступных сетей связи, в том числе, сети Интернет.

11.2.5.1. Перечень информации, подлежащей защите

- Заявление на создание сертификата ключа проверки ЭП;
- Заявление на аннулирование (отзыв) сертификата ключа проверки ЭП;
- Ключевая фраза пользователя. Передаваемая из КУЦ информация:
- Бланк копии сертификата ключа проверки ЭП для вывода на бумажный носитель;
- Список сертификатов ключа проверки ЭП Пользователя КУЦ и их статус;
- Список запросов на сертификаты ключей проверки ЭП Пользователя КУЦ и их статус;
- Список запросов на аннулирование (отзыв) сертификатов ключей проверки ЭП Пользователя КУЦ и их статус.

11.3. Организационные меры защиты информации

11.3.1. Предъявляемые требования к персоналу КУЦ

Персонал КУЦ, производящий обслуживание КУЦ, имеет высшее профессиональное образование и профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области более 2 лет.

11.3.2. Организация доступа персонала к документам и документации

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

11.3.3. Охрана здания и помещений

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

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

11.4. Юридические меры защиты информации

КУЦ имеет разрешение (лицензии) по всем видам деятельности, связанных с предоставлением услуг.

Системы безопасности КУЦ 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 КУЦ введены в действие приказами руководителя КУЦ.

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

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

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

12. Взаимодействие КУЦ с федеральными органами исполнительной власти в сфере использования электронной подписи

Для использования пользователями КУЦ квалифицированной электронной подписи и создания квалифицированных сертификатов ключей проверки ЭП КУЦ 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.