УТВЕРЖДАЮ

Генеральный директор
ЗАО «ПФ «СКБ Контур»

_____ Д. М. Мраморов

"___" _____ 2010 г.

система защищенного
электронного документооборота

КОНТУР-ЭКСТЕРН

Версия 6.0

Руководство пользователя

Информационная безопасность

ЗАО «ПФ «СКБ Контур»

Екатеринбург

Содержание

1. ВВЕДЕНИЕ

В соответствии с действующим на территории Российской Федерации законодательством, порядок использования средств криптографической защиты информации, предназначенных для защиты сведений, не составляющих государственную тайну, регулируется ФСБ России. В соответствии с этим порядком (утвержденным Положением о криптографической защите ПКЗ-2005 и уточненным в некоторых других нормативных актах), пользователи средств криптографической защиты информации (СКЗИ) в системах защищенного электронного документооборота не должны иметь специальных лицензий на использование этих средств (при наличии определенных лицензий у организатора системы). Однако пользователи должны быть ознакомлены с определенными правилами эксплуатации СКЗИ.

Следует отметить, что и помимо требований законодательства в любом случае возникает необходимость ознакомить пользователя с правилами организации защиты информации на его рабочем месте при работе в системе «Контур-Экстерн». Доступ бухгалтера в Интернет, отправка конфиденциальных сведений по защищенным каналам связи могут создавать дополнительные риски нарушения информационной безопасности на предприятии при несоблюдении определенных требований. С другой стороны, при выполнении этих требований уровень защищенности технологии отправки данных налоговой и бухгалтерской отчетности в электронном виде по телекоммуникационным каналам связи оказывается несоизмеримо выше, чем уровень защищенности технологии представления сведений на бумаге (нарочным или почтовым отправлением).

Настоящая книга руководства пользователя предназначена для обязательного ознакомления выделенному в организации сотруднику, отвечающему за информационную безопасность при использовании СКЗИ и работе в защищенной телекоммуникационной системе «Контур-Экстерн». В первую очередь в этой связи важна вторая глава, которая содержит общие требования и рекомендации по информационной безопасности при работе в системе «Контур-Экстерн.

В третьей главе приводится регламент Удостоверяющего центра ЗАО «ПФ «СКБ Контур». Удостоверяющий центр – основа ключевой инфраструктуры всей системы «Контур-Экстерн», от его функционирования зависит возможность корректного разрешения любых конфликтных ситуаций, связанных с применением электронной цифровой подписи. Регламент Удостоверяющего центра является договором присоединения, который подписывает каждый абонент системы «Контур-Экстерн» при подключении к системе.

Удостоверяющий центр ЗАО «ПФ «СКБ Контур» обслуживает все те региональные сегменты системы, в которых специализированным оператором связи является ЗАО «ПФ «СКБ Контур», а также ряд других: Сахалинская область, Магаданская область, Томская область, Алтайский край, Тюменская область, Курганская область, республика Удмуртия, республика Карелия, Мурманская область, Смоленская область. В ряде других регионов функционируют собственные Удостоверяющие центры, регламент которых может отличаться от приведенного ниже в главе 3.

2. Обеспечение информационной безопасности

Большая часть той информации, которая обращается в системе «Контур-Экстерн», является конфиденциальной. Утеря такой информации, искажение, или попадание информации в руки третьих лиц может потенциально нанести серьезный вред владельцу информации. Поэтому в системе «Контур-Экстерн» вопросам информационной безопасности уделяется особое место.

Сама по себе предметная область защиты информации бурно развивается в последнее время, совершенствуются методы защиты и сейчас можно гарантировать очень высокий уровень защищенности данных в системе, при условии соблюдения абонентами определенных требований по защите информации. Для того, чтобы понимать и уметь выполнять эти требования, необходимо внимательно ознакомиться с материалами данной главы.

1. Основные понятия

Средство криптографической защиты информации — средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Владелец сертификата ключа подписи — физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств ЭЦП создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Средства ЭЦП — аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций — создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Сертификат средства ЭЦП — документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средства ЭЦП установленным требованиям.

Закрытый ключ ЭЦП — уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств ЭЦП.

Открытый ключ ЭЦП — уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому пользователю информационной системы и предназначенная для подтверждения использованием средств ЭЦП подлинности электронной цифровой подписи в электронном документе.

Сертификат ключа (сертификат ключа подписи) — документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, включающий в себя открытый ключ шифрования и/или ЭЦП, которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи, идентификации владельца сертификата ключа подписи и/или обеспечения конфиденциальности информации.

Подтверждение подлинности электронной цифровой подписи в электронном документе — положительный результат проверки соответствующим сертифицированным средством ЭЦП с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанного данной электронной цифровой подписью электронном документе.

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

- Потеря ключевых носителей.
- Потеря ключевых носителей с их последующим обнаружением.
- Увольнение сотрудников, имевших доступ к ключевой информации.
- Нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа.
- Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
- Нарушение печати на сейфе с ключевыми носителями.
- Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

2. Общие принципы организации защиты информации в системе

Криптографическая подсистема среды «Контур-Экстерн» опирается на отечественное законодательство в области защиты информации (в том числе, на действующие ГОСТы и руководящие документы ФСБ (ФАПСИ) и ФСТЭК (Гостехкомисии)), а также на международный стандарт X.509, определяющий принципы и протоколы, используемые при построении систем с открытыми ключами.

Инфраструктура открытых ключей — это система, в которой каждый пользователь имеет пару ключей — секретный (закрытый) и открытый. При этом по секретному ключу можно построить соответствующий ему открытый ключ, а обратное преобразование неосуществимо или требует огромных временных затрат. Каждый пользователь системы генерирует себе секретный ключ, вычисляет по нему открытый ключ, и, сохраняя свой секретный ключ в строгой тайне, делает открытый ключ общедоступным. С точки зрения инфраструктуры открытых ключей, *шифрование* представляет собой преобразование сообщения, осуществляемое с помощью открытого ключа получателя информации. В самом деле, только получатель, зная свой собственный секретный ключ, сможет провести обратное преобразование и прочитать сообщения, а больше никто сделать этого не сможет, в том числе — и сам отправить шифрограммы. *Электронная подпись* в инфраструктуре открытых ключей — это преобразование сообщение с помощью секретного ключа отправителя. Любой желающий может провести обратное преобразование, применив общедоступный открытый ключ автора документа, но никто не сможет имитировать такой документ, не зная закрытого ключа автора.

Обязательным участником любой инфраструктуры открытых ключей является Удостоверяющий центр — программно-аппаратный комплекс и система мероприятий, выполняющие функции центра доверия всей системы документооборота. Главная задача Удостоверяющего центра заключается в выпуске *сертификатов открытых ключей* пользователей системы документооборота. Сертификат открытого ключа — это электронный документ, заверенный электронной подписью Удостоверяющего центра и заверяющий факт владения того или иного участника документооборота тем или иным

открытым ключом. Благодаря сертификатам, пользователи системы могут опознавать друг друга, а, кроме того, проверять принадлежность электронной подписи конкретному абоненту и целостность (неизменность) содержания подписанного электронного документа.

Все вышесказанное является, конечно, только очень грубым первым приближением, но нашей целью здесь не является регламентация технических нюансов; мы хотим дать абсолютно незнакомому с областью защиты информации пользователю некоторое представление о процессах, которые скрываются за терминами «зашифровать» или «подписать».

Естественно, сами преобразования сообщений с использованием тех или иных ключей достаточно сложны, и производятся автоматизированно, с помощью специальных программ. В системе «Контур-Экстерн» для этих целей используется средство криптографической защиты информации (СКЗИ) «Крипто-Про CSP». СКЗИ — это программа, которая осуществляет электронную цифровую подпись (ЭЦП), шифрование, обладает способностью генерировать ключи, работать с сертификатами и т.д. Благодаря применению «Крипто-Про CSP» в системе «Контур-Экстерн» удается решить все основные задачи защиты информации, а именно:

- *задача защиты от несанкционированного доступа* решается с помощью автоматического шифрования всех конфиденциальных электронных документов, которые обращаются в системе; система следит за тем, чтобы каждый такой документ в момент отправки обязательно шифровался на открытом ключе получателя и, таким образом, оставался бы закрытым на всем пути до рабочего места адресата;
- *задача подтверждения авторства* решается благодаря применению электронной цифровой подписи, которая автоматически ставится на все возникающие в системе электронные документы; система следит за тем, чтобы ни один документ (вне зависимости от того, кто автор этого документа, кому и для чего он предназначается), не отправлялся в путь без ЭЦП, которая позволяет в последствии решать на законодательно закрепленной основе любые споры в отношении авторства документа;
- *задача обеспечения неотрекаемости* также решается с помощью механизма ЭЦП, а также благодаря обязательному автоматическому резервному копированию всех документов на сервере системы, у отправителя и получателя; таким образом, подписанный документ обладает юридической силой с самого момента подписания и ни его содержание, ни сам факт существования документа не могут быть оспорены никем, включая автора документа;
- *задача обеспечения целостности электронного документа* тоже решается с помощью ЭЦП, которая содержит в себе *хэш-значение* (усложненный аналог контрольной суммы) подписываемого документа; таким образом, при попытке изменить хотя бы один символ в документе или в его подписи после того, как документ был подписан, уже невозможно — это приведет к нарушению правильности ЭЦП и будет немедленно диагностировано;
- *задача аутентификации абонента в системе* решается каждый раз при начале сеанса работы абонента с помощью сертификатов открытых ключей; сервер системы и абонент автоматически предъявляют друг другу свои сертификаты и, таким образом, избегают опасности вступить в информационный обмен с анонимным лицом или с лицом, выдающим себя за другого.

Важно понимать, что уровень защищенности информации в системе в целом равняется уровню защищенности информации в самом слабом месте системы. Поэтому, учитывая то, что система обеспечивает высочайший уровень конфиденциальности на всем пути следования электронных документов между абонентами, необходимо также

тщательно соблюдать меры безопасности непосредственно на рабочих местах абонентов. За сохранность информации до того момента, как она начинает обрабатываться в системе, несет ответственность только ее владелец, и в его силах обезопасить себя от возможных негативных последствий, связанных с утечкой, разглашением или искажением данных.

3. Инструкция по безопасности на рабочем месте абонента

Автоматизированное рабочее место абонента системы «Контур-Экстерн» использует средства криптографической защиты информации (СКЗИ) для обеспечения целостности, авторства и конфиденциальности информации, передаваемой в рамках информационной системы.

Порядок обеспечения информационной безопасности при работе в системе «Контур-Экстерн» определяется руководителем организации, подключающейся к системе, на основе рекомендаций по организационно-техническим мерам защиты, изложенных в данном разделе и эксплуатационной документации на СКЗИ КриптоПро CSP (см. «КриптоПро CSP. Правила пользования» (ЖТЯИ.00005-01 90 07)) и рекомендательных и нормативных материалов ФСТЭК (Гостехкомиссии России) по организации защиты информации.

Владелец сертификата ключа обязан:

- Не использовать для электронной цифровой подписи и шифрования открытые и закрытые ключи, если ему известно, что эти ключи используются или использовались ранее;
- Хранить в тайне закрытый ключ;
- Немедленно требовать приостановления действия сертификата ключа при наличии оснований полагать, что тайна закрытого ключа нарушена (компрометация ключа).
- Обновлять сертификат ключа подписи в соответствии с установленным регламентом.

Рекомендуется:

- Установка и настройка СКЗИ на Автоматизированное рабочее место (АРМ) должна выполняться в присутствии администратора. Перед установкой необходимо проверить целостность программного обеспечения СКЗИ. Запрещается устанавливать СКЗИ, целостность которого нарушена.
- В организации должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации с закрытыми ключами ЭЦП и шифрования, который должен полностью исключать возможность несанкционированного доступа к ним.
- Должен быть утвержден список лиц, имеющих доступ к ключевой информации.
- Для хранения носителей закрытых ключей ЭЦП и шифрования в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами с двумя экземплярами ключей (один у исполнителя, другой в службе безопасности).
- Использовать АРМ со встроенными средствами криптографической защиты в однопользовательском режиме. В отдельных случаях, при необходимости использования АРМ несколькими лицами, эти лица должны обладать равными правами доступа к информации.
- При загрузке операционной системы и при возвращении после временного отсутствия пользователя на рабочем месте должен запрашиваться пароль, состоящий не менее чем из 6 символов. В отдельных случаях при невозможности использования парольной защиты, допускается загрузка ОС без запроса пароля.

При этом должны быть реализованы дополнительные организационно-режимные меры, исключающие несанкционированный доступ к этим АРМ.

- Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства АРМ со встроенными СКЗИ.
- Должны быть предусмотрены меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленными СКЗИ.
- Установленное на АРМ программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.
- Администрирование должно осуществляться доверенными лицами.
- Средствами BIOS исключить возможность сетевой загрузки ОС рабочей станции.
- Средствами BIOS исключать возможность работы на ПЭВМ, если во время ее начальной загрузки не проходят встроенные тесты.
- Вхождение пользователей в режим конфигурирования BIOS штатными средствами BIOS должно осуществляться только с использованием парольной защиты при длине пароля не менее 6 символов.
- При использовании ОС Windows 98/ME/NT/2000/XP все пользователи рабочей станции должны иметь право доступа ко всей конфиденциальной информации, обрабатываемой на этой станции.
- При использовании ОС Windows NT/2000/XP принять меры, исключающие доступ пользователя к системному реестру.
- Ограничить либо исключить использование программного продукта Scheduler (планировщик заданий), входящего в состав ОС Windows. При использовании Scheduler состав запускаемого программного обеспечения на АРМ согласовывается с администратором безопасности.
- При использовании ОС Windows NT/2000/XP исключить возможность удаленного редактирования системного реестра пользователями (исключая администратора).
- При использовании ОС Windows NT/2000/XP переименовать пользователя Administrator, отключить учетную запись для гостевого входа (Guest).
- В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям (ЭЦП и шифрования), должна быть проведена смена ключей, к которым он имел доступ.

Не допускается:

- Снимать несанкционированные копии с ключевых носителей.
- Знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным.
- Выводить секретные ключи на дисплей (монитор) ПЭВМ или принтер.
- Устанавливать ключевой носитель в считывающее устройство (дисковод) ПЭВМ АРМ, не предусмотренных функционированием системы, а также в другие ПЭВМ.
- Записывать на ключевой носитель постороннюю информацию.
- Хранить пароли в виде записей на бумажном носителе.

Пароли должны учитываться, обновляться и храниться в соответствии с нормативными документами, подготовленными сотрудниками, отвечающими за информационную безопасность, и утвержденными руководителем организации. Действия, связанные с

эксплуатацией СКЗИ, должны фиксироваться в журнале, который ведет лицо, ответственное за обеспечение информационной безопасности.
В журнал кроме этого записываются факты компрометации ключевых документов, нештатные ситуации, происходящие в системе «Контур-Экстерн» и связанные с использованием СКЗИ, проведение регламентных работ, данные о полученных у администратора безопасности организации ключевых носителях, нештатных ситуациях, произошедших на АРМ, с установленным ПО СКЗИ.
В журнале может отражаться следующая информация:

- дата, время;
- запись о компрометации ключа;
- запись об изготовлении личного ключевого носителя пользователя, идентификатор носителя;
- запись об изготовлении копий личного ключевого носителя пользователя, идентификатор носителя;
- запись об изготовлении резервного ключевого носителя пользователя, идентификатор носителя
- запись о получении сертификата открытого ключа ЭЦП, полный номер ключевого носителя, соответствующий сертификату;
- записи, отражающие выдачу на руки пользователям (ответственным исполнителям) и сдачу ими на хранение личных ключевых носителей, включая резервные ключевые носители;
- события, происходившие на АРМ пользователя с установленным ПО СКЗИ, с указанием причин и предпринятых действий.

3. Регламент Удостоверяющего центра ЗАО «Производственная фирма «СКБ Контур»

Внимание! Приводимый ниже текст не является официальной публикацией Регламента услуг Удостоверяющего центра ЗАО «ПФ «СКБ Контур». Актуальная версия регламента со всеми необходимыми приложениями опубликована в Интернете на узле http://ca.skbkontur.ru.

Публикация основной части текста Регламента по состоянию на 1 февраля 2008 года осуществляется в справочных целях, для того чтобы обеспечить пользователя доступной информацией о порядке действий в случае наступления внештатных ситуаций (например, компрометации секретного ключа) и о порядке разрешения конфликтных ситуаций.

1. Сведения об Удостоверяющем Центре

Закрытое акционерное общество «ПФ «СКБ Контур», именуемое в дальнейшем «*Удостоверяющий Центр*», зарегистрировано на территории Российской Федерации в городе Екатеринбурге. Свидетельство о регистрации №0870-1 II-ОИ, выдано 26.03.1996 г. Администрацией Орджоникидзевского района г. Екатеринбург.

Удостоверяющий Центр в качестве участника рынка услуг по изготовлению и выдаче сертификатов ключей подписи осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий:

1. Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Б342428 рег.№2242У от 18.01.2005 г. на право предоставления услуг в области шифрования информации.
2. Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Б342421 рег. №2240Х от 18.01.2005 г. на право технического обслуживания шифровальных (криптографических) средств.
3. Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Б342427 рег. №2241Р от 18.01.2005 г. на право распространения шифровальных (криптографических) средств.

Юридический адрес: 620017, г. Екатеринбург, проспект Космонавтов, д. 56.

Фактическое местонахождение: 620017, г. Екатеринбург, проспект Космонавтов, д. 56.

Банковские реквизиты (наименование банка, БИК, ИНН, р/с, к/с):

- ОАО «Альфа-Банк»
- БИК 044525593
- ИНН 7728168971
- Р/с 40702810710010035884
- К/с 30101810100000000854

Контактные телефоны, факс, адрес электронной почты:

тел./факс: (343) 228-29-98; e-mail: ca@skbkontur.ru.

2. Термины и определения

Владелец сертификата ключа подписи – *Пользователь УЦ*, на имя которого *Удостоверяющим Центром* выдан сертификат ключа подписи, и которое владеет соответствующим *Закрытым ключом электронной цифровой подписи*, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная *Владельцу сертификата ключа подписи* и предназначенная для создания в электронных документах электронной цифровой подписи с использованием

средств электронной цифровой подписи. Закрытый ключ электронной цифровой подписи действует на определенный момент времени (является действующим закрытым ключом) если:

- наступил момент начала действия закрытого ключа;
- срок действия закрытого ключа не истек;
- сертификат ключа подписи, соответствующий данному Закрытому ключу не аннулирован (отозван) и действие его не приостановлено.

Копия сертификата ключа подписи – документ на бумажном носителе, содержащий информацию из сертификата ключа подписи и заверенный собственноручными подписями *Владельца сертификата ключа подписи* и *Уполномоченного лица Удостоверяющего Центра, а также* печатью *Удостоверяющего Центра*.

Оператор Удостоверяющего Центра – физическое лицо, являющееся сотрудником *Удостоверяющего Центра*, занимающееся рассмотрением и обработкой заявлений на изготовление, аннулирование (отзыв), приостановление/возобновление действия сертификатов ключей подписи.

Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая *Закрытому ключу электронной цифровой подписи*, доступная любому пользователю и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Пользователь УЦ – физическое лицо, признающее данный регламент и получающее услуги *Удостоверяющего Центра*.

Реестр Удостоверяющего Центра – набор документов *Удостоверяющего Центра* в электронной и/или бумажной форме, включающий следующую информацию:

- реестр поступивших заявлений о присоединении к *Регламенту Удостоверяющего Центра*;
- реестр поступивших заявлений на изготовление сертификата ключа подписи;
- реестр поступивших заявлений на аннулирование (отзыв) сертификата ключа подписи;
- реестр поступивших заявлений на приостановление/возобновление действия сертификата ключа подписи;
- реестр изготовленных сертификатов ключей подписи;
- реестр изготовленных *Списков отозванных сертификатов*;
- служебную информацию *Удостоверяющего Центра*.

Сертификат ключа подписи – электронный документ с электронной цифровой подписью *Уполномоченного лица Удостоверяющего Центра*, структура которого определяется данным *Регламентом* и который выдается *Удостоверяющим Центром Пользователю УЦ* для подтверждения подлинности электронной цифровой подписи и идентификации *Владельца сертификата ключа подписи*.

Список отозванных сертификатов (СОС) – электронный документ с электронной цифровой подписью *Уполномоченного лица Удостоверяющего Центра*, включающий в себя список серийных номеров *Сертификатов ключей подписи*, которые на определенный момент времени были аннулированы (отозваны), или действие которых было приостановлено.

Средства электронной цифровой подписи – средства криптографической защиты информации (СКЗИ)

- «КриптоПро CSP» версии 2, вариант исполнения 1, в составе, определенном формуляром ЖТЯИ.00005-01 30 01,

- «КриптоПро CSP» версии 3, в составе, определенном формуляром ЖТЯИ.00015-01 30 01,

обеспечивающие реализацию следующих функций – создание электронной цифровой подписи в электронном документе с использованием *Закрытого ключа электронной цифровой подписи*, подтверждение с использованием *Открытого ключа электронной цифровой подписи* подлинности электронной цифровой подписи в электронном документе, создание *Закрытых и Открытых ключей электронных цифровых подписей*.

Уполномоченное лицо Удостоверяющего Центра – физическое лицо, являющееся сотрудником *Удостоверяющего Центра* и наделенное *Удостоверяющим Центром* полномочиями по заверке *Сертификатов ключей подписи* и *Списков отозванных сертификатов*.

Уполномоченный сотрудник ЦР – физическое лицо, являющееся сотрудником *Удостоверяющего Центра* либо сотрудником *Центра Регистрации*, которому делегирован ряд функций при предоставлении услуг *Удостоверяющего Центра*.

Центр Регистрации – самостоятельное по отношению к *Удостоверяющему Центру* юридическое лицо, из числа сотрудников которого назначается *Уполномоченный сотрудник ЦР*.

Электронный документ – документ, информация в котором представлена в электронно-цифровой форме.

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием *Закрытого ключа электронной цифровой подписи* и позволяющий идентифицировать *Владельца сертификата ключа подписи*, а также установить отсутствие искажения информации в электронном документе.

Public Key Cryptography Standarts (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security; *Удостоверяющий Центр* осуществляет свою работу в соответствии со следующими стандартами PKCS:

- PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений; *Удостоверяющий Центр* использует описанный в PKCS#7 тип данных PKCS#7 Signed – подписанные данные;
- PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат ключа подписи.

Кодовая фраза – последовательность символов, используемая для аутентификации *Пользователя УЦ Оператором Удостоверяющего Центра* для выполнения удаленного управления сертификатом ключа подписи.

3. Общие положения

3.1 Статус Регламента

3.1.1 Регламент оказания услуг *Удостоверяющего Центра*, именуемый в дальнейшем «*Регламент»,* разработан в соответствии с законодательством Российской Федерации.

3.1.2 *Регламент* устанавливает общий порядок и условия предоставления *Удостоверяющим Центром Пользователю УЦ,* присоединившемуся к *Регламенту* в порядке, предусмотренном статьёй 428 ГК РФ, услуг по изготовлению и выдаче сертификатов ключей подписи и дополнительных услуг, связанных с управлением сертификатами ключей подписи.

3.1.3 Любое заинтересованное лицо может ознакомиться с *Регламентом* на сайте *Удостоверяющего Центра* по адресу http://ca.skbkontur.ru либо по запросу

получить его копию в офисе *Удостоверяющего Центра* за плату, не превышающую расходов на ее изготовление.

3.1.4 Присоединение к *Регламенту* производится путем подписания *Пользователем УЦ* заявления на присоединение к *Регламенту*, по форме, указанной в Приложении № 1 к *Регламенту*, либо путем заключения между *Удостоверяющим Центром* и *Пользователем УЦ* гражданско-правового договора, предусматривающего присоединение *Пользователя УЦ* к *Регламенту*.

3.1.5 *Пользователь УЦ* имеет право в одностороннем порядке прекратить взаимодействие с *Удостоверяющим Центром* в рамках *Регламента*, письменно уведомив об этом *Удостоверяющий Центр*. Данное письменное уведомление, полученное *Удостоверяющим Центром* от *Пользователя УЦ*, является основанием для обязательного аннулирования (отзыва) сертификатов ключей подписи *Пользователя УЦ*. Аннулирование (отзыв) указанных сертификатов *Пользователя УЦ* производится в течение одного месяца с момента получения *Удостоверяющим Центром* уведомления.

3.1.6 Прекращение взаимоотношений *Пользователя УЦ* и *Удостоверяющего Центра* не освобождает Стороны от исполнения обязательств, возникших до указанного прекращения, и не освобождает от ответственности за их неисполнение (ненадлежащее исполнение).

3.2 Толкование Регламента

3.2.1 Стороны понимают термины и определения, применяемые в *Регламенте*, строго в контексте общего смысла *Регламента*.

3.2.2 В случае противоречия и/или расхождения названия какой-либо статьи со смыслом какого-либо содержащегося в ней пункта, Стороны принимают доминирующим смысл формулировок каждого конкретного пункта.

3.2.3 В случае противоречия и/или расхождения смысла положений какого-либо приложения к *Регламенту* с положениями собственно *Регламента*, Стороны принимают доминирующим смысл положений *Регламента*.

3.3 Изменения (дополнения) Регламента

3.3.1 Внесение изменений (дополнений) в *Регламент*, в том числе Приложений к нему, производится *Удостоверяющим Центром* в одностороннем порядке.

3.3.2 Уведомление *Пользователей УЦ* о внесении изменений (дополнений) в *Регламент* осуществляется *Удостоверяющим Центром* путем размещения очередной версии *Регламента*, включающей указанные изменения (дополнения) на сайте *Удостоверяющего Центра* по адресу http://ca.skbkontur.ru.

3.3.3 Изменения (дополнения), вносимые *Удостоверяющим Центром* в *Регламент,* кроме изменений (дополнений), вызванных изменениями законодательства РФ и нормативными документами государственных органов, вступают в силу и становятся обязательными для Сторон по истечении 10 (Десяти) календарных дней с даты размещения указанных изменений и дополнений в *Регламенте* на сайте *Удостоверяющего Центра* по адресу http://ca.skbkontur.ru.

3.3.4 Изменения (дополнения), вносимые *Удостоверяющим Центром* в *Регламент* в связи с изменением законодательства РФ и нормативными документами государственных органов, регулирующих деятельность удостоверяющих центров, вступают в силу одновременно с вступлением в силу соответствующих законодательных и нормативных актов.

3.3.5 Действие изменений и дополнений в *Регламенте* с момента их вступления в силу распространяется на всех *Пользователей УЦ*, в том числе присоединившихся к *Регламенту* ранее даты вступления изменений (дополнений) в силу.

3.4 Перечень услуг, предоставляемых Удостоверяющим Центром

3.4.1 Изготовление сертификатов ключей подписи *Пользователей УЦ* в электронной форме.
3.4.2 Изготовление *Копий сертификатов ключей подписи Пользователей УЦ* на бумажном носителе.
3.4.3 Предоставление в форме электронных документов *Копий сертификатов ключей подписи Пользователей УЦ*, находящихся в *Реестре* изготовленных сертификатов.
3.4.4 Аннулирование (отзыв), приостановление и возобновление действия сертификатов ключей подписи *Пользователей УЦ*.
3.4.5 Предоставление сведений об аннулированных и приостановленных сертификатах ключей подписи *Пользователей УЦ*.
3.4.6 Подтверждение подлинности электронных цифровых подписей *Уполномоченного лица Удостоверяющего Центра* в изготовленных им сертификатах ключей подписи *Пользователей УЦ*.
3.4.7 Подтверждение подлинности электронных цифровых подписей *Пользователей УЦ* в электронных документах.

4. Вознаграждение Удостоверяющего Центра

4.1 *Удостоверяющий Центр* осуществляет свою деятельность на платной основе.

4.2 Стоимость, сроки и порядок расчетов за оказанные услуги *Удостоверяющего Центра* регулируются отдельными соглашениями между *Удостоверяющим Центром* и, либо непосредственно *Пользователем УЦ*, либо организацией, сотрудником которой является *Пользователь УЦ*, либо организацией, выполняющей функции *Центра Регистрации*.

4.3 Оплата осуществляется в российских рублях по безналичному расчету путем перечисления денежных средств на расчетный счет или иным способом, предусмотренным законодательством Российской Федерации.

4.4 В случае выполнения внеплановой смены ключей *Уполномоченного лица Удостоверяющего Центра* (в соответствии с процедурой, определенной *Регламентом*) *Удостоверяющий Центр* выполняет изготовление сертификатов ключей подписи *Пользователей УЦ* безвозмездно.

4.5 Предоставление участникам информационных систем в форме электронных документов *Копий сертификатов ключей подписи Пользователей УЦ*, находящихся в *Реестре* изготовленных сертификатов, а также информации об их действии в виде *Списков отозванных сертификатов* осуществляется безвозмездно.

4.6 *Удостоверяющий Центр* выполняет аннулирование (отзыв) действия сертификата ключа подписи и приостановление/возобновление действия сертификата ключа *Пользователя УЦ* безвозмездно.

4.7 Услуга удаленного управления сертификатом ключа подписи с аутентификацией *Пользователя УЦ* по *Кодовой фразе,* предоставляется *Удостоверяющим Центром* безвозмездно.

5. Предоставление информации

5.1 Удостоверяющий Центр предоставляет Пользователю УЦ по его требованию:
5.1.1 Копию лицензии на право предоставления услуг в области шифрования информации.
5.1.2 Копию лицензии на осуществление деятельности по техническому обслуживанию шифровальных (криптографических) средств.

5.1.3 Копию Сертификата соответствия СФ/114-1000 от 05.06.2007г. на СКЗИ КриптоПро CSP версии 2, вариант исполнения 1.
5.1.4 Копию Сертификата соответствия СФ/124-0810 от 12.09.2005г. на СКЗИ КриптоПро CSP версии 3.
5.1.5 Копию Сертификата соответствия СФ/128-1060 от 24.09.2007г. на программно-аппаратный комплекс «Удостоверяющий центр» КриптоПро УЦ».

5.2 Удостоверяющий Центр вправе запросить у Пользователя УЦ, а Пользователь УЦ обязан предоставить Удостоверяющему Центру документы, подтверждающие следующую информацию:
5.2.1 Наименование, основной государственный регистрационный номер, идентификационный номер налогоплательщика и регистрационный номер страхователя в системе персонифицированного учета ПФР организации, сотрудником которой является *Пользователь УЦ.*
5.2.2 Сведения, необходимые для идентификации *Пользователя УЦ*: фамилия, имя, отчество, паспортные данные (серия, номер, когда и кем выдан), идентификационный номер налогоплательщика.
5.2.3 Место регистрации и адрес места жительства *Пользователя УЦ.*

6. Права и обязанности Сторон

6.1 Пользователь УЦ имеет право:
6.1.1 Получить *Список отозванных сертификатов*, изготовленный *Удостоверяющим Центром*.
6.1.2 Применять *Список отозванных сертификатов*, изготовленный *Удостоверяющим Центром*, для проверки статуса сертификатов ключей подписи, изготовленных *Удостоверяющим Центром*.
6.1.3 Получить сертификат ключа подписи *Уполномоченного лица Удостоверяющего Центра*.
6.1.4 Получить копии сертификатов открытого ключа ЭЦП в электронной форме, находящихся в реестре сертификатов открытых ключей *Удостоверяющего Центра.*
6.1.5 Применять сертификат ключа подписи *Уполномоченного лица Удостоверяющего Центра* для проверки электронной цифровой подписи *Уполномоченного лица Удостоверяющего Центра* в сертификатах ключей подписи, изготовленных *Удостоверяющим Центром*.
6.1.6 Применять сертификат ключа подписи *Пользователя УЦ* для проверки электронной цифровой подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа подписи *Пользователя УЦ.*
6.1.7 Обратиться в *Удостоверяющий Центр* для аннулирования (отзыва) принадлежащего ему сертификата ключа подписи в течение срока действия этого сертификата.
6.1.8 Обратиться в *Удостоверяющий Центр* для приостановления действия принадлежащего ему сертификата ключа подписи в течение срока действия этого сертификата.
6.1.9 Обратиться в *Удостоверяющий Центр* для возобновления действия принадлежащего ему сертификата ключа подписи в течение срока действия этого сертификата и срока, на который действие сертификата было приостановлено.
6.1.10 Использовать услугу удаленного управления сертификатом ключа подписи с аутентификацией *Пользователя УЦ* по *Кодовой фразе*.
6.1.11 Обратиться в *Удостоверяющий Центр* за подтверждением подлинности электронной цифровой подписи *Уполномоченного лица Удостоверяющего Центра* в изготовленных им сертификатах ключей подписи.

6.1.12 Обратиться в *Удостоверяющий Центр* за подтверждением подлинности электронной цифровой подписи электронных документов.

6.2 Удостоверяющий Центр имеет право:

6.2.1 Отказать в изготовлении сертификата ключа подписи *Пользователя УЦ* в случае ненадлежащего оформления заявления на изготовление сертификата ключа подписи.

6.2.2 Отказать в изготовлении сертификата ключа подписи *Пользователя УЦ* в случае, если использованное *Пользователем УЦ* для формирования запроса на сертификат ключа подписи средство криптографической защиты информации не поддерживается *Удостоверяющим Центром*.

6.2.3 Отказать в аннулировании (отзыве) сертификата ключа подписи *Пользователя УЦ* в случае ненадлежащего оформления заявления на аннулирование (отзыв) сертификата ключа подписи.

6.2.4 Отказать в приостановлении/возобновлении действия сертификата ключа подписи *Пользователя УЦ* в случае ненадлежащего оформления заявления на приостановление/возобновление действия сертификата ключа подписи.

6.2.5 Отказать *Пользователю УЦ* в исполнении услуги удаленного управления сертификатом ключа подписи в случае невозможности аутентификации *Пользователя УЦ* по *Кодовой фразе.*

6.2.6 Отказать в аннулировании (отзыве) сертификата ключа подписи *Пользователя УЦ* в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату.

6.2.7 Отказать в приостановлении/возобновлении действия сертификата ключа подписи *Пользователя УЦ* в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату.

6.2.8 Аннулировать (отозвать) сертификат ключа подписи *Пользователя УЦ* в случае установленного факта компрометации соответствующего закрытого ключа, с уведомлением *Владельца аннулированного (отозванного) сертификата ключа подписи* и указанием обоснованных причин.

6.2.9 Приостановить действие сертификата ключа подписи *Пользователя УЦ* с уведомлением *Владельца сертификата ключа подписи*, действие которого приостановлено, и указанием обоснованных причин.

6.3 Сторона, присоединившаяся к Регламенту, обязана:

6.3.1 Извещать *Удостоверяющий Центр* об изменениях в документах, приведенных в п.5.2. и предоставлять их по требованию *Удостоверяющего Центра* в течение 5 (Пяти) рабочих дней с момента регистрации изменений.

6.3.2 С целью обеспечения гарантированного ознакомления с полным текстом изменений и дополнений *Регламента* до вступления их в силу не реже одного раза в тридцать календарных дней обращаться на сайт *Удостоверяющего Центра* по адресу http://ca.skbkontur.ru за сведениями об изменениях и дополнениях, внесенных в *Регламент*.

6.4 Владелец сертификата ключа подписи обязан:

6.4.1 Хранить в тайне личный закрытый ключ, принимать все возможные меры для предотвращения его утери, раскрытия, искажения и несанкционированного использования.

6.4.2 Немедленно обратиться в *Удостоверяющий Центр* с заявлением на аннулирование (отзыв) сертификата ключа подписи в случае утери, раскрытия, искажения личного закрытого ключа, а также в случае, если *Пользователю* стало известно, что этот ключ используется или использовался ранее другими лицами.

6.4.3 Применять для формирования электронной цифровой подписи только действующий личный закрытый ключ.

6.4.4 Применять личный закрытый ключ только в соответствии с областями действия, указанными в соответствующем данному ключу сертификате ключа подписи.

6.4.5 Не использовать личный закрытый ключ, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

6.4.6 Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на аннулирование (отзыв) которого подано в *Удостоверяющий Центр*, в течение времени, исчисляемого с момента подачи заявления на аннулирование (отзыв) сертификата в *Удостоверяющий Центр* по момент времени официального уведомления *Пользователя* об аннулировании (отзыве) сертификата.

6.4.7 Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на приостановление действия которого подано в *Удостоверяющий Центр*, в течение времени, исчисляемого с момента подачи заявления на приостановление действия сертификата в *Удостоверяющий Центр* по момент времени официального уведомления *Пользователя* о приостановлении действия сертификата.

6.4.8 Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, который аннулирован (отозван) или действие которого приостановлено.

6.5 Удостоверяющий Центр обязан:

6.5.1 Использовать для изготовления закрытого ключа *Уполномоченного лица Удостоверяющего Центра* и формирования ЭЦП только сертифицированные в соответствии с правилами сертификации Российской Федерации средства криптографической защиты информации.

6.5.2 Использовать закрытый ключ *Уполномоченного лица Удостоверяющего Центра* только для подписи издаваемых им сертификатов ключей подписи *Пользователей УЦ* и *Списков отозванных сертификатов*.

6.5.3 Принять меры по защите закрытого ключа *Уполномоченного лица Удостоверяющего Центра* от несанкционированного доступа.

6.5.4 Организовать свою работу по GMT (Greenwich Mean Time, Среднее Время по Гринвичскому Меридиану) с учетом часового пояса города Екатеринбурга и синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

6.5.5 В случае изготовления Удостоверяющим Центром закрытого ключа подписи Пользователя УЦ:

- выполнять процедуру генерации ключей только с использованием сертифицированного в соответствии с правилами сертификации Российской Федерации средства криптографической защиты информации;
- обеспечить сохранение в тайне изготовленного закрытого ключа подписи *Пользователя УЦ*;

6.5.6 Обеспечить изготовление сертификатов ключей подписи *Пользователей УЦ* в соответствии с порядком, определенным в *Регламенте*.

6.5.7 Обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей подписи *Пользователей УЦ*.

6.5.8 Предоставить копии сертификатов открытых ключей ЭЦП в электронной форме, находящиеся в реестре УЦ, всем участникам обмена электронными документами, обратившимся за указанными копиями в *УЦ*.

6.5.9 Обеспечить уникальность значений открытых ключей в изготовленных сертификатах ключей подписи *Пользователей УЦ*.

6.5.10 Вносить изготавливаемые сертификаты ключей подписи *Пользователей УЦ* в *Реестр* изготовленных сертификатов ключей подписи.

6.5.11 Аннулировать (отозвать) сертификат ключа подписи *Пользователя УЦ* по заявлению на аннулирование (отзыв) сертификата ключа подписи, поступающему от его владельца, в соответствии с порядком, определенным в *Регламенте*.
6.5.12 Приостановить действие сертификата ключа подписи *Пользователя УЦ* по заявлению на приостановление действия сертификата ключа подписи, поступающему от его владельца, в соответствии с порядком, определенным в *Регламенте*.
6.5.13 Возобновить действие сертификата ключа подписи *Пользователя УЦ* по заявлению на возобновление действия сертификата ключа подписи, поступающему от его владельца, в соответствии с порядком, определенным в *Регламенте*.
6.5.14 Аннулировать (отозвать) сертификат ключа подписи *Пользователя УЦ* в случае, если истек срок, на который действие данного сертификата было приостановлено.
6.5.15 В случае плановой замены сертификата *Пользователя* в связи с предстоящим истечением срока его действия, не аннулировать (отзывать) действующий сертификат, если до истечения его срока действия остаётся не больше чем двадцать один день.
6.5.16 Опубликовывать актуальный *Список отозванных сертификатов* на сайте *Удостоверяющего Центра* по адресу http://ca.skbkontur.ru с периодичностью один раз в неделю.
6.5.17 Предоставлять *Пользователям УЦ* сертификат ключа подписи *Уполномоченного лица Удостоверяющего Центра* в электронной форме.

7. Ответственность сторон

7.1. Сторона, не исполнившая или ненадлежащим образом исполнившая свои обязательства по *Регламенту*, несет имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного другой Стороне. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

7.2. Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по *Регламенту*, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной *Регламента* своих обязательств.

7.3. *Удостоверяющий Центр* не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по *Регламенту*, а также возникшие в связи с этим убытки в случаях:

- если *Удостоверяющий Центр* обоснованно полагался на сведения, указанные в заявлении *Пользователя УЦ*;
- подделки, подлога либо иного искажения *Пользователем УЦ* либо третьими лицами информации, содержащейся в заявлении либо иных документах, предоставленных одной стороне от имени другой стороны.

7.4. *Удостоверяющий Центр* несет ответственность за убытки при использовании *Закрытого ключа подписи и сертификата ключа подписи Пользователя УЦ,* только в случае если данные убытки возникли при компрометации закрытого ключа *Уполномоченного лица Удостоверяющего Центра,* либо вследствие несоответствий сведений в сертификате ключа подписи сведениям, указанным в заявлении *Пользователя УЦ*.

7.5. Ответственность Сторон, не урегулированная положениями *Регламента,* регулируется законодательством Российской Федерации.

7.6. *УЦ* не несёт ответственности за компрометацию *Кодовой фразы* и возможность ложной аутентификации *Пользователя УЦ* и не возмещает ущерб, причиненный возникшими обстоятельствами.

8. Разрешение споров

8.1. Сторонами в споре, в случае его возникновения, считаются *Удостоверяющий Центр* и Сторона, присоединившаяся к *Регламенту*.

8.2. При рассмотрении спорных вопросов, связанных с настоящим *Регламентом*, Стороны должны руководствоваться действующим законодательством Российской Федерации.

8.3. Стороны должны принять все необходимые меры для того, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

8.4. Сторона, получившая от другой Стороны претензию, обязана в течение 20 (Двадцати) дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа.

8.5. Все споры и разногласия между Сторонами, возникающие из *Регламента* или в связи с ним, в том числе касающиеся его заключения, действия, исполнения, изменения, прекращения или действительности, и по которым не было достигнуто соглашение, разрешаются в Арбитражном суде в соответствии с действующим законодательством Российской Федерации.

9. Порядок пользования услугами Удостоверяющего Центра

9.1. Общая схема взаимодействия Пользователей УЦ с Удостоверяющим Центром
Чтобы получить сертификат ключа подписи, отозвать сертификат ключа подписи, приостановить/возобновить действие сертификата ключа подписи *Пользователь УЦ* обращается в офис одного из *Центров Регистрации* и непосредственно взаимодействует с *Уполномоченным сотрудником ЦР*.
Для оперативного удовлетворения вышеперечисленных запросов *Пользователя УЦ Уполномоченный сотрудник ЦР* взаимодействует с *Оператором Удостоверяющего Центра* по защищенному электронному каналу. Таким каналом может служить электронная почта с использованием ЭЦП и шифрования на базе персонального сертификата ключа подписи *Уполномоченного сотрудника ЦР*, либо специализированная система документооборота между *Центром Регистрации* и *Удостоверяющим Центром*, вход в которую *Уполномоченный сотрудник ЦР* осуществляет при помощи персонального сертификата ключа подписи.
В течение первых пяти рабочих дней каждого месяца *Уполномоченный сотрудник ЦР* обеспечивает доставку курьерской почтой в *Удостоверяющий Центр* следующих документов, накопившихся в *Центре Регистрации* за прошедший месяц:

- заявления **о присоединении к *Регламенту Удостоверяющего Центра*;**
- заявления на изготовление сертификатов ключей подписи *Пользователей УЦ*;
- *копии сертификатов ключей* подписи *Пользователей УЦ* на бумажном носителе;
- заявления на аннулирование (отзыв) сертификатов ключей подписи *Пользователей УЦ*;
- заявления на приостановление действия сертификатов ключей подписи *Пользователей УЦ*;

- заявления на возобновление действия сертификатов ключей подписи *Пользователей УЦ*;
- документы, необходимость доставки которых описана в должностных инструкциях *Уполномоченного сотрудника ЦР*.

9.2. Изготовление и получение ключей подписи и сертификата ключа подписи

9.2.1. Изготовление и получение ключей подписи

Изготовление новых ключей подписи *Пользователя УЦ* осуществляется при получении нового сертификата ключа подписи *Пользователя УЦ*, а также при плановой и внеплановой смене *Закрытого ключа подписи Пользователя УЦ*.

Изготовление ключей подписи *Пользователя УЦ* осуществляется либо *Пользователем УЦ* самостоятельно, либо *Уполномоченным сотрудником ЦР*. В последнем случае *Пользователь УЦ* должен выдать *Уполномоченному сотруднику ЦР* Доверенность на изготовление его ключей подписи. Форма Доверенности приведена в Приложении № 2 к *Регламенту*.

Изготовление ключей подписи *Пользователя УЦ* производится при помощи специализированных программных средств, предоставляемых *Удостоверяющим Центром*. Одновременно с изготовлением ключей подписи производится формирование файла с запросом на сертификат ключа подписи *Пользователя УЦ* в формате PKCS#10.

Данные о *Пользователе УЦ*, содержащиеся в запросе на сертификат ключа подписи *Пользователя УЦ*, должны совпадать с данными, указанными в заявлении на изготовление сертификата ключа подписи *Пользователя УЦ.* Невыполнение этого условия служит безусловной причиной для отказа в изготовлении сертификата ключа подписи *Пользователя УЦ.*

В случае если изготовление ключей подписи *УЦ* осуществляется *Уполномоченным сотрудником ЦР*, ключи, записанные на ключевой носитель, выдаются *Пользователю УЦ* по окончании процедуры изготовления сертификата ключа подписи этого *Пользователя УЦ.* При этом *Пользователь УЦ* расписывается в получении ключевого носителя в журнале регистрации, учета и выдачи ключевых документов и носителей.

9.2.2. Изготовление и получение сертификата ключа подписи

Изготовление сертификата ключа подписи *Пользователя УЦ* осуществляется *Удостоверяющим Центром* на основании заявления на изготовление сертификата ключа подписи при личном прибытии *Пользователя УЦ* в офис одного из *Центров Регистрации*. Заявление на изготовление сертификата ключа подписи заверяется собственноручной подписью владельца сертификата (*Пользователя УЦ*). Форма заявления на изготовление сертификата ключа подписи *Пользователя УЦ* приведена в Приложении № 3 к *Регламенту*.

Уполномоченный сотрудник ЦР выполняет процедуру идентификации *Пользователя УЦ* путем установления личности *Пользователя УЦ* по документам, перечень которых приведён в Приложении № 11.

После положительной идентификации *Пользователя УЦ Уполномоченный сотрудник ЦР* принимает документы и файл с запросом на сертификат ключа подписи *Пользователя УЦ*. В случае если изготовление ключей подписи доверено *Уполномоченному сотруднику ЦР,* он выполняет процедуру изготовления ключей подписи в соответствии с порядком, определенным в *Регламенте*. Затем он передает содержащуюся в принятых документах информацию и файл с запросом на сертификат ключа подписи *Пользователя УЦ Оператору Удостоверяющего Центра* на рассмотрение.

Заявление на изготовление сертификата ключа подписи *Пользователя УЦ* рассматривается *Оператором Удостоверяющего Центра* в течение 3 (Три)

рабочих дней с момента поступления. Принятое решение о выдаче сертификата ключа подписи сообщается *Уполномоченному сотруднику ЦР.*

В случае отказа в изготовлении сертификата ключа подписи *Пользователя УЦ*, заявление на изготовление сертификата ключа подписи вместе с приложениями возвращается заявителю с отметкой *Уполномоченного сотрудника ЦР*.

При принятии положительного решения, *Оператор Удостоверяющего Центра* незамедлительно изготавливает сертификат ключа подписи *Пользователя УЦ* и две *Копии сертификата ключа подписи Пользователя УЦ* на бумажном носителе по форме, определенной Приложением № 4 к *Регламенту.* Обе копии сертификата ключа подписи *Пользователя УЦ* на бумажном носителе заверяются собственноручной подписью *Пользователя УЦ*, а также собственноручной подписью *Уполномоченного лица Удостоверяющего Центра* и печатью *Удостоверяющего Центра*.

По окончании процедуры изготовления сертификата ключа подписи *Пользователю УЦ* выдаются:

- ключи, записанные на ключевой носитель, если их изготовление было доверено *Уполномоченному сотруднику ЦР*;
- сертификат ключа подписи *Пользователя УЦ* в электронной форме, соответствующий его закрытому ключу;
- *Копия сертификата ключа* подписи *Пользователя УЦ* на бумажном носителе;
- *Копия сертификата ключа подписи Уполномоченного лица Удостоверяющего Центра* в электронной форме.

Указанные выше данные, передаваемые *Пользователю УЦ* в электронной форме (кроме ключей), записываются в виде файлов на электронный носитель, предоставляемый *Центром Регистрации*.

В случае принятия *Оператором Удостоверяющего Центра* положительного решения об изготовлении сертификата ключа подписи *Пользователя УЦ*, *Уполномоченный сотрудник ЦР* обеспечивает доставку заявления на изготовление сертификата ключа подписи *Пользователя УЦ* и одной *Копии сертификата ключа подписи Пользователя УЦ* на бумажном носителе в *Удостоверяющий Центр* в соответствии с порядком, определенным в *Регламенте.*

9.3. Аннулирование (отзыв) сертификата ключа подписи

Для осуществления аннулирования (отзыва) сертификата ключа подписи *Пользователь УЦ* подает письменное заявление на аннулирование (отзыв) принадлежащего ему сертификата ключа подписи в свой *Центр Регистрации*, либо использует услугу удаленного управления сертификатом ключа подписи согласно разделу 9.5. *Регламента.*

Заявление на аннулирование (отзыв) сертификата ключа подписи заверяется собственноручной подписью владельца сертификата (*Пользователя УЦ*). Форма заявления на аннулирование (отзыв) сертификата ключа подписи *Пользователя УЦ* приведена в Приложении № 5 к *Регламенту*.

Уполномоченный сотрудник ЦР выполняет процедуру идентификации *Пользователя УЦ* путем установления личности по документам, перечень которых приведён в Приложении № 11.

После положительной идентификации *Пользователя УЦ Уполномоченный сотрудник ЦР* принимает заявление на аннулирование (отзыв) сертификата ключа подписи *Пользователя УЦ* и передает содержащуюся в нем информацию *Оператору Удостоверяющего Центра* на рассмотрение.

Заявление на аннулирование (отзыв) сертификата ключа подписи *Пользователя УЦ* рассматривается *Оператором Удостоверяющего Центра* в течение 3 (Три) рабочих дней с момента поступления. Принятое решение об аннулировании (отзыве) сертификата сообщается *Уполномоченному сотруднику ЦР.*

При принятии положительного решения, *Оператор Удостоверяющего Центра* выполняет действия по аннулированию (отзыву) сертификата ключа подписи *Пользователя УЦ* с серийным номером, указанным в заявлении.

Оповещение *Пользователя УЦ* об аннулировании (отзыве) его сертификата ключа подписи производится в течение одной недели с момента выполнения *Оператором Удостоверяющего Центра* действий по аннулированию (отзыву) сертификата ключа подписи *Пользователя УЦ* путем публикации актуального *Списка отозванных сертификатов* на сайте *Удостоверяющего Центра* в соответствии с *Регламентом.*

Временем аннулирования (отзыва) сертификата ключа подписи *Пользователя УЦ* признается время официального уведомления *Пользователя УЦ* об аннулировании (отзыве) данного сертификата.

В случае принятия *Оператором Удостоверяющего Центра* положительного решения об аннулировании (отзыве) сертификата ключа подписи *Пользователя УЦ*, *Уполномоченный сотрудник ЦР* обеспечивает доставку заявления на аннулирование (отзыв) сертификата ключа подписи *Пользователя УЦ* в *Удостоверяющий Центр* в соответствии с порядком, определенным в *Регламенте.*

9.4. Приостановление/возобновление действия сертификата ключа подписи

9.4.1. Приостановление действия сертификата ключа подписи

Для приостановления действия сертификата ключа подписи *Пользователь УЦ* подает заявление на приостановление действия принадлежащего ему сертификата ключа подписи в свой *Центр Регистрации*, либо использует услугу удаленного управления сертификатом ключа подписи согласно разделу 9.5. *Регламента*.

Заявление на приостановление действия сертификата ключа подписи заверяется собственноручной подписью владельца сертификата (*Пользователя УЦ*). Форма заявления на приостановление действия сертификата ключа подписи *Пользователя УЦ* приведена в Приложении № 6 к *Регламенту*.

Уполномоченный сотрудник ЦР выполняет процедуру идентификации *Пользователя УЦ* путем установления личности по документам, перечень которых приведён в Приложении № 11.

После положительной идентификации *Пользователя УЦ Уполномоченный сотрудник ЦР* принимает заявление на приостановление действия сертификата ключа подписи *Пользователя УЦ* и передает содержащуюся в нем информацию *Оператору Удостоверяющего Центра* на рассмотрение.

Заявление на приостановление действия сертификата ключа подписи *Пользователя УЦ* рассматривается *Оператором Удостоверяющего Центра* в течение 3 (Три) рабочих дней с момента поступления. Принятое решение о приостановлении действия сертификата сообщается *Уполномоченному сотруднику ЦР.*

При принятии положительного решения, *Оператор Удостоверяющего Центра* приостанавливает действие сертификата ключа подписи *Пользователя УЦ* с серийным номером, указанным в заявлении.

Оповещение *Пользователя УЦ* о приостановлении действия его сертификата ключа подписи производится в течение одной недели с момента приостановления *Оператором Удостоверяющего Центра* действия сертификата ключа подписи *Пользователя УЦ* путем публикации актуального *Списка отозванных сертификатов* на сайте *Удостоверяющего Центра* в соответствии с *Регламентом.*

Временем приостановления действия сертификата ключа подписи *Пользователя УЦ* признается время официального уведомления *Пользователя УЦ* о приостановлении действия данного сертификата.

В случае если в течение срока приостановления действия сертификата ключа подписи *Пользователя УЦ* в *Удостоверяющий Центр* не поступает заявление от

Пользователя УЦ о возобновлении действия этого сертификата, сертификат аннулируется (отзывается) *Удостоверяющим Центром*.

В случае принятия *Оператором Удостоверяющего Центра* положительного решения о приостановлении действия сертификата ключа подписи *Пользователя УЦ, Уполномоченный сотрудник ЦР* обеспечивает доставку заявления на приостановление действия сертификата ключа подписи *Пользователя УЦ* в *Удостоверяющий Центр* в соответствии с порядком, определенным в *Регламенте.*

9.4.2. Возобновление действия сертификата ключа подписи

Возобновление действия сертификата ключа подписи *Пользователя УЦ* возможно только в течение срока, на который было приостановлено действие этого сертификата.

Для осуществления возобновления действия сертификата ключа подписи *Пользователь УЦ* подает заявление на возобновление действия принадлежащего ему сертификата ключа подписи в офис одного из *Центров Регистрации*, либо использует услугу удаленного управления сертификатом ключа подписи согласно разделу 9.5. *Регламента*.

Заявление на возобновление действия сертификата ключа подписи заверяется собственноручной подписью владельца сертификата (*Пользователя УЦ*). Форма заявления на возобновление действия сертификата ключа подписи *Пользователя УЦ* приведена в Приложении № 7 к *Регламенту*.

Уполномоченный сотрудник ЦР выполняет процедуру идентификации *Пользователя УЦ* путем установления личности по документам, перечень которых приведён в Приложении № 11.

После положительной идентификации *Пользователя УЦ Уполномоченный сотрудник ЦР* принимает заявление на возобновление действия сертификата ключа подписи *Пользователя УЦ* и передает содержащуюся в нем информацию *Оператору Удостоверяющего Центра* на рассмотрение.

Заявление на возобновление действия сертификата ключа подписи *Пользователя УЦ* рассматривается *Оператором Удостоверяющего Центра* в течение 3 (Три) рабочих дней с момента поступления. Принятое решение о возобновлении действия сертификата сообщается *Уполномоченному сотруднику ЦР.*

При принятии положительного решения, *Оператор Удостоверяющего Центра* выполняет действия по возобновлению действия сертификата ключа подписи *Пользователя УЦ* с серийным номером, указанным в заявлении.

Оповещение *Пользователя УЦ* о возобновлении действия его сертификата ключа подписи производится в течение одной недели с момента выполнения *Оператором Удостоверяющего Центра* действий по возобновлению действия сертификата ключа подписи *Пользователя УЦ* путем публикации актуального *Списка отозванных сертификатов* на сайте *Удостоверяющего Центра* в соответствии с *Регламентом.*

Временем возобновления действия сертификата ключа подписи *Пользователя УЦ* признается время официального уведомления *Пользователя УЦ* о возобновлении действия данного сертификата.

В случае принятия *Оператором Удостоверяющего Центра* положительного решения о возобновлении действия сертификата ключа подписи *Пользователя УЦ, Уполномоченный сотрудник ЦР* обеспечивает доставку заявления на возобновление действия сертификата ключа подписи *Пользователя УЦ* в *Удостоверяющий Центр* в соответствии с порядком, определенным в *Регламенте.*

9.5. Удаленное управление сертификатом ключа подписи с аутентификацией Пользователя УЦ по Кодовой фразе, связанные с этим риски.

9.5.1. Удаленное управление сертификатом ключа подписи с аутентификацией Пользователя УЦ по Кодовой фразе

Услуга удаленное управление сертификатом ключа подписи позволяет *Пользователю УЦ* выполнить следующие действия: аннулирование (отзыв) действия сертификата ключа подписи и приостановление/возобновление действия сертификата ключа подписи без подачи заявления в *Центр Регистрации.*

Для возможности выполнения перечисленных действий *Пользователь УЦ* по средствам телефонной связи сообщает *Оператору Удостоверяющего Центра* данные своего сертификата ключа подписи, которые включают в себя: фамилию, имя, отчество *Владельца сертификата ключа подписи*, наименование организации, представителем, которой является *Пользователь УЦ*, и другие сведения, необходимые *Оператору* для поиска сертификата в базе данных УЦ, этой организации и *Кодовую фразу.*

Оператор Удостоверяющего Центра проводит аутентификацию *Пользователя УЦ* по *Кодовой фразе.*

После положительной аутентификации *Пользователя УЦ* по *Кодовой фразе Оператор Удостоверяющего Центра* принимает решение о совершении действий по аннулированию (отзыву), либо приостановлению/возобновлению действия сертификата ключа подписи.

При принятии положительного решения, *Оператор Удостоверяющего Центра* выполняет действия по аннулированию (отзыву) либо приостановлению/возобновлению действия сертификата ключа подписи сертификата, указанного *Пользователем УЦ.*

Пользователь УЦ по своему желанию может заказать услугу удаленного управления сертификатом ключа подписи при формировании запроса на сертификат ключа подписи, либо заказать ее путем составления отдельного заявление на пользование этой услугой. (Приложение №9)

Пользователь УЦ в любое время может отказаться от услуги удаленного управления сертификатом ключа подписи, путём подачи заявления в *Центр Регистрации* об отказе от данной услуги. (Приложение №10)

Заявление на заказ услуги и отказ от нее заверяется собственноручной подписью *Пользователя УЦ.*

При заказе услуги *Пользователем УЦ* во время оформления запроса на сертификат ключа подписи необходимо указать *Кодовую фразу*, по которой и будет происходить его аутентификация в запросе на сертификат.

9.5.2. Риски, связанные с использованием услуги удаленного управления сертификатом ключа подписи с аутентификацией Пользователя УЦ по Кодовой фразе.

Пользователь УЦ несет риск компрометации *Кодовой фразы* и ложной аутентификации и связанных с этим последствий ненужного аннулирования (отзыва) либо приостановления /возобновления действия сертификата ключа подписи.

9.6. Предоставление копий сертификатов открытых ключей ЭЦП в электронной форме, находящихся в реестре *УЦ*, всем участникам обмена электронными документами, обратившимся за указанными копиями в *УЦ.*

Чтобы получить копии сертификатов открытых ключей ЭЦП в электронной форме, находящиеся в реестре *УЦ*, участник информационных систем направляет письмо в адрес одного из *Центров Регистрации* с запросом на предоставление копии сертификата открытого ключа ЭЦП в электронной форме. В запросе необходимо указать известную информацию, позволяющую идентифицировать сертификат в реестре сертификатов *УЦ*. При необходимости, для идентификации запрашиваемого сертификата и (или) для его получения *Уполномоченный сотрудник ЦР* взаимодействует с *Оператором Удостоверяющего Центра.* Если указанной в запросе информации достаточно для однозначной идентификации

сертификата в реестре *УЦ*, то *Уполномоченный сотрудник ЦР* предоставляет участнику обмена электронными документами копию сертификата открытого ключа ЭЦП в электронном виде.

9.7. Подтверждение подлинности ЭЦП Уполномоченного лица Удостоверяющего Центра в выданных сертификатах ключей подписи

Для подтверждения подлинности ЭЦП *Уполномоченного лица Удостоверяющего Центра* в изданном им сертификате ключа подписи *Пользователь УЦ* подает в офис одного из *Центров Регистрации* заявление на подтверждение подлинности ЭЦП *Уполномоченного лица Удостоверяющего Центра* в сертификате ключа подписи *Пользователя УЦ*. Форма заявления на подтверждение подлинности ЭЦП *Уполномоченного лица Удостоверяющего Центра* в сертификате ключа подписи *Пользователя УЦ* приведена в Приложении № 8 к *Регламенту*.

Обязательным приложением к заявлению на подтверждение подлинности ЭЦП *Уполномоченного лица Удостоверяющего Центра* в сертификате ключа подписи *Пользователя УЦ* является сменный магнитный носитель, содержащий файл сертификата ключа подписи *Пользователя УЦ* формата PKCS#7 в кодировке Base64, подвергающегося процедуре проверки.

Уполномоченный сотрудник ЦР выполняет процедуру идентификации *Пользователя УЦ* путем установления личности по документам, перечень которых приведён в Приложении № 11.

После положительной идентификации *Пользователя УЦ Уполномоченный сотрудник ЦР* принимает заявление на подтверждение подлинности ЭЦП *Уполномоченного лица Удостоверяющего Центра* в сертификате ключа подписи *Пользователя УЦ* и передает содержащуюся в нем информацию *Оператору Удостоверяющего Центра* на рассмотрение.

Проведение работ по подтверждению подлинности ЭЦП *Уполномоченного лица Удостоверяющего Центра* в сертификате ключа подписи *Пользователя УЦ* осуществляет комиссия, сформированная из числа сотрудников *Удостоверяющего Центра*.

Срок проведения работ по подтверждению подлинности ЭЦП *Уполномоченного лица Удостоверяющего Центра* в сертификате ключа подписи *Пользователя УЦ* составляет 15 (Пятнадцать) рабочих дней с момента поступления заявления в *Удостоверяющий Центр*.

Результатом проведения работ по подтверждению подлинности ЭЦП *Уполномоченного лица Удостоверяющего Центра* в сертификате ключа подписи *Пользователя УЦ* является заключение *Удостоверяющего Центра* в письменной форме, подписанное всеми членами комиссии и заверенное печатью *Удостоверяющего Центра*. Заключение содержит:

- результат проверки ЭЦП *Уполномоченного лица Удостоверяющего Центра* (ЭЦП *Уполномоченного лица Удостоверяющего Центра* в сертификате ключа подписи *Пользователя УЦ* верна/неверна);
- на момент времени, указанного в заявлении, сертификат ключа подписи *Пользователя УЦ* действовал/не действовал;
- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- содержание и результаты проверки с указанием примененных методов;
- обоснование результатов проверки;
- данные, представленные для проведения проверки.

Отчет по выполненной проверке составляется в простой письменной форме и заверяется собственноручными подписями всех членов комиссии.
Уполномоченному сотруднику ЦР сообщаются результаты работы комиссии и высылается курьерской почтой заключение о произведенной проверке. *Уполномоченный сотрудник ЦР* обеспечивает доставку заключения *Пользователю УЦ*.

9.8. Подтверждение подлинности ЭЦП в электронных документах
По желанию Стороны, присоединившейся к *Регламенту*, *Удостоверяющий центр* осуществляет проведение экспертных работ по подтверждению электронной цифровой подписи в электронном документе.
Состав экспертной комиссии, набор исходных данных для проведения указанной экспертизы, состав и содержание отчетных документов (акты, заключения и т.д.), сроки проведения работ, размер вознаграждения *Удостоверяющего центра* определяются Сторонами на основании заключаемого соглашения (договора).

10. Прочие условия

10.1. Конфиденциальность
Типы конфиденциальной информации
10.1.1. Закрытый ключ, соответствующий сертификату ключа подписи *Пользователя УЦ* является конфиденциальной информацией данного *Пользователя УЦ. Удостоверяющий Центр* не осуществляет хранение закрытых ключей *Пользователей УЦ*.
Персональная информация *Пользователей УЦ*, содержащаяся в *Удостоверяющем Центре*, не подлежащая непосредственной рассылке в качестве части сертификата ключа подписи, считается конфиденциальной.
10.1.2. Типы информации, не являющейся конфиденциальной
Информация, не являющаяся конфиденциальной, считается открытой.
Информация, содержащаяся в *Регламенте*, не является конфиденциальной.
Информация, включаемая в сертификаты ключей подписи *Пользователей УЦ* и *Списки отозванных сертификатов*, издаваемых *Удостоверяющим Центром*, не является конфиденциальной.
Тем не менее, информационный массив, представляющий собой совокупность персональных сведений абонентов (базы данных, *Реестр* изготовленных сертификатов), подлежит защите в соответствии с режимом, принятым для конфиденциальной информации.
Открытая информация может публиковаться по решению *Удостоверяющего Центра*. Место, способ и время публикации открытой информации определяется *Удостоверяющим Центром*.
10.1.3. Исключительные полномочия Удостоверяющего центра
Удостоверяющий Центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации.

10.2. Плановая смена ключей Уполномоченного лица Удостоверяющего Центра
Плановая смена ключей (*Закрытого* и соответствующего ему *Открытого ключа подписи*) *Уполномоченного лица Удостоверяющего Центра* выполняется не ранее, чем через 1 (Один) год и не позднее, чем через 2 (Два) года после начала действия закрытого ключа (сертификата ключа подписи) *Уполномоченного лица Удостоверяющего Центра*.
Процедура плановой смены ключей *Уполномоченного лица Удостоверяющего Центра* осуществляется в следующем порядке:

- *Уполномоченное лицо Удостоверяющего Центра* формирует новый *Закрытый* и *соответствующий ему Открытый ключ;*
- *Уполномоченное лицо Удостоверяющего Центра* изготавливает сертификат нового ключа подписи и подписывает его электронной цифровой подписью с использованием нового закрытого ключа.

Старый закрытый ключ *Уполномоченного лица Удостоверяющего Центра* используется в течение своего срока действия для формирования *Списков отозванных сертификатов* из числа тех сертификатов, которые были изданы *Удостоверяющим Центром* в период действия старого закрытого ключа *Уполномоченного лица Удостоверяющего Центра*.

10.3. Внеплановая смена ключей Уполномоченного лица Удостоверяющего Центра

В случае компрометации или угрозы компрометации закрытого ключа *Уполномоченного лица Удостоверяющего Центра* выполняется внеплановая смена ключей *Уполномоченного лица Удостоверяющего Центра*.

Процедура внеплановой смены ключей *Уполномоченного лица Удостоверяющего Центра* выполняется в порядке, определенном процедурой плановой смены ключей *Уполномоченного лица Удостоверяющего Центра*.

Сертификаты ключей подписи *Пользователей УЦ* аннулируются (отзываются) путем занесения в *Список отозванных сертификатов*.

После выполнения процедуры внеплановой смены ключей, сертификат ключа подписи *Уполномоченного лица Удостоверяющего Центра* аннулируется (отзывается) путем занесения в *Список отозванных сертификатов*.

Список отозванных сертификатов подписывается старым закрытым ключом (подвергшимся процедуре внеплановой смены) *Уполномоченного лица Удостоверяющего Центра*.

Удостоверяющий Центр официально уведомляет *Пользователей УЦ* о факте внеплановой смены ключа *Уполномоченного лица Удостоверяющего Центра*.

После получения официального уведомления о факте внеплановой смены ключа *Уполномоченного лица Удостоверяющего Центра Пользователям УЦ* необходимо выполнить процедуру получения новых ключей и сертификатов ключей подписи в соответствии с порядком, установленным *Регламентом*.

10.4. Компрометация ключа Владельца сертификата ключа подписи

Владелец сертификата ключа подписи самостоятельно принимает решение о факте или угрозе компрометации своего закрытого ключа.

В случае компрометации или угрозы компрометации закрытого ключа *Владелец сертификата ключа подписи* подает в *Удостоверяющий Центр* заявление на аннулирование (отзыв) своего сертификата ключа подписи либо использует услугу удаленного управления сертификатом ключа подписи согласно разделу 9.5. *Регламента.*

10.5. Использования факсимиле подписи Уполномоченного лица УЦ

Регламент устанавливает возможность использования факсимиле подписи (клише с подписи) *Уполномоченного лица УЦ* на подписание сертификатов ключей подписи *Пользователей УЦ* и списков отозванных сертификатов. Документы, подписанные факсимиле *Уполномоченного лица* имеют такую же юридическую силу, как и документы, подписанные *Уполномоченным лицом* собственноручно.

10.6. Прекращение оказания услуг Удостоверяющим Центром

Прекращение оказания услуг *Удостоверяющим центром* может быть произведено на основании одностороннего решения ЗАО «ПФ «СКБ КОНТУР» в порядке, установленном законодательством Российской Федерации.

Все сертификаты ключей подписи, изготовленные *Удостоверяющим Центром,* аннулируются (отзываются).

10.7. Сроки действия ключей и сертификатов ключей подписи

10.7.1. Сроки действия ключей Уполномоченного лица Удостоверяющего Центра

Срок действия закрытого ключа *Уполномоченного лица Удостоверяющего Центра* составляет 3 (Три) года. Начало периода действия закрытого ключа *Уполномоченного лица Удостоверяющего Центра* исчисляется с даты и времени начала действия сертификата ключа подписи *Уполномоченного лица Удостоверяющего Центра*.

Срок действия сертификата ключа подписи, соответствующего закрытому ключу *Уполномоченного лица Удостоверяющего Центра,* составляет 6 (Шесть) лет.

10.7.2. Сроки действия ключей Владельцев сертификатов ключей подписи

Срок действия закрытого ключа *Владельца сертификата ключа подписи* составляет не более 1 (Одного) года. Начало периода действия закрытого ключа *Владельца сертификата ключа подписи* исчисляется с даты и времени начала действия сертификата ключа подписи владельца сертификата.

Срок действия сертификата ключа подписи, соответствующего закрытому ключу *Владельца сертификата ключа подписи,* составляет не более 1 (Одного) года.

10.8. Хранение сертификатов ключей подписи в Удостоверяющем Центре

Хранение в *Удостоверяющем Центре* сертификатов ключей подписи *Пользователей УЦ* осуществляется в течение всего периода их действия и 5 (Пять) лет после их аннулирования (отзыва) или истечения срока их действия.

По истечении указанного срока хранения сертификаты ключей подписи переводятся в режим архивного хранения.

10.9. Архивное хранение

Документы *Удостоверяющего Центра* на бумажных носителях хранятся в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

Перечень документов *Удостоверяющего Центра*, подлежащих архивному хранению:

- Аннулированные (отозванные) сертификаты ключей подписи *Уполномоченного лица Удостоверяющего Центра*;
- Аннулированные (отозванные) сертификаты ключей подписи *Пользователей УЦ*;
- Заявления о присоединении к *Регламенту Удостоверяющего Центра*;
- Заявления на изготовление сертификатов ключей подписи *Пользователей УЦ*;
- *Копии сертификатов* ключей подписи *Пользователей УЦ* на бумажном носителе;
- Заявления на аннулирование (отзыв) сертификатов ключей подписи *Пользователей УЦ*;
- Заявления на приостановление действия сертификатов ключей подписи *Пользователей УЦ*;
- Заявления на возобновление действия сертификатов ключей подписи *Пользователей УЦ*;
- Служебные документы *Удостоверяющего Центра*.

Документы *Удостоверяющего Центра*, подлежащие архивному хранению, являются документами временного хранения. Срок хранения архивных документов – 5 (Пять) лет.

Выделение архивных документов к уничтожению и их уничтожение осуществляется комиссией, формируемой из числа сотрудников *Удостоверяющего Центра*.

10.10. Структура сертификатов ключей подписи и Списка отозванных сертификатов

Удостоверяющий центр издает сертификаты открытых ключей *Пользователей УЦ* в электронной форме формата X.509 версии 3 и *Списки отозванных сертификатов* (СОС) в электронной форме формата X.509 версии 2.

Структура сертификата ключа подписи *Уполномоченного лица Удостоверяющего Центра* приведена в Приложении № 12 к *Регламенту*.

Структура сертификата ключа подписи *Пользователя УЦ* приведена в Приложении № 13 к *Регламенту*.

Структура *Списка отозванных сертификатов* приведена в Приложении № 14 к *Регламенту*.

4. Информация о разработчике

«Система защищенного электронного документооборота «Контур-Экстерн», версия 6.0
ЗАО «ПФ «СКБ Контур»
Россия, г. Екатеринбург, пр. Космонавтов, 56
Телефон/Факс: (343) 270-55-66
E-mail: gni@skbkontur.ru