Приложение 2

к приказу ОПФР по Тверской области

от

«Приложение 2

к приказу Управляющего ОПФР по Тверской области

от 26.10.2015 № 302

**РЕГЛАМЕНТ**

работы Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области
при выполнении функций аккредитованного удостоверяющего центра

2018

Оглавление

[ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 4](#_Toc511997670)

[Перечень сокращений 7](#_Toc511997671)

[1. ВВЕДЕНИЕ 8](#_Toc511997672)

[1.1. Назначение Регламента 8](#_Toc511997673)

[1.2. Идентификация Регламента 8](#_Toc511997674)

[1.3. Публикация Регламента 8](#_Toc511997675)

[1.4. Область применения Регламента 8](#_Toc511997676)

[1.5. Срок действия Регламента 8](#_Toc511997677)

[1.6. Присоединение к Регламенту 8](#_Toc511997678)

[1.7. Порядок утверждения и внесения изменений в Регламент 8](#_Toc511997679)

[2. ОБЩИЕ ПОЛОЖЕНИЯ 10](#_Toc511997680)

[2.1. Основания осуществления деятельности Удостоверяющего центра 10](#_Toc511997681)

[2.2. Информация о месте нахождения, местах осуществления деятельности и графике работы Удостоверяющего центра 10](#_Toc511997682)

[2.3. Контактная информация Удостоверяющего центра 10](#_Toc511997683)

[2.4. Стоимость услуг Удостоверяющего центра 10](#_Toc511997684)

[2.5. Пользователи Удостоверяющего центра 10](#_Toc511997685)

[2.6. Разрешение споров 10](#_Toc511997686)

[2.7. Прекращение деятельности Удостоверяющего центра 11](#_Toc511997687)

[3. ОКАЗЫВАЕМЫЕ УСЛУГИ И РЕАЛИЗУЕМЫЕ ФУНКЦИИ 12](#_Toc511997688)

[3.1. Услуги, оказываемые Удостоверяющим центром 12](#_Toc511997689)

[3.2. Функции, реализуемые Удостоверяющим центром 12](#_Toc511997690)

[4. ПРАВА 15](#_Toc511997691)

[4.1. Права Удостоверяющего центра 15](#_Toc511997692)

[4.2. Права Пользователей Удостоверяющего центра 16](#_Toc511997693)

[5. ОБЯЗАННОСТИ 17](#_Toc511997694)

[5.1. Обязанности Удостоверяющего центра 17](#_Toc511997695)

[5.2. Обязанности Пользователя 20](#_Toc511997696)

[6. ОТВЕТСТВЕННОСТЬ 22](#_Toc511997697)

[6.1. Ответственность Удостоверяющего центра 22](#_Toc511997698)

[6.2. Ответственность Пользователя 22](#_Toc511997699)

[7. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ 23](#_Toc511997700)

[7.1. Виды конфиденциальной информации 23](#_Toc511997701)

[7.2. Виды информации, не относящейся к конфиденциальной 23](#_Toc511997702)

[7.3. Предоставление конфиденциальной информации 23](#_Toc511997703)

[8. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 24](#_Toc511997704)

[9. ПОРЯДОК ОКАЗАНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ 25](#_Toc511997705)

[9.1. Регистрация Пользователей Удостоверяющего центра 25](#_Toc511997706)

[9.2. Идентификация Пользователя Удостоверяющего центра 25](#_Toc511997707)

[9.3. Создание ключа электронной подписи и запроса на сертификат 25](#_Toc511997708)

[9.4. Создание и выдача квалифицированного сертификата ключа проверки электронной подписи 25](#_Toc511997709)

[9.5. Сроки действия ключей электронной подписи Пользователя 27](#_Toc511997710)

[9.6. Смена ключей электронной подписи Пользователя 27](#_Toc511997711)

[9.6.1. Плановая смена ключей электронной подписи Пользователя 27](#_Toc511997712)

[9.6.2. Внеплановая смена ключей электронной подписи Пользователя 28](#_Toc511997713)

[9.6.3. Аннулирование квалифицированного сертификата 28](#_Toc511997714)

[9.6.4. Прекращение действия квалифицированного сертификата 28](#_Toc511997715)

[9.7. Смена ключей электронной подписи Удостоверяющего центра 29](#_Toc511997716)

[9.7.1. Сроки действия ключей электронной подписи Удостоверяющего центра 29](#_Toc511997717)

[9.7.2. Плановая смена ключей электронной подписи Удостоверяющего центра 29](#_Toc511997718)

[9.7.3. Внеплановая смена ключей электронной подписи Удостоверяющего центра 29](#_Toc511997719)

[9.8. Подтверждение подлинности электронной подписи Удостоверяющего центра в выданных квалифицированных сертификатах 29](#_Toc511997720)

[9.9. Подтверждение подлинности электронной подписи Пользователя в электронном документе 30](#_Toc511997721)

[9.10. Механизм доказательства обладания ключом электронной подписи 31](#_Toc511997722)

[9.11. Проверка уникальности ключей ЭП 31](#_Toc511997723)

[9.12. Порядок предоставления доступа к реестру квалифицированных сертификатов Удостоверяющего центра 31](#_Toc511997724)

[9.13. Порядок регистрации Пользователей в Единой системе идентификации и аутентификации 31](#_Toc511997725)

[10. СОДЕРЖАНИЕ И ФОРМА КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА 32](#_Toc511997726)

[11. СТРУКТУРА СПИСКА АННУЛИРОВАННЫХ СЕРТИФИКАТОВ 33](#_Toc511997727)

[12. МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 34](#_Toc511997728)

[13. ПРИЛОЖЕНИЯ: 35](#_Toc511997729)

[Приложение 1 36](#_Toc511997730)

[Приложение 2 37](#_Toc511997731)

[Приложение 3 38](#_Toc511997732)

[Приложение 4 40](#_Toc511997733)

[Приложение 5 41](#_Toc511997734)

[Приложение 6 42](#_Toc511997735)

[Приложение 7 43](#_Toc511997736)

[Приложение 8 44](#_Toc511997737)

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

***Аккредитованный удостоверяющий центр*** - удостоверяющий центр, прошедший процедуру признания уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» (далее - Федеральный закон «Об электронной подписи»).

***Аутентификация*** - проверка принадлежности субъекту доступа предъявленного им идентификатора.

***Владелец сертификата ключа проверки электронной подписи (далее - владелец сертификата)*** - лицо, которому в установленном Федеральным законом «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

***Доверенное лицо Удостоверяющего центра*** - третье лицо, наделенное Удостоверяющим центром полномочиями по вручению сертификатов ключей проверки электронных подписей от имени Удостоверяющего центра и осуществляющее функции по установлению личности получателя сертификата (Заявителя) либо полномочия лица, выступающего от имени Заявителя, по обращению за получением сертификата.

***Единая система идентификации и аутентификации*** - федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

***Запрос на сертификат ключа проверки электронной подписи*** - электронное сообщение определенного формата и синтаксиса, созданное в соответствии со стандартом PKCS#10 и содержащее необходимую информацию для создания сертификата.

***Заявитель*** – орган ПФР на территории Тверской области, обратившийся в Удостоверяющий центр за получением сертификата ключа проверки электронной подписи.

***Идентификация*** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

***Изменение статуса сертификата*** – аннулирование сертификата, прекращение действия сертификата.

***Информационная система общего пользования*** - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

***Информационная система Удостоверяющего центра*** – автоматизированная информационная система, обеспечивающая регистрацию Пользователей в Удостоверяющем центре и выполнение сервисных операций в процессе создания и выдачи Пользователям квалифицированных сертификатов ключей проверки электронных подписей.

***Квалифицированная электронная подпись*** - электронная подпись, которая соответствует всем признакам квалифицированной электронной подписи, определенным Федеральным законом «Об электронной подписи».

***Квалифицированный сертификат ключа проверки электронной подписи (далее -квалифицированный сертификат)*** - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - Уполномоченный федеральный орган).

***Ключ электронной подписи (далее - ключ ЭП)*** - уникальная последовательность символов, предназначенная для создания электронной подписи.

***Ключ проверки электронной подписи (далее - ключ проверки ЭП)*** - уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности электронной подписи (далее - проверка ЭП).

***Ключевой носитель*** - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.

***Ключевой документ*** - физический носитель определенной структуры, содержащий ключевую информацию (ключи электронной подписи).

***Компрометация ключа электронной подписи*** - нарушение конфиденциальности ключа электронной подписи, связанное с утратой доверия к тому, что используемый ключ электронной подписи недоступен посторонним лицам или подозрением, что ключ электронной подписи был временно доступен неуполномоченным лицам.

***Конфиденциальная информация*** - сведения, независимо от формы их предоставления, которые не могут быть переданы лицом, получившим доступ к данным сведениям, третьим лицам без согласия их владельца, а также информация, доступ к которой ограничен в соответствии с действующим законодательством Российской Федерации.

***Корпоративная информационная система*** - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

***Несанкционированный доступ к информации*** - доступ к информации в нарушение должностных полномочий работника или доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

***Плановая смена ключей электронной подписи*** - смена ключей электронной подписи, производимая в период действия ключей электронной подписи в соответствии с установленной в Удостоверяющем центре периодичностью, не вызванная компрометацией ключей электронной подписи.

***Пользователь Удостоверяющего центра (далее - Пользователь)*** — работник органа ПФР, который указан в качестве владельца сертификата наряду с указанием наименования юридического лица в выданном Удостоверяющим центром сертификате ключа проверки электронной подписи.

***Пункт регистрации*** - территориальный орган ПФР, осуществляющие от имени Удостоверяющего центра функции по регистрации пользователей, вручению квалифицированных сертификатов ключей проверки электронных подписей и иные функции, предусмотренные Федеральным законом «Об электронной подписи».

***Регистрационная информация пользователя*** - информация, предоставляемая Пользователем в целях создания квалифицированного сертификата ключа проверки электронной подписи.

***Регистрации Пользователя в Удостоверяющем центре*** – внесение регистрационной информации пользователя в базу данных Удостоверяющего центра.

***Реестр Пользователей*** – база данных Удостоверяющего центра, содержащая регистрационную информацию Пользователей.

***Реестр сертификатов*** - база данных Удостоверяющего центра, содержащая сведения о созданных Удостоверяющим центром сертификатах.

***Сертификат ключа проверки электронной подписи (далее - сертификат)*** - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

***Список аннулированных сертификатов*** - электронный документ или отдельный раздел Реестра сертификатов представляющий собой перечень уникальных серийных номеров сертификатов, которые были аннулированы или действие которых было прекращено Удостоверяющим центром до истечения срока их действия, а также информацию о датах и об основаниях аннулирования или прекращения действия этих сертификатов.

***Средства криптографической зашиты информации (далее - СКЗИ)*** - аппаратные, программные и аппаратно-программные средства, системы и комплексы, осуществляющие криптографические преобразования информации для обеспечения ее защиты от несанкционированного доступа, от навязывания ложной информации и/или обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием ключа электронной подписи, подтверждение с использованием ключа проверки электронной подписи подлинности электронной подписи, создание ключей электронной подписи и ключей проверки электронной подписи.

***Средства электронной подписи (далее - средства ЭП)*** - 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.

***Средства удостоверяющего центра (далее - средства УЦ)*** - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

***Удостоверяющий центр (далее - УЦ)*** - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом «Об электронной подписи».

***Уполномоченное лицо Удостоверяющего центра –*** физическое лицо, являющееся работником удостоверяющего центра и наделенное полномочиями по заверению своей электронной цифровой подписью изготавливаемых Удостоверяющим центром Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области сертификатов ключей подписи пользователей и заверению собственноручной подписью и печатью УЦ сертификатов ключей подписи на бумажном носителе.

***Электронный документ (далее - ЭД)*** - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

***Электронная подпись (далее - ЭП)*** - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

***Lotus*** - торговая марка программных продуктов компании IBM.

***ViPNet*** – торговая марка программных продуктов компании «ИнфоТеКС».

# Перечень сокращений

САС – список аннулированных сертификатов

ИНН – идентификационный номер налогоплательщика

НСД – несанкционированный доступ

ОГРН – основной государственный регистрационный номер

ОС – операционная система

ПК – программный комплекс

ПО – программное обеспечение

СНИЛС – страховой номер индивидуального лицевого счета

УЦ – Удостоверяющий центр

ЭП – электронная подпись

# 1. ВВЕДЕНИЕ

Государственное учреждение – Отделение Пенсионного фонда Российской Федерации по Тверской области (далее - Отделение) выполняет функции аккредитованного Удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи» и является ответчиком по всем юридическим вопросам деятельности Удостоверяющего центра.

# 1.1. Назначение Регламента

Настоящий Регламент определяет порядок реализации функций удостоверяющего центра и предоставления им услуг по созданию и выдаче квалифицированных сертификатов, включая права, обязанности и ответственность Удостоверяющего центра и Пользователей Удостоверяющего центра (далее - стороны), процедуры взаимодействия сторон, форматы документов и данных, а также основные организационно-технические меры по обеспечению информационной безопасности при использовании ключевой информации и средств электронной подписи.

# 1.2. Идентификация Регламента

Наименование документа: «Регламент работы Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области при выполнении функций аккредитованного удостоверяющего центра» (далее – Регламент УЦ ОПФР).

Версия: 1.0.

Дата: 20.04.2018

# 1.3. Публикация Регламента

Настоящий Регламент публикуется в электронном виде на сайте:

http://www.pfrf.ru/branches/tver/info/~strahovatel/4156

# 1.4. Область применения Регламента

Настоящий Регламент предназначен служить средством официального уведомления и информирования всех заинтересованных сторон о взаимоотношениях, возникающих в процессе предоставления и использования услуг Удостоверяющего центра, а также соглашением, налагающим обязанности на все вовлеченные в эти взаимоотношения стороны.

# 1.5. Срок действия Регламента

1.5.1. Настоящий регламент вступает в силу со дня его публикации и действует до момента уведомления Удостоверяющим центром о прекращении действия Регламента.

1.5.2. Уведомление о прекращении действия Регламента осуществляется способом, определенным в разделе «Публикация Регламента».

# 1.6. Присоединение к Регламенту

1.6.1. Настоящий Регламент со всеми приложениями к нему является договором присоединения в соответствии со ст. 428 Гражданского кодекса РФ.

1.6.2. Присоединение к настоящему Регламенту осуществляется путем подачи Заявителем заявки на регистрацию в Удостоверяющем центре (далее – Заявка) в соответствии с Приложением №1 к настоящему Регламенту. С момента подачи Заявки Заявитель считается присоединившимся к Регламенту и становится стороной Регламента – Пользователем Удостоверяющего центра.

1.6.3. Факт присоединения Заявителя к Регламенту является полным принятием им условий настоящего Регламента и всех его положений в редакции, действующей на момент подачи Заявки. Сторона, присоединившаяся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

# 1.7. Порядок утверждения и внесения изменений в Регламент

1.7.1. Оригинал настоящего Регламента формируется в форме документа на бумажном носителе и заверяется собственноручной подписью руководителя и печатью Удостоверяющего центра.

1.7.2. Сообщения об ошибках в положениях настоящего Регламента, а также предложения по уточнению его положений могут направляться в Удостоверяющий центр в соответствии с контактной информацией, указанной в разделе 2.3 настоящего Регламента.

1.7.3. Изменения и дополнения в Регламент вносятся Удостоверяющим центром в одностороннем порядке.

1.7.4. Изменения в разделы настоящего Регламента, которые по оценкам Удостоверяющего центра не оказывают либо оказывают незначительное влияние на работу пользователей, вносятся без изменения номера версии данного документа.

1.7.5. Изменения в разделы настоящего Регламента, которые по оценкам Удостоверяющего центра могут иметь значительное влияние на работу пользователей, вносятся с увеличением номера версии данного документа.

1.7.6. Уведомление пользователей о внесении изменений в Регламент осуществляется способом, определенным в разделе «Публикация Регламента».

# 2. ОБЩИЕ ПОЛОЖЕНИЯ

# 2.1. Основания осуществления деятельности Удостоверяющего центра

2.1.1. Удостоверяющий центр осуществляет свою деятельность на основании разрешительных документов на осуществление видов деятельности, связанных с предоставлением услуг Удостоверяющего центра:

- Лицензия на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выданная УФСБ по Тверской области от 18.03.2015 ЛСЗ № 0005716.

- Свидетельство об аккредитации удостоверяющего центра.

- Распоряжение Правления Пенсионного фонда Российской Федерации от 25.03.2013 №108р «О мерах по совершенствованию юридически значимого электронного документооборота в информационных системах Пенсионного фонда Российской Федерации».

2.1.2. Копии документов, указанных в пункте 2.1.1, публикуются на сайте Отделения

http://www.pfrf.ru/branches/tver/info/~strahovatel/4156

# 2.2. Информация о месте нахождения, местах осуществления деятельности и графике работы Удостоверяющего центра

2.2.1. Адрес места нахождения Удостоверяющего центра Отделения: ул. Вагжанова, д. 9 стр. 1, Тверь, 170100.

2.2.2. График работы Удостоверяющего центра: ежедневно, кроме выходных и праздничных дней, с 08:30 до 17:30 (в пятницу и предпраздничные дни с 08:30 до 16:30), обеденный перерыв с 12:30 до 13:18, по местному времени, в соответствии с часовым поясом места нахождения Отделения (UTC/GMT+4).

# 2.3. Контактная информация Удостоверяющего центра

Телефоны: 8 (4822) 32-96-60, 32-96-64.

Факс: 8 (4822) 777-460.

Адрес электронной почты: 078uc@078.pfr.ru

# 2.4. Стоимость услуг Удостоверяющего центра

Удостоверяющий центр осуществляет свою деятельность на безвозмездной основе.

# 2.5. Пользователи Удостоверяющего центра

Пользователями Удостоверяющего центра могут быть только органы ПФР на территории Тверской области, присоединившиеся к настоящему Регламенту, в лице руководителя и работников, действующие на основании учредительных документов юридического лица, доверенности или распорядительного документа о наделении работника полномочиями электронной подписи от имени юридического лица.

# 2.6. Разрешение споров

2.6.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и сторона, присоединившаяся к Регламенту.

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

2.6.3. 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.

2.6.4. Все споры и разногласия между сторонами, возникающие из Регламента или в связи с ним, и по которым не было достигнуто соглашение, разрешаются в Арбитражном суде Тверской области в соответствии с законодательством РФ.

# 2.7. Прекращение деятельности Удостоверяющего центра

В случае принятия решения о прекращении своей деятельности Удостоверяющий центр обязан:

- сообщить об этом в Уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;

- передать в Уполномоченный федеральный орган реестр выданных Удостоверяющим центром квалифицированных сертификатов в соответствии с «Порядком передачи реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи, в случае прекращения деятельности аккредитованного удостоверяющего центра», утвержденного приказом Минкомсвязи России от 14.08.2017 № 416 (Зарегистрировано в Минюсте России 11.09.2017 №48141);

- передать на хранение в Уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

# 3. ОКАЗЫВАЕМЫЕ УСЛУГИ И РЕАЛИЗУЕМЫЕ ФУНКЦИИ

# 3.1. Услуги, оказываемые Удостоверяющим центром

3.1.1. Создание и выдача квалифицированных сертификатов лицам, обратившимся за их получением, при условии установления личности получателя сертификата (Заявителя) либо полномочия лица, выступающего от его имени по обращению за получением данного сертификата.

3.1.2. Выдача по обращениям Пользователей средств электронной подписи, обеспечивающих возможность самостоятельного создания ключа электронной подписи и ключа проверки электронной подписи, создания и проверки электронных подписей.

3.1.3. Создание по обращениям Пользователей ключей электронной подписи и ключей проверки электронной подписи с записью их на ключевой носитель и гарантией обеспечения конфиденциальности.

3.1.4. Прекращение действия созданных и выданных Удостоверяющим центром квалифицированных сертификатов, по заявлению владельца сертификата.

3.1.5. Предоставление доступа к информации из реестра квалифицированных сертификатов Удостоверяющего центра, в том числе с использованием информационно-телекоммуникационной сети «Интернет».

3.1.6. Осуществление по обращениям Пользователей подтверждения подлинности электронных подписей, созданных с использованием выданных Удостоверяющим центром квалифицированных сертификатов.

3.1.7. Осуществление по обращениям Пользователей подтверждения подлинности электронной подписи Удостоверяющего центра в выданных Удостоверяющим центром квалифицированных сертификатах.

3.1.8. Выдача по обращениям владельцев квалифицированных сертификатов в форме документов на бумажных носителях, заверенных Удостоверяющим центром.

3.1.9. Регистрация владельцев квалифицированных сертификатов, выданных Удостоверяющим центром, в Единой системе идентификации и аутентификации.

3.1.10. Иные, связанные с использованием электронной подписи, услуги.

# 3.2. Функции, реализуемые Удостоверяющим центром

3.2.1. В соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» Удостоверяющий центр выполняет следующие основные функции:

3.2.1.1. Создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (Заявителям).

3.2.1.1.1. Осуществляет в соответствии с настоящим Регламентом подтверждения владения ключом электронной подписи подтверждение владения Заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата.

3.2.1.2. Устанавливает сроки действия сертификатов.

3.2.1.3. Аннулирует созданные и выданные Удостоверяющим центром сертификаты.

3.2.1.4. Прекращает действие созданных и выданных Удостоверяющим центром сертификатов.

3.2.1.5. 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.

3.2.1.6. Ведет реестр созданных и аннулированных Удостоверяющим центром сертификатов (далее – реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных Удостоверяющим центром сертификатах, а также сведения о датах прекращения действия или аннулирования сертификатов и основаниях таких прекращения или аннулирования.

3.2.1.7. Обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети «Интернет».

3.2.1.8. Создает по обращениям Заявителей ключи электронных подписей и ключи проверки электронных подписей.

3.2.1.9. Проверяет уникальность ключей проверки электронных подписей в реестре сертификатов.

3.2.1.10. Осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей.

3.2.2. Функционирование Удостоверяющего центра обеспечивается реализацией следующих функций:

3.2.3. Административные функции

3.2.3.1. Управление деятельностью Удостоверяющего центра.

3.2.3.2. Координация деятельности Удостоверяющего центра и Уполномоченных лиц Удостоверяющего центра.

3.2.3.3. Взаимодействие с Пользователями в части разрешения вопросов, связанных с применением предоставленных средств электронной подписи, ключей электронных подписей и квалифицированных сертификатов.

3.2.3.4. Взаимодействие с Пользователями в части разрешения вопросов подтверждения подлинности электронных подписей, созданных с использованием выданных Удостоверяющим центром квалифицированных сертификатов.

3.2.3.5. Взаимодействие с Пользователями в части разрешения вопросов, связанных с подтверждением электронной подписи Удостоверяющего центра в квалифицированных сертификатах, выданных Удостоверяющим центром в форме электронного документа.

3.2.4. Функции регистрации

3.2.4.1. Установление личности лица - физического лица, указанного в качестве владельца сертификата наряду с указанием наименования юридического лица, обратившегося за получением квалифицированного сертификата.

3.2.4.2. Проверка правомочий лица, выступающего от имени Заявителя - юридического лица, обращаться за получением квалифицированного сертификата.

3.2.4.3. Проверка достоверности регистрационных данных Пользователей на основании информации, содержащейся в представленных Пользователем документах, а также полученной из государственных информационных ресурсов с использованием инфраструктуры Отделения.

3.2.4.4. Ведение реестра выданных и аннулированных Удостоверяющим центром квалифицированных сертификатов, в том числе включающего в себя информацию, содержащуюся в выданных этим Удостоверяющим центром сертификатах, и информацию о датах прекращения действия или аннулирования сертификатов, а также об основаниях прекращения действия или аннулирования сертификатов.

3.2.4.5. Передача в Единую систему идентификации и аутентификации сведений о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в Единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате.

3.2.4.6. Иное взаимодействие с Пользователями в соответствии с настоящим Регламентом.

3.2.5. Функции безопасности

3.2.5.1. Выполнение комплекса организационно-технических мероприятий по защите ключей электронных подписей Удостоверяющего центра и Пользователей, а также информационных ресурсов Удостоверяющего центра, включающих, в частности, информацию, содержащуюся в реестре сертификатов, от несанкционированного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

3.2.5.2. Обеспечение выполнения процедур создания, использования, хранения и уничтожения ключевой информации в соответствии с требованиями эксплуатационной документации на средства электронной подписи.

3.2.5.3. Осуществление в соответствии с правилами подтверждения владения ключом электронной подписи подтверждения владения получателем квалифицированного сертификата, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата.

3.2.5.4. Реализация средствами Удостоверяющего центра протоколов аннулирования или прекращения действия сертификатов, формирования, обновления и публикации списков аннулированных сертификатов.

# 4. ПРАВА

# 4.1. Права Удостоверяющего центра

Удостоверяющий центр имеет право:

4.1.1. Отказать в регистрации лицам, обратившимся в Удостоверяющий центр, с указанием причин отказа.

4.1.2. Отказать в создании ключей электронных подписей Пользователям, обратившимся в Удостоверяющий центр, с указанием причин отказа.

4.1.3. Отказать в выдаче сертификата Пользователям, обратившимся в Удостоверяющий центр за получением сертификата, с указанием причин отказа.

4.1.4. Запрашивать у Заявителей документы для подтверждения сведений, представленных ими при обращении в Удостоверяющий центр.

4.1.5. С использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, запрашивать и получать у операторов базовых государственных информационных ресурсов сведения, необходимые для осуществления проверки достоверности документов и сведений, представленных Заявителем.

4.1.6. Запросить у Заявителя дополнительные, подтверждающие достоверность представленных им сведений, документы в случае наличия противоречий между сведениями, представленными Заявителем, и сведениями, полученными Удостоверяющим центром в соответствии с частью 2.2 статьи 18 Федерального закона «Об электронной подписи».

4.1.7. Не принимать от Заявителя документы, не соответствующие требованиям нормативных правовых актов Российской Федерации.

4.1.8. Отказать в прекращении действия сертификата владельцу сертификата, подавшему заявление на прекращении действия сертификата, в случае если сертификат уже аннулирован или прекратил свое действие по другим основаниям.

4.1.9. Отказать в прекращении действия сертификата владельцу сертификата, подавшему заявление на прекращение действия сертификата, в случае если истек установленный срок действия ключа электронной подписи, соответствующего ключу проверки электронной подписи в сертификате.

4.1.10. Прекратить действие сертификата без соответствующего заявления владельца сертификата в следующих случаях:

- при наличии у Удостоверяющего центра существенных оснований полагать, что соответствующий ключ электронной подписи был скомпрометирован;

- при наличии у Удостоверяющего центра существенных оснований полагать, что документы, представленные Заявителем в целях создания и получения им сертификата, не являются подлинными и/или не подтверждают достоверность информации, включенной в данный сертификат;

- если установлено, что сертификат содержит сведения, утратившие свою достоверность в связи с изменением регистрационных данных Пользователя;

- если установлено, что в результате технической ошибки сертификат содержит недостоверные или неполные сведения;

- в случае невыполнения владельцем сертификата обязанностей, установленных законодательством Российской Федерации в области электронной подписи и настоящим Регламентом;

- в случае получения Удостоверяющим центром мотивированного обращения или предписания со стороны уполномоченных федеральных органов, содержащего указание на необходимость прекращения действия сертификата.

4.1.11. Осуществлять отправку сервисной информации в составе email-сообщений, направляемых на указанный Пользователем при регистрации адрес корпоративной электронной почты Lotus в целях получения Пользователем услуг Удостоверяющего центра.

# 4.2. Права Пользователей Удостоверяющего центра

Пользователи Удостоверяющего центра имеют право:

4.2.1. Получить и применять сертификат Удостоверяющего центра для проверки электронной подписи Удостоверяющего центра в сертификатах, созданных Удостоверяющим центром.

4.2.2. Обращаться в Удостоверяющий центр с целью получения квалифицированного сертификата.

4.2.3. Обращаться в Удостоверяющий центр с целью получения ключа электронной подписи.

4.2.4. Обращаться в Удостоверяющий центр с целью получения средств электронной подписи.

4.2.5. Использовать имеющиеся или предоставленные Удостоверяющим центром средства электронной подписи для формирования ключа электронной подписи и запроса на квалифицированный сертификат.

4.2.6. Получать список аннулированных сертификатов и использовать его для установления статуса сертификатов, созданных Удостоверяющим центром.

4.2.7. Получить сертификат как в форме электронного документа, так и в форме документа на бумажном носителе, заверенного Удостоверяющим центром.

4.2.8. Обращаться в Удостоверяющий центр с заявлением на выполнение Удостоверяющим центром действий, предусмотренных настоящим Регламентом.

4.2.9. Использовать имеющиеся или предоставленные Удостоверяющим центром средства электронной подписи для создания ключей электронной подписи и запросов на квалифицированный сертификат.

4.2.10. Обращаться в Удостоверяющий центр за подтверждением подлинности электронных подписей, созданных с использованием выданных Удостоверяющим центром квалифицированных сертификатов, в соответствии с порядком, определенным настоящим Регламентом.

4.2.11. Обращаться в Удостоверяющий центр за подтверждением подлинности электронной подписи Удостоверяющего центра в выданных Удостоверяющим центром квалифицированных сертификатах в соответствии с порядком, определенным настоящим Регламентом.

4.2.12. Обращаться в Удостоверяющий центр с заявлениями на прекращение действия квалифицированного сертификата, в течение срока действия сертификата.

# 5. ОБЯЗАННОСТИ

# 5.1. Обязанности Удостоверяющего центра

5.1.1. По работе с ключами и сертификатами ключей проверки электронных подписей Удостоверяющего центра

5.1.1.1. Удостоверяющий центр для подписания от своего имени создаваемых квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет Уполномоченный федеральный орган. Удостоверяющему центру 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.

5.1.1.2. Удостоверяющий центр обязан использовать ключ электронной подписи Удостоверяющего центра только для подписи создаваемых им квалифицированных сертификатов и списков аннулированных сертификатов.

5.1.1.3. Для подписи создаваемых квалифицированных сертификатов Удостоверяющий центр должен использовать только один ключ электронной подписи и соответствующий ему квалифицированный сертификат, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, с самой поздней датой создания. Остальные ключи электронных подписей и соответствующие им квалифицированные сертификаты Удостоверяющий центр могут использоваться только для подписи списков аннулированных сертификатов.

5.1.1.4. Удостоверяющий центр обязан строго соблюдать срок действия ключей электронной подписи Удостоверяющего центра, используемых для подписания создаваемых сертификатов, распределяя сроки их действия таким образом, чтобы по окончании таких сроков все подписанные этими ключами сертификаты прекратили свое действие.

5.1.1.5. Удостоверяющий центр обязан принимать меры по защите ключей электронной подписи Удостоверяющего центра в соответствии с положениями настоящего Регламента и действующими нормативными правовыми актами РФ.

5.1.2. По синхронизации времени

Удостоверяющий центр обязан синхронизировать по времени все программные и технические средства обеспечения деятельности Удостоверяющего центра.

5.1.3. По регистрации Пользователей

5.1.3.1. Удостоверяющий центр обеспечивает регистрацию Пользователей в реестре пользователей по их Заявкам в соответствии с порядком, изложенном в настоящем Регламенте.

5.1.3.2. Удостоверяющий центр не вправе разглашать (публиковать) регистрационные данные Пользователей, за исключением информации, включаемой в состав создаваемых сертификатов, а также подлежащей распространению в соответствии с федеральными законами и иными нормативными правовыми актами.

5.1.4. По созданию ключей электронных подписей и ключей проверки электронных подписей Пользователей

5.1.4.1. Удостоверяющий центр создает ключи электронных подписей и ключи проверки электронных подписей на основании соответствующих обращений Пользователей. Создание ключей электронных подписей и ключей проверки электронных подписей осуществляется при помощи средств электронной подписи, входящих в состав программно-технических средств Удостоверяющего центра, которые имеют подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи».

5.1.4.2. Удостоверяющий центр обязан обеспечить уникальность создаваемых ключей проверки электронных подписей в реестре квалифицированных сертификатов Удостоверяющего центра.

5.1.4.3. Удостоверяющий центр обязан обеспечить конфиденциальность созданных Удостоверяющим центром ключей электронных подписей.

5.1.4.4. Удостоверяющий центр обязан информировать в письменной форме Пользователей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, а также о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

5.1.5. По созданию квалифицированных сертификатов

5.1.5.1. Удостоверяющий центр обеспечивает создание квалифицированных сертификатов по обращениям Пользователей, в соответствии с порядком, определенным настоящим Регламентом.

5.1.5.2. Удостоверяющий центр обязан обеспечить уникальность номеров создаваемых квалифицированных сертификатов в реестре квалифицированных сертификатов Удостоверяющего центра.

5.1.5.3. Удостоверяющий центр обязан включать в создаваемые сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами.

5.1.5.4. В соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи», Удостоверяющий центр обязан направлять в Единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат ключа проверки электронной подписи, в объеме, необходимом для регистрации в Единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра).

5.1.5.5. По желанию лица, которому выдан квалифицированный сертификат, Удостоверяющий центр обязан безвозмездно осуществить регистрацию указанного лица в Единой системе идентификации и аутентификации.

5.1.5.6. Удостоверяющий центр обязан отказать Заявителю в создании сертификата в случае, если не было подтверждено то, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения сертификата.

5.1.5.7. Удостоверяющий центр обязан отказать Заявителю в создании сертификата в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного Заявителем для получения сертификата.

5.1.6. По аннулированию квалифицированных сертификатов

Удостоверяющий центр аннулирует квалифицированный сертификат в случаях, установленных Федеральным законом «Об электронной подписи», а именно:

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

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

- вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

5.1.7. По прекращению действия квалифицированных сертификатов

Удостоверяющий центр обязан прекратить действие квалифицированного сертификата по заявлению на прекращение действия сертификата, в соответствии с порядком и на основаниях, указанных в разделе 9.6.4. настоящего Регламента.

5.1.8. По уведомлению о факте аннулирования или прекращения действия квалифицированного сертификата

5.1.8.1. Удостоверяющий центр обязан внести информацию о квалифицированном сертификате, который был аннулирован или действие которого было досрочно прекращено, в список аннулированных сертификатов в течение 12 часов с момента возникновения обстоятельств, послуживших основанием для аннулирования или прекращения действия квалифицированного сертификата.

5.1.8.2. Датой и временем аннулирования или прекращения действия квалифицированного сертификата признается дата и время внесения информации о квалифицированном сертификате, который был аннулирован или действие которого было досрочно прекращено, в список аннулированных сертификатов.

5.1.8.3. Удостоверяющий центр обязан официально уведомить о факте аннулирования сертификата его владельца.

5.1.8.4. Срок уведомления об аннулировании сертификата – не позднее 24 часов с момента включения сведений об аннулированном сертификате в список аннулированных сертификатов.

5.1.8.5. Официальным уведомлением о факте аннулирования сертификата является опубликование списка аннулированных сертификатов, содержащего сведения об аннулированном сертификате, а также направление email-сообщений на указанный Пользователем при регистрации адрес корпоративной электронной почты Lotus.

5.1.8.6. Временем опубликования списка аннулированных сертификатов признается включенное в список аннулированных сертификатов время его создания.

5.1.8.7. Удостоверяющий центр обязан осуществлять публикацию списков аннулированных сертификатов в точках распространения, указанных в полях СRLDistributionPoints и AuthorityInfoAccess выдаваемых Удостоверяющим центром квалифицированных сертификатов.

5.1.9. По ведению реестра сертификатов

5.1.9.1. Удостоверяющий центр обязан обеспечивать формирование и ведение реестра квалифицированных сертификатов в течение всего срока деятельности Удостоверяющего центра.

5.1.9.2. Реестр квалифицированных сертификатов ведется Удостоверяющим центром в электронном виде и кроме информации, содержащейся в квалифицированных сертификатах, включает также информацию о датах прекращения действия или аннулирования квалифицированных сертификатов и об основаниях прекращения действия или аннулирования, а также иную информацию, подлежащую включению в реестр в соответствии с требованиями нормативных правовых документов.

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

5.1.9.4. Удостоверяющий центр обязан обеспечить любому лицу в любое время, за исключением периодов планового или внепланового технического обслуживания, доступ с использованием информационно-телекоммуникационных сетей общего пользования к реестру сертификатов Удостоверяющего центра в соответствии с п. 9.12. настоящего Регламента.

5.1.10. По обеспечению деятельности Удостоверяющего центра

5.1.10.1. Удостоверяющий центр обязан хранить информацию:

- о реквизитах основного документа, удостоверяющего личность физического лица, указанного в качестве владельца сертификата наряду с указанием наименования юридического лица;

- о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени Заявителя, обращаться за получением квалифицированного сертификата;

- о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.

5.1.10.2. Удостоверяющий центр должен хранить информацию, указанную п. 5.1.10.1, 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.

5.1.10.3. Удостоверяющий центр обязан выполнять свои функции и обязанности в соответствии с настоящим Регламентом, Федеральным законом «Об электронной подписи» и иными нормативными правыми актам, принимаемыми соответствии с Федеральным законом «Об электронной подписи».

5.1.10.4. Удостоверяющий центр не вправе наделять третьих лиц полномочиями по созданию ключей квалифицированных электронных подписей и квалифицированных сертификатов от имени Удостоверяющего центра.

# 5.2. Обязанности Пользователя

5.2.1. Обязанности лица, проходящего процедуру регистрации в Удостоверяющем центре

5.2.1.1. Лицо, проходящее процедуру регистрации в Удостоверяющем центре, обязано предоставить регистрационные данные в объеме, необходимом для получения услуг Удостоверяющего центра.

5.2.1.2. Лицо, проходящее процедуру регистрации в Удостоверяющем центре, несет ответственность за достоверность предоставленных регистрационных данных.

5.2.2. Обязанности лица, пользующегося услугами Удостоверяющего центра (владельца квалифицированного сертификата)

5.2.2.1. Принимать все возможные меры для предотвращения компрометации ключа электронной подписи, принадлежащего владельцу сертификата, а также меры по обеспечению конфиденциальности аутентификационных данных, используемых для доступа к ключевой информации на ключевом носителе.

5.2.2.2. Не использовать принадлежащий владельцу сертификата ключ электронной подписи в случае его компрометации.

5.2.2.3. Немедленно обращаться в Удостоверяющий центр с заявлением на прекращение действия сертификата в следующих случаях:

- при компрометации ключа электронной подписи, принадлежащего владельцу сертификата;

- при компрометации аутентификационной информации Пользователя, используемой для получения доступа к ключевой информации на ключевом носителе.

5.2.2.4. Обращаться в Удостоверяющий центр с заявлением на прекращение действия сертификата, содержащего сведения, утратившие свою достоверность в связи с изменением регистрационных данных Пользователя, не позднее 3 (трех) рабочих дней с даты регистрации таких изменений.

5.2.2.5. Извещать Удостоверяющий центр обо всех изменениях своих регистрационных данных в течение 3 (трех) рабочих дней с даты регистрации изменений. При этом Удостоверяющий центр вправе затребовать у пользователя документы, подтверждающие изменение регистрационных данных.

5.2.2.6. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки, а также запросов на квалифицированный сертификат, только средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи».

5.2.2.7. При создании ключей электронных подписей и запросов на квалифицированный сертификат выполнять требования о соблюдении конфиденциальности информации, установленные Федеральным законом от 27.07.2016 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5.2.2.8. Не использовать ключ электронной подписи, связанный с квалифицированным сертификатом, который аннулирован, действие которого прекращено или заявление на прекращение действия которого подано в Удостоверяющий центр.

# 6. ОТВЕТСТВЕННОСТЬ

# 6.1. Ответственность Удостоверяющего центра

6.1.1. Удостоверяющий центр несет ответственность за неисполнение либо ненадлежащее исполнение обязательств по настоящему Регламенту, за исключением случаев, предусмотренных пунктом 6.1.2 настоящего Регламента, в соответствии с законодательством Российской Федерации.

6.1.2. Удостоверяющий центр не несет ответственности за неисполнение либо ненадлежащее исполнение обязательств по настоящему Регламенту и за причиненные в результате этого убытки, в случаях нарушения Пользователем настоящего Регламента, а также в случаях подделки, подлога либо иного искажения Пользователем или третьими лицами документов либо их заверенных копий, подтверждающих правомочия лица, выступающего от имени Заявителя или содержащих регистрационные данные Пользователя.

# 6.2. Ответственность Пользователя

6.2.1. Пользователь несет ответственность за достаточность принимаемых им мер по обеспечению безопасности использования электронной подписи и средств электронной подписи, включая защиту хранящегося у него ключа электронной подписи от компрометации, потери, уничтожения или изменения.

6.2.2. Пользователь несет ответственность за последствия, возникшие в результате неисполнения им положений настоящего Регламента.

# 7. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

# 7.1. Виды конфиденциальной информации

7.1.1. Ключ электронной подписи является конфиденциальной информацией лица, являющегося владельцем соответствующего квалифицированного сертификата. Удостоверяющий центр не осуществляет хранение ключей электронных подписей Пользователей Удостоверяющего центра.

7.1.2. Конфиденциальной является идентификационная и аутентификационная информация, предоставляемая Пользователю в процессе прохождения процедуры регистрации и получения сертификата ключа поверки электронной подписи.

7.1.3. Персональные данные и корпоративная информация Пользователей, не подлежащая включению в состав квалифицированного сертификата, считается конфиденциальной.

# 7.2. Виды информации, не относящейся к конфиденциальной

7.2.1. Информация, не относящаяся к конфиденциальной информации, является открытой информацией.

7.2.2. Открытая информация может публиковаться по решению Удостоверяющего центра. Место, способ и время публикации определяется решением Удостоверяющего центра.

7.2.3. Информация, включаемая в создаваемые Удостоверяющим центром квалифицированные сертификаты и списки аннулированных сертификатов, не считается конфиденциальной.

7.2.4. Также не считается конфиденциальной информация о настоящем Регламенте.

# 7.3. Предоставление конфиденциальной информации

Удостоверяющий центр не должен раскрывать информацию, относящуюся к конфиденциальной, каким бы то ни было третьим лицам за исключением случаев:

- определенных в настоящем Регламенте;

- требующих раскрытия в соответствии с законодательством РФ или при наличии судебного постановления.

# 8. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

8.1. При оказании услуг по выдаче квалифицированного сертификата ключа проверки электронной подписи Удостоверяющий центр, в соответствии с требованиями, установленными согласно Федеральному закону «Об электронной подписи», обрабатывает следующие персональные данные физических лиц, указанного в качестве владельца сертификата наряду с указанием наименования юридического лица, обращающегося за получением квалифицированного сертификата:

- Фамилия, имя, отчество.

- Наименование занимаемой должности.

- Место работы.

- Адрес электронной почты.

- Страховой номер индивидуального лицевого счета в системе персонифицированного учета ПФР.

8.2. Присоединение Заявителя к настоящему Регламенту является подтверждением того, что:

- перечисленные в пункте 8.1 настоящего Регламента персональные данные физического лица, указанного в качестве владельца сертификата наряду с указанием наименования юридического лица, передаются Удостоверяющему центру в целях создания квалифицированного сертификата ключа проверки электронной подписи с согласия этого физического лица;

- физическое лицо, указанное в качестве владельца сертификата наряду с указанием наименования юридического лица, согласно на обработку Удостоверяющим центром его персональных данных, перечисленных в пункте 8.1 настоящего Регламента, в целях создания квалифицированного сертификата.

При этом Удостоверяющему центру предоставляется право на обработку персональных данных любыми способами, в том числе путем включения в электронные базы, осуществление всех действий (операций) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, обновление, изменение, извлечение, использование, обезличивание, блокирование, удаление, уничтожение, а также передачу персональных данных в Единую систему идентификации и аутентификации.

- физическое лицо, указанное в качестве владельца сертификата наряду с указанием наименования юридического лица, согласно на поручение Удостоверяющим центром обработки его персональных данных, перечисленных в пункте 8.1 настоящего Регламента, другому лицу в целях проверки регистрационных данных Пользователя и вручения квалифицированного сертификата подписи его владельцу.

- физическое лицо, указанное в качестве владельца сертификата наряду с указанием наименования юридического лица, уведомлено юридическим лицом о том, что реестр квалифицированных сертификатов ключей проверки электронных подписей, а также в создаваемый сертификат ключа проверки электронной подписи, в которые включаются персональные данные этого физического лица в составе, определенном пунктом 8.1 настоящего Регламента, относятся к общедоступным источникам персональных данных.

8.3. В соответствии с пунктом 1 статьи 8 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» физическое лицо, указанное в качестве владельца сертификата наряду с указанием наименования юридического лица, при регистрации в качестве Пользователя Удостоверяющего центра направляет в письменной форме согласие на включение персональных данных пользователя Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области в общедоступные источники персональных данных (Приложение № 2).

# 9. ПОРЯДОК ОКАЗАНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

# 9.1. Регистрация Пользователей Удостоверяющего центра

9.1.1. Под регистрацией Пользователей Удостоверяющего центра понимается внесение регистрационных данных Пользователей в реестр Удостоверяющего центра.

9.1.2. Регистрация Пользователя Удостоверяющего центра осуществляется на основании Заявки, содержащей регистрационные данные Заявителя, включая информацию, подлежащую внесению в квалифицированный сертификат в соответствии с частью 2 статьи 17 Федерального закона «Об электронной подписи».

9.1.3. Заявка может быть подана Заявителем одним из следующих способов:

- путем подачи Заявки в форме документа на бумажном носителе, в Удостоверяющий центр;

- путем подачи Заявки в форме документа на бумажном носителе, Доверенному лицу Удостоверяющего центра.

# 9.2. Идентификация Пользователя Удостоверяющего центра

9.2.1. Идентификация Пользователя выполняется в процессе его регистрации в реестре Пользователей Удостоверяющего центра.

9.2.2. Результатом идентификации является присвоение Пользователю идентификатора и внесение идентификатора в реестр Пользователей Удостоверяющего центра.

9.2.3. Идентификатором зарегистрированного Пользователя являются идентификационные данные, содержащиеся в поданной им Заявке.

# 9.3. Создание ключа электронной подписи и запроса на сертификат

Создание ключа электронной подписи и запроса на сертификат осуществляется одним из двух способов:

9.3.1. Пользователь самостоятельно создает ключ электронной подписи и запрос на сертификат при помощи сертифицированного средства электронной подписи.

Передача созданного Пользователем файла запроса на сертификат ключа проверки электронной подписи осуществляется методами, предусмотренными технической документацией на сертифицированное средство электронной подписи и программных комплексов ViPNet.

9.3.2. Создание ключа электронной подписи и запроса на сертификат осуществляется Удостоверяющим центром, при наличии соответствующего обращения со стороны Пользователя.

Создание ключей электронных подписей и запросов на сертификаты Доверенными лицами категорически запрещено.

# 9.4. Создание и выдача квалифицированного сертификата ключа проверки электронной подписи

9.4.1. Создание квалифицированного сертификата осуществляется Удостоверяющим центром путем обработки полученного запроса на сертификат или при создании ключа электронной подписи, при наличии соответствующего обращения со стороны Пользователя, после проверки достоверности содержащихся в нем сведений путем сравнения их со сведениями, полученными Удостоверяющим центром из государственных информационных ресурсов.

9.4.2. Для получения квалифицированного сертификата Пользователь представляет Удостоверяющий центр или Уполномоченному лицу Удостоверяющего центра в Пункте регистрации документы, определенные Федеральным законом «Об электронной подписи», а также дополнительные документы, определенные требованиями отдельных информационных систем, для обеспечения информационного взаимодействия с участниками которых предназначен запрашиваемый сертификат. Перечень и формы необходимых документов публикуются на сайте Удостоверяющего центра.

9.4.3. К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

9.4.4. При выдаче или вручении квалифицированного сертификата Удостоверяющий центр или Доверенное лицо Удостоверяющего центра выполняет следующие действия:

9.4.4.1 Устанавливает личность полномочного лица Заявителя - физического лица, указанного в качестве владельца сертификата наряду с указанием наименования юридического лица, обратившегося за получением квалифицированного сертификата. При этом:

 личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность, – паспорту гражданина Российской Федерации. В исключительных случаях отсутствия у гражданина Российской Федерации основного документа, удостоверяющего личность, Удостоверяющий центр может удостоверить его личность по иному документу, удостоверяющему личность, в соответствии с законодательством Российской Федерации;

 личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства, с учетом требований пункта 9.4.4 настоящего Регламента;

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

9.4.4.2 Осуществляет проверку правомочия лица, выступающего от имени Заявителя, обращаться за получением квалифицированного сертификата.

9.4.4.3 Осуществляет проверку достоверности документов и сведений, представленных Заявителем в целях получения квалифицированного сертификата, используя при этом, в частности, документы и сведения, полученные Удостоверяющим центром из государственных информационных ресурсов:

 выписка из Единого государственного реестра юридических лиц в отношении Заявителя - юридического лица;

 сведения о достоверности страхового номера индивидуального лицевого счета в отношении Заявителя – физического лица, указанного в качестве владельца сертификата наряду с указанием наименования юридического лица.

9.4.5. При выдаче квалифицированного сертификата Пользователь под расписку ознакомляется с информацией, содержащейся в выдаваемом квалифицированном сертификате. Для этого выполняются следующие действия:

9.4.5.1. Уполномоченное лицо или Доверенное лицо Удостоверяющего центра осуществляет формирование бланка с информацией, содержащейся в выдаваемом сертификате, в виде документа на бумажном носителе по форме Приложения 3 к настоящему Регламенту и передаёт его Пользователю.

9.4.5.2. Пользователь знакомится с информацией, содержащейся в выдаваемом ему сертификате, и возвращает подписанный им бланк Уполномоченному лицу или Доверенному лицу Удостоверяющего центра.

9.4.6. Одновременно с квалифицированным сертификатом Пользователю выдаются:

- созданный Удостоверяющим центром ключ электронной подписи Пользователя, в случае наличия соответствующего обращения со стороны Пользователя;

- средство электронной подписи, имеющее подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи», в случае наличия соответствующего обращения со стороны Пользователя;

- руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи в письменной форме, содержащее информацию 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.

9.4.7. Допускается не указывать в качестве владельца сертификата физическое лицо, действующее от имени юридического лица, в квалифицированном сертификате, используемом для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами (далее – государственных услуг). Владельцем такого сертификата признается юридическое лицо, информация о котором содержится в таком сертификате. При этом распорядительным актом юридического лица определяется физическое лицо, ответственное за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе при оказании государственных услуг. В случае отсутствия указанного распорядительного акта лицом, ответственным за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе при оказании государственных услуг является руководитель юридического лица. В случае возложения федеральным законом полномочий по исполнению государственных функций на конкретное должностное лицо ответственным за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе при исполнении государственных функций является это должностное лицо.

# 9.5. Сроки действия ключей электронной подписи Пользователя

Сроки действия ключа электронной подписи, ключа проверки электронной подписи Пользователя не могут превышать 12 месяцев.

Срок действия квалифицированного сертификата, выдаваемого Удостоверяющим центром, не должен превышать срок действия квалифицированного сертификата Удостоверяющего центра.

# 9.6. Смена ключей электронной подписи Пользователя

# 9.6.1. Плановая смена ключей электронной подписи Пользователя

9.6.1.1. Плановая смена ключей электронной подписи производится не ранее чем за 15 (пятнадцать), и не позднее чем за 2 (двух) календарных дней до окончания срока действия текущего квалифицированного сертификата (ключа электронной подписи и ключа проверки электронной подписи) Пользователя.

9.6.1.2. Создание новых ключа электронной подписи, ключа проверки электронной подписи и запроса на квалифицированный сертификат осуществляется Пользователем самостоятельно, с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи».

9.6.1.3. Запрос на сертификат, сформированный с использованием средства электронной подписи, установленного на автоматизированном рабочем месте Пользователя, должен быть подписан квалифицированной электронной подписью Пользователя, основанной на действующем квалифицированном сертификате ключа проверки электронной подписи Пользователя, и передан в Удостоверяющий центр.

9.6.1.4. При выдаче или вручении нового сертификата Удостоверяющий центр или Доверенное лицо Удостоверяющего центра осуществляет проверку актуальности содержащейся в сертификате информации, используя документы, полученные из государственных информационных ресурсов:

- выписка из Единого государственного реестра юридических лиц в отношении Заявителя.

9.6.1.5. Перед выдачей или вручением нового сертификата Удостоверяющий центр или Доверенное лицо Удостоверяющего центра осуществляет проверку правомочия лица, выступающего от имени юридического лица, обращаться за получением квалифицированного сертификата.

9.6.1.6. В случае если Пользователь не произвел плановую смену ключа электронной подписи в указанные в п. 9.6.1.1 сроки, создание новых ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата ключа проверки электронной подписи производится в порядке, определенном разделами 9.3 и 9.4 настоящего Регламента.

# 9.6.2. Внеплановая смена ключей электронной подписи Пользователя

9.6.2.1. Внеплановая смена ключей электронной подписи производится:

- по инициативе владельца сертификата в случае прекращения действия квалифицированного сертификата до истечения срока его действия по основаниям, указанным в пунктах 5.2.2.3 и 5.2.2.4 настоящего Регламента;

- по инициативе владельца сертификата в случае если требуется получение квалифицированного сертификата с новыми дополнительными объектными идентификаторами (OID);

- при компрометации ключа электронной подписи Удостоверяющего центра;

- в иных случаях, связанных с невозможностью использования имеющегося ключа электронной подписи.

9.6.2.2. Создание новых ключа электронной подписи, ключа проверки электронной подписи и выдача квалифицированного сертификата при внеплановой смене ключа электронной подписи Пользователя производится в порядке, определенном разделами 9.3 и 9.4 настоящего Регламента.

# 9.6.3. Аннулирование квалифицированного сертификата

9.6.3.1. Удостоверяющий центр аннулирует квалифицированный сертификат в следующих случаях:

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

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

- в связи с вступлением в силу решения суда, которым, в частности, установлено, что квалифицированный сертификат содержит недостоверную информацию.

9.6.3.2 До внесения в реестр сертификатов информации об аннулировании квалифицированного сертификата Удостоверяющий центр уведомляет владельца квалифицированного сертификата об аннулировании его сертификата путем уведомления в форме электронного документа в составе email-сообщения, направляемых на указанный Пользователем при регистрации адрес корпоративной электронной почты Lotus.

# 9.6.4. Прекращение действия квалифицированного сертификата

Удостоверяющий центр прекращает действие квалифицированного сертификата в следующих случаях:

- на основании заявления владельца квалифицированного сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа с квалифицированной электронной подписью владельца квалифицированного сертификата, поданного в Удостоверяющий центр по форме Приложения 4 к настоящему Регламенту;

- в случаях, указанных в пункте 4.1.10 настоящего Регламента.

# 9.7. Смена ключей электронной подписи Удостоверяющего центра

# 9.7.1. Сроки действия ключей электронной подписи Удостоверяющего центра

Сроки действия ключа электронной подписи, ключа проверки электронной подписи в соответствии с требованиями эксплуатационной документации на средства УЦ устанавливается равным 36 месяцев.

# 9.7.2. Плановая смена ключей электронной подписи Удостоверяющего центра

9.7.2.1. Плановая смена ключей электронной подписи Удостоверяющего центра и соответствующего сертификата ключа проверки электронной подписи Удостоверяющего центра выполняется не позднее 15 месяцев с момента начала действия текущего ключа электронной подписи Удостоверяющего центра.

9.7.2.2. Выполнение плановой смены ключей электронной подписи Удостоверяющего центра и соответствующего сертификата ключа проверки электронной подписи Удостоверяющего центра не влечет за собой необходимости смены ключей электронных подписей и соответствующих сертификатов ключей проверки электронных подписей Пользователей.

# 9.7.3. Внеплановая смена ключей электронной подписи Удостоверяющего центра

9.7.3.1. Внеплановая смена ключей электронной подписи Удостоверяющего центра производится в случае компрометации или угрозы компрометации ключа электронной подписи Удостоверяющего центра.

9.7.3.2. Внеплановая смена ключей электронной подписи Удостоверяющего центра выполняется в порядке, определенном эксплуатационной документацией на средства УЦ.

9.7.3.3. В случае выполнения внеплановой смены ключей электронной подписи Удостоверяющего центра прекращается действие всех сертификатов, подписанных электронной подписью Удостоверяющего центра, созданной с использованием скомпрометированного ключа электронной подписи, с включением сведений о прекращении действия этих сертификатов в реестр сертификатов.

9.7.3.4. В случае выполнения внеплановой смены ключей электронной подписи Удостоверяющего центра должны быть проведены работы по внеплановой смене ключей электронных подписей Пользователей, сертификаты ключей проверки которых подписаны электронной подписью Удостоверяющего центра, созданной с использованием скомпрометированного ключа электронной подписи Удостоверяющего центра.

# 9.8. Подтверждение подлинности электронной подписи Удостоверяющего центра в выданных квалифицированных сертификатах

9.8.1. Удостоверяющий центр осуществляет подтверждение подлинности электронной подписи Удостоверяющего центра в выданных Удостоверяющим центром квалифицированных сертификатах по заявлению Пользователя на подтверждение подлинности электронной подписи Удостоверяющего центра в квалифицированном сертификате пользователя, поданного в Удостоверяющий центр по форме Приложения 5 к настоящему Регламенту.

9.8.2. Обязательным приложением к заявлению на подтверждение подлинности электронной подписи Удостоверяющего центра в квалифицированном сертификате пользователя является внешний носитель информации, содержащий файл сертификата, подвергающегося процедуре проверки, в формате X.509 в кодировке Base64 (CER).

9.8.3. Срок проведения работ по подтверждению подлинности электронной подписи Удостоверяющего центра в выданном Удостоверяющим центром квалифицированном сертификате и предоставлению заключения о произведенной проверке составляет 3 (три) рабочих дня с момента поступления в Удостоверяющий центр заявления пользователя на подтверждение подлинности электронной подписи Удостоверяющего центра в выданном им квалифицированном сертификате.

9.8.4. Результатом проведения работ по подтверждению подлинности электронной подписи Удостоверяющего центра в квалифицированном сертификате пользователя является заключение Удостоверяющего центра, заверенное собственноручной подписью ответственного работника и печатью Удостоверяющего центра.

# 9.9. Подтверждение подлинности электронной подписи Пользователя в электронном документе

9.9.1. Подтверждение подлинности электронной подписи в электронном документе осуществляется Удостоверяющим центром по обращению Пользователя на основании заявления в простой письменной форме на подтверждение подлинности электронной подписи в электронном документе.

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

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

9.9.4. Обязательным приложением к заявлению на подтверждение электронной подписи в электронном документе является внешний носитель информации, содержащий электронный документ с электронной подписью в формате PKCS#7.

9.9.5. Срок проведения работ по подтверждению подлинности электронной подписи в электронном документе составляет 3 (три) рабочих дня с момента поступления заявления в Удостоверяющий центр.

9.9.6. В ходе проведения работ по подтверждению подлинности электронной подписи в электронном документе Удостоверяющим центром может быть запрошена дополнительная информация.

9.9.7. Результатом проведения работ по подтверждению подлинности электронной подписи в электронном документе является ответ в письменной форме, заверенный собственноручной подписью ответственного работника и печатью Удостоверяющего центра.

Ответ должен содержать:

- результат проверки средством электронной подписи, имеющим подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи», принадлежности электронной подписи в электронном документе владельцу квалифицированного сертификата и отсутствия искажений в подписанном данной электронной подписью электронном документе;

- детальный отчет по выполненной проверке (экспертизе).

9.9.8. Детальный отчет по выполненной проверке должен включать следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);

- основания для проведения проверки (экспертизы);

- сведения об эксперте или экспертной комиссии (фамилия, имя, отчество, образование, специальность, стаж работы, ученая степень и/или ученое звание, занимаемая должность), которым поручено проведение проверки (экспертизы);

- вопросы, поставленные перед экспертом или экспертной комиссией;

- объекты исследований и материалы по заявлению, представленные для проведения проверки (экспертизы);

- содержание и результаты исследований с указанием примененных методов;

- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;

- иные сведения.

9.9.9. Материалы и документы, иллюстрирующие заключение эксперта или экспертной комиссии, прилагаются к детальному отчету и являются его составной частью.

9.9.10. Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами экспертной комиссии.

# 9.10. Механизм доказательства обладания ключом электронной подписи

9.10.1. В случае если ключ электронной подписи Пользователя создавался по его обращению Удостоверяющим центром, факт обладания ключом электронной подписи подтверждается фактом передачи Пользователю ключевого документа.

9.10.2. В случае если ключ электронной подписи создавался Пользователем самостоятельно, в Удостоверяющий центр представляется запрос на сертификат, подписанный созданным ключом электронной подписи, соответствующим ключу проверки электронной подписи, содержащемуся в запросе на сертификат. Положительный результат проверки электронной подписи в предоставленном Пользователем файле запроса на сертификат, выполняемой при помощи средств Удостоверяющего центра, является подтверждением обладания Пользователем ключом электронной подписи. При отрицательном результате проверки электронной подписи в файле запроса на сертификат Удостоверяющий центр отказывает Пользователю в создании и выдаче сертификата.

# 9.11. Проверка уникальности ключей ЭП

При обработке запроса на сертификат Удостоверяющий центр производит проверку на наличие в реестре сертификатов Удостоверяющего центра сертификатов, содержащих ключ проверки электронной подписи, идентичный ключу, содержащемуся в запросе. При обнаружении таких сертификатов запрос на сертификат отклоняется.

# 9.12. Порядок предоставления доступа к реестру квалифицированных сертификатов Удостоверяющего центра

Информация, содержащаяся в реестре квалифицированных сертификатов Удостоверяющего центра, доступна любому лицу в любое время.

Получение информации из реестра сертификатов осуществляется на основании запроса по форме Приложения 6 к настоящему Регламенту, направленного на адрес электронной почты Удостоверяющего центра - 078UC@078.pfr.ru)

# 9.13. Порядок регистрации Пользователей в Единой системе идентификации и аутентификации

9.13.1. Удостоверяющий центр осуществляет регистрацию Пользователей Удостоверяющего центра в Единой системе идентификации и аутентификации на основании заявления, поданного в Удостоверяющий центр в форме документа на бумажном носителе с собственноручной подписью владельца сертификата (Приложение 7 к настоящему Регламенту).

9.13.2. Удостоверяющий центр осуществляет регистрацию в Единой системе идентификации и аутентификации физических лиц, указанных в качестве владельца квалифицированного сертификата наряду с наименованием юридического лица, которым был выдан квалифицированный сертификат.

9.13.3. Регистрация в Единой системе идентификации и аутентификации юридических лиц осуществляется самостоятельно физическими лицами, имеющими право действовать от имени юридического лица без доверенности, после прохождения ими процедуры регистрации в Единой системе идентификации и аутентификации в качестве физических лиц.

# 10. СОДЕРЖАНИЕ И ФОРМА КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА

Удостоверяющий центр создает по обращениям Заявителей и выдает квалифицированные сертификаты, содержание которых соответствует требованиям, установленным Федеральным законом «Об электронной подписи», а форма - требованиям к форме квалифицированного сертификата ключа проверки электронной подписи, установленным приказом ФСБ России от 27.12.2011 № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

# 11. СТРУКТУРА СПИСКА АННУЛИРОВАННЫХ СЕРТИФИКАТОВ

Удостоверяющий центр формирует списки аннулированных сертификатов в соответствии с рекомендациями IETF RFC 5280 (2008) "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

# 12. МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

12.1. Удостоверяющий центр обеспечивает выполнение мер по защите информации, в соответствии с требованиями о соблюдении конфиденциальности информации, установленными Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также требованиями, установленными технической документацией к средствам удостоверяющего центра и электронной подписи.

12.2. Для обеспечения своей деятельности Удостоверяющий центр использует средства удостоверяющего центра, включая средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи».

# 13. ПРИЛОЖЕНИЯ:

1. Форма заявления на регистрацию в Удостоверяющем центре Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области.

2. Форма согласия на включение персональных данных пользователя Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области в общедоступные источники персональных данных (реестр выданных аккредитованным удостоверяющим центром квалифицированных сертификатов ключей проверки электронной подписи).

3. Форма бланка с информацией, содержащейся в выдаваемом сертификате ключа проверки электронной подписи.

4. Форма заявления на прекращение действия сертификата ключа проверки электронной подписи.

5. Форма заявления на подтверждение подлинности электронной подписи Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области в сертификате ключа проверки электронной подписи Пользователя.

6. Форма заявления на получение информации из реестра сертификатов Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области.

7. Форма заявления на регистрацию в Единой системе идентификации и аутентификации.

8. Руководство по обеспечению безопасности использования квалифицированных ключей электронной подписи и средств квалифицированной электронной подписи.

**Приложение 1**

к Регламенту УЦ ОПФР

Начальнику Удостоверяющего центра

Государственного учреждения - Отделения

Пенсионного фонда Российской Федерации

 по Тверской области

**Заявление**

**на регистрацию в Удостоверяющем центре Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области**

Государственное учреждение — \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (далее – орган ПФР) в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, просит:

** зарегистрировать и сформировать ключи электронной подписи**

** записать сформированный ключ электронной подписи на носитель ключевой информации**

** изготовить квалифицированный сертификат ключа проверки электронной подписи**

для полномочного представителя органа ПФР в соответствии с указанными в настоящем заявлении идентификационными данными:

**Идентификационные данные**

|  |
| --- |
| Информация об органе ПФР |
| Наименование заявителя (CommonName)  |  |
| Наименование организации (organizationName) |  |
| Область, край (stateOrProvinceName) | 78 Тверская область |
| Страна (countryName) | RU |
| Город (localityName) |  |
| Адрес, улица, дом (streetAddress) |  |
| ОГРН организации (OGRN) |  |
| ИНН организации (INN) |  |
| Полномочный представитель органа ПФР: |
| Фамилия (surname) |  |
| Имя отчество (givenName) |  |
| СНИЛС (SNILS) |  |
| Адрес электронной почты (E-Mail (E)) |  |
| Подразделение организации (organizationUnitName) |  |
| Должность (title) |  |
| Табельный номер |  |
| Дополнительная информация |
| Дата, номер и наименование документа о назначении полномочного представителя органа ПФР |  |
| Адрес корпоративной электронной почты Lotus |  |
| Дополнительный объектный идентификатор OID |  |

Наименование средств электронной подписи, с которыми используется данный сертификат ключа проверки электронной подписи: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Обязуюсь выполнять требования Регламента работы УЦ ОПФР, инструкции пользователя к установленному программному обеспечению и требования по обеспечению безопасности информации и применению средств электронной подписи.

Возражений против обработки и хранения моих персональных данных в реестре УЦ ОПФР, а также использования владельцами ключей проверки электронной подписи системы электронного документооборота ПФР данных, включаемых в сертификат ключа проверки электронной подписи, не имею.

Полномочный представитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

 (подпись)(фамилия и инициалы)

|  |
| --- |
| Достоверность сведений, указанных в заявлении, проверил:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Уполномоченное лицо Заявителя (подпись) (фамилия и инициалы) |

**Отметка УЦ ОПФР**

|  |
| --- |
| Дата регистрации пользователя «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20 г. |
| Уполномоченное лицо УЦ ОПФР \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) (фамилия и инициалы) |

**Приложение 2**

к Регламенту УЦ ОПФР

**СОГЛАСИЕ**

**на включение персональных данных пользователя Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области в общедоступные источники персональных данных
(реестр выданных аккредитованным удостоверяющим центром квалифицированных сертификатов ключей проверки электронной подписи)**

Я (далее – Пользователь УЦ), \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

 *(фамилия, имя, отчество)*

документ, удостоверяющий личность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ серия \_\_\_\_\_\_\_ №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(вид документа)*

выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(кем и когда)*

зарегистрированный(ая) по адресу:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

даю свое согласие государственному учреждению – Отделению Пенсионного фонда Российской Федерации по Тверской области (далее – Удостоверяющий центр), ОГРН 1026900566880, ИНН 6903005441, зарегистрированному по адресу: ул. Вагжанова, д. 9 стр. 1, Тверь, 170100, на включение моих персональных данных в общедоступные источники персональных данных (далее ПДн), на следующих условиях:

1. Настоящее согласие дается в целях выполнения Удостоверяющим центром функций, возложенных Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и иных нормативных правовых актов, регламентирующих применение усиленной квалифицированной электронной подписи.

2. Перечень ПДн, на которые дается согласие:

* фамилия, имя, отчество (при наличии);
* сведение о месте работы;
* занимаемая должность;
* страховой номер страхового свидетельства обязательного пенсионного страхования;
* e-mail.

3. Пользователь УЦ дает свое согласие на следующие действия:

* обработку (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание и блокирование ПДн;
* передачу ПДн третьим лицам или распространение в случаях, установленных Федеральным законом от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» и Регламентом УЦ.

4. Общедоступные источники персональных данных могут издаваться в виде справочников (реестров), передаваться на бумажных носителях или в электронном виде.

5. Настоящее согласие действует бессрочно.

6. Пользователь УЦ подтверждает, что он ознакомлен с Регламентом работы Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области при выполнении функций аккредитованного удостоверяющего центра.

Подтверждаю, что ознакомлен(а) с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», права и обязанности в области защиты ПДн мне разъяснены.

|  |  |  |
| --- | --- | --- |
| «\_\_\_» \_\_\_\_\_\_\_\_\_20\_\_\_ г. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| *Дата* | *Подпись* |  *Фамилия И.О.* |

**Приложение 3**

к Регламенту УЦ ОПФР

|  |  |  |  |
| --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
|

|  |  |
| --- | --- |
| ViPNet Administrator [Удостоверяющий и ключевой центр] |  |

 |

 |
| **Сертификат ключа проверки электронной подписи** |
| **Кому выдан:**  |
| **Кем выдан: ОПФР по Тверской области** |
| **Действителен с \_\_ \_\_\_\_ 20\_\_ г. по \_\_\_\_\_\_\_\_ 20\_\_ г.** |
|

|  |  |
| --- | --- |
| Назначение: | * Подтверждает удаленному компьютеру идентификацию вашего компьютера.
* Защищает сообщения электронной почты.
* Класс средства ЭП КС1.
* Класс средства ЭП КС2.
 |
|  |  |  |

 |
|

|  |  |
| --- | --- |
| Версия: | V3 |
| Серийный номер: |  |
| Алгоритм электронной подписи: | ГОСТ Р 34.10/34.11-2001 |
| Издатель: | Имя: ОПФР по Тверской областиПодразделение: Отдел по защите информацииОрганизация: ОПФР по Тверской областиЭлектронная почта: Область: 69 Тверская областьГород: ТверьСтрана: RUИНН: ОГРН: Адрес, улица: ул.Вагжанова, д9. стр.1 |
| Действителен с: |  |
| Действителен по: |  |
| Субъект: | Имя: Должность: Подразделение: Организация: Область: Тверская областьГород: Страна: RUАдрес, улица: СНИЛС: ОГРН: ИНН: Фамилия:  |
| Открытый ключ: | ГОСТ Р 34.10-2001 (512 бит) |
| **Расширения сертификата X.509** |
| Использование ключа:   | Электронная подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (F8) |
| Расширенное использование ключа:   | Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)Защищенная электронная почта (1.3.6.1.5.5.7.3.4) |
| Точки распространения списков отзыва (CRL):   | [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://ca.pfrf.ru/ot\_tver/ot\_tver\_2017.crl  |
| Средство электронной подписи владельца:   | Средство криптографической защиты информации (СКЗИ) ViPNet CSP 4.2 |
| Средство электронной подписи издателя:   | Наименование средства электронной подписи=Средство криптографической защиты информации (СКЗИ) ViPNet CSP 4.2Наименование средства Удостоверяющего центра=Программный комплекс "ViPNet Удостоверяющий центр 4 (версия 4.6)"Реквизиты соответствия средства электронной подписи=Сертификат соответствия №СФ/124-2860 от 15.03.2016 г.Реквизиты соответствия средства Удостоверяющего центра=Сертификат соответствия №СФ/128-2932 от 10.08.2016 г. |
| Идентификатор ключа центра сертификатов:   | Идентификатор ключа=B4 0C 58 BA 3B E6 DC 04 6B AA 6F CD FD 84 B9 EF 09 79 A0 B8Издатель сертификата: E=dit@minsvyaz.ruC=RUS=77 г. МоскваL=МоскваSTREET="125375 г. Москва, ул. Тверская, д. 7"O=Минкомсвязь РоссииOGRN=1047702026701INN=007710474375CN=Головной удостоверяющий центрСерийный номер сертификата=00 93 AB 27 0F 00 00 00 00 01 4A |
| Политики сертификата:   | [1]Политика сертификата: Идентификатор политики=Класс средства ЭП KC1 [2]Политика сертификата: Идентификатор политики=Класс средства ЭП KC2  |
| Идентификатор ключа субъекта:   | 5A 3B A1 0E 3E 2B 85 F4 1F 7C C2 5E 2E 61 67 41 09 57 01 03 |
| Основные ограничения:   | Тип субъекта=Пользователь |

 |
| **Результат проверки сертификата** |
| Сертификат действителен.Проверен  |
|

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Владелец**

|  |
| --- |
| Подпись |

"\_\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_\_ | **Уполномоченное лицо**

|  |  |
| --- | --- |
| Подпись | МП |

"\_\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_\_  |

 |

Подписывая настоящий документ получатель квалифицированного сертификата подтверждает:

1. что создание квалифицированного сертификата ключа проверки электронной подписи, содержащего вышеперечисленные данные, осуществлено Удостоверяющим центром Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области на основании заявки, поданной лицом, указанным в качестве владельца сертификата, что означает присоединение этого лица к Регламенту работы Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области при выполнении функций аккредитованного удостоверяющего центра, опубликованному на сайте http://www.pfrf.ru/branches/tver/info/~strahovatel/4156, и полное принятие этим лицом условий Регламента и всех его положений, в том числе и в части обработки ОПФР по Тверской области персональных данных лица, указанного в качестве владельца сертификата;

2. получение руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

|  |
| --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ФИО (полностью) |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ г.  |
|  Подпись  |
|  |
| Личность и полномочия получателя сертификата установил:  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(должность уполномоченного (доверенного) лица УЦ)  | \_\_\_\_\_\_\_\_\_\_\_\_\_(подпись) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(ФИО уполномоченного (доверенного) лица УЦ) |
| «\_\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ г.(дата вручения сертификата)  |

**Приложение 4**

к Регламенту УЦ ОПФР

Начальнику Удостоверяющего центра

Государственного учреждения - Отделения

Пенсионного фонда Российской Федерации

 по Тверской области

**Заявление**

**на прекращение действия квалифицированного сертификата**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование органа ПФР)

в связи с:

****компрометацией ключа ЭП

****увольнением работника

****переводом работника на должность не связанную с применением ЭП

****выходом из строя ключевого носителя

****изменение регистрационной информации работника

****иное:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(указать причину)

просит прекратить действие выданного Удостоверяющим центром Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области сертификата ключа проверки электронной подписи со следующими реквизитами:

Серийный номер сертификата: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Фамилия, имя, отчество физического лица, указанного в качестве владельца сертификата наряду с наименованием юридического лица:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ИНН: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

КПП: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Подпись и расшифровка подписи физического лица, указанного в качестве владельца сертификата наряду с наименованием юридического лица, или физического лица, имеющего право действовать от имени юридического лица без доверенности (руководителя юридического лица):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (должность) (подпись) (фамилия, инициалы)

«\_\_\_»\_\_\_\_\_\_\_\_\_20\_\_\_ г.

**Отметки Удостоверяющего центра Государственного учреждения - Отделения
Пенсионного фонда Российской Федерации по Тверской области**

Действие сертификата ключа проверки электронной подписи по заявке прекращено

 в \_\_\_\_ ч. \_\_\_\_ мин. «\_\_\_»\_\_\_\_\_\_\_\_\_20\_\_\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (должность) (подпись) (фамилия, инициалы)

**Приложение 5**

к Регламенту УЦ ОПФР

Начальнику Удостоверяющего центра

Государственного учреждения - Отделения

Пенсионного фонда Российской Федерации

 по Тверской области

**Заявление
на подтверждение подлинности электронной подписи Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области в сертификате ключа проверки электронной подписи Пользователя**

 (полное наименование организации, включая организационно-правовую форму)

в лице

(должность) (фамилия, имя. отчество)

действующего на основании

просит подтвердить подлинность электронной подписи Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области в изданном Удостоверяющим центром сертификате ключа проверки электронной подписи и установить его статус (действует/не действует) на основании предоставленных исходных данных:

1. Файл сертификата ключа проверки электронной подписи на прилагаемом к заявлению внешнем носителе данных.
2. Время и дата, на момент наступления которых требуется установить статус сертификата:

« : » « / / »

 час минута день месяц год

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность руководителя организации) (подпись) (фамилия, инициалы руководителя организации)

«\_\_\_»\_\_\_\_\_\_\_\_\_20\_\_\_ г.

МП.

**Приложение 6**

к Регламенту УЦ ОПФР

Начальнику Удостоверяющего центра

Государственного учреждения - Отделения

Пенсионного фонда Российской Федерации

 по Тверской области

**Заявление
на получение информации из реестра сертификатов
Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области**

(полное наименование организации, включая организационно-правовую форму юридического лица)

в лице\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(должность)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(фамилия, имя, отчество)

действующего на основании\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(полное фамилия, имя, отчество физического лица)

просит предоставить информацию о статусе следующего сертификата ключа проверки электронной подписи, выданного Удостоверяющим центром Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области:

Общее имя (CommonName)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Серийный номер сертификата ключа подписи (SerialNumber):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Время (период времени) на момент наступления которого требуется установить статус сертификата:

с «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_» по «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_».

Предоставить сертификат проверки ключа подписи в электронной форме в формате X.509 \_\_\_\_\_\_\_\_\_\_(Да/Нет)

Ответ отправить на электронный адрес: \_\_\_\_ @\_\_\_\_\_\_.\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность руководителя организации) (подпись) (фамилия, инициалы руководителя организации)

«\_\_\_»\_\_\_\_\_\_\_\_\_20\_\_\_ г.

МП.

**Приложение 7**

к Регламенту УЦ ОПФР

Начальнику Удостоверяющего центра

Государственного учреждения - Отделения

Пенсионного фонда Российской Федерации

 по Тверской области

**Заявление**

**на регистрацию в Единой системе идентификации и аутентификации**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, являясь Пользователем Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области, в соответствии с частью 5 статьи 18 Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи» прошу зарегистрировать меня в Единой системе идентификации и аутентификации на основании следующих данных:

Фамилия заявителя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (в именительном падеже)

Имя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Отчество: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (в именительном падеже) (при наличии, в именительном падеже)

Пол: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Дата рождения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (мужской / женский) (в формате ДД.ММ.ГГГГ)

Место рождения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

СНИЛС: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Гражданство: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (например, Россия)

Адрес электронной почты: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер мобильного телефона: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (в формате +7(xxx)xxxxxxx)

Данные документа, удостоверяющего личность:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (наименование документа)

номер \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (серия и номер документа) (кем выдан)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_дата выдачи: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ код подразделения: \_\_\_\_\_\_\_\_\_\_\_\_\_

 (когда выдан)

Настоящим даю согласие на обработку ОПФР по Тверской области персональных данных, содержащихся в настоящем Заявлении, включая передачу этих данных в Единую систему идентификации и аутентификации.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись) (фамилия, инициалы)

Дата подачи заявления: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Приложение 8**

к Регламенту УЦ ОПФР

**РУКОВОДСТВО
по обеспечению безопасности использования квалифицированных ключей электронной подписи и средств квалифицированной электронной подписи**

**1. Общие положения**

Настоящее «Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи» (далее – Руководство) составлено в соответствии со следующими нормативно-правовыми актами:

- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

- Приказ ФСБ РФ от 09.02.2005 № 66 (ред. от 12.04.2010) «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

и является средством официального информирования лиц, являющихся Пользователями Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области, 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.

Руководство предназначено для обязательного ознакомления Пользователей Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области и, использующих квалифицированную электронную подпись и средства квалифицированной электронной подписи при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

**2. Организационно-технические меры обеспечения безопасности квалифицированной электронной подписи и средств квалифицированной электронной подписи**

2.1. Помещения, в которых размещаются ПЭВМ со средствами электронной подписи должны обеспечивать конфиденциальность проводимых работ и исключать возможность бесконтрольного проникновения в них посторонних лиц.

В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты информации и подписываемую информацию.

Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

2.2. ПЭВМ со средствами электронной подписи должны быть оснащены средствами контроля вскрытия (опечатаны, опломбированы), при выявлении факта несанкционированного вскрытия работа на такой ПЭВМ должна быть прекращена.

2.3. На время отсутствия Пользователя ключевые документы должны быть убраны в опечатываемое хранилище.

2.4. Хранить ключевые документы, средства электронной подписи, соответствующую эксплуатационную и техническую документацию следует в шкафах (ящиках, хранилищах) индивидуального использования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

2.5. Должны быть предусмотрены меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленными средствами электронной подписи.

2.6. Установленное на АРМ программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

2.7. При увольнении или переводе в другое подразделение (на другую должность), изменении функциональных обязанностей работника, имевшего доступ к ключевым документам, должна быть проведена смена ключей электронной подписи.

2.8. ПЭВМ со средствами электронной подписи должны быть оснащены только лицензионным программным обеспечением, в случае обнаружения посторонних программ, нарушения целостности программного обеспечения, работа на такой ПЭВМ должна быть прекращена.

2.9. ПЭВМ со средствами электронной подписи должны быть сконфигурированы с учетом следующих требований:

- вхождение в режим конфигурирования BIOS штатными средствами BIOS должно осуществляться только с использованием парольной защиты при длине пароля не менее 6 символов;

– на средствах вычислительной техники с установленными средствами квалифицированной электронной подписи должна быть установлена только одна операционная система;

– не использовать нестандартные, измененные или отладочные версии операционных систем;

– исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;

- 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 операционной системы без запроса пароля. При этом должны быть реализованы дополнительные организационно – режимные меры, исключающие несанкционированный доступ к этим АРМ.

– исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;

– все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);

– режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;

– всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;

Кроме того, необходимо организовать стирание (по окончанию сеанса работы средств квалифицированной электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

2.10. На ПЭВМ со средствами электронной подписи должно быть исключено попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий.

2.11. Необходимо регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий.

2.12. В случае подключения технических средств с установленными средствами квалифицированной электронной подписи к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети. С целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем к программному обеспечению, в окружении которого функционируют средства квалифицированной электронной подписи и к компонентам средств квалифицированной электронной подписи со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN-сетей и т.п.). Все средства защиты, должны иметь сертификат уполномоченного органа по сертификации средств защиты.

2.13. Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.

2.14. Организовать и использовать комплекс мероприятий по антивирусной защите.

**3. Правила работы с квалифицированной электронной подписью и средствами квалифицированной электронной подписи**

3.1. При работе с квалифицированной электронной подписью и средствами электронной подписи Пользователь Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области области **обязан**:

3.1.1. не разглашать конфиденциальную информацию, к которой имеется допуск;

3.1.2. соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием средств электронной подписи;

3.1.3. не нарушать целостность ключевой информации;

3.1.4. сохранять в тайне ПИН-код для доступа к ключевому носителю;

3.1.5. обеспечить условия хранения ключевого носителя, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования и копирования;

3.1.6. сохранять в тайне содержание средств электронной подписи;

3.1.7. использовать для создания, проверки квалифицированной электронной подписи только сертифицированные средства электронной подписи;

3.1.8. использовать квалифицированную электронную подпись в соответствии с ограничениями, содержащимися в квалифицированном сертификате (если такие ограничения установлены);

3.1.9. не допускать использование принадлежащего ему ключа электронной подписи без согласия другими лицами;

3.1.10. своевременно обновлять сертификат ключа проверки электронной подписи при истечении его срока действия в соответствии с Регламентом Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области;

3.1.11. не использовать ключ электронной подписи и немедленно обратиться в Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области, выдавший квалифицированный сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;

3.1.12. не использовать ключ электронной подписи, сертификат ключа проверки электронной подписи которого аннулирован или прекратил действие;

3.1.13. немедленно уведомить удостоверяющий центр о фактах утраты ключевых носителей, содержащих ключи квалифицированной электронной подписи, средств электронной подписи и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки такой информации;

3.1.14. сдать ключи квалифицированной электронной подписи, средства квалифицированной электронной подписи, эксплуатационную и техническую документацию к ним в соответствии с порядком, установленным при увольнении или отстранении от исполнения обязанностей, связанных с использованием средств квалифицированной электронной подписи.

3.2. Пользователю Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области **запрещается**:

3.2.1. оставлять без контроля вычислительные средства, на которых эксплуатируется средства квалифицированной электронной подписи после ввода ключевой информации либо иной конфиденциальной информации;

3.2.2. вносить изменение в программное обеспечение средств электронной подписи;

3.2.3. работать на компьютере, если во время его начальной загрузки не проходит встроенный тест ОЗУ, предусмотренный в ПЭВМ;

3.2.4. осуществлять несанкционированное копирование ключевых носителей;

3.2.5. разглашать содержимое носителей ключевой информации или передавать носители лицам к ним не допущенным;

3.2.6. выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;

3.2.7. использовать ключевые носители в режимах, не предусмотренных функционированием средств квалифицированной электронной подписи;

3.2.8. записывать на ключевые носители постороннюю информацию;

3.2.9. вставлять ключевой носитель в устройство считывания при проведении работ, не являющихся штатными процедурами использования средств электронной подписи;

3.2.10. изменять настройки, установленные программой установки средства квалифицированной электронной подписи или администратором в соответствии с технической документацией.

**4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи**

4.1. Меры защиты ключей квалифицированной электронной подписи

Ключи квалифицированной электронной подписи при их создании должны записываться на типы ключевых носителей, которые поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним.

Ключи квалифицированной электронной подписи на ключевом носителе могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей электронной подписи, в соответствии с требованиями на используемое средство квалифицированной электронной подписи.

Если процедуру генерации ключей выполняет работник Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области, то он должен сообщить сформированный пароль (ПИН-код) владельцу ключа квалифицированной электронной подписи. Пользователь после получения ключевого носителя должен сменить пароль (ПИН-код).

Ответственность за обеспечение конфиденциальности пароля (ПИН-кода) возлагается на владельца сертификата.

4.2. Обращение с ключевой информацией и ключевыми носителями

Недопустимо пересылать файлы с ключевой информацией для работы в системах обмена электронными документами по электронной почте сети Интернет или по внутренней электронной почте (кроме запросов на сертификат и сертификатов ключей проверки электронной подписи).

Ключевая информация должна размещаться на сменном носителе информации (USB-flash накопитель, eToken/JaCarta). Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной электронной подписи, запрещено.

Носители ключевой информации должны использоваться только их владельцем либо уполномоченным лицом на использование данного носителя, и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

Сохранение пароля (ПИН-кода) на носитель ключевой информации запрещено. Ввод пароля (ПИН-кода) только во время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи.

На носителе ключевой информации (USB-flash накопителе) недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

4.3. Обеспечение безопасности АРМ с установленными средствами квалифицированной электронной подписи

С целью контроля исходящего и входящего подозрительного трафика, технические средства с установленными средствами квалифицированной электронной подписи должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. Эти средства должны пресекать отправку в Интернет информации, инициированную программами, не имеющими соответствующих полномочий.

В качестве автоматизированного рабочего места для работы в системах обмена электронными документами крайне не рекомендуется выбирать переносной компьютер (ноутбук). Если выбран ноутбук, недопустимо его подключение к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.д.), без применения сертифицированных средств межсетевого экранирования и обеспечивающих защищенный канал. При этом для хранения ключевой информации должен использоваться только индивидуальные ключи eToken/JaCarta.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной электронной подписи, необходимо гарантированно удалить всю информацию, использование которой третьими лицами может потенциально нанести вред организации, в том числе средства квалифицированной электронной подписи, журналы работы систем обмена электронными документами и т.д.).

**5. Дополнительные требования**

Перечень рекомендаций, приведенных в настоящем Руководстве, не является исчерпывающим. Пользователь Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области обязан выполнять иные действия, предусмотренные нормативными документами в области защиты информации по предотвращению несанкционированного использования электронной подписи и средств электронной подписи. Пользователь Удостоверяющего центра Государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Тверской области также обязан в полной мере выполнять требования технической документации на используемые средства электронной подписи, и средства криптографической защиты информации.

Начальник отдела по защите информации С.Б. Кулагин»