ООО «ИНТЕРФОРУМ»

УТВЕРЖДАЮ
Генеральный директор
_____/Рябоволик Б.Б./
М.П.
«02» марта 2020 г.

Регламент (Порядок) Удостоверяющего центра

Актуальная версия	http://www.if-spb.ru/files/ReglamentUC.pdf
Версия	2.3 от 2 марта 2020

Содержание

1. Общие положения.

1.1. Предмет регулирования.

Регламент устанавливает общий порядок реализации функций Удостоверяющего центра, условия предоставления и правила пользования услугами Удостоверяющего центра, включая права, обязанности, ответственность Удостоверяющего цента, Заявителя и Владельца сертификата, форматы данных, организационные мероприятия, направленные на обеспечение работы Удостоверяющего центра.

Настоящий Регламент публикуется в форме электронного документа на сайте ООО «ИНТЕРФОРУМ» по адресу: http://if-spb.ru/files/ReglamentUC.pdf. Опубликование Регламента, включая распространение его текста в глобальной компьютерной сети Интернет на сайте Удостоверяющего центра, должно рассматриваться всеми заинтересованными лицами как публичное предложение (оферта) со Стороны ООО «ИНТЕРФОРУМ» заключить договор на предоставление услуг Удостоверяющего центра, существенные условия которого зафиксированы в настоящем Регламенте.

Настоящий Регламент вводится в действие с момента его утверждения.

Настоящий Регламент разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

Субъекты области действия Регламента - все лица, которые в силу настоящего Регламента, договора или действующего законодательства обязаны соблюдать правила и выполнять все требования, предусмотренные настоящим Регламентом: Заявитель, Участники электронного взаимодействия, Владелец сертификата, Удостоверяющий центр (далее – Субъекты).

1.2. Присоединение к Регламенту.

Заключение соглашения с Удостоверяющим центром производится путем совершения письменного акцепта условий настоящего Регламента. Акцепт настоящего Регламента производится путем направления в адрес ООО «ИНТЕРФОРУМ» Заявления о присоединении к Регламенту (Приложение № 1 к Регламенту).

Заключение соглашения с Удостоверяющим центром производится на условиях, предусмотренных для договора присоединения в соответствии со ст. 428 ГК РФ, т.е. путем присоединения к Регламенту в целом, с учетом условий, которые изложены в приложениях к настоящему Регламенту.

Удостоверяющий центр вправе отказать любому лицу в присоединении к Регламенту с указанием обоснованных причин.

Акцепт будет считаться совершенным с момента регистрации указанного заявления в ООО «ИНТЕРФОРУМ». Отметка о регистрации заявления производится работником ООО «ИНТЕРФОРУМ». Факт присоединения лица к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент регистрации заявления о присоединении к Регламенту в реестре Удостоверяющего центра. Лицо, присоединившееся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

Основанием для начала предоставления услуг является оплата услуг в соответствии с заключенным договором об оказании услуг при условии, что к этому моменту договор о присоединении к Регламенту также является заключенным.

1.3. Стороны соглашения.

Сторонами соглашения являются:

Удостоверяющий центр, предоставляющий свои услуги в соответствии с данным Регламентом и условиями договора, заключаемого с Клиентом;

Клиент – юридическое или физическое лицо, присоединившееся к данному Регламенту и которому Удостоверяющий центр, предоставляет свои услуги;

1.4. Порядок расторжения соглашения.

Действие настоящего соглашения может быть прекращено по инициативе одной из Сторон в следующих случаях:

- по собственному желанию одной из Сторон;
- нарушения одной из Сторон условий настоящего Регламента.

В случае расторжения соглашения инициативная Сторона письменно уведомляет другую Сторону о своих намерениях за тридцать календарных дней до даты расторжения соглашения. Стороны осуществляют окончательные взаиморасчеты в течение 10 (Десяти) дней с даты расторжения соглашения.

Клиент имеет право в одностороннем порядке прекратить взаимодействие с Удостоверяющим центром в рамках Регламента, направив в Удостоверяющий центр заявление на отзыв (аннулирование) сертификата.

Прекращение действия соглашения не освобождает Стороны от исполнения обязательств, возникших до указанного дня прекращения действия соглашения, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

1.5. Изменения (дополнения) Регламента.

Настоящий Регламент действует весь срок до своей отмены.

Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

Уведомление о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем обязательного размещения указанных изменений (дополнений) на сайте Удостоверяющего центра по адресу – https://www.if-spb.ru/.

Все изменения (дополнения), вносимые Удостоверяющим центром в настоящий Регламент по собственной инициативе и не связанные с изменением законодательства РФ, могут быть связаны с улучшением условий предоставления действующих услуг, добавления нового вида услуг, изменением адресов регистрации и размещения Удостоверяющего центра, а также адресов размещения электронных ресурсов, изменениями в структуре Удостоверяющего центра, и вступают в силу и становятся обязательными для Клиентов по истечении 10 (десяти) календарных дней с даты опубликования нового Регламента на сайте Удостоверяющего центра.

Все изменения (дополнения), вносимые Удостоверяющим центром в Регламент в связи с изменением действующего законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу. В случае несогласия с изменениями (дополнениями) Сторона Регламента имеет право до вступления в силу таких изменений (дополнений) на расторжение Регламента в порядке, предусмотренном разделом 1.4 настоящего Регламента.

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

1.6. Сведения об Удостоверяющем центре.

Удостоверяющий центр – организация, осуществляющая функции по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей и иные функции удостоверяющего центра в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон № 63-ФЗ).

Общество с ограниченной ответственностью «ИНТЕРФОРУМ» (ИНН/КПП 7838433333/783801001), именуемой в дальнейшем «Удостоверяющий центр», зарегистрировано на территории РФ в городе Санкт-Петербург. Свидетельство о регистрации № Р51001 выдано 27.10.2009 межрайонной инспекцией Федеральной налоговой службы №15 по Санкт-Петербургу.

Удостоверяющий центр в качестве участника рынка услуг по созданию и выдаче сертификатов ключей проверки электронных подписей осуществляет свою деятельность на территории Российской федерации на основание следующих документов:

- приказа Министерства связи и массовых коммуникаций № 127 от 22.04.2015.г. "Об аккредитации удостоверяющих центров";

- лицензии Управления Федеральной службы безопасности Российской Федерации по городу Санкт-Петербургу и Ленинградской области от 19.12.2018 рег. № 1196Н на бланке ЛСЗ 0001054 на осуществление деятельности по разработке, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказанию услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица и индивидуального предпринимателя).

Юридический адрес: 190013, Санкт-Петербург, ул. Рузовская, д. 8, литер Б, офис 213

Фактический адрес: 191124, г. Санкт-Петербург, ул. Красного Текстильщика 10\12 лит. Д

Адрес для корреспонденции: 191124 г. Санкт-Петербург, ул. Красного Текстильщика 10\12 лит. Э оф. 605\4.

Удостоверяющий центр осуществляет свою работу по графику. Информация о времени посещения офиса Удостоверяющего центра предоставляется при обращении Заявителя по контактным данным, указанным на официальном сайте удостоверяющего центра https://www.if-spb.ru/

График работы Удостоверяющего центра:

Понедельник	9:00-18:00
Вторник	9:00-18:00
Среда	9:00-18:00
Четверг	9:00-18:00
Пятница	9:00-18:00
Суббота	Закрыто
Воскресенье	Закрыто

1.7. Порядок информирования о предоставлении услуг Удостоверяющего центра.

Информирование по вопросам предоставления услуг Удостоверяющего центра осуществляется следующими способами:

1) по контактному номеру телефона: тел.: +7 (812) 318-05-79;

2) по адресу электронной почты: e-mail: rudc@inter-forum.org;

3) путем опубликования информации на официальном сайте: https://www.if-spb.ru/.

Информирование субъектов Удостоверяющим центром производится посредством направления электронного письма на адрес, указанный при обращении и/или ином взаимодействии с Удостоверяющим центром, посредством направления SMS-уведомлений на телефонный номер, представленный Заявителем в Удостоверяющий центр, и/или посредством размещения информации на сайте по адресу https://www.if-spb.ru/.

Адреса местонахождения, справочные телефоны, адреса электронной почты Удостоверяющего центра опубликованы на официальном сайте Удостоверяющего центра https://www.if-spb.ru/

1.8. Стоимость услуг удостоверяющего центра.

Удостоверяющий центр осуществляет свою деятельность на платной основе.

Стоимость и состав услуг Удостоверяющего центра устанавливается прайс-листом Удостоверяющего центра. С ценами на услуги Удостоверяющего центра и их составом можно ознакомиться на официальном сайте: https://www.if-spb.ru/.

Сроки и порядок расчетов за услуги, оказываемые Удостоверяющим центром, регулируются условиями договора между Удостоверяющим центром и Клиентом.

Оплата услуг Удостоверяющего центра осуществляется в российских рублях по безналичному расчету путем перечисления денежных средств на расчетный счет или иным способом, предусмотренным законодательством РФ.

ООО «ИНТЕРФОРУМ» осуществляет выставление счета Клиенту за оказываемые по настоящему Регламенту услуги с использованием общедоступных средств связи, таких как: электронная почта, факсимильная связь, почтовое отправление. По желанию Клиента счет может выдаваться представителю Клиента.

В случае выполнения внеплановой смены Ключа электронной подписи Удостоверяющего центра, Удостоверяющий центр безвозмездно создаёт Сертификаты для всех Владельцев сертификатов, чьи сертификаты прекращают действие в связи с внеплановой заменой.

Удостоверяющий центр безвозмездно представляет Сертификаты в форме электронных документов из Реестра выданных сертификатов Удостоверяющего центра, а также безвозмездно публикует Списки отозванных сертификатов.

В случае нарушения Клиентом любого из положений финансовых условий настоящего Регламента и приложений к нему в отношении оплаты услуг Удостоверяющего центра в полном объеме, последний имеет право не оказывать Клиенту услуги до исполнения обязательств по Регламенту надлежащим образом. В этом случае риск возможных убытков Клиента полностью ложится на Клиента (п.1. ст. 406 части первой ГК РФ).

Услуги Удостоверяющего центра считаются оказанными, если Клиент не предъявил претензий в письменном виде по их качеству и объему в течение 3 (трех) рабочих дней со дня их оказания, с обязательным предварительным уведомлением Удостоверяющего центра о выставлении претензии по телефону, факсимильной связи, электронной почте или с использованием других средств связи.

1.9. Нормативные ссылки.

Удостоверяющий центр осуществляет свою деятельность в соответствии с положениями следующих нормативных документов:

- Федеральный Закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- Приказ ФСБ РФ от 27 декабря 2011 г. N 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи»;
- Приказ ФСБ РФ от 27 декабря 2011 г. N 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра»;

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Гражданский Кодекс Российской Федерации (часть первая) от 30.11.1994 №51-ФЗ (принят Государственной Думой РФ 21.10. 1994);
- ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая информация. Процессы формирования и проверки электронной цифровой подписи»;
- ГОСТ Р 34.11-94 «Информационная технология. Криптографическая информация. Функции хеширования»;
- Приказ Минкомсвязи России от 13.08.2018 №397 «Об утверждении требований к порядку реализации функции аккредитованного удостоверяющего центра и исполнения его обязанностей»;
- ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая информация. Процессы формирования и проверки электронной цифровой подписи».

1.10. Термины и определения.

В Регламенте используются термины и определения, установленные Федеральным законом № 63-ФЗ, а также термины и определения их дополняющие и конкретизирующие.

Аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального Закона № 63-ФЗ;

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности электронной подписи;

Владелец сертификата ключа проверки электронной подписи (Владелец сертификата) – лицо, которому в установленном настоящим Регламентом порядке выдан сертификат ключа проверки электронной подписи, в соответствии с Федеральным законом № 63-ФЗ. Для Сертификата юридического лица вторым Владельцем является физическое лицо, данные о котором по заявлению юридического лица внесены в его Сертификат (Уполномоченный представитель Заявителя). В случаях, предусмотренных пунктом 3 статьи 14 Федерального закона № 63-ФЗ, данные о физическом лице в Сертификат не вносятся, единственным Владельцем сертификата является юридическое лицо;

Доверенное лицо – физическое лицо, которое действует от имени физического или юридического лица, уполномоченное ими на передачу документов для получения квалифицированного сертификата и получение квалифицированного сертификата.

Заявитель − юридическое лицо независимо от организационно-правовой формы, физическое лицо или иной хозяйствующий субъект (в том числе индивидуальный предприниматель, адвокат, нотариус и т.д.), обращающиеся в Удостоверяющий центр для получения Сертификата. После создания Сертификата Заявитель становится Владельцем сертификата.

Квалифицированная электронная подпись (КЭП) – усиленная электронная

подпись, соответствующая следующим признакам:

- получена в результате криптографического преобразования информации с использованием
- ключа электронной подписи и средств (средства) электронной подписи, получивших (получившего) подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после его подписания;
- ключ проверки электронной подписи указан в квалифицированном сертификате ключа проверки электронной подписи.

Квалифицированный сертификат ключа проверки ЭП (далее - квалифицированный сертификат) - сертификат ключа проверки ЭП, выданный аккредитованным УЦ или доверенным

лицом аккредитованного УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования ЭП (далее - уполномоченный федеральный орган);

Ключ электронной подписи (Ключ ЭП) – уникальная последовательность символов, известная Владельцу ключа электронной подписи и предназначенная для создания в электронных документах электронной подписи.

Ключ проверки электронной подписи (Ключ проверки ЭП**)** – уникальная последовательность символов, соответствующая ключу электронной подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной подписи подлинности электронной подписи в электронном документе;

Ключевой контейнер – совокупность данных определенной структуры, содержащих ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию;

Ключевой носитель - носитель, предназначенный для хранения и содержащий ключ электронной подписи и/или дополнительную служебную информацию;

Компрометация ключа подписи – утрата доверия к тому, что используемые закрытые ключи недоступны посторонним лицам. К событиям, связанным с компрометацией ключей, относятся следующие ситуации:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку ключевой информации или ее искажение;
- нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
- доступ посторонних лиц к ключевой информации.

Конфиденциальность информации – характеристика информации, означающая ограничение круга лиц, имеющих к ней доступ;

Подтверждение подлинности электронной подписи в электронном документе – положительный результат проверки соответствующим средством электронной подписи с использованием сертификата ключа проверки электронной подписи принадлежности данной электронной подписи в электронном документе Владельцу сертификата ключа проверки электронной подписи и отсутствия искажений в электронном документе, подписанном данной электронной подписью;

Реестр сертификатов – реестр выданных и отозванных Удостоверяющим центром Сертификатов, включающий в себя информацию, содержащуюся в выданных этим Удостоверяющим центром Сертификатах, информацию о датах прекращения действия или аннулирования Сертификатов и об основаниях такого прекращения и аннулирования.

Сертификат ключа проверки электронной подписи (далее – Сертификат) - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи Владельцу сертификата ключа проверки электронной подписи;

Список отозванных сертификатов – электронный документ с электронной подписью уполномоченного лица удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей подписи, которые на определенный момент времени были отозваны;

Средство удостоверяющего центра – программное и (или) аппаратное средство, используемое Удостоверяющим центром для выполнения своих функций.

Средства электронной подписи – средства криптографической защиты информации, обеспечивающие реализацию следующих функций: создание электронной подписи в электронном документе с использованием ключа электронной подписи, подтверждение с использованием ключа проверки электронной подписи подлинности электронной подписи в электронном документе, создание ключей электронных подписей;

Удостоверяющий центр – функциональное подразделение ООО «ИНТЕРФОРУМ», осуществляющее выполнение целевых функций Удостоверяющего центра в соответствии с действующим законодательством Российской Федерации;

Уполномоченное лицо Удостоверяющего центра – физическое лицо, являющееся сотрудником удостоверяющего центра и наделенное удостоверяющим центром полномочиями по выдаче квалифицированных сертификатов ключей проверки электронной подписи, а также иными полномочиями согласно настоящему Регламенту.

Участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане.

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.

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

1.11. Используемые сокращения.

АРМ - автоматизированное рабочее место

ГОСТ - Государственный стандарт

ЕГРИП - Единый государственный реестр индивидуальных предпринимателей

ЕГРЮЛ - Единый государственный реестр юридических лиц

ИНН - Индивидуальный номер налогоплательщика

ИП - Индивидуальный номер налогоплательщика

ОГРН - Основной государственный регистрационный номер

ООО - Общество с ограниченной ответственностью

ОС - Операционная система

ПИН-код - Секретная последовательность персонального идентификационного номера

ПО - программное обеспечение

РФ - Российская Федерация

СЗИ - Средство защиты информации

СНИЛС - Страховой номер индивидуального лицевого счета

УЦ - Удостоверяющий центр

Федеральный закон № 63-ФЗ - Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

ФЗ - Федеральный закон

ФСБ - Федеральная Служба Безопасности России

ЭП - Электронная подпись

CMS - (Cryptographic Message Syntax) стандарт криптографических сообщений

GMT - (Greenwich Mean Time) - астрономическое (Среднее солнечное) время меридиана, проходящего через прежнее место расположения Гринвичской королевской обсерватории около Лондона

2. Перечень реализуемых удостоверяющим центром функций (оказываемых услуг).

- Создание и выдача Сертификатов.
- Изготовление заверенных копий Сертификатов на бумажном носителе по запросу.
- Осуществление подтверждения владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному для получения Сертификата.
- Установление сроков действия Сертификатов.
- Прекращение действия (аннулирование) Сертификатов по запросам Владельцев сертификатов и в иных случаях, установленных Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между Удостоверяющим центром и Заявителем, а также настоящим Порядком. Услуги оказывается путём внесения сведений о прекращении действия в Реестр сертификатов.
- Выдача Средств электронной подписи, обеспечивающих возможность создания Ключа электронной подписи и Ключа проверки.
- Ведение реестра Сертификатов.
- Создание Ключей электронной подписи и Ключей проверки электронной подписи с гарантией обеспечения конфиденциальности Ключей электронной подписи.
- Проверка уникальности Ключей проверки в реестре Сертификатов.
- Проверка действительности ЭП, Ключи проверки которых содержатся в Сертификатах, выданных Удостоверяющим центром, в Электронных документах.
- Предоставление сведений об аннулированных Сертификатах и Сертификатах, действие которых прекращено, в том числе опубликование Реестра сертификатов по адресам, вносимым в соответствующее дополнение Сертификатов.
- Выдача инструкций по информационной безопасности, содержащих условия и порядок использования сертификатов ЭП, ключей ЭП и средств ЭП.
- Информирование лиц, обращающихся в Удостоверяющий центр для выдачи Сертификата, о рисках, связанных с использованием ЭП.
- Предоставление возможности Заявителю создать Ключи проверки и Ключи электронной подписи с гарантией обеспечения конфиденциальности Ключей электронной подписи в Удостоверяющем центре на специализированном рабочем месте.
- Представление по запросу Участников электронного взаимодействия Сертификатов, внесённых в Реестр сертификатов Удостоверяющего центра, в форме электронных документов.
- Выполнение иных функций, установленных действующим законодательством Российской Федерации.

3. Права и обязанности удостоверяющего центра. Ответственность удостоверяющего центра.

3.1. Права Удостоверяющего центра.

Удостоверяющий центр имеет право:

3.1.1. Запросить у Заявителя документы для подтверждения любой содержащейся в заявлении на выдачу Сертификата информации, а также документы, необходимые для разрешения противоречий между данными в заявлении на выдачу Сертификата и данными в иных представленных документах.

3.1.2. Обрабатывать персональные данные Заявителя и его представителей с использованием технических средств и без них.

3.1.3. Не принимать документы, не соответствующие требованиям действующих нормативных актов Российской Федерации, требованиям настоящего Порядка.

3.1.4. Отказать в выдаче Сертификата и/или изготовлении ключей в случае ненадлежащего оформления необходимых документов, предоставления неполной или недостоверной информации, а также в случае, если услуга по созданию и выдаче Сертификата не оплачена в надлежащем порядке.

3.1.5. Отказать в выдаче Сертификата в случае, если Заявитель-физическое лицо или Уполномоченный представитель Заявителя не предоставил письменного согласия на обработку своих персональных данных, в том числе на обработку персональных данных с использованием технических средств.

3.1.6. Отказать в выдаче Сертификата в случае, если Заявитель отказывается или уклоняется от посещения Удостоверяющего центра лично, когда это необходимо в целях подтверждения его волеизъявления, предоставленной информации и документов или удостоверения его личности.

3.1.7. Отказать с указанием причин в аннулировании (отзыве) Сертификата Владельцу сертификата, подавшему заявление на аннулирование (отзыв) сертификата, в случае ненадлежащего оформления заявления на аннулирование сертификата, а также в случае, если Сертификат аннулирован или прекратил свое действие по другим основаниям.

3.1.8. Без уведомления прекратить действие Сертификата в случае невыполнения Владельцем сертификата обязанностей, указанных в подразделе 4.3 Регламента, а также в случае появления достоверных сведений о том, что документы, представленные в соответствии с подразделом 4.1 настоящего Регламента, не являются подлинными или не подтверждают достоверность всей информации, включённой в данный Сертификат, и/или в случае, если услуга по созданию и выдаче данного Сертификата не оплачена в надлежащем порядке.

3.1.9. Прекратить действие Сертификата в случае получения Удостоверяющим центром подтверждения факта смерти Владельца сертификата − физического лица, факта внесения в Единый государственный реестр юридических лиц записи о ликвидации Владельца сертификата юридического лица, факта утраты силы государственной регистрации Владельца сертификата-физического лица в качестве индивидуального предпринимателя, главы крестьянского (фермерского) хозяйства, а также в случае вступления в силу судебного решения о дисквалификации Уполномоченного представителя Владельца сертификата.

3.1.10. Использовать представленные Заявителем номера мобильной связи и адреса электронной почты для рассылки уведомлений об окончании срока действия Сертификата, и иной информации.

3.1.11. Выдавать Сертификаты как в форме электронных документов, так и в форме документов на бумажном носителе.

3.1.12. Предоставлять копии Сертификатов в электронной форме, находящихся в Реестре Удостоверяющего центра, всем лицам, обратившимся за копиями в Удостоверяющий центр.

3.2. Обязанности Удостоверяющего центра.

- Информировать в письменной форме заявителей об условиях и о прядке 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.
- Предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к Реестру сертификатов информацию, содержащуюся в Реестре сертификатов, в том числе информацию об аннулировании Сертификата.
- Использовать для изготовления Закрытого ключа Уполномоченного лица Удостоверяющего центра и формирования ЭП только сертифицированные в соответствии с правилами сертификации РФ средства ЭП;
- Оказывать услуги в соответствии с требованиями, устанавливаемыми Федеральным законом № 63-ФЗ, другими Федеральными законами и принимаемыми в соответствии с ними нормативными актами.
- При выдаче Сертификата установить личность заявителя – физического лица, обратившегося за получением Сертификата и получить от лица, выступающего от имени заявителя юридического лица, подтверждения правомочия обращаться за получением Сертификата.
- С использованием инфраструктуры СМЭВ осуществлять обращение к государственным реестрам для проверки достоверности документов и сведений, представленных заявителем.
- Вносить в создаваемые Сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами и сведениями, полученными из государственных реестров.
- При выдаче Сертификата установить личность заявителя – физического лица, обратившегося за получением Сертификата и получить от лица, выступающего от имени заявителя юридического лица, подтверждения правомочия обращаться за получением Сертификата.
- Отказать заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи.
- Отказать заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи.
- В течение срока деятельности Удостоверяющего центра, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации, хранить информацию о реквизитах основного документа, удостоверяющего личность владельца Сертификата физического лица; о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя – юридического лица, обращаться за получением Сертификата; о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца Сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца Сертификата включена в Сертификат.
- Использовать Закрытый ключ Уполномоченного лица Удостоверяющего центра только для подписи издаваемых им Сертификатов и Списков отозванных сертификатов.
- Принимать меры по защите Закрытого ключа Уполномоченного лица Удостоверяющего центра от несанкционированного доступа.

- Организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса города Санкт-Петербург. Удостоверяющий центр обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.
- Обеспечить уникальность серийных номеров изготавливаемых Сертификатов.
- Проверять и обеспечивать уникальность значений Открытых ключей в изготовленных Сертификатах.
- Обеспечить конфиденциальность созданных Удостоверяющим центром ключей электронных подписей в пределах средств, находящихся в зоне ответственности Удостоверяющего центра.
- Обеспечить формирование закрытого ключа средствами ЭП, предусматривающими запись Закрытого ключа непосредственно на ключевой носитель, без сохранения сформированной ключевой информации на каком-либо ином носителе.
- Аннулировать (отозвать) Сертификат Пользователя УЦ в случае компрометации Закрытого ключа Уполномоченного лица Удостоверяющего центра, с использованием которого был издан Сертификат.
- Обеспечивать круглосуточную доступность Реестра сертификатов в сети Интернет, за исключением периодов планового или внепланового технического обслуживания.
- Осуществлять формирование и ведение Реестра сертификатов.
- Обеспечивать актуальность информации, содержащейся в Реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.
- Осуществлять выдачу копий Сертификатов в электронной форме по обращениям Владельцев сертификата.
- В случае принятия решения о прекращении своей деятельности, сообщить об этом на сайте http://www.if-spb.ru и в уполномоченный федеральный орган не позднее, чем за 1 (Один) месяц до даты прекращения своей деятельности, и передать в уполномоченный федеральный орган Реестр выданных сертификатов и Реестр зарегистрированных владельцев сертификатов.
- Произвести регистрацию Сертификата в Единой системе идентификации и аутентификации в соответствии с пунктом 5 статьи 18 Федерального закона № 63-ФЗ.
- Предоставить Заявителю по его требованию копии документов, на основании которых осуществляет свою деятельность.
- Исполнять прочие обязанности, предусмотренные Федеральным законом № 63-ФЗ, другими Федеральными законами и иными нормативными актами.

3.3. Ответственность Удостоверяющего центра.

Удостоверяющий центр несет гражданско-правовую и (или) административную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных Федеральным законом № 63-ФЗ и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также порядком реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей.

Удостоверяющий центр в соответствии с законодательством Российской Федерации будет нести ответственность за вред, причиненный третьим лицам в результате:

- неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг Удостоверяющего центра;
- неисполнения или ненадлежащего исполнения обязанностей, предусмотренных действующим законодательством и настоящим Регламентом.

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

- если Удостоверяющий центр обоснованно полагался на сведения, предоставленных Заявителем;
- подделки, подлога либо иного искажения Заявителем, Владельцем Сертификата либо третьими лицами информации, содержащейся в заявлении либо иных документах, представленных в Удостоверяющий центр;
- если Владелец Сертификата своевременно не осуществил процедуру по аннулированию (отзыву) Сертификата при компрометации Закрытого ключа;

Удостоверяющий центр не будет нести ответственность за невозможность использования Сертификата в случае, если такая невозможность возникла после создания Сертификата и вызвана изменением требований информационных систем или действующих нормативно-правовых актов.

Удостоверяющий центр несет ответственность за убытки при использовании созданного Удостоверяющим центром Закрытого ключа и Сертификата в том случае, если данные убытки возникли по причине компрометации Закрытого ключа Уполномоченного лица Удостоверяющего центра или вследствие несоответствия сведений в Сертификате сведениям, указанным в заявлении на выдачу Сертификата.

Удостоверяющий центр обладает необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед третьими лицами за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в Сертификатах, выданных Удостоверяющим центром, и/или недостоверности информации, содержащейся в реестре, который Удостоверяющий центр ведет в соответствии с Федеральным законом № 63-ФЗ.

Размер финансовых гарантий определяется законодательством РФ.

Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется законодательством РФ.

4. Права и обязанности Заявителя и Владельца сертификата.

4.1. Обязанности Заявителя.

4.1.1. Предъявить документы, удостоверяющие личность Доверенного лица Заявителя, Уполномоченного представителя Заявителя, Заявителя-физического лица в соответствии с подразделом 6.2.4 настоящего Регламента.

4.1.2. Обеспечить личную явку в Центр выдачи Заявителя либо его представителя.

4.1.3. Представить в Удостоверяющий центр документы, предусмотренные Федеральным законом № 63-ФЗ, другими Федеральными законами и принимаемыми в соответствии с ними нормативными актами, локальными документами отдельных информационных систем, и иные необходимые для создания Сертификата документы. Перечень документов, необходимых для создания Сертификата, определяется Профилем Сертификата с учетом положений пункта 3.1.1 настоящего Регламента.

4.1.4. По требованию Удостоверяющего центра обеспечить личную явку в Удостоверяющий центр определенных представителей Заявителя, а также совершить иные действия, направленные на обеспечение безопасности и законности процесса выдачи Сертификата (в том числе с использованием различных технических средств).

4.2. Права Владельца сертификата.

4.2.1. Обратиться в Удостоверяющий центр для прекращения действия выданного ему Сертификата в течение срока его действия.

4.2.2. Получить средства (средство) электронной подписи, получившие (получившее) подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ, и неисключительную лицензию на право его использования (при выдаче программного или программно-аппаратного средства).

4.2.3. Получить от Удостоверяющего центра инструкции по обеспечению безопасности использования электронной подписи и Средств электронной подписи.

4.3. Обязанности Владельца сертификата.

4.3.1. Все обязанности, предусмотренные подразделом 5.2 настоящего Регламента.

4.3.2. Обеспечить выполнение Правил по обеспечению безопасности на рабочем месте, опубликованных на сайте https://www.if-spb.ru/.

4.3.3. Обеспечивать конфиденциальность Ключей электронных подписей, в частности, не допускать использование принадлежащих им Ключей электронных подписей без их согласия.

4.3.4. Не использовать Ключ электронной подписи, Сертификат ключа проверки которой выдан Удостоверяющим центром, и немедленно обратиться в Удостоверяющий центр для прекращения действия этого Сертификата, при наличии оснований полагать, что конфиденциальность этого Ключа электронной подписи нарушена.

4.3.5. Уведомлять Удостоверяющий центр о нарушении конфиденциальности Ключа электронной подписи, Сертификат которой выдан Удостоверяющим центром, в течение не более чем 1 (Одного) рабочего дня со дня получения информации о таком нарушении.

4.3.6. При выдаче Сертификата под расписку ознакомиться с информацией, включаемой в Сертификат

4.3.7. В случае самостоятельного создания Ключа электронной подписи предоставить Удостоверяющему центру запрос на сертификат в формате, описанном в рекомендациях IETF RFC 2986 “PKCS #10: Certification Request Syntax Specification (2000)”, IETF RFC 4491 “Using GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, RFC 6986 «GOST R 34.11-2012: Hash Function», RFC 7091 «GOST R 34.10-2012: Digital Signature Algorithm», RFC 7836 «Guidelines on

the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R34.11-2012» с выполнением требований, предъявляемых к таким электронным документам используемыми Удостоверяющим центром Средствами удостоверяющего центра. Запрос на Сертификат должен содержать всю информацию, представляемую для включения в выдаваемый Сертификат, сведения о Средствах электронной подписи, использовавшихся для создания Ключа электронной подписи и Ключа проверки, и о Средствах электронной подписи, с которыми будет использоваться Сертификат.

4.3.8. Известить Удостоверяющий центр об изменениях в документах, и по требованию Удостоверяющего центра предоставить их в течение 5-ти рабочих дней с момента регистрации изменений.

4.3.9. С целью обеспечения гарантированного ознакомления Стороны, присоединившейся к Регламенту, с полным текстом изменений и дополнений Регламента до вступления их в силу не реже одного раза в десять календарных дней обращаться на сайт Удостоверяющего центра по адресу http://www.if-spb.ru/ за сведениями об изменениях и дополнениях в Регламент;

4.3.10. В случае прекращения полномочий лица, действующего от имени юридического лица без доверенности, вновь назначенное лицо, уполномоченное действовать от имени юридического лица без доверенности, обязано отозвать Сертификат лица, чьи полномочия прекращены, и/или сертификат ключа ЭП юридического лица и одновременно представить в Удостоверяющий центр нотариальную копию заявления в ЕГРЮЛ, содержащую сведения о новом лице, уполномоченном действовать от имени юридического лица без доверенности. Все риски неисполнения или несвоевременного исполнения данной обязанности несет юридическое лицо;

5. Права и обязанности участников электронного взаимодействия.

5.1. Права Участников электронного взаимодействия.

5.1.1. Использовать Реестр сертификатов для проверки действительности Сертификатов, созданных и выданных Удостоверяющим центром.

5.1.2. Получить Сертификат Удостоверяющего центра.

5.1.3. Получить Сертификат, находящийся в Реестре сертификатов Удостоверяющего центра.

5.1.4. Применять Сертификат для проверки ЭП в электронных документах.

5.1.5. Обратиться в Удостоверяющий центр за проверкой действительности ЭП, созданной с помощью Сертификата, выданного Удостоверяющим центром.

5.1.6. При обращении за выдачей Сертификата получить информацию о рисках, связанных с использованием ЭП.

5.1.7. Обратиться в Удостоверяющий центр за подтверждением подлинности ЭП в документах, представленных в электронной форме.

5.2. Обязанности Участников электронного взаимодействия.

5.2.1. Обеспечивать конфиденциальность Ключей ЭП, в частности, не допускать использование принадлежащих им Ключей ЭП без их согласия.

5.2.2. Использовать ЭП в соответствии с ограничениями, содержащимися в Сертификате ключа проверки этой электронной подписи.

5.2.3. Уведомлять Удостоверяющий центр, выдавший Сертификат, и иных участников электронного взаимодействия о нарушении конфиденциальности Ключа электронной подписи в течение не более чем 1 (Одного) рабочего дня со дня получения информации о таком нарушении.

5.2.4. Не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

5.2.5. Использовать для создания и проверки ЭП, ключа проверки ЭП и ключа ЭП средства электронной подписи в соответствии с Федеральным законом № 63-ФЗ.

6. Порядок и сроки выполнения процедур (действий) необходимых для предоставления услуг Удостоверяющим центром.

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

6.1.1. Порядок создания ключей электронных подписей и ключей проверки электронных подписей.

Создание ключа электронной подписей и ключа проверки электронной подписей возможно с использование следующих способов создания:

6.1.1.1. Порядок создания Ключей электронной подписи заявителем до обращения в удостоверяющий центр.

Заявитель самостоятельно создает ключ электронной подписи и ключ проверки электронной подписи с соблюдением правил пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» с изменениями, внесенными приказом ФСБ России 12 апреля 2010 г. № 173 «О внесении изменений в некоторые нормативные правовые акты ФСБ России» (зарегистрирован Министерством юстиции Российской Федерации 25 мая 2010 г., регистрационный № 17350);

При самостоятельном создании Ключей электронной подписи до обращения в удостоверяющий центр заявитель должен:

- использовать для создания ключа электронной подписи и соответствующего ему ключа проверки электронной подписи средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи» и совместимые со средствами электронной подписи, используемыми в удостоверяющем центре по форматам ключей и сертификатов;
- использовать для хранения ключа электронной подписи ключевой носитель, входящий в перечень ключевых носителей, определяемый удостоверяющим центром в Приложении 6 к настоящему Регламенту;
- обеспечивать конфиденциальность ключа электронной подписи с момента создания;
- при обращении в удостоверяющий центр предоставить файл запроса на квалифицированный сертификат в формате PKCS#10, содержащий ключ проверки электронной подписи и информацию, идентифицирующую владельца ключа проверки электронной подписи в объеме, определенном Федеральным законом «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Регламентом.

В случае самостоятельного создания ключа электронной подписи до обращения в удостоверяющий центр, заявитель должен подтвердить владение ключом электронной подписи при обращении в удостоверяющий центр с заявлением на создание и выдачу квалифицированного сертификата. Подтверждение владения ключом электронной подписи производится путем проверки электронной подписи в файле запроса на квалифицированный сертификат, который предоставляет заявитель, с использованием средств удостоверяющего центра. При отрицательном результате проверки электронной подписи в предоставленном файле запроса на квалифицированный сертификат удостоверяющий центр отказывает заявителю в создании и выдаче квалифицированного сертификата.

6.1.1.2 Порядок создания Ключей электронной подписи в Удостоверяющем центре

Создание ключа электронной подписи и ключа проверки электронной подписи при личном обращении в Удостоверяющий центр производиться заявителем самостоятельно или

Уполномоченным лицом Удостоверяющего центра в присутствии заявителя с использованием автоматизированного рабочего места, аттестованного на соответствие требованиям законодательства Российской Федерации по технической защите информации, находящегося в контролируемой зоне, и с соблюдением правил пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)». Ключ электронной подписи, созданный таким образом, записывается на ключевой носитель с пометкой «неэкспортируемый», который передается заявителю либо доверенному лицу заявителя по окончании процедуры создания и выдачи квалифицированного сертификата.

Ключ ЭП и Ключ проверки ЭП, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона "Об электронной подписи" создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности. При создании Ключевой пары выполняются требования, установленные постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79 (Собрание законодательства Российской Федерации, 2012, N 7, ст. 863; 2016, N 26, ст. 4049) в отношении автоматизированного рабочего места Удостоверяющего центра, используемого для создания Ключа ЭП и Ключа проверки ЭП для Заявителя.

При создании ключа электронной подписи в удостоверяющем центре подтверждения владения ключом электронной подписи не требуется.

6.1.2. Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра. Порядок информирования владельцев Сертификатов об осуществлении такой смены.

Плановая смена Ключей ЭП Удостоверяющего Центра (Ключа ЭП и соответствующего ему Ключа проверки ЭП) выполняется не ранее, чем через 1 год, и не позднее, чем через 1 год и 3 месяца после начала действия соответствующего Ключа.

Основанием для плановой смены Ключей Удостоверяющего центра является истечение соответствующего срока.

Процедура плановой смены Ключей Удостоверяющего центра осуществляется в течение 1 (одного) рабочего дня в следующем порядке:

1) Уполномоченное лицо удостоверяющего центра формирует новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи, а также запрос на квалифицированный сертификат в формате PKCS#10 Base-64.

2) Сгенерированный файл запроса с соответствующим заявлением отправляется в головной удостоверяющий центр федерального органа исполнительной власти, уполномоченного в сфере использования электронной подписи (Уполномоченный орган) для создания и выдачи квалифицированного сертификата удостоверяющего центра.

3) Уполномоченный орган с использованием средств головного удостоверяющего центра выдает квалифицированный сертификат удостоверяющего центра и публикует его в Реестре сертификатов головного удостоверяющего центра.

4) Уполномоченный сотрудник УЦ устанавливает полученный квалифицированный сертификат на средства Удостоверяющего центра и публикует новый квалифицированный сертификат Удостоверяющего центра на сайте Удостоверяющего центра.

5) Старый Ключ электронной подписи Удостоверяющего центра (подвергшийся процедуре плановой смены) используется в течение своего срока действия для формирования списков отозванных сертификатов в электронной форме, изданных Удостоверяющим центром в период действия предыдущих ключей Удостоверяющего центра.

6) Удостоверяющий центр информирует пользователей о плановой смене ключей электронной подписи Удостоверяющего центра путем публикации нового квалифицированного

сертификата Удостоверяющего центра в реестре Уполномоченного органа, и также посредством размещения информации на официальном сайте Удостоверяющего центра: https://www.if-spb.ru/.

6.1.3. Порядок смены ключей электронной подписи Удостоверяющего центра в случае нарушения их конфиденциальности: основания, процедуры и сроки осуществления смены ключей электронной подписи Удостоверяющего центра. Порядок информирования владельцев Сертификатов об осуществлении такой смены.

При использовании Ключа электронной подписи Удостоверяющего центра существуют различные угрозы нарушения конфиденциальности.

Угроза, реализованная путем уязвимости информационной системы, называется атакой. Существует три основные категории (цели) атак:

- нарушение нормального функционирования объекта атаки (отказ в обслуживании);
- раскрытие конфиденциальной и критичной информации;
- модификация и фальсификация данных (нарушение целостности).

Для предотвращения атак на Ключ электронной подписи Удостоверяющего центра реализован изолированным режим работы программно-аппаратного комплекса Удостоверяющего центра − комплекс организационно-технических мер, при выполнении которых нарушитель не располагает программно-аппаратными средствами взаимодействия с Удостоверяющим центром.

Реализованные меры защиты нацелены на предотвращение компрометации или угрозы компрометации Ключа электронной подписи Удостоверяющего центра.

Компрометация или угроза компрометации Ключа электронной подписи Удостоверяющего центра является основанием полагать, что конфиденциальность Ключа электронной подписи нарушена.

Под компрометацией Ключа электронной подписи понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых Ключ электронной подписи может стать доступными несанкционированным лицам и (или) процессам. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

• Физическая утрата ключевого носителя, содержащего ключ электронной подписи;

• Нарушение правил хранения и использования ключа электронной подписи Удостоверяющего центра, установленных эксплуатационной документацией на средства удостоверяющего центра;

• Несанкционированное копирование ключа электронной подписи Удостоверяющего центра;

• Несанкционированный доступ постороннего лица в место размещения технических средств Удостоверяющего центра или подозрение на то, что такое событие произошло (нарушение слепков печатей, повреждение замков);

• Увольнение сотрудников, имевших доступ к ключевой информации;

• Нарушение работоспособности или нештатное функционирование технических средств защиты информации, обрабатываемой на средствах Удостоверяющего центра.

• Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.

• Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями

(в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации Закрытого ключа Уполномоченного лица Удостоверяющего центра.

Процедура внеплановой смены ключей Удостоверяющего центра осуществляется в следующем порядке:

1) Уполномоченное лицо удостоверяющего центра при обнаружебнии факта компрометации незамедлительно уведомляет об этом Уполномоченный орган;

2) Уполномоченный орган с использованием средств головного удостоверяющего центра аннулирует (отзывает) квалифицированный сертификат удостоверяющего центра.

3) Уполномоченное лицо Удостоверяющего центра получает новый квалифицированный сертификат Удостоверяющего центра в срок и порядке, определенном процедурой плановой смены таких Ключей, согласно пункту 6.1.2. настоящего Регламента.

Одновременно со сменой Ключа электронной подписи Удостоверяющего центра прекращается действие всех Сертификатов, подписанных этим Ключом электронной подписи, с занесением сведений об этих сертификатах в Реестр сертификатов.

После выполнения процедуры внеплановой смены Ключа электронной подписи Удостоверяющего центра прекращается действие Сертификата Ключа проверки электронной подписи, Ключ электронной подписи которого подвергнут процедуре внеплановой смены.

Перечень прекративших свое действие сертификатов подписывается старым Ключом электронной подписи (подвергшимся процедуре внеплановой смены).

Удостоверяющий центр информирует Владельцев сертификатов, которые прекращают свое действие, о факте внеплановой смены Ключей Удостоверяющего центра посредством уведомления на электронную почту, указанную в сертификате и размещения информации на официальном сайте Удостоверяющего центра: https://www.if-spb.ru/.

После получения уведомления о факте внеплановой смены Ключей Удостоверяющего центра Владельцам сертификатов необходимо выполнить процедуру создания и выдачи новых Сертификатов в соответствии с порядком, установленным подразделом 6.2 настоящего Регламента, процедура выполняется на безвозмездной основе.

Владельцы Сертификатов могут доверенным способом получить новый сертификат в Удостоверяющем центре.

6.1.4 Порядок осуществления Удостоверяющим центром смены ключа электронной подписи владельца Сертификата.

Смена ключа электронной подписи владельца Сертификата осуществляется в случаях, Указанных в пунктах 1,2,4 части 6 и части 6.1. статьи 14 Федерального закона № 63-ФЗ.

Заявление на смену ключа электронной подписи составляется по форме, установленной Удостоверяющим центром. Образец заявления (Приложение №1) публикуется на сайте https://www.if-spb.ru/ и является неотъемлемы приложением настоящего Регламента.

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

Процедура выдачи Сертификата и ключа электронной подписи (при необходимости), определяется в соответствии с действующим законодательством Российской Федерации и настоящим Регламентом

6.2. Процедура создания и выдачи Сертификатов.

6.2.1. Порядок подачи заявления на создание и выдачу Сертификатов.

Заявитель обращается за выдачей Сертификата в Удостоверяющий центр. В Удостоверяющем центре производится формирование счета, заявления на выдачу Сертификата, принимаются представленные Заявителем документы, вручаются готовые Сертификаты.

Создание и выдача Сертификата осуществляется Удостоверяющим центром на основании Заявления на выдачу Сертификата и оплаченного счета.

6.2.2. Требования к заявлению на создание и выдачу Сертификатов

Заявление подается по форме, утвержденной Удостоверяющим центром. Заявление на выдачу Сертификата может быть оформлено как на бумажном носителе, подписанное

Заявителем собственноручно, так и в электронном виде, подписанное КЭП. С примерами заявлений на выдачу Сертификата можно ознакомиться по адресу https://www.if-spb.ru/. Данные примеры носят исключительно ознакомительный характер, за получением актуальных форм заявлений на выдачу Сертификата Заявитель обращается в Удостоверяющий центр (адреса Удостоверяющего центра публикуется на сайте https://www.if-spb.ru/). Актуальную форму заявления на выдачу Сертификата

Удостоверяющий центр определяет самостоятельно и по своей инициативе вправе вносить в нее любые изменения без уведомления Участников электронного взаимодействия. Собственноручное подписание Заявления на бумажном носителе производится чернилами (пастой) синего цвета. Использование факсимиле (клише подписи) на заявлении на выдачу Сертификата не допускается.

6.2.3. Порядок установления личности заявителя.

Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность – паспорту гражданина РФ. В исключительных случаях отсутствия у гражданина РФ основного документа, удостоверяющего личность, Удостоверяющий центр может удостоверить его личность по иному документу, удостоверяющему личность, признаваемому таковым действующим законодательством.

Личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства (при наличии официального перевода на русский язык, заверенного нотариусом или дипломатическими (консульскими) органами) или по иному документу, удостоверяющему личность гражданина иностранного государства, признаваемому таковым действующим законодательством.

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

6.2.4. Перечень документов, запрашиваемых Удостоверяющим центром у заявителя для изготовления и выдачи Сертификатов. Порядок предоставления необходимых документов.

Перечень документов и сведений, необходимых для изготовления и выдачи Сертификата устанавливается частью 2 статьи 17 и частью 2 статьи 18 Федерального закона № 63-ФЗ.

Удостоверяющий центр выполняет свою обязанность по внесению в Сертификат только достоверной и актуальной информации путем сбора и хранения сканкопий документов, представленных Заявителем, а также путем запроса соответствующих сведений из государственных реестров

Заявитель представляет в Удостоверяющий центр документы (или их надлежащим образом заверенные копии), необходимые для удостоверения личности Доверенного лица Заявителя, Уполномоченного представителя Заявителя, Заявителя-физического лица, а также документы, на основании которых Удостоверяющим центром вносятся сведения в Сертификат, такие как: полное или сокращенное наименование, основной государственный регистрационный номер, юридический адрес, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, наименование должности и иные данные.

Если для подтверждения каких-либо сведений, вносимых в Сертификат, действующим законодательством или настоящим Регламентом установлена определенная форма документа, Заявитель представляет в Удостоверяющий центр документ соответствующей формы.

При обращении в Удостоверяющий центр Доверенного лица или Уполномоченного представителя Заявителя его полномочия должны быть подтверждены соответствующей доверенностью.

Надлежащим способом заверения копий документов может являться нотариальное заверение копий, заверение копий органом власти (например, налоговыми органами), заверение копий документов Заявителем самостоятельно. При необходимости копии с документов могут быть сняты и заверены Доверенным лицом Удостоверяющего центра.

Нотариально заверенные копии документов должны содержать штамп нотариуса «копия верна», штамп с информацией о нотариусе, должны быть заверены печатью нотариуса и иметь подпись нотариуса.

Копии, заверенные Заявителем, могут предоставлять исключительно юридические лица и индивидуальные предприниматели, имеющие собственную печать. Многостраничные копии либо должны быть прошиты и заверены на листе сшивки, либо на каждой странице такой копии должна иметься отдельная заверительная надпись. Образец заверительной надписи:

ВЕРНО

Должность с указанием наименования организации/индивидуального предпринимателя

Подпись Расшифровка подписи (фамилия и инициалы полностью)

Дата заверения документа

Оттиск печати

Копии документов, заверенные органом власти, должны содержать подпись и расшифровку подписи должностного лица, их заверившего, а также печать/штамп данного органа власти.

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

Если Заявитель выступает в интересах третьих лиц, то, по требованию Удостоверяющего центра, представляет документы, подтверждающие такие полномочия.

6.2.5. Порядок проверки достоверности документов и сведений, предоставленных заявителем.

Для заполнения Сертификата в соответствии с частью 2 статьи 17 Федерального закона № 63-ФЗ Удостоверяющий центр запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные частью 2.2 статьи 18 Федерального закона № 63-ФЗ.

В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в Сертификат, и Удостоверяющим центром установлена личность заявителя – физического лица или получено подтверждение правомочий лица, выступающего от имени заявителя – юридического лица, на обращение за получением Сертификата, Удостоверяющий центр осуществляет процедуру создания и выдачи заявителю Сертификата. В противном случае Удостоверяющий центр отказывает заявителю в выдаче Сертификата.

6.2.6. Порядок создания Сертификата.

Удостоверяющим центром в Сертификат вносится информация на основании заявления на выдачу Сертификата. Если Владельцем сертификата является юридическое лицо, то наряду с наименованием такого юридического лица в Сертификат может вноситься информация об Уполномоченном представителе. Удостоверяющий центр проверяет данные в Заявлении на выдачу Сертификата на соответствие данным, содержащимся в иных представленных Заявителем документах, и устанавливает:

- факт принадлежности документов предоставившему их лицу и/или лицу, чьи интересы оно представляет;
- факт соответствия сведений, указанных в заявлении на выдачу Сертификата, представленным документам и, в необходимых случаях в соответствии с Федеральным законом № 63-ФЗ, информации, полученной из государственных реестров;
- факт отсутствия явных признаков подделки документов.

В случае внесения в Сертификат персональных данных физического лица, Заявитель - физическое лицо или Уполномоченный представитель Заявителя предоставляет свое письменное согласие на обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Текст согласия включен в заявление на выдачу Сертификата. Персональные данные, внесенные в Сертификат, становятся общедоступными в соответствии с Федеральным законом № 63-ФЗ. Согласие должно быть подписано

собственноручно лицом, данные о котором вносятся в Сертификат (субъектом персональных данных). Также согласие на обработку персональных данных может быть подписано представителем субъекта персональных данных, действующим на основании нотариальной доверенности, которая должна быть выдана от имени субъекта персональных данных, должна содержать полномочие на предоставление согласия на обработку персональных данных от имени субъекта персональных данных, а также должна соответствовать иным требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

В Удостоверяющим центре Сертификат изготавливается ответственным сотрудником на специализированном рабочем месте при личном присутствии Заявителя или его доверенного представителя. В процессе генерации Закрытый ключ автоматически размещается на ключевом носителе, предоставленном Заявителем или самим Удостоверяющим центром по запросу Заявителя, с пометкой «не экспортируемый».

В случае предоставления заявителем ключевого носителя должны выполняться следующие требования:

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

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

Удостоверяющий центр на основаниях, предусмотренных действующим законодательством Российской Федерации и/или настоящим Регламентом, вправе отказать в создании Сертификата.

Удостоверяющий центр издает Сертификаты в форме электронного документа формата X.509 версии 3.

6.2.7. Порядок выдачи Сертификата.

По окончании процедуры создания Сертификата Заявитель получает:

- Ключ электронной подписи и Сертификат (с ключом проверки ЭП);
- Копию Сертификата на бумажном носителе;
- Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи.

Владелец сертификата при получении Сертификата подписывает и передает в Удостоверяющий центр Расписку, в двух экземплярах, на бумажном носителе, содержащую описание информации, включенной в Сертификат.

Заявителю, получившему созданный Сертификат (Владельцу сертификата), Удостоверяющим центром выдается «Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи».

Факт создания Ключа электронной подписи и соответствующего ему Ключа проверки электронной подписи, содержащегося в Сертификате, Удостоверяющим центром, подтверждает факт владения Владельцем сертификата Ключом электронной подписи, соответствующим Ключу проверки электронной подписи, указанному в таком Сертификате. Каких-либо иных подтверждений владения Участники электронного взаимодействия не оформляют.

6.2.8. Срок создания и выдачи Сертификата. Условия для срочного создания и выдачи Сертификата.

Создание Сертификата производится в течение трех рабочих дней с момента подачи заявления на выдачу Сертификата, при условии подтверждения всех фактов соответствия сведений в заявлении на выдачу Сертификата согласно подразделу 6.2.6 настоящего Регламента.

Срочное создание и выдача Сертификата производится в соответствии с условиями прайс-листа Удостоверяющего центра, опубликованного на официальном сайте https://if-spb.ru/.

6.3. Подтверждение действительности электронной подписи, использованной для подписания электронных документов.

6.3.1. Требования к заявлению на подтверждение действительности электронной подписи. Перечень прилагаемых к заявлению документов.

Подтверждение действительности ЭП в электронном документе, авторство или содержание которого оспаривается, осуществляется на основании заявления на подтверждение действительности ЭП, форма которого установлена Приложением №2 к настоящему Регламенту.

К заявлению прикладывается электронный документ и ЭП, подтверждение которой производится.

6.3.2. Срок предоставления услуг по подтверждению действительности электронной подписи в электронном документе.

Срок проведения работ по подтверждению действительности ЭП в электронном документе составляет 15 (пятнадцать) рабочих дней с момента поступления заявления с в Удостоверяющий центр и при условии поступления оплаты стоимости данных услуг на расчетный счет Удостоверяющего центра.

6.3.3. Порядок оказания услуг.

Процедура подтверждения действительности ЭП осуществляется с использованием программного комплекса, входящего в состав сертифицированного программно-аппаратного комплекса Удостоверяющего центра, комиссией, сформированной из числа сотрудников УЦ.

Проверка действительности ЭП включает в себя:

- определение сертификата или нескольких сертификатов, необходимых для проверки ЭП;
- проверка ЭП электронного документа с использованием каждого сертификата;
- определение даты формирования каждой ЭП в электронном документе;
- проверка ЭП каждого сертификата, путем построения цепочки сертификатов до сертификата аккредитованного удостоверяющего центра, выданного ему головным удостоверяющим центром;
- проверка действительности сертификатов на текущий момент времени;
- проверка отсутствия сертификатов в списках отозванных сертификатов (CRL).

По результатам оказания услуги оформляется заключение.

Заключение содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- результат проверки ЭП электронного документа;
- данные, представленные комиссии для проведения проверки.
- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- содержание и результаты проверки;
- обоснование результатов проверки.

Заключение Удостоверяющего центра по выполненной проверке составляется в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

Проверка ЭП под электронными документами, созданными не Удостоверяющим центром, при технической совместимости используемых средств Удостоверяющего центра производится при представлении правил документирования, в соответствии с которыми были созданы электронный документ и проверяемая ЭП. При проведении работ Удостоверяющим центром может быть запрошена дополнительная информация.

6.4. Процедуры, осуществляемые при прекращении действия и аннулировании Сертификата.

6.4.1. Основания прекращения действия или аннулирования сертификата.

Сертификат прекращает свое действие в случаях, установленных статье 14 Федеральным законом № 63-ФЗ.

Сертификат прекращает свое действие:

1) в связи с истечением установленного срока его действия;

2) на основании заявления Владельца сертификата о прекращении действия Сертификата, подаваемого в форме документа на бумажном носителе или в форме электронного документа. Форма такого заявления приведена в Приложении №3;

3) в случае увольнения сотрудника Удостоверяющего центра, которому был выдан Сертификат для выполнения трудовых обязанностей;

4) в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;

5) в иных случаях, установленных Федеральным законом № 63-ФЗ, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.

Удостоверяющий центр аннулирует Сертификат в следующих случаях:

1) не подтверждено, что Владелец сертификата владеет Ключом ЭП, соответствующим Ключу проверки ЭП, указанному в таком Сертификате;

2) установлено, что содержащийся в Сертификате Ключ проверки ЭП уже содержится в ином ранее созданном Сертификате;

3) вступило в силу решение суда, которым установлено, что Сертификат содержит недостоверную информацию.

6.4.2. Порядок действий Удостоверяющего центра при прекращении действия (аннулировании) Сертификата.

Доверенное лицо Удостоверяющего центра при приеме заявления на прекращение действия Сертификата получает от лица, выступающего от имени Владельца сертификата, подтверждение правомочия обращаться за прекращением действия Сертификата.

Направление заявления о прекращении действия Сертификата производиться по форме, приведенной в Приложении №3 и может быть осуществлено как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью

Приём заявлений осуществляется в Удостоверяющем центре в рабочие дни в рабочее время (не ранее 9:00 и не позднее 18:00 местного времени).

Информация о прекращении действия или аннулировании Сертификата вносится в Реестр сертификатов. Действие Сертификата прекращается с момента публикации Реестра сертификатов, в который внесён этот Сертификат. Срок внесения в Реестр сертификатов сведений о прекращении действия или аннулировании Сертификата составляет не более 12 (двенадцати) часов с момента приема заявления на прекращение действия Сертификата или наступления иного события, предусмотренного подразделом 6.4.1 настоящего Регламента.

6.5. Порядок ведения реестра Сертификатов.

6.5.1. Формы ведения реестра Сертификатов.

Формирование и ведение Реестра сертификатов осуществляется Удостоверяющим центром в порядке, установленном Федеральным законом № 63-ФЗ.

Ведение Реестра сертификатов включает в себя:

- внесение изменений в Реестр сертификатов в случае изменения содержащихся в нем сведений;

- внесение в Реестр сертификатов сведений о прекращении действия или об аннулировании Сертификатов.

Информация, внесенная в Реестр сертификатов, подлежит хранению в течение всего срока деятельности Удостоверяющего центра, если более короткий срок не установлен законодательством Российской Федерации.

Хранение информации, содержащейся в Реестре сертификатов, осуществляется в форме, позволяющей проверить ее целостность и достоверность. Хранение в Удостоверяющем центре всех выданных Сертификатов осуществляется постоянно в форме электронных документов.

Удостоверяющий центр обеспечивает защиту информации, содержащейся в Реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности. Формирование и ведение Реестра сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему.

Для предотвращения утраты сведений о Сертификатах, содержащихся в Реестре сертификатов, формируется его резервная копия.

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в Реестре сертификатов.

Структура Реестра сертификатов формируется и ведется в соответствии с требованиями Федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий.

Удостоверяющий центр ведет перечень прекративших свое действие (аннулированных) Сертификатов в электронной форме формата X.509 версии 2.

6.5.2. Сроки внесения информации о прекращении действия или аннулирования Сертификатов в Реестр сертификатов.

Срок внесения в Реестр сертификатов сведений о прекращении действия или аннулировании Сертификатов составляет не более 12 (двенадцати) часов с момента приема заявления на прекращение действия Сертификата или наступления иного события, предусмотренного пунктом 6.4.1 настоящего Регламента.

6.6. Порядок технического обслуживания Реестра сертификатов

6.6.1. Максимальные сроки проведения технического обслуживания.

Максимальный срок планового технического обслуживания составляет 3 (три) часа.

Внеплановое техническое обслуживание проводится при появлении такой необходимости в оперативном режиме. Срок проведения внепланового технического обслуживания составляет 3 (три) часа. Срок проведения внепланового технического обслуживания может быть увеличен по объективным причинам.

Максимальные сроки проведения планового и внепланового технического обслуживания Реестра сертификатов не может превышать установленные сроки внесения информации в Реестр сертификатов.

6.6.2. Порядок уведомления участников информационного взаимодействия о проведении технического обслуживания.

Удостоверяющий центр информирует участников информационного взаимодействия о проведении технического обслуживания производится посредством размещения информации на официальном сайте Удостоверяющего центра: https://www.if-spb.ru/.

6.7. Подтверждение действительности электронной подписи Удостоверяющего центра в выданных Сертификатах.

Подтверждения подлинности ЭП Удостоверяющего центра осуществляется на основании заявления (форма Заявления приведена в Приложении №4).

К заявлению прилагается носитель информации с файлом, содержащим Сертификат, подвергающийся процедуре проверки.

Проведение работ по подтверждению подлинности ЭП Удостоверяющего центра в Сертификате осуществляет комиссия Удостоверяющего центра с использованием технических средств Удостоверяющего центра.

Срок проведения экспертизы составляет 15 (пятнадцать) рабочих дней с момента поступления заявления в Удостоверяющий центр при условии поступления оплаты стоимости данной услуги на расчетный счет Удостоверяющего центра.

Результатом проведения работ по подтверждению подлинности ЭП уполномоченного лица Удостоверяющего центра в выданном сертификате является заключение Удостоверяющего центра.

Заключение содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- результат проверки ЭП электронного документа;
- данные, представленные комиссии для проведения проверки.
- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- содержание и результаты проверки;
- обоснование результатов проверки.

Заключение Удостоверяющего центра по выполненной проверке составляется в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

7. Порядок исполнения обязанностей Удостоверяющего центра.

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

Удостоверяющий центр информирует Заявителя об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки, посредством ознакомления с «Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи», которое выдается Заявителю одновременно с выдачей Сертификата, а также путем размещения «Правил по обеспечению информационной безопасности на рабочем месте» на официальном сайте УЦ: https://www.if-spb.ru/.

7.2. Выдача по обращению заявителя средств электронной подписи.

Выдаваемые средства электронной подписи должны в соответствии с частью 4 статьи 6 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» обеспечивать возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями.

7.3. Обеспечение актуальности информации, содержащейся в Реестре сертификатов, и ее защиты.

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в Реестре Сертификатов, путем соблюдения сроков внесения сведений о прекращении действия и/или аннулировании Сертификатов, установленных Федеральным законом № 63-ФЗ.

Защита информации, содержащейся в Реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается путем:

- предотвращения несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременным обнаружением фактов несанкционированного доступа к информации;
- предупреждением возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможностью незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянным контролем за обеспечением уровня защищенности информации;
- нахождением баз данных информации в контролируемой зоне, исключающей свободное пребывание посторонних лиц;

- использованием средств защиты информации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

7.4. Обеспечение доступности Реестра сертификатов.

Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей к Реестру сертификатов, через форму запроса на официальном сайте Удостоверяющего центра: https://www.if-spb.ru/, в любое время, за исключением периодов технического обслуживания Реестра сертификатов.

7.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей.

Ключ электронной подписи является конфиденциальной информацией Владельца Сертификата. Владелец Сертификата обязан обеспечивать конфиденциальность Ключа электронной подписи, в частности, не допускать использование Ключа электронной подписи без его согласия.

В Удостоверяющем центре Ключ электронной подписи создается уполномоченным сотрудником Удостоверяющего центра на автоматизированном рабочем месте, аттестованном на соответствие требованиям по безопасности информации, размещенном в помещении специализированном помещении, доступ в которое ограничен. Ключ электронной подписи, созданный таким образом, записывается на ключевой носитель и имеете пометку «не экспортируемый». После окончания процедуры создания Ключа электронной подписи Заявитель или Доверенное лицо Заявителя забирает ключевой носитель с записанным на нем Ключом электронной подписи.

Для создания Ключа электронной подписи в УЦ используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ.

В случае нарушения конфиденциальности Ключа электронной подписи, а также в случаях наличия оснований полагать, что конфиденциальность Ключа электронной подписи была нарушена, Владелец сертификата Ключа проверки электронной подписи, соответствующего такому Ключу электронной подписи, должен прекратить использование этого Ключа и подать в Удостоверяющий центр заявление на прекращение действия этого Сертификата.

7.6. Осуществление регистрации квалифицированного Сертификата в единой системе идентификации и аутентификации.

При выдаче Сертификата КЭП Удостоверяющий центр, в соответствии с частью 5 статьи 18 Федерального закона №63, направляет в Единую систему идентификации и аутентификации (далее – ЕСИА) сведения о лице, получившем Сертификат КЭП, в объеме, необходимом для регистрации в ЕСИА, и о полученном им Сертификате КЭП (уникальный номер сертификата КЭП, даты начала и окончания его действия, наименование Удостоверяющего центра).

7.7. Осуществление по желанию лица, которому выдан квалифицированный Сертификат, безвозмездной регистрации указанного лица в единой системе идентификации и аутентификации.

При выдаче сертификата КЭП Удостоверяющий центр по желанию лица, которому выдан Сертификат КЭП, безвозмездно осуществляет регистрацию указанного лица в ЕСИА.

7.8. Предоставление доступа к Реестру сертификатов.

Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", к реестру квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, в том числе путем публикации перечня прекративших свое действие (аннулированных) сертификатов на официальном сайте Удостоверяющего центра: https://www.if-spb.ru/

Для получения доступа к Реестру выданных сертификатов заинтересованное лицо заполняет размещенную на сайте https://www.if-spb.ru форму запроса. Обработка запроса осуществляется в рабочие дни с 9.00 до 18.00. Информация предоставляется заинтересованному лицу в форме электронного сообщения на адрес электронной почты, указанный в запросе.

7.9. Сроки действия Ключей и Сертификатов.

Срок действия Ключей электронной подписи Удостоверяющего центра составляет не более 3 (Трех) лет. Начало периода действия Ключей электронной подписи Удостоверяющего центра исчисляется с момента начала действия его Сертификата.

Срок действия Сертификата Удостоверяющего центра составляет не более 15 лет.

Максимальный срок действия Ключа электронной подписи Заявителя устанавливается эксплуатационной документацией средства электронной подписи (системы криптографической защиты информации), с использованием которого такой Ключ создается. Начало периода действия Ключа электронной подписи Заявителя исчисляется с момента начала действия Сертификата, соответствующего данному Ключу.

Срок действия Сертификата, создаваемого Удостоверяющим центром для Заявителя, равен сроку действия Ключа электронной подписи, соответствующего данному Сертификату.

8. Структуры сертификатов и списков отозванных сертификатов.

8.1. Структура сертификата, изготавливаемого Удостоверяющим Центром в электронной форме.

Удостоверяющий Центр издает Сертификаты Пользователей УЦ и Уполномоченного лица Удостоверяющего Центра в электронной форме в соответствии с рекомендациями Международного союза телекоммуникаций ITU-T X.509 версии 3 и требованиям Приказа ФСБ РФ от 27 декабря 2011 года №795 «Об утверждении требований к форме квалифицированного Сертификата».

Общая структура Сертификата приведена далее в таблице:

Название	Описание	Содержание
Базовые поля сертификата		
version	Версия	V3
serialNumber	Серийный номер	Уникальный серийный номер сертификата
signature	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001; ГОСТ Р 34.11/34.10-2012
issuer	Издатель сертификата	CN = Псевдоним Уполномоченного лица Удостоверяющего центра OU = Подразделение = Удостоверяющий Центр O = Организация = ООО ИНТЕРФОРУМ L = Город = Санкт-Петербург C = Страна/Регион = RU E = Электронная почта = xxxxxx
validity	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
subject	Владелец сертификата	CN = Фамилия, Имя, Отчество или псевдоним OU = Подразделение O = Организация UA = Юридический адрес организации UN = Индивидуальный номер налогоплательщика Locality = Город State = Субъект Федерации Country = Страна = RU Компонента имени CN обязательна для заполнения, необходимость заполнения остальных значений определяется Владельцем сертификата. В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 3280
subjectPublicKeyInfo	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2001; ГОСТ Р 34.11/34.10-2012)

Название	Описание	Содержание
issuerUniqueIdentifier	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001; ГОСТ Р 34.11/34.10-2012
subjectUniqueIdentifier	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001; ГОСТ Р 34.11/34.10-2012
Расширения сертификата		
keyUsage	Использование ключа	Проверка ЭП под ЭД (кроме сертификатов и списков отозванных сертификатов); невозможность отказа от ЭП под ЭД (кроме сертификатов и списков отозванных сертификатов); зашифрование закрытых и секретных ключей; зашифрование данных; согласование ключей
subjectKeyIdentifier	Идентификатор ключа Владельца сертификата	Идентификатор закрытого ключа Владельца сертификата
authorityKeyIdentifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего центра, на котором подписан данный сертификат
certificatePolicies	Политики сертификации, в соответствии с которыми должен использоваться сертификат	Идентификатор класса средств ЭП КС1, КС2: 1.2.643.100.113.1, 1.2.643.100.113.2
CRLDistributionPoint	Точка распространения списка отозванных сертификатов	Адреса, по которым Удостоверяющий центр публикует Списки отозванных сертификатов
AuthorityInformationAccess	Адрес Службы актуальных статусов сертификатов	Адреса, по которым Удостоверяющий центр опубликовал Сертификат Удостоверяющего центра, атрибуты имени которого указаны в поле «Издатель сертификата»
subjectSignTool	Наименование средства ЭП, используемое Владельцем сертификата	Заполняется в соответствии с приказом ФСБ России № 795 от 27.12.2011
IssuerSignTool	Наименование средств ЭП и средств УЦ, которые	Заполняется в соответствии с приказом ФСБ России № 795 от 27.12.2011

Название	Описание	Содержание
	использованы для создания ключа ЭП, ключа проверки ЭП, сертификата, а также реквизиты документов, подтверждающих соответствие указанных средств требованиям, установленным 63-ФЗ	

Дополнительно в выдаваемые Сертификаты может быть занесено:

- в поле Subject (идентифицирует Владельца сертификата):
- Поле E (Email) - адрес электронной почты;
- Поле T (Title) - должность полномочного представителя

юридического лица, данные которого занесены в Сертификат наряду с наименованием юридического лица (если Владелец Сертификата - юридическое лицо);

- Расширение Private Key Validity Period - срок действия ключа электронной подписи, соответствующего Сертификату, следующего формата:
- Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC;
- Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC;
- расширение Extended Key Usage (Расширенное использование ключа) - набор объектных идентификаторов, устанавливающих ограничения на применение квалифицированной электронной подписи совместно с Сертификатом (если такие ограничения установлены);
- иные поля и расширения по усмотрению Удостоверяющего центра.

8.2. Поддерживаемые параметры и идентификаторы алгоритмов.

Удостоверяющий центр обеспечивает формирование ключей ЭП в соответствии с параметрами:

Алгоритм подписи:	ГОСТ Р 34.10-2001
Описание:	Стандарт ЭП, основанный на арифметике эллиптических кривых. OID «1.2.643.2.2.19»
Параметры ключа проверки ЭП:	ГОСТ Р 34.10-2001 Параметры по умолчанию
	ГОСТ Р 34.10-2001 «Оскар»
	ГОСТ Р 34.10-2001 Параметры подписи С
Параметры подписи:	Набор параметров по умолчанию (рекомендуется). OID «1.2.643.2.2. 35.1»
	Набор параметров В OID «1.2.643.2.2. 35.2»
	Набор параметров С OID «1.2.643.2.2. 35.3»
Длина ключа:	512
Алгоритм подписи:	ГОСТ Р 34.10-2012/1024

Описание:	Стандарт ЭП, основанный на арифметике эллиптических кривых. OID «1.2.643.7.1.1.1.2»
Параметры ключа проверки ЭП:	ГОСТ Р 34.10-2012 Параметры А ГОСТ Р 34.10-2012 Параметры В
Параметры подписи:	Набор параметров «ТК 26» (Параметры А) (рекомендуется) OID «1.2.643.7.1.2.1.2.1» Набор параметров «ТК 26» (Параметры В) OID «1.2.643.7.1.2.1.2.2»
Длина ключа:	1024

8.3. Формы имени.

В сертификате поля идентификационных данных уполномоченного лица Удостоверяющего центра и Владельца сертификата содержат атрибуты имени формата X.500.

Обязательными атрибутами поля идентификационных данных уполномоченного лица Удостоверяющего центра являются:

Common Name	Фамилия, имя, отчество
Organization	Наименование организации, являющейся Владельцем Удостоверяющего центра
Organization Unit	Наименование подразделения, сотрудником которого является уполномоченное лицо Удостоверяющего центра
Country	RU
State	Субъект Федерации, где зарегистрирована организация, являющейся Владельцем Удостоверяющего центра
OGRN	Основной государственный регистрационный номер организации являющейся Владельцем Удостоверяющего центра
INN	Идентификационный номер налогоплательщика организации, являющейся Владельцем Удостоверяющего центра

Обязательными атрибутами поля идентификационных данных Владельца сертификата, являющегося физическим лицом, являются:

Common Name	Фамилия, имя, отчество
Country	RU
SNILS	Страховой номер индивидуального лицевого счета Владельца сертификата

Обязательными атрибутами поля идентификационных данных Владельца сертификата, являющегося физическим лицом и представляющего юридическое лицо, являются:

Common Name	Фамилия, имя, отчество
Organization	Наименование организации, которую представляет Владелец сертификата
Organization Unit	Наименование подразделения организации, сотрудником которого является Владелец сертификата
Title	Должность Владельца сертификата
Country	RU

State	Субъект Федерации, где зарегистрирована организация, которую представляет Владелец сертификата
INN	Идентификационный номер налогоплательщика организации, являющейся Владельцем Удостоверяющего центра
SNILS	Страховой номер индивидуального лицевого счета Владельца сертификата
OGRN	Основной государственный регистрационный номер Владельца сертификата

Обязательными атрибутами поля идентификационных данных Владельца сертификата, являющегося индивидуальным предпринимателем, являются:

Common Name	Фамилия, имя, отчество
Organization	Наименование организации, которую представляет Владелец сертификата
Country	RU
State	Субъект Федерации, где зарегистрирована организация, которую представляет Владелец сертификата
INN	Идентификационный номер налогоплательщика организации, являющейся Владельцем Удостоверяющего центра
SNILS	Страховой номер индивидуального лицевого счета Владельца сертификата
OGRNIP	Основной государственный регистрационный номер индивидуального предпринимателя

8.4. Структура списка отозванных сертификатов, изготавливаемого Удостоверяющим центром в электронной форме.

Удостоверяющий центр издает Списки отозванных сертификатов Пользователей УЦ и уполномоченного лица Удостоверяющего центра в электронной форме формата X.509 версии 2.

Удостоверяющий центр издает списки аннулированных сертификатов в электронной форме формата X.509 версии 2. Описание и содержание формы списка аннулированных сертификатов (CRL) Удостоверяющего центра представлено ниже:

Название	**Описание**	**Содержание**
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель списка отозванных сертификатов	Идентификационные данные Удостоверяющего центра
thisUpdate	Время издания списка отозванных сертификатов	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен список отозванных	дд.мм.гггг чч:мм:сс GMT

	сертификатов	
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reson Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001; ГОСТ Р 34.11/34.10-2012
Issuer Sign	Подпись издателя списка отозванных сертификатов	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001; ГОСТ Р 34.11/34.10-2012
Расширения списка отозванных сертификатов		
AuthorityKeyIdentifier	Идентификатор ключа издателя	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего центра, на котором подписан список отозванных сертификатов
CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата Уполномоченного лица Удостоверяющего центра

9. Обеспечение безопасности Удостоверяющего центра.

9.1. Инженерно-технические меры защиты информации.

9.1.1. Размещение технических средств Удостоверяющего центра.

Серверное и телекоммуникационное оборудование размещены в специальной стойке выделенного серверного помещения Удостоверяющего центра.

Остальные технические средства Удостоверяющего центра размещаются в рабочих помещениях Удостоверяющего центра.

9.1.2. Контроль защищенности вычислительной техники .

Технические средства Удостоверяющего центра включают следующую функциональность:

- контроль доступа к сервисам и ролям Удостоверяющего центра;
- идентификация и аутентификация соответствующих работников;
- криптографическая защита передаваемых сообщений и базы данных;
- архивирование данных пользователей и аудита;
- аудит событий, относящихся к обеспечению безопасности;
- механизмы резервного копирования и восстановления системы Удостоверяющего центра.

Данная функциональность предоставляется средствами ОС и комбинацией средств ОС, ПО, СЗИ и физических средств обеспечения безопасности.

9.1.3. Физический доступ.

Серверное помещение Удостоверяющего центра оборудовано системой контроля доступа с идентификацией по карте.

Серверное помещение оборудовано замками механического и электромеханического типа.

Рабочие и служебные помещения Удостоверяющего центра оборудованы механическими замками.

Помещения, в которых осуществляется работа со средствами ЭП и криптографической защиты информации, опечатываются ответственными работниками. Контроль целостности печатей осуществляется в начале каждой рабочей смены.

Контроль целостности программных и технических средств Удостоверяющего центра осуществляется при каждой загрузке, также встроены механизмы периодического (раз в 24 часа) тестирования целостности ПО.

9.1.4. Электроснабжение и кондиционирование воздуха.

Технические средства Удостоверяющего центра подключены к общегородской сети электроснабжения.

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

Серверные компоненты и телекоммуникационное оборудование подключены к источникам бесперебойного питания, обеспечивающие их работу в течение не менее 1 часа после прекращения основного электроснабжения.

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

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

Рабочие и прочие служебные помещения Удостоверяющего центра оборудованы средствами вентиляции и кондиционирования воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством РФ.

9.1.5. Подверженность воздействию влаги.

Защита серверного и телекоммуникационного оборудования от воздействия влаги обеспечивается их размещением в шкафу-стойке в выделенном помещении.

9.1.6. Предупреждение и защита от возгорания.

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

Пожарная безопасность помещений Удостоверяющего центра обеспечивается в соответствии с нормами и требованиями СНиП, устанавливаемыми законодательством РФ.

9.1.7. Хранение документированной информации.

Документальный фонд Удостоверяющего центра подлежит хранению в соответствии с действующим законодательством РФ по делопроизводству и архивному делу.

9.1.8. Уничтожение документированной информации.

Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется работниками Удостоверяющего центра, обеспечивающими документирование.

9.2. Программно-аппаратные меры защиты информации.

9.2.1. Организация доступа к программным средствам Удостоверяющего центра.

Серверные компоненты и рабочие места, входящие в состав Удостоверяющего центра, оснащены сертифицированными программно-аппаратными комплексами защиты от несанкционированного доступа типа «электронный замок», которые осуществляют контроль доступа пользователей и контроль целостности компонентов и программной среды.

9.2.2. Контроль целостности программного обеспечения.

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

- программные модули средств ЭП и криптографической защиты информации;
- программные модули серверных компонентов;
- программные модули АРМ администраторов.

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

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

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

Периодичность выполнения мероприятий по контролю целостности - ежесуточно.

9.2.3. Контроль целостности технических средств.

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

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

Контроль целостности печатей осуществляется в начале каждой рабочей смены.

9.2.4. Защита от вредоносного программного обеспечения.

Серверные компоненты и рабочие места, входящие в состав Удостоверяющего центра, оснащены сертифицированными средствами защиты от вредоносного ПО, которые осуществляют непрерывный контроль программной среды данных компонентов на предмет наличия вредоносного ПО. Также контролю подвергаются съемные носители, используемые для передачи информации между изолированными компонентами Удостоверяющего центра.

9.3. Организационные меры защиты информации.

9.3.1. Предъявляемые требования к персоналу Удостоверяющего центра.

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

Работники, отвечающие за обеспечение безопасности Удостоверяющего центра имеют высшее профессиональное образование и прошли курсы повышения квалификации в области информационной безопасности с получением специализации в области систем с открытым распределением ключей.

9.3.2. Организация доступа персонала к документам и документации.

Доступ работников Удостоверяющего центра к документам и документации, составляющей документальный фонд организации, организован в соответствии с должностными инструкциями и функциональными обязанностями.

9.3.3. Охрана здания и помещений.

Удостоверяющий центр имеет службу охраны здания и помещений, обеспечивающую:

- обнаружение и задержание нарушителей, пытающихся проникнуть в здание (помещения) Удостоверяющего центра;
- сохранность материальных ценностей и документов;
- предупреждение происшествий и ликвидацию их последствий.

9.4. Юридические меры защиты информации.

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

Системы обеспечения безопасности Удостоверяющего центра созданы и поддерживаются силами Удостоверяющего центра на основании лицензий, полученных в соответствии с действующим законодательством РФ.

Для обеспечения деятельности Удостоверяющий центр использует средства ЭП и криптографической защиты информации, сертифицированные в соответствии с действующим законодательством РФ.

Исключительные имущественные права на информационные ресурсы Удостоверяющего центра находятся в собственности Удостоверяющего центра.

Пользователям УЦ предоставляются неисключительные имущественные права на копии сертификатов и списков отозванных сертификатов, изготавливаемые Удостоверяющим центром.

10. Приложения

- Приложение №1 – Заявление (Заявка) на изготовление квалифицированного сертификата ключа проверки электронной подписи.
- Приложение №2 – Заявление на подтверждение подлинности электронной подписи.
- Приложение №3 – Заявление на прекращение (аннулирование) действия сертификата ключа проверки электронной подписи.
- Приложение №4 – Заявление на подтверждение подлинности электронной подписи уполномоченного лица удостоверяющего центра в квалифицированном сертификате.
- Приложение №5 – Образец доверенности.
- Приложение №6 – Перечень ключевых носителей

Лист изменений

Версия	Дата	Номер раздела, рисунка или таблицы	Тип изменений	Автор	Краткое содержание сути изменения
2.0.	1.09.2019		Создание	Морозов А.А.	
2.1.	09.12.2019	Пункт 6.5	Дополнение	Морозов А.А.	
2.1.	09.12.2019	Пункт 6.6	Дополнение	Морозов А.А.	
2.2.	17.01.2020	Пункт 6.1.1.	Дополнение	Морозов А.А.	Порядок создания ключей
2.2.	17.01.2020	Пункт 6.1.2.	Корректировка	Морозов А.А.	Процедура смены ключей УЦ
2.2.	17.01.2020	Пункт 6.1.3.	Корректировка	Морозов А.А.	Процедура внеплановой смены ключей УЦ
2.2.	17.01.2020	Пункт 6.1.4.	Дополнение	Морозов А.А.	
2.2.	17.01.2020	Пункт 6.2.6.	Дополнение	Морозов А.А.	
2.2.	17.01.2020	Пункт 6.2.7.	Дополнение	Морозов А.А.	
2.2.	17.01.2020	Пункт 6.5.	Удален	Морозов А.А.	Приостановление действие сертификата
2.2.	17.01.2020	Пункт 6.6.	Удален	Морозов А.А.	Возобновление действие сертификата
2.2.	17.01.2020	Пункт 6.7. /6.8. /6.9.	Изменена нумерация	Морозов А.А.	Изменена нумерация пунктов и подпунктов на 6.5. /6.6. /6.7. соответственно
2.3.	02.03.2020	Пункт 10.	Добавлен раздел	Морозов А.А.	Приложения
2.3.	02.03.2020	Пункт 6.2.6.	Изменен	Морозов А.А.	
2.3.	02.03.2020	Пункт 1.9.	Изменен	Морозов А.А.	Актуализирован перечень НПА
2.3.	02.03.2020	Пункт 6.1.1.	Изменен	Морозов А.А.	
2.3.	02.03.2020	Пункт 6.1.2.	Изменен	Морозов А.А.	
2.3.	02.03.2020	Пункт 6.1.3.	Изменен	Морозов А.А.	
2.3.	02.03.2020	Пункт 6.1.4.	Уточнение	Морозов А.А.	Статья ФЗ № 63
2.3.	02.03.2020	Пункт 2.	Изменен	Морозов А.А.	
2.3.	02.03.2020	Пункт 3.1.	Изменен	Морозов А.А.	
2.3.	02.03.2020	Пункт 3.2.	Изменен	Морозов А.А.	
2.3.	02.03.2020	Пункт 4.2.	Изменен	Морозов А.А.	
2.3.	02.03.2020	Пункт 4.3.	Корректировка	Морозов А.А.	Скорректирована нумерация пунктов
2.3.	02.03.2020	Пункт 6.2.7.	Изменен	Морозов А.А.	
2.3.	02.03.2020	Пункт 5.1.	Изменен	Морозов А.А.	
2.3.	02.03.2020	Пункт 1.10.	Изменен	Морозов А.А.	
2.3.	02.03.2020	Пункт 6.2.3.	Дополнен	Морозов А.А.	Уточнено законодательство
2.3.	02.03.2020	Пункт 6.2.8.	Дополнен	Морозов А.А.	Уточнено размещение прайс-листа