УТВЕРЖДЕНО

Приказ № 4.3/02 от 14.09.2021г.

Генеральный директор
ООО «ТЦИ»
А.Н.Рогдев

ПОРЯДОК

РЕАЛИЗАЦИИ ФУНКЦИЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА И ИСПОЛНЕНИЯ ЕГО ОБЯЗАННОСТЕЙ ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ТЕХНИЧЕСКИЙ ЦЕНТР ИНТЕРНЕТ»

Редакция 1

Москва, 2021 г.

Содержание

1. Введение.

1.1. Порядок реализации функций удостоверяющего центра Обществом с ограниченной ответственностью «Технический центр Интернет» и исполнения его обязанностей (далее соответственно также – Порядок, Удостоверяющий центр) определяет условия предоставления услуг Удостоверяющего центра, включая права, обязанности и ответственность Удостоверяющего центра, а также права, обязанности и ответственность лиц, присоединившихся к Порядку.

1.2. Настоящий Порядок разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

1.3. В настоящем Порядке используются следующие термины и понятия:

Удостоверяющий центр – удостоверяющий центр ООО «ТЦИ»

администратор Удостоверяющего центра (далее также – Администратор УЦ) – сотрудник ООО «ТЦИ», наделенный полномочиями по созданию ключей электронной подписи, ключей проверки электронной подписи, сертификатов ключей проверки электронной подписи (далее также – сертификат), управлению и обслуживанию сертификатов, выданных Удостоверяющим центром, полномочиями по заверению копий сертификатов ключей проверки электронной подписи на бумажном носителе, администрированию и обслуживанию средств Удостоверяющего центра, а также иными полномочиями согласно настоящему Порядку. Администратор УЦ в рамках своих полномочий вправе оформлять (заверять) как документы на бумажном носителе, подписанные собственноручной подписью так и в форме электронных документов подписанных усиленной неквалифицированной подписью;

заявитель – лицо, обратившееся в Удостоверяющий центр для получения сертификата или для получения иных услуг Удостоверяющего центра;

сертификат ключа проверки электронной подписи Удостоверяющего центра (далее также – сертификат УЦ) – самоподписанный сертификат, сгенерированный Удостоверяющим центром и использующийся для проверки подлинности электронной подписи Удостоверяющего центра в созданных им сертификатах и списках отозванных сертификатов;

ключ электронной подписи Удостоверяющего центра – ключ электронной подписи, использующийся Удостоверяющим центром для создания сертификатов и списков отозванных сертификатов;

копия сертификата ключа проверки электронной подписи (далее также – копия сертификата) – документ на бумажном носителе, подписанный собственноручной подписью уполномоченным на это действие сотрудником Удостоверяющего центра и заверенный печатью Удостоверяющего центра. Содержательная часть копии сертификата ключа проверки

электронной подписи на бумажном носителе соответствует содержательной части сертификата, выданного в форме электронного документа;

оператор Удостоверяющего центра (далее также – Оператор УЦ) – уполномоченное лицо Удостоверяющего центра, являющееся работником общества с ограниченной ответственностью «Технический центр Интернет», наделенное полномочиями по созданию ключей электронной подписи, ключей проверки электронной подписи, сертификатов, обслуживанию сертификатов, выданных Удостоверяющим центром, а также полномочиями по заверению копий сертификатов на бумажном носителе, выданных Удостоверяющим центром. Оператор УЦ в рамках своих полномочий вправе оформлять (заверять) как документы на бумажном носителе, подписанные собственноручной подписью так и в форме электронных документов подписанных усиленной неквалифицированной подписью;

пользователь Удостоверяющего центра (далее также – Пользователь УЦ) – лицо, прошедшее процедуру регистрации в Удостоверяющем центре, сведения о котором включены в реестр пользователей Удостоверяющего центра, в том числе владелец сертификата (далее также – владелец сертификата);

список отозванных сертификатов – электронный документ с электронной подписью Удостоверяющего центра, формируемый на определенный момент времени и включающий в себя список серийных номеров сертификатов, которые на этот определенный момент времени аннулированы или действие которых было прекращено;

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

Иные понятия и термины, используемые в настоящем Порядке, применяются в значениях, определенных федеральными законами № 63-ФЗ от 06.04.2011 «Об электронной подписи» (далее – Федеральный закон «Об электронной подписи»), № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон «Об информации, информационных технологиях и о защите информации»)), № 152-ФЗ от 27.07.2006 «О персональных данных» (далее – Федеральный закон «О персональных данных»), № 126-ФЗ от 07.07.2003 «О связи» (далее – Федеральный закон «О связи»), и принимаемыми в соответствии с ними нормативными правовыми актами.

2. Общие положения.

2.1. Предмет регулирования.

2.1.1. Предметом регулирования Порядка являются отношения в области использования электронных подписей, возникающие между Удостоверяющим центром и участниками

электронного взаимодействия при оказании услуг Удостоверяющего центра, реализации его функций и исполнении обязанностей.

2.1.2. Настоящий Порядок является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

2.1.3. Сторонами настоящего Порядка является Удостоверяющий центр и лица, присоединившиеся к Порядку.

2.1.4. Настоящий Порядок является средством официального уведомления и информирования всех Сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг Удостоверяющего центра.

2.1.5. Публикация и распространение настоящего Порядка.

Настоящий Порядок распространяется в форме электронного документа путем размещения (публикации) на сайте Удостоверяющего центра в информационно-телекоммуникационной сети «Интернет» (далее также – сеть Интернет) по адресу https://ca.tcinet.ru.

2.1.6. Присоединение к настоящему Порядку.

2.1.6.1. Присоединение к настоящему Порядку осуществляется путем собственноручного подписания и предоставления в Удостоверяющий центр заявления об изготовлении сертификата ключа проверки электронной подписи (далее по тексту – Заявление), а также Заявления, подписанного усиленной квалифицированной электронной подписью заявителя или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре.

2.1.6.2. С момента предоставления заявителем в Удостоверяющий центр Заявления и регистрации Удостоверяющим центром Заявления, заявитель считается полностью и безоговорочно принявшим условия настоящего Порядка и всех его приложений и присоединившимся к Порядку в действующей редакции. Заявитель, присоединившийся к Порядку, принимает все дальнейшие изменения, которые могут вноситься в Порядок Удостоверяющим центром, в соответствии с условиями, установленными в Порядке (пункт 2.1.8.). Заявитель, присоединившийся к настоящему Порядку, самостоятельно отслеживает изменения и/или дополнения, вносимые в настоящий Порядок путем ознакомления с информацией об изменении и/или введении в действие новой редакции Порядка, размещенными (опубликованными) на сайте Удостоверяющего центра в сеть Интернет по адресу https://ca.tcinet.ru.

2.1.6.3. Удостоверяющий центр вправе отказать любому лицу в приеме и регистрации Заявления в случае ненадлежащего оформления заявителем документов, необходимых для оказания услуг, предоставления неактуальных документов или сведений, предоставления их не в полном объеме или предоставления заявителем не достоверных сведений.

2.1.7. Порядок прекращения присоединения к настоящему Порядку.

2.1.7.1. Действие настоящего Порядка может быть прекращено по инициативе одной из Сторон в следующих случаях:

волеизъявления одной из Сторон;

нарушения одной из Сторон условий настоящего Порядка.

2.1.7.2. Сторона, принявшая решение о прекращении договорных отношений должна письменно уведомить другую Сторону о своих намерениях за 1 (один) месяц до даты расторжения настоящего Порядка. Договорные отношения в соответствии с настоящим Порядком считаются расторгнутым после выполнения Сторонами своих обязанностей.

2.1.7.3. Прекращение действия договорных отношений, определенных настоящим Порядком, не освобождает Стороны от исполнения обязанностей, возникших до указанного дня их прекращения, и не освобождает от ответственности за их неисполнение (ненадлежащее исполнение).

2.1.8. Внесение изменений и дополнений в Порядок.

2.1.8.1. Внесение изменений и дополнений в настоящий Порядок, включая внесение изменений и дополнений в приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

2.1.8.2. Внесение изменений и/или дополнений в Порядок осуществляется Удостоверяющим центром путем обязательного размещения (публикации) на сайте Удостоверяющего центра в сети Интернет по адресу https://ca.tcinet.ru новой версии Порядка, утвержденного приказом Генерального директора ООО «ТЦИ».

2.1.8.3. Все изменения и дополнения, вносимые Удостоверяющим центром в настоящий Порядок по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными в дату, указанную в соответствующем приказе об утверждении новой версии Порядка, но не ранее, чем через 1 (один) месяц с даты публикации новой версии Порядка на сайте Удостоверяющего центра.

2.1.8.4. Все изменения, вносимые Удостоверяющим центром в Порядок в связи с изменениями, которые вносятся в нормативные правовые акты, регулирующие отношения в области использования электронных подписей, вступают в силу одновременно с вступлением в силу вышеуказанных изменений.

2.1.8.5. Все изменения в Порядке с момента вступления в силу новой версии Порядка распространяются на всех лиц, присоединившихся к Порядку, в том числе присоединившихся к Порядку ранее даты вступления новой версии Порядка в силу. В случае несогласия с вышеуказанными изменениями Сторона, присоединившаяся к Порядку до вступления в силу таких изменений, имеет право прекратить договорные отношения и расторгнуть настоящий

Порядок, письменно уведомив Удостоверяющий центр о своих намерениях за 1 (один) месяц до даты расторжения настоящего Порядка.

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

2.1.9. Применение Порядка.

2.1.9.1. Стороны понимают понятия и термины, применяемые в настоящем Порядке, строго в контексте общего смысла Порядка.

2.1.9.2. В случае противоречия и (или) расхождения названия какого-либо раздела Порядка со смыслом какого-либо пункта в нем содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

2.1.9.3. В случае противоречия и (или) расхождения положений какого-либо приложения к настоящему Порядку с положениями собственно Порядка, Стороны считают доминирующим смысл и формулировки Порядка.

2.1.10. Ответственность Сторон.

2.1.10.1. За невыполнение или ненадлежащее выполнение обязанностей, определенных настоящим Порядком, Стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязанностей другой Стороной. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

2.1.10.2. Стороны не несут ответственность за неисполнение, либо ненадлежащее исполнение своих обязанностей, определенных настоящим Порядком, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной своих обязанностей.

2.1.10.3. Стороны несут ответственность за неисполнение обязанностей, установленных Федеральным законом «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, соглашением Сторон, в том числе настоящим Порядком.

2.1.10.4. Ответственность Сторон, не урегулированная положениями настоящего Порядка, регулируется законодательством Российской Федерации.

2.1.11. Разрешение споров.

2.1.11.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Сторона, присоединившаяся к настоящему Порядку.

2.1.11.2. При рассмотрении спорных вопросов, связанных с настоящим Порядком, Стороны будут руководствоваться действующим законодательством Российской Федерации.

2.1.11.3. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

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

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

2.2. Сведения об Удостоверяющем центре.

2.2.1. Общество с ограниченной ответственностью «Технический центр Интернет» осуществляет оказание услуг, реализацию функций и исполнение обязанностей Удостоверяющего центра на основании:

Устава Общества с ограниченной ответственностью «Технический центр Интернет»;

лицензии на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации техническому обслуживанию 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 или индивидуального предпринимателя), выданной Центром по лицензированию, сертификации и защите государственной тайны ФСБ России от 17 сентября 2019 г. № 17433 Н (ЛСЗ № 0016560). Виды работ (услуг), выполняемых (оказываемых) в составе лицензируемого вида деятельности: работы, предусмотренные пунктами 7,11, 12, 13, 14, 20, 21, 22, 23, 25, 26, 28 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося приложением к Положению, утвержденному постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313;

2.2.2. Реквизиты Удостоверяющего центра.

Полное наименование юридического лица: Общество с ограниченной ответственностью «Технический центр Интернет».

Сокращенное наименование юридического лица: ООО «ТЦИ».

ОГРН: 5177746150720, ИНН: 7714417530, КПП: 771401001

Банковские реквизиты:

Отделение – Филиал Банка ВТБ (ПАО) г. Москва

р/с 40702810103800000332

кор/сч 30101810700000000187

БИК 044525187

2.2.3. Информация о месте нахождения и графике работы Удостоверяющего центра.

Место нахождения и почтовый адрес: 127083, г. Москва, улица 8 Марта, дом 1, строение 12, офис Э. 7, ПМ. XL К. 23-32.

Адрес оказания услуг Удостоверяющего центра: 127083, г. Москва, улица 8 Марта, дом 1, строение 12, офис Э. 7, ПМ. XLII.

График работы Удостоверяющего центра: ежедневно с 12:00 до 17:00 кроме выходных, праздничных дней и нерабочих дней, которые определяются в соответствии с федеральным законодательством на основании нормативных актов уполномоченных государственных органов.

2.3. Порядок информирования о предоставлении услуг Удостоверяющего центра.

2.3.1. Справочные телефоны Удостоверяющего центра: +7 (495) 730-29-70.

2.3.2. Адреса электронной почты: ca@tcinet.ru.

2.3.3. Адрес сайта Удостоверяющего центра в сети Интернет: https://ca.tcinet.ru.

2.3.4. Порядок получения информации заинтересованными лицами по вопросам предоставления услуг Удостоверяющего центра.

Любые заинтересованные лица могут получить информацию по вопросам предоставления услуг Удостоверяющего центра с использованием следующих способов:

ознакомиться с информацией, опубликованной на сайте Удостоверяющего центра;

направить запрос по электронной почте на адрес ca@tcinet.ru. Срок ответа по запросу, направленному по электронной почте, составляет не более 3 (трех) рабочих дней со дня получения Удостоверяющим центром данному запроса, если для подготовки ответа не потребуется более длительный срок, о чем Удостоверяющий центр уведомит лицо, направившее запрос по электронной почте;

направить письменное обращение в адрес Удостоверяющего центра. Данное обращение рассматривается в течение 30 (тридцати) дней со дня его поступления в Удостоверяющий центр.

Форма информирования Удостоверяющим центром лица, обратившегося в Удостоверяющий центр, соответствует форме обращения такого лица, возможна иная форма информирования с учетом пожеланий обратившегося лица и (или) характера обращений.

2.4. Стоимость услуг Удостоверяющего центра.

2.4.1. Услуги, оказываемые Удостоверяющим центром, предоставляются на платной основе.

2.4.2. Стоимость услуг, оказываемых Удостоверяющим центром на платной основе, определяется прейскурантом, утвержденным приказом. Прейскурант публикуется на сайте Удостоверяющего центра в сети Интернет по адресу https://ca.tcinet.ru.

2.4.3. Сроки и порядок расчетов за оказываемые на платной основе услуги Удостоверяющего центра регулируются отдельными договорами (соглашениями), заключаемыми между Обществом с ограниченной ответственностью «Технический центр Интернет» и заявителем, лицом заключившим договор (соглашение) и осуществляющим оплату в интересах заявителя.

Оплата осуществляется в российских рублях по безналичному расчету путем перечисления денежных средств на расчётный счёт Общества с ограниченной ответственностью «Технический центр Интернет». Датой оплаты считается дата поступления денежных средств на расчетный счет Общества с ограниченной ответственностью «Технический центр Интернет».

2.4.4. По обращениям участников электронного взаимодействия Удостоверяющий центр на безвозмездной основе оказывает следующие услуги:

предоставление участникам электронного взаимодействия информации, содержащейся в реестре выданных, аннулированных и прекративших свое действие сертификатов ключей проверки электронных подписей (далее также – реестр сертификатов);

аннулирование выданных Удостоверяющим центром сертификатов в соответствии с правилами, определенными настоящим Порядком;

создание и выдача сертификатов, выданных Удостоверяющим центром, в случае выполнения процедуры внеплановой смены ключа электронной подписи Удостоверяющего центра.

3. Перечень функций (оказываемых услуг), реализуемых Удостоверяющим центром.

В процессе реализации своей деятельности Удостоверяющий центр:

создает сертификаты и выдает сертификаты лицам, обратившимся за их получением, при условии установления личности заявителя либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата;

осуществляет проверку достоверности документов и сведений, представленных заявителем;

осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи,

соответствующим ключу проверки электронной подписи, указанному им для получения сертификата;

устанавливает сроки действия сертификатов;

выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

ведет реестр сертификатов, обеспечивает безвозмездный доступ к нему с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, обеспечивает актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

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

осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

обеспечивает конфиденциальность созданных удостоверяющим центром ключей электронных подписей, за исключением ключей электронных подписей, полученных заявителями;

обеспечивает целостность, достоверность и конфиденциальность информации, подлежащей хранению в удостоверяющем центре;

осуществляет сопровождение сертификатов, выдаваемых Удостоверяющим центром, в том числе обеспечивает внесение реестр сертификатов информации об аннулированных или прекративших свое действие сертификатах ключей проверки электронной подписи;

обеспечивает актуализацию и публикацию списка отозванных сертификатов в электронном виде, предоставляет к нему безвозмездный доступ с использованием сети Интернет;

осуществляет информирование лиц, обращающихся в Удостоверяющий центр для получения сертификатов, 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

оказывает техническую поддержку Пользователей УЦ и осуществляет предоставление консультаций по вопросам использования электронной подписи и средств электронной

подписи, в том числе по вопросам обеспечения безопасности при использовании электронной подписи и средств электронной подписи;

осуществляет мероприятия по техническому сопровождению и обеспечению бесперебойного функционирования средств удостоверяющего центра, обновлению программных и технических средств удостоверяющего центра;

обеспечивает информационную безопасность удостоверяющего центра и осуществляет мероприятия по технической защите информации, обрабатываемой с использованием средств удостоверяющего центра;

осуществляет иную связанную с использованием электронной подписи деятельность.

4. Права и обязанности Удостоверяющего центра.

4.1. Права Удостоверяющего центра.

Удостоверяющий центр имеет право:

1) запрашивать у заявителя документы, необходимые для установления личности получателя сертификата (заявителя) либо документы, подтверждающие полномочия лица, выступающего от имени заявителя;

2) запрашивать у заявителя документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи сертификата;

3) отказать заявителю в выдаче сертификата в следующих случаях:

не предоставлены документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи сертификата;

документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания сертификата, представлены не в полном объеме или они не надлежаще оформлены, а также в случае, когда достоверность и актуальность представленных заявителем сведений не подтверждается;

не установлена личность заявителя – физического лица, обратившегося за получением сертификата;

не получено подтверждение правомочий лица, выступающего от имени заявителя – юридического лица, обращаться за получением сертификата;

4) отказать заявителю в прекращении действия сертификата, выданного Удостоверяющим центром, в следующих случаях:

соответствующие заявительные документы не оформлены, оформлены ненадлежащим образом или не получено подтверждение правомочий лица, выступающего от имени заявителя;

сертификат был аннулирован или прекратил свое действие в соответствии с частями 6 и 6.1 статьи 14 Федерального закона «Об электронной подписи».

5) в одностороннем порядке прекратить действие сертификата, выданного Удостоверяющим центром, с одновременным направлением соответствующего уведомления его владельцу, в следующих случаях:

при наличии у Удостоверяющего центра достоверных сведений о нарушении конфиденциальности ключа проверки электронной подписи, принадлежащего владельцу соответствующего сертификата;

Удостоверяющему центру стало известно и получены официальные сведения о том, что документы или сведения, представленные заявителем для получения сертификата, не являются подлинными или не подтверждают достоверность информации, включенной в сертификат;

6) в одностороннем порядке прекратить действие сертификата, выданного Удостоверяющим центром, с направлением соответствующего уведомления его владельцу не позднее, чем за один рабочий день до прекращения действия сертификата, в случае невыполнения владельцем сертификата обязанностей, установленных Федеральным законом «Об электронной подписи», иными принимаемыми в соответствии с ним нормативными правовыми актами, настоящим Порядком или договором оказания услуг Удостоверяющего центра;

7) устанавливать сроки действия сертификатов;

8) выдавать - сертификаты как в форме электронных документов, так и в форме документов на бумажном носителе;

9) в одностороннем порядке вносить изменения и дополнения в Порядок в соответствии с пунктом 2.1.8 настоящего Порядка.

4.2. Обязанности Удостоверяющего центра.

Удостоверяющий центр обязан:

1) осуществлять деятельность в соответствии с требованиями федеральных законов «Об электронной подписи», «Об информации, информационных технологиях и о защите информации», «О персональных данных», иными нормативными правовыми актами в области использования электронной подписи и защиты информации, настоящим Порядком;

2) обеспечить размещение настоящего Порядка на сайте Удостоверяющего центра;

3) информировать в письменной форме 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;

4) обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, к реестру сертификатов в любое время в течение срока деятельности Удостоверяющего центра;

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

6) обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей, за исключением ключей электронных подписей, полученных заявителями;

7) обеспечивать бесперебойное функционирование средств удостоверяющего центра, осуществлять мероприятия по технической защите информации, обрабатываемой с использованием средств удостоверяющего центра, принимать меры по обеспечению безопасности персональных данных при их обработке в Удостоверяющем центре;

8) организовать свою работу с учетом часового пояса по местонахождению Удостоверяющего центра и обеспечить синхронизацию по времени средств Удостоверяющего центра;

9) осуществлять процедуру плановой смены ключей электронной подписи Удостоверяющего центра, используемого для подписания сертификатов, выдаваемых Удостоверяющим центром;

10) использовать для реализации функций Удостоверяющего центра средства удостоверяющего центра, соответствующие требованиям к средствам удостоверяющего центра, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796;

11) осуществлять проверку достоверности документов и сведений, представленных заявителем;

12) установить личность заявителя - физического лица, обратившегося к нему за получением сертификата;

13) получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением сертификата;

14) осуществить подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата;

15) создать и выдать сертификат заявителю в соответствии с настоящим Порядком при условии подтверждения достоверности информации, представленной заявителем для включения в сертификат, установления личности заявителя - физического лица или получения подтверждения правомочий лица, выступающего от имени заявителя - юридического лица;

16) создать по обращению заявителя ключ электронной подписи и ключ проверки электронной подписи;

17) выдать по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные

удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

18) осуществлять по обращениям участников электронного взаимодействия проверку электронных подписей;

19) обеспечивать уникальность ключей проверки электронных подписей и номеров сертификатов, выдаваемых Удостоверяющим центром;

20) при выдаче сертификата:

ознакомить под расписку владельца сертификата с информацией, содержащейся в сертификате;

внести в реестр сертификатов информацию о выданном сертификате не позднее указанной в нем даты начала действия такого сертификата;

21) 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;

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

23) отказать заявителю в выдаче сертификата в случае, если не подтверждена достоверность информации, представленной заявителем для включения в сертификат, или не установлена личность заявителя - физического лица или не получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением сертификата;

24) аннулировать сертификат, выданный Удостоверяющим центром, в следующих случаях:

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

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

вступило в силу решение суда, которым, в частности, установлено, что сертификат содержит недостоверную информацию.

25) прекратить действие сертификата на основании надлежаще оформленного заявления владельца сертификата, подаваемого в форме документа на бумажном носителе или в форме электронного документа, подписанного квалифицированной электронной подписью владельца сертификата;

26) внести в реестр сертификатов информацию о прекращении действия сертификата в течение 12 (двенадцати) часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона «Об электронной подписи», или в течение 12 (двенадцати) часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств;

27) уведомить владельца сертификата о фактах, которые стали известны Удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата, выданного Удостоверяющим центром владельцу сертификата, в том числе об аннулировании или прекращении действия сертификата;

28) официально уведомить участников электронного взаимодействия об аннулировании или прекращении действия сертификата посредством внесения соответствующей информации в список отозванных сертификатов;

29) публиковать список отозванных сертификатов на сайте Удостоверяющего центра, обеспечить его актуальность и круглосуточную доступность. Информация о адресах публикации списка отозванных сертификатов указывается в сертификатах, выдаваемых Удостоверяющим центром;

30) хранить информацию, внесенную в реестр сертификатов, в течение всего срока деятельности Удостоверяющего центра;

31) обеспечить целостность и достоверность информации, хранящейся в Удостоверяющем центре;

32) обеспечить хранение следующей информации:

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

33) в случае принятия решения о прекращении деятельности Удостоверяющего центра:

уведомить не менее чем за один месяц до даты прекращения деятельности Удостоверяющего центра владельцев сертификатов, имеющих сертификаты, срок действия которых не истек.

5. Права и обязанности Стороны, присоединившейся к Порядку.

5.1. Права Стороны, присоединившейся к Порядку, права Пользователя УЦ.

5.1.1. Сторона, присоединившаяся к Порядку, имеет право:

1) обратиться в Удостоверяющий центр для получения услуг, оказываемых Удостоверяющим центром в соответствии с настоящим Порядком, в том числе для регистрации в Удостоверяющем центре в качестве Пользователя УЦ и получения сертификата;

2) получить сертификат Удостоверяющего центра в форме электронного документа и его копию на бумажном носителе, заверенную Удостоверяющим центром;

3) получать в электронной форме списки отозванных сертификатов, созданные Удостоверяющим центром;

4) применять сертификат Удостоверяющего центра и список отозванных сертификатов для проверки сертификатов, выданных Удостоверяющим центром;

5) применять сертификаты, выданные Удостоверяющим центром, для проверки электронных подписей в электронных документах в соответствии со сведениями, указанными в сертификатах;

6) получать средства электронной подписи, обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи;

7) создавать с использованием средства электронной подписи ключ электронной подписи и ключ проверки электронной подписи;

8) обращаться в Удостоверяющий центр для проведения проверки подлинности электронной подписи, основанной на сертификате, выданном Удостоверяющим центром;

9) обращаться в Удостоверяющий центр для получения консультаций по вопросам использования электронной подписи, средств электронной подписи, вопросам обеспечения безопасности использования электронной подписи и средств электронной подписи.

5.1.2. Пользователь УЦ имеет все права Стороны, присоединившейся к Порядку, а также имеет право:

1) получить в соответствии с настоящим Порядком сертификат, созданный Удостоверяющим центром для данного Пользователя УЦ, при условии установления Удостоверяющим центром личности лица, обращающегося за получением данного сертификата и подтверждения его правомочий;

2) при получении сертификата:

получить копию сертификата на бумажном носителе, заверенную Удостоверяющим центром;

получить ключ электронной подписи и ключ проверки электронной подписи Пользователя УЦ, созданные Удостоверяющим центром;

3) запрашивать и получать в Удостоверяющем центр в форме электронного документа сертификаты иных Пользователей УЦ, информация о которых включена в реестр сертификатов Удостоверяющего центра;

4) обращаться в Удостоверяющий центр для прекращения действия (отзыва), сертификата, владельцем которого он является, в течение срока действия данного сертификата;

5) обращаться в Удостоверяющий центр для получения технической поддержки по вопросам использования электронной подписи и средств электронной подписи.

5.2. Обязанности Стороны, присоединившейся к Порядку, обязанности Пользователя УЦ.

5.2.1. Сторона, присоединившаяся к Порядку, обязана:

1) исполнять требования, установленные Федеральным законом «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами и Порядком;

2) предоставлять в соответствии с настоящим Порядком в Удостоверяющий центр актуальные и достоверные документы либо их надлежащим образом заверенные копии и сведения, в том числе необходимые для получения сертификата;

3) использовать для создания и проверки электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии Федеральным законом «Об электронной подписи»;

4) обеспечивать конфиденциальность используемых ключей электронных подписей, в частности не допускать использование ключей электронных подписей иными лицами без своего согласия;

5) предоставлять подтверждение, что лицо, обратившееся за получением сертификата, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата;

6) уведомлять Удостоверяющий центр и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

7) не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

8) не использовать ключ электронной подписи, срок действия которого истек;

9) оплатить услуги Удостоверяющего центра, если это предусмотрено договором оказания услуг Удостоверяющего центра;

5.2.2. Пользователь УЦ должен соблюдать все обязанности Стороны, присоединившейся к Порядку, а также обязан:

1) при получении сертификата:

ознакомится с информацией, содержащейся в сертификате;

2) не использовать ключ электронной подписи и незамедлительно обратиться в Удостоверяющий центр для прекращения действия сертификата, владельцем которого он

является, при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;

3) использовать электронную подпись с учетом ограничений, содержащихся в сертификате, если такие ограничения установлены;

4) не использовать ключ электронной подписи, связанный с сертификатом, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр до момента времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия;

5) не использовать ключ электронной подписи, связанный с сертификатом, который аннулирован или действие которого прекращено;

6) при создании или проверке электронной подписи осуществлять проверку действительности сертификата на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

7) при проверке электронной подписи осуществлять проверку принадлежности владельцу сертификата электронной подписи, с помощью которой подписан электронный документ, а также осуществлять проверку отсутствия изменений, внесенных в этот документ после его подписания;

8) информировать Удостоверяющий центр об изменении регистрационных данных владельца сертификата, влияющих на актуальность сведений, содержащихся в сертификате, и обратиться в Удостоверяющий центр для прекращения действия такого сертификата в случае наличия оснований полагать, что несоответствие данных о владельце сертификата и сведений, содержащихся в сертификате, может повлиять на результат проверки электронной подписи при осуществлении обмена информацией с иными участниками информационного взаимодействия.

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.

Создание ключей электронных подписей и ключей проверки электронных подписей осуществляется Удостоверяющим центром или самостоятельно заявителем.

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

6.1.1.1. Создание ключей электронных подписей и ключей проверки электронных подписей, предназначенных для создания и проверки усиленной неквалифицированной электронной подписи, осуществляется заявителем с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, в соответствии с эксплуатационной и технической документацией на используемые средства электронной подписи.

6.1.1.2. Создание ключей электронных подписей и ключей проверки электронных подписей должно осуществляться заявителем в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

6.1.1.3. Сторона, присоединившаяся к Порядку, имеет право получить средства электронной подписи при обращении в Удостоверяющий центр в соответствии с настоящим Порядком.

6.1.1.4. При создании ключа электронной подписи и ключа проверки электронной подписи заявитель формирует запрос на создание сертификата в электронной форме (файл в формате PKCS#10) и в форме бумажного документа, подписанного заявителем собственноручно.

Сформированный запрос на создание сертификата прикладывается к заявительным документам при обращении заявителя в Удостоверяющий центр для получения сертификата.

6.1.1.5. Заявитель должен обеспечивать конфиденциальность ключей электронных подписей и паролей доступа к ключевой информации, принимать все возможные меры для предотвращения их потери, раскрытия, искажения и несанкционированного использования.

6.1.1.6. Хранение и использование ключей электронных подписей должно осуществляться заявителем в соответствии с Инструкцией ФАПСИ № 152, правилами пользования применяемых СКЗИ, иной документацией на применяемое СКЗИ.

6.1.1.7. При создании ключа электронной подписи и ключа проверки электронной подписи заявителем основанием подтверждения владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата, является одновременное соблюдение следующих условий:

подтверждена достоверность документов и сведений, предоставляемых в Удостоверяющий центр заявителем;

установлена личность заявителя или получено подтверждение правомочий лица, выступающего от имени заявителя, обращающегося за получением сертификата;

информация, указанная в запросе на создание сертификата, в том числе информация о полномочиях лица, подписавшего запрос, соответствуют сведениям, указанными заявителем в документах, предоставляемых в Удостоверяющий центр;

сформированный заявителем запрос на создание сертификата на бумажном носителе, подписанный собственноручной подписью заявителя, либо запрос в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре;

имеется положительный результат проверки электронной подписи, с помощью которой подписан запрос на создание сертификата, в случае если он предоставлен в электронной форме.

6.1.2. Порядок создания ключей электронных подписей и ключей проверки электронных подписей Удостоверяющим центром для заявителя.

6.1.2.1. Ключи электронных подписей и ключи проверки электронных подписей создаются Удостоверяющим центром с использованием средств электронной подписи и средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, в соответствии с эксплуатационной и технической документацией на используемые средства электронной подписи и средства удостоверяющего центра.

6.1.2.2. Удостоверяющий центр создает ключ электронной подписи и ключ проверки электронной подписи в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

6.1.2.3. Создание ключа электронной подписи и ключа проверки электронной подписи осуществляется Удостоверяющим центром для заявителя, присоединившегося к настоящему Порядку, при личном прибытии заявителя или его уполномоченного представителя в Удостоверяющий центр, при условии установления личности заявителя или получения подтверждения правомочий лица, выступающего от имени заявителя.

6.1.2.4. Ключ электронной подписи и ключ проверки электронной подписи создается Удостоверяющим центром одновременно с созданием сертификата в соответствии с пунктом

6.1 настоящего Порядка, при условии подтверждения достоверности документов и сведений, предоставленных заявителем.

6.1.2.5. В случае создания ключа электронной подписи и ключа проверки электронной подписи при личном прибытии заявителя или его уполномоченного представителя в Удостоверяющий центр основанием подтверждения владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата, является одновременное соблюдение следующих условий:

подтверждена достоверность документов и сведений, предоставляемых в Удостоверяющий центр заявителем;

установлена личность заявителя или получено подтверждение правомочий лица, выступающего от имени заявителя, обращающегося за получением сертификата;

заявитель или его уполномоченный представитель под расписку ознакомился с информацией, содержащейся в запросе на создание сертификата, сформированном Удостоверяющим центром.

6.2. Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра.

6.2.1. В процессе организации деятельности Удостоверяющего центра осуществляется планирование мероприятий по осуществлению его деятельности, в том числе мероприятий по смене ключей электронной подписи Удостоверяющего центра и мероприятий по выводу ключей электронной подписи Удостоверяющего центра из эксплуатации.

6.2.2. Основаниями для выполнения процедуры плановой смены ключа электронной подписи Удостоверяющего центра и процедуры его вывода из эксплуатации являются запланированные мероприятия по осуществлению деятельности Удостоверяющего центра.

6.2.3. Выполнение процедуры плановой смены ключа электронной подписи Удостоверяющего центра осуществляется в период срока действия ключа электронной подписи Удостоверяющего центра, не ранее, чем через шесть месяцев, и не позднее, чем через один год после начала действия ключа электронной подписи Удостоверяющего центра. Процедура создания нового ключа электронной подписи Удостоверяющего центра осуществляется заранее, не позднее, чем за 15 дней до истечения одного года после начала срока действия ключа электронной подписи Удостоверяющего центра.

6.2.4. Выполнение процедуры вывода из эксплуатации ключа электронной подписи Удостоверяющего центра осуществляется не позднее, чем за один рабочий день до окончания срока действия ключа электронной подписи Удостоверяющего центра, установленного в соответствии с технической и эксплуатационной документацией на средства удостоверяющего центра и средства электронной подписи, с использованием которого данный ключ электронной подписи был создан.

6.2.5. Срок действия ключа электронной подписи Удостоверяющего центра составляет максимально допустимый срок действия, установленный в соответствии с технической и эксплуатационной документацией на средства удостоверяющего центра и средства электронной подписи, с использованием которого данный ключ электронной подписи был создан.

Начало периода действия ключа электронной подписи Удостоверяющего центра исчисляется с даты и времени создания ключа электронной подписи Удостоверяющего центра.

6.2.6. Порядок смены ключей электронной подписи Удостоверяющего центра.

6.2.6.1. Плановая смены ключей электронной подписи Удостоверяющего центра осуществляется в следующем порядке:

6.2.6.1.1. Администратор Удостоверяющего центра с использованием сертифицированных по требованиям безопасности средств удостоверяющего центра и средств электронной подписи создает новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи, записывает их на сертифицированный учтенный ключевой носитель и обеспечивает его хранение в соответствии с требованиями, предъявляемыми к обеспечению целостности и конфиденциальности ключа электронной подписи Удостоверяющего центра;

Одновременно с созданием вышеуказанных ключей производится выпуск самоподписанного сертификата Удостоверяющего центра.

6.2.6.1.2. после издания самоподписанного сертификата Администратор Удостоверяющего центра, по истечении шести месяцев после начала срока действия предыдущего ключа электронной подписи Удостоверяющего центра:

осуществляет ввод в эксплуатацию и установку нового ключа электронной подписи, ключа проверки электронной подписи и сертификата Удостоверяющего центра;

производит в соответствии с технической и эксплуатационной документацией настройку средств удостоверяющего центра для использования нового ключа электронной подписи, ключа проверки электронной подписи и сертификата Удостоверяющего центра;

обеспечивает хранение и использование ключей электронной подписи и ключей проверки электронной подписи Удостоверяющего центра в соответствии с требованиями безопасности, в форме, позволяющей обеспечить целостность и конфиденциальность ключей электронной подписи Удостоверяющего центра.

6.2.6.2. Информирование участников электронного взаимодействия о проведении плановой смены ключа электронной подписи Удостоверяющего центра осуществляется посредством размещения на сайте Удостоверяющего центра информации о новом сертификате

Удостоверяющего центра, соответствующему новому ключу проверки электронной подписи и ключу электронной подписи Удостоверяющего центра.

6.2.6.3. Предыдущий ключ электронной подписи Удостоверяющего центра действует в течение своего срока действия до вывода его из эксплуатации и используется для создания и подписания списка отозванных сертификатов, созданных Удостоверяющим центром в период действия предыдущего ключа электронной подписи Удостоверяющего центра.

6.2.6.4. Введенный в эксплуатацию новый ключ электронной подписи Удостоверяющего центра используется только для подписания создаваемых Удостоверяющим центром сертификатов и списков отозванных сертификатов.

6.2.6.5. Доверенными способами получения сертификата Удостоверяющего центра являются:

получение заявителем сертификата Удостоверяющего центра непосредственно в Удостоверяющем центре;

загрузка сертификата Удостоверяющего центра с сайта Удостоверяющего центра;

6.3. Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности.

6.3.1. В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра или реализации угрозы нарушения его конфиденциальности осуществляется внеплановая смена ключа электронной подписи и ключа проверки электронной подписи Удостоверяющего центра.

6.3.2. К случаям нарушения конфиденциальности ключей электронной подписи Удостоверяющего центра, относятся:

получение доступа неуполномоченного лица к ключу электронной подписи Удостоверяющего центра или к ключевому носителю, содержащего ключ электронной подписи Удостоверяющего центра;

утрата или хищение ключевого носителя, содержащего ключ электронной подписи Удостоверяющего центра;

утрата или хищение ключевого носителя, содержащего ключ электронной подписи Удостоверяющего центра, с его последующим обнаружением;

получение доступа неуполномоченного лица к техническим средствам Удостоверяющего центра или средствам электронной подписи, содержащих ключ электронной подписи Удостоверяющего центра;

несанкционированное копирование ключа электронной подписи Удостоверяющего центра;

нарушение правил хранения и использования ключа электронной подписи Удостоверяющего центра, которое привело или могло привести к его компрометации;

6.3.3. Виды угроз нарушения конфиденциальности ключей электронной подписи Удостоверяющего центра:

угрозы, непосредственно связанные с нарушением конфиденциальности ключа электронной подписи Удостоверяющего центра;

угрозы, связанные с несанкционированным доступом в помещения, где размещаются технические средства удостоверяющего центра, или доступам к хранилищам ключевой информации;

угрозы, связанные с несанкционированным доступом к средствам удостоверяющего центра;

угрозы, связанные с лицами, имеющими доступ в контролируемую зону, к средствам Удостоверяющего центра, ключам электронной подписи Удостоверяющего центра;

угрозы, связанные с проведением нарушителем атак на технические средства удостоверяющего центра, в том числе на носители защищаемой информации, средства вычислительной техники, среду функционирования средств криптографической защиты информации, каналы (линии) связи.

6.3.4. Удостоверяющего центр начинает процедуру внеплановой смены ключа электронной подписи Удостоверяющего центра после устранения причин, повлекших нарушение конфиденциальности электронной подписи Удостоверяющего центра.

6.3.5. Процедура внеплановой смены ключей электронной подписи Удостоверяющего центра осуществляется в порядке, определенном процедурой плановой смены ключей Удостоверяющего центра в соответствии с пунктом 6.1 настоящего Порядка.

6.3.6. Одновременно со сменой ключа электронной подписи Удостоверяющего центра прекращается действие всех ранее выданных сертификатов, подписанных ключом электронной подписи Удостоверяющего центра, который скомпрометирован.

6.3.7. Удостоверяющий центр уведомляет о факте компрометации ключа электронной подписи Удостоверяющего центра всех владельцев сертификатов путем направления соответствующего уведомления по электронной почте и (или) публикации информации на сайте Удостоверяющего центра.

6.3.8. После смены ключа электронной подписи Удостоверяющего центра и изготовления нового сертификата Удостоверяющего центра Удостоверяющий центр уведомляет всех владельцев сертификатов о возможности получения ими новых сертификатов.

6.3.9. Доверенными способами получения нового сертификата Удостоверяющего центра являются:

получение заявителем сертификата Удостоверяющего центра непосредственно в Удостоверяющем центре;

загрузка нового сертификата Удостоверяющего центра с сайта Удостоверяющего центра.

6.4. Порядок осуществления Удостоверяющим центром смены ключа электронной подписи Пользователя УЦ.

6.4.1. Сроки действия ключей электронной подписи и сертификатов, выдаваемых Удостоверяющим центром Пользователям УЦ.

6.4.1.1. Срок действия ключа электронной подписи и сертификата, выдаваемого Удостоверяющим центром Пользователю УЦ, включается в состав сертификата и составляет 1 (один) год.

6.4.1.2. Начало периода действия ключа электронной подписи исчисляется с даты и времени начала действия соответствующего сертификата.

6.4.1.3. Время начала действия сертификата включается в поле «Действителен с» («NotBefore») сертификата. Время окончания действия сертификата включается в поле «Действителен по» («NotAfter») сертификата.

6.4.2. Смена ключа электронной подписи Пользователя УЦ осуществляется владельцем сертификата в следующих случаях:

1) в связи с истечением установленного срока действия ключа электронной подписи;

2) на основании заявления, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

3) вступило в силу решение суда, которым, в частности, установлено, что сертификат содержит недостоверную информацию;

4) изменение сведений о владельце сертификата, в результате которых сведения, внесенные в сертификат, перестали быть достоверными;

5) нарушение конфиденциальности ключа электронной подписи владельца сертификата;

6) осуществлена процедура внеплановой смена ключа электронной подписи Удостоверяющего центра. В таком случае создание новых ключей электронной подписи для Пользователя УЦ и соответствующих им сертификатов осуществляется в соответствии с пунктом 6.2 настоящего Порядка;

7) в иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, настоящим Порядком или договором оказания услуг удостоверяющего центра.

6.4.3. В случае наступления обстоятельств, указанных в подпункте 3 пункта 6.4.2 настоящего Порядка, Удостоверяющий центр аннулирует сертификат владельца сертификата и уведомляет об этом владельца сертификата. Информация о прекращении действия

сертификата вносится Удостоверяющим центром в реестр сертификатов в течение 12 (двенадцати) часов с момента наступления указанных обстоятельств, или в течение 12 (двенадцати) часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата прекращается с момента внесения записи об этом в реестр сертификатов.

6.4.4. В случае наступления обстоятельств, указанных в подпунктах 4 и 5 пункта 6.4.2 настоящего Порядка, Сторона, присоединившаяся к Порядку, обязана обратиться в Удостоверяющий центр с заявлением на прекращение действия сертификата.

6.4.5. Смена ключа электронной подписи Пользователя УЦ осуществляется по его инициативе Стороны, присоединившейся к Порядку, в соответствии процедурой создания ключей электронных подписей и ключей проверки электронных подписей, приведенной в пункте 6.1 настоящего Порядка.

6.4.6. Создание Удостоверяющим центром нового ключа электронного подписи осуществляется одновременно с созданием и выдачей Пользователю УЦ ключа проверки электронной подписи и сертификата на основании соответствующего заявления Стороны, присоединившейся к Порядку, и документов, представленных в Удостоверяющий центр.

6.4.7. Требования к заявлению на смену ключа электронной подписи Пользователя УЦ.

Заявление на смену ключа электронной подписи Пользователя УЦ оформляется по форме заявления на создание и выдачу сертификата, приведенной в приложении № 1 или приложения № 2 к настоящему Порядку, и должно соответствовать требованиям к заявлению на создание и выдачу сертификата, указанным в пункте 6.5.2 и следующим требованиям:

1) в случае, если заявителем является юридическое лицо, заявление должно быть оформлено на бланке организации (при наличии) и заверено печатью юридического лица;

2) в случае, если заявителем является физическое лицо, заявление должно содержать:

собственноручную подпись физического лица и дату подписания;

собственноручную подпись физического лица и дату подписания в предоставляемом согласии на обработку персональных данных;

3) в случае, если заявитель самостоятельно осуществил создание ключа электронной подписи и ключа проверки электронной подписи в соответствии с пунктом 6.1.1 настоящего Порядка, к вышеуказанному заявлению прикладывается сформированный заявителем запрос на создание сертификата на бумажном носителе, подписанный собственноручной подписью заявителя, либо запрос в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре.

6.4.8. Заявитель имеет право создать заявление на смену ключа электронной подписи Пользователя УЦ в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре, при этом заявление должно соответствовать требованиями, указанным в пунктах 6.4.7 и 6.5.2 настоящего Порядка.

Процедура смены ключа электронной подписи Пользователя УЦ осуществляется заявителем в соответствии с пунктами 6.1 и 6.4 настоящего Порядка в том же порядке, как и создание ключа электронной подписи, при этом осуществляется также создание сертификата в соответствии с пунктом 6.5 настоящего Порядка.

В случае, если смена ключа электронной подписи Пользователя УЦ связана с нарушением его конфиденциальности или реализацией угрозы нарушения конфиденциальности, соответствующее заявление должно быть подписано усиленной квалифицированной электронной подписью заявителя или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре, основанной на действующем сертификате, не связанном с ключом электронной подписи, конфиденциальность которого нарушена.

6.5. Процедура создания и выдачи сертификатов.

6.5.1. Порядок подачи заявления на создание и выдачу сертификатов.

6.5.1.1. Заявитель обязан ознакомиться с положениями настоящего Порядка, опубликованного на сайте Удостоверяющего центра, в том числе с приложениями к настоящему Порядку.

6.5.1.2. Присоединение к Порядку осуществляется в соответствии с пунктом 2.1.6 настоящего Порядка. Для присоединения к настоящему Порядку и возможности получения услуг Удостоверяющего центра заявитель направляет Заявление по форме приложения № 1 или приложения № 2 к настоящему Порядку.

6.5.1.3. Удостоверяющий центр осуществляет создание сертификатов при условии выполнения Стороной, присоединившейся к Порядку, своих обязанностей.

6.5.1.4. Создание сертификата осуществляется Удостоверяющим центром на основании заявления на создание и выдачу сертификата, а также документов и сведений, представленных заявителем в Удостоверяющий центр, при условии установления личности заявителя или получения подтверждения правомочий лица, выступающего от имени заявителя, обращаться за получением сертификата.

6.5.1.5. Для регистрации в Удостоверяющем центре лица, на имя которого будет создан сертификат, в качестве Пользователя УЦ, заявитель направляет в Удостоверяющий центр заявление на создание и выдачу сертификата на бумажном носителе или в форме

электронного документа, подписанного усиленной квалифицированной подписью заявителя или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре.

6.5.1.6. Заявитель имеет право предоставить в Удостоверяющий центр Заявление по форме приложения № 1 или приложения № 2 к настоящему Порядку, а также документы и сведения, необходимые для регистрации Пользователя УЦ и создания сертификата, одним пакетом документов при личном прибытии заявителя или его уполномоченного представителя в Удостоверяющий центр, либо посредством почтовой или курьерской связи, либо предоставить указанные документы в форме электронных документов, подписанных усиленной квалифицированной подписью заявителя или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре, на электронном носителе информации или направив их в Удостоверяющий центр по информационно-телекоммуникационной сети, в том числе сети Интернет.

6.5.1.7. В случае, если представляемые заявителем документы содержат персональные данные, не являющиеся общедоступными, или иную конфиденциальную информацию, заявитель обязан обеспечить конфиденциальность такой информации при ее направлении в Удостоверяющий центр, в том числе с использованием сертифицированных средств криптографической информации, либо представить такие документы при личном прибытии в Удостоверяющий центр.

6.5.1.8. В случае, если Сторона, присоединившаяся к Порядку, обращается в Удостоверяющий центр для проведения плановой смены ключа электронной подписи, ключа проверки электронной подписи и сертификата Пользователя УЦ и сведения, содержащиеся в ранее представленных документах, потеряли свою актуальность и достоверность, Сторона, присоединившаяся к Порядку, предоставляет в Удостоверяющий центр заявление на создание и выдачу сертификата, а также актуальные документы и сведения, необходимые для создания сертификата.

6.5.1.9. После получения Удостоверяющим центром от заявителя Заявления по форме приложения № 1 или приложения № 2 к настоящему Порядку, в случае, если заявителем не представлены документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи сертификата, либо они представлены не полном объеме или их достоверность и актуальность не подтверждается, Удостоверяющий центр имеет право запросить, а Сторона, присоединившаяся к Порядку, обязана предоставить документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи сертификата.

6.5.1.10. Удостоверяющий центр имеет право отказать заявителю в регистрации Пользователя УЦ и создании сертификата, в случае, если Сторона, присоединившаяся к Порядку, не предоставила документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи сертификата, либо они представлены не полном объеме или они не надлежаще оформлены, а также в случае, когда достоверность и актуальность представленных заявителем сведений не подтверждается.

6.5.2. Требования к заявлению на создание и выдачу сертификата.

6.5.2.1. Требования к оформлению заявления на создание и выдачу сертификата.

6.5.2.1.1. В случае, если заявителем является юридическое лицо, заявление оформляется по форме, приведенной в приложении № 1 к настоящему Порядку, на бланке организации (при наличии) и заверено печатью юридического лица, а также должно содержать:

1) сведения, необходимые для создания сертификата, а также сведения о средстве электронной подписи, используемом заявителем;

2) реквизиты (дата и номер письма);

3) собственноручную подпись физического лица, действующего от имени юридического лица на основании учредительных документов юридического лица или доверенности;

4) собственноручную подпись физического лица в предоставляемом согласии на обработку персональных данных, в случае, если сведения о нем указаны в заявлении на создание сертификата.

6.5.2.1.2. В случае, если заявителем является физическое лицо, заявление оформляется по форме, приведенной в приложении № 2 к настоящему Порядку, и должно содержать:

1) сведения, необходимые для создания сертификата, а также сведения о средстве электронной подписи, используемом заявителем;

2) собственноручную подпись физического лица и дату подписания;

3) собственноручную подпись физического лица и дату подписания в предоставляемом согласии на обработку персональных данных.

6.5.2.2. В случае, если заявитель самостоятельно осуществил создание ключа электронной подписи и ключа проверки электронной подписи в соответствии с пунктом 6.1.1 настоящего Порядка, к заявлению прикладывается сформированный заявителем запрос на создание сертификата на бумажном носителе, подписанный собственноручной подписью заявителя, либо запрос в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя или усиленной неквалифицированной

подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре.

6.5.2.3. Требования к сведениям, включаемым в заявление на создание и выдачу сертификата, если заявителем является юридическое лицо:

6.5.2.3.1. В случае, если заявителем является юридическое лицо, в заявлении в обязательном порядке указывается следующая информация:

1) наименование юридического лица;

2) место нахождения юридического лица;

6.5.2.3.2. В случае, если заявителем является иностранная организация (в том числе филиал, представительство или иное обособленное подразделение иностранной организации), в заявлении в обязательном порядке указывается следующая информация:

1) наименование юридического лица;

2) место нахождения юридического лица;

6.5.2.3.3. В случае выдачи сертификата юридическому лицу в качестве владельца сертификата наряду с указанием наименования юридического лица указывается физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности (далее также – уполномоченный представитель юридического лица), в связи с чем в заявлении на создание и выдачу сертификата дополнительно указываются следующая информация:

1) фамилия, имя и отчество (если имеется) уполномоченного представителя юридического лица;

2) подразделение организации (при наличии);

3) должность уполномоченного представителя юридического лица (при наличии).

6.5.2.3.4. Допускается не указывать в качестве владельца сертификата физическое лицо, действующее от имени юридического лица, в сертификате, используемом для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе. В этом случае в заявлении допускается указывать только информацию, предусмотренную пунктом 6.5.2.3.1 настоящего Порядка.

6.5.2.4. Требования к сведениям, включаемым в заявление на создание и выдачу сертификата, если заявителем является физическое лицо:

6.5.2.4.1. В случае, если заявителем является физическое лицо, не являющееся индивидуальным предпринимателем, в заявлении в обязательном порядке указывается следующая информация:

1) фамилия, имя и отчество (если имеется) физического лица;

6.5.2.4.2. В случае, если заявителем является физическое лицо, являющееся индивидуальным предпринимателем, в заявлении в обязательном порядке указывается

следующая информация:

1) фамилия, имя и отчество (если имеется) физического лица;

6.5.2.5. Заявление на создание и выдачу сертификата должно содержать информацию о наименовании и классе средства электронной подписи, используемом заявителем.

6.5.2.6. В случае, если заявителем представлены в Удостоверяющий центр документы, подтверждающие его право действовать от имени третьих лиц, в сертификат может быть включена информация о таких правомочиях заявителя и сроке их действия.

6.5.2.7. Заявитель имеет право указать на ограничения использования сертификата (если такие ограничения им устанавливаются) для их включения в сертификат.

6.5.2.8. Заявитель имеет право оформить заявление на создание и выдачу сертификата как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре.

6.5.3. Порядок установления личности заявителя.

При выдаче сертификата Удостоверяющий центр идентифицирует заявителя, обратившегося к нему за получением сертификата, руководствуясь следующими положениями:

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

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

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

6.5.4. Перечень документов, запрашиваемых Удостоверяющим центром у заявителя для изготовления и выдачи сертификата.

При обращении в Удостоверяющий центр заявитель указывает на ограничения использования сертификата (если такие ограничения им устанавливаются) и представляет документы либо их надлежащим образом заверенные копии и сведения.

6.5.4.1. Заявители, являющиеся юридическими лицами, предоставляют:

1) основной документ, удостоверяющий личность физического лица, действующего от имени юридического лица на основании учредительных документов юридического лица, либо основной документ, удостоверяющий личность уполномоченного представителя юридического лица, действующего по доверенности, если сведения

об этом лице включаются в сертификат наряду с указанием наименования юридического лица. Допускается вместо основного документа, удостоверяющего личность физического лица, предоставлять его надлежащим образом заверенную копию;

2) информационную справку о компании, содержащую основные регистрационные данные (ОГРН, ИНН, КПП), выписку из единого государственного реестра юридических лиц;

3) иные документы, запрашиваемые по требованию Удостоверяющего центра, включая но не ограничиваясь, учредительные документы юридического лица либо их надлежащим образом заверенные копии, документы, подтверждающие полномочия физического лица, действовать от имени юридического лица на основании учредительных документов юридического лица;

Если за получением сертификата в Удостоверяющий центр обращается физическое лицо, не указанное в заявлении на создание и выдачу сертификата, дополнительно предоставляется:

4) основной документ, удостоверяющий личность физического лица, обращающегося в Удостоверяющий центр за получением сертификата, либо его надлежащим образом заверенную копию;

5) доверенность, подтверждающая право физического лица обращаться в Удостоверяющий центр от имени юридического лица за получением сертификата, оформленную в соответствии с формой, приведенной в приложении № 3 к настоящему Порядку.

6.5.4.2. Заявители, являющиеся физическими лицами, предоставляют:

1) основной документ, удостоверяющий личность, либо его надлежащим образом заверенную копию;

6.5.4.3. Заявители, являющиеся индивидуальными предпринимателями, предоставляют:

1) основной документ, удостоверяющий личность, либо его надлежащим образом заверенную копию;

6.5.4.4. В случае, если документы и сведения, предоставляемые заявителем, оформлены не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

6.5.4.5. В случае, если для подтверждения сведений, вносимых в сертификат, законодательством Российской Федерации установлена определенная форма документа, заявитель представляет в Удостоверяющий центр документ соответствующей формы.

6.5.5. Порядок проверки достоверности документов и сведений, представленных заявителем.

6.5.5.1. При получении от заявителя документов и сведений, необходимых для создания и выдачи сертификата, Оператор УЦ, в целях определения возможности регистрации Пользователя УЦ, в течение не более чем одного рабочего дня со дня их получения осуществляет предварительную проверку представленных заявителем документов и сведений на предмет их надлежащего оформления и полноты представления, соответствия положениям части 3 статьи 14, части 2 статьи 17 Федерального закона «Об электронной подписи», а также требованиям, указанным в пунктах 6.5.2 и 6.5.4 настоящего Порядка.

6.5.5.2. В случае, если Сторона, присоединившаяся к Порядку, обращается в Удостоверяющий центр для проведения плановой смены ключа электронной подписи, ключа проверки электронной подписи и сертификата зарегистрированного Пользователя УЦ, и документы, представленные заявителем ранее, имеются в Удостоверяющем центре, Оператор УЦ осуществляет проверку их актуальности и достоверности, а также соответствия сведений, содержащихся в заявлении на создание сертификата, с регистрационными данными Пользователя УЦ.

6.5.5.3. В случае, если документы представлены заявителем в форме электронных документов, подписанных усиленной квалифицированной электронной подписью или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре, Оператор УЦ осуществляет ее проверку в соответствии со статьей 11 Федерального закона «Об электронной подписи».

6.5.6. Порядок создания сертификата.

6.5.6.1. Создание сертификата осуществляется Удостоверяющим центром в соответствии с положениями статей 13 и 14 Федерального закона «Об электронной подписи» и настоящим Порядком.

Заявителям, которым услуги Удостоверяющего центра оказываются в соответствии с заключенным договором на оказание услуг удостоверяющего центра, сертификаты создаются при выполнении Стороной, присоединившейся к Порядку, обязанностей, предусмотренных настоящим Порядком и вышеуказанным договором.

6.5.6.2. Удостоверяющий центр в течение не более чем одного рабочего дня со дня положительного результата проведения проверки документов и сведений, предоставленных заявителем, уведомляет об этом заявителя и, в целях установления личности физического лица, обращающего за получением сертификата, а также для предоставления заявителем (при необходимости) оригиналов документов или их надлежаще заверенных копий, согласовывает с заявителем дату и время прибытия заявителя либо его уполномоченного представителя в Удостоверяющий центр.

6.5.6.3. Допускается осуществлять процедуру создания сертификата без прибытия заявителя или его уполномоченного представителя в Удостоверяющий центр при одновременном соблюдении следующих условий:

1) информационной взаимодействие, осуществляется способами, позволяющими обеспечить целостность информации и ее конфиденциальность, в случае передачи конфиденциальной информации;

2) документы, которые должны составляться исключительно на бумажном носителе, предоставляются посредством курьерской или почтовой связи;

3) личность лица, обращающегося за получением сертификата, была установлена Удостоверяющим центром ранее;

4) лицо, обращающееся за получением сертификата, является владельцем сертификата, который ранее был выдан Удостоверяющим центром;

5) получен положительный результат проведения проверки документов и сведений, предоставленных заявителем, в том числе подтверждены полномочия заявителя и лица, обращающего за получением сертификата;

6) сведения о лице, обращающегося за получением сертификата, который является владельцем сертификата, выданным Удостоверяющим центром, не изменились;

7) подтверждена актуальность и достоверность документов и сведений о владельце сертификата, которые получены Удостоверяющим центром ранее, в том числе оригиналов документов или их надлежаще заверенных копий;

8) создание ключа электронной подписи осуществлено заявителем самостоятельно и заявителем представлен в Удостоверяющий центр запрос на создание сертификата в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре;

9) имеется положительный результат проверки запроса на создание сертификата в форме электронного документа, представленного заявителем, а также подтверждено владение лицом, обращающегося за получением сертификата, ключом электронной подписи и ключом проверки электронной подписи, соответствующему запросу на создание сертификата;

10) имеется положительный результат проверки электронной подписи документов, представленных заявителем в электронной форме, в том числе запроса на создание сертификата, представленного заявителем в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре.

6.5.6.4. При прибытии заявителя либо его уполномоченного представителя в Удостоверяющий центр, Оператор УЦ осуществляет установление его личности и проверку оригиналов документов или их надлежаще заверенных копий, проверку соответствия сведений, а также проверку доверенностей (в случае, если за получением сертификата обращается лицо, не указанное в заявлении на создание и выдачу сертификата).

6.5.6.5. Если заявителем не представлены надлежащим образом заверенные копии документов, такие копии заверяется в Удостоверяющем центре при предоставлении оригиналов документов.

6.5.6.6. В случае установления личности лица, обращающегося за получением сертификата, и положительного результата проверки документов и сведений, Оператор УЦ осуществляет создание сертификата для соответствующего ранее зарегистрированного Пользователя УЦ с использованием одного из следующих способов:

на основании запроса на создание сертификата, сформированного и представленного заявителем в форме электронного документа (файла запроса на создание сертификата), подписанного усиленной квалифицированной электронной подписью заявителя или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре;

на основании запроса на создание сертификата, сформированного с использованием средств Удостоверяющего центра.

6.5.6.7. Процедура создания сертификата Пользователя УЦ на основании запроса на создание сертификата, сформированного и представленного заявителем.

6.5.6.7.1. При получении от заявителя запроса на создание сертификата Оператор УЦ осуществляет проверку:

сформированного заявителем запроса на создание сертификата на бумажном носителе, подписанного собственноручной подписью заявителя, либо запроса в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре;

владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата, в соответствии с пунктом 6.1.1 настоящего Порядка и в соответствии с пунктом 6.4 настоящего Порядка, если выполняется смена ключа электронной подписи владельца сертификата;

уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата, в реестре сертификатов Удостоверяющего центра.

6.5.6.7.2. В случае, если запрос на создание сертификата не представлен в форме документа бумажном носителе на бланке запроса на создание сертификата, подписанного

собственноручной подписью заявителя или его уполномоченного представителя, действующего по доверенности, либо в форме его копии в электронном виде, подписанной квалифицированной электронной подписью заявителя или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре, Оператор УЦ распечатывает в бумажном виде на бланке запроса на создание сертификата в двух экземплярах предварительно проверенный запрос на создание сертификата, представленный заявителем в виде электронного документа, и предоставляет его для ознакомления и подписания лицу, обратившемуся за получением сертификата. Один экземпляр бланка запроса на создание сертификата, подписанного заявителем или его уполномоченным представителем, действующего по доверенности, остается в Удостоверяющем центра, другой его экземпляр передается заявителю или его уполномоченному представителю.

6.5.6.7.3. Ознакомление под расписку лицом, обратившимся за получением сертификата, со сведениями, содержащимися в запросе на создание сертификата, и их соответствие со сведениями, содержащимися в заявлении на создание и выдачу сертификата и иных представленных заявителем документах, является одним из условий подтверждения владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата.

6.5.6.7.4. При положительных результатах проверки документов и сведений, представленных заявителем, если установлена личность заявителя – физического лица или получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением сертификата, а также если подтверждено владение заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата, и уникальность ключа проверки электронной подписи, указанного заявителем для получения сертификата, подтверждена, Оператор УЦ на основании запроса на создание сертификата, представленного заявителем в виде электронного документа, осуществляет создание сертификата Пользователя УЦ с использованием средств Удостоверяющего центра. В противном случае создание и выдача сертификата Пользователя УЦ не осуществляется и заявителю возвращаются представленные им документы с пояснением причин отказа. Удостоверяющий центр имеет право сохранить у себя копии документов, на основании которых было отказано заявителю в создании и выдаче сертификата.

6.5.6.8. Процедура создания сертификата Пользователя УЦ на основании запроса на создание сертификата, сформированного с использованием средств Удостоверяющего центра.

6.5.6.8.1. Создание сертификата Пользователя УЦ на основании запроса на создание сертификата, сформированного с использованием средств Удостоверяющего центра,

осуществляется Удостоверяющим центром только при личном прибытии заявителя либо его уполномоченного представителя в Удостоверяющий центр в случае получения Удостоверяющим центром положительных результатов проверки документов и сведений, представленных заявителем, если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем, установлена личность заявителя – физического лица или получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением сертификата. В противном случае создание и выдача сертификата Пользователя УЦ не осуществляется и заявителю возвращаются представленные им документы с пояснением причин отказа. Удостоверяющий центр имеет право сохранить у себя копии документов, на основании которых было отказано заявителю в создании и выдаче сертификата.

6.5.6.8.2. Для создания сертификата Пользователя УЦ Оператор УЦ осуществляет:

проверку работоспособности ключевого носителя, представленного заявителем, в том числе его проверку на наличие вредоносного программного обеспечения или посторонней информации и, при необходимости, выполняет его инициализацию (форматирование), если он не был ранее проинициализирован;

с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации, осуществляет создание ключа электронной подписи и ключа проверки электронной подписи Пользователя УЦ в соответствии с пунктом 6.1.2 настоящего Порядка и в соответствии пунктом 6.4 настоящего Порядка, если выполняется смена ключа электронной подписи владельца сертификата. При создании ключа электронной подписи и ключа проверки электронной подписи производится их запись непосредственно на ключевой носитель, представленный заявителем;

одновременно с созданием ключа электронной подписи и ключа проверки электронной подписи Оператор УЦ осуществляет формирование запроса на создание сертификата в форме электронного документа, проверяет уникальность созданного ключа проверки электронной подписи, распечатывает на бумажном носителе сформированный запрос на создание сертификата на соответствующем бланке в двух экземплярах и предоставляет его для ознакомления и подписания лицу, обратившемуся за получением сертификата. Один экземпляр бланка запроса на создание сертификата, подписанного заявителем или его уполномоченным представителем, действующего по доверенности, остается в Удостоверяющем центра, другой его экземпляр передается заявителю или его уполномоченному представителю;

на основании сформированного в виде электронного документа запроса на создание сертификата, осуществляет создание сертификата Пользователя УЦ с использованием средств

Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации.

6.5.6.8.3. Ознакомление под расписку лицом, обратившимся за получением сертификата, со сведениями, содержащимися в запросе на создание сертификата, и их соответствие со сведениями, содержащимися в заявлении на создание и выдачу сертификата и иных представленных заявителем документах, является одним из условий подтверждения владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата.

6.5.7. Порядок выдачи сертификата.

6.5.7.1. Выдача сертификата, созданного Удостоверяющим центром, осуществляется при личном прибытии заявителя либо его уполномоченного представителя в Удостоверяющий центр.

6.5.7.2. Допускается выдача сертификата без личного прибытия заявителя либо его уполномоченного представителя в Удостоверяющий центр, при одновременном соблюдении всех условий, указанных в пункте 6.5.6.3 настоящего Порядка, при этом создание и (или) смена ключа электронной подписи и ключа проверки электронной подписи осуществляется заявителем в соответствии с пунктами 6.1.1 и 6.4 настоящего Порядка.

Выдача сертификата без личного прибытия заявителя либо его уполномоченного представителя в Удостоверяющий центр осуществляется по указанным владельцем сертификата каналам связи, при этом:

информационное взаимодействие между Удостоверяющим центром и заявителем должно осуществляется способами, позволяющими обеспечить целостность информации и ее конфиденциальность, в случае передачи конфиденциальной информации;

ключ электронной подписи создается заявителем с использованием сертифицированных средств электронной подписи и не передается в Удостоверяющий центр;

документы и их копии в электронной форме, должны подписываться действующей усиленной квалифицированной электронной подписью уполномоченного лица Удостоверяющего центра или заявителя соответственно, или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре, и усиленной неквалифицированной подписью уполномоченного лица Удостоверяющего центра, проверку которой на стороне заявителя возможно осуществить аналогичным проверке усиленной неквалифицированной подписи заявителя образом;

документы, которые должны составляться исключительно на бумажном носителе, предоставляются посредством курьерской или почтовой связи.

6.5.7.3. Процедура выдачи сертификата, созданного Удостоверяющим центром.

После создания сертификата в соответствии с пунктом 6.5.6 настоящего Порядка, установления личности заявителя или его уполномоченного представителя, а также получения подтверждения их полномочий, с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации, Оператор УЦ:

1) обеспечивает ознакомление заявителя под расписку с информацией, содержащейся в сертификате, в следующем порядке:

распечатывает в двух экземплярах на бумажном носителе копию сертификата ключа проверки электронной подписи владельца сертификата, соответствующего электронной форме сертификата Пользователя УЦ (далее также – бланк сертификата), и заверяет его собственноручной подписью;

предоставляет на ознакомление и подпись заявителю или его уполномоченному представителю;

заявитель или его уполномоченный представитель проверяет соответствие сведений, содержащихся в распечатанном бланке сертификата Пользователя УЦ и, при успешной проверке сведений, заверяет его собственноручной подписью;

один экземпляр заверенного бланка сертификата передается владельцу сертификата или его уполномоченному представителю, другой экземпляр остается в Удостоверяющем центре;

2) в случае, если ключ электронной подписи создан с использованием средств Удостоверяющего центра:

предоставляет владельцу сертификата парольную информацию, необходимую для получения доступа к ключу электронной подписи, содержащемся на ключевом носителе, а также информирует его о необходимости обязательной смены пароля доступа к ключевой информации. По согласованию с владельцем сертификата осуществляет тестирование работоспособности контейнера ключа электронной подписи, содержащейся на ключевом носителе, смену пароля доступа к нему, либо предоставляет эту возможность владельцу сертификата;

передает владельцу сертификата или его уполномоченному представителя ключевой носитель, содержащий ключ электронной подписи и сертификат ключа проверки электронной подписи. Указанный ключевой носитель передается владельцу сертификата или его уполномоченному представителю под расписку и записью в соответствующих журналах поэкземплярного учета Удостоверяющего центра, в том числе журнале учета сертификатов ключей проверки электронной подписи. Удостоверяющий центр не осуществляет хранение ключа электронной подписи заявителя в Удостоверяющем центре или его копирование на иные ключевые носители, не принадлежащие заявителю;

3) по согласованию с владельцем сертификата осуществляет формирование ключевой фразы, которая в дальнейшем использоваться для аутентификации Пользователя УЦ при его обращении в Удостоверяющий центр;

4) выдает владельцу сертификата или его уполномоченному представителя сертификат, созданный Удостоверяющим центром в форме электронного документа, сертификат Удостоверяющего центра и сертификат головного удостоверяющего центра;

5) информирует под расписку владельца сертификата или его уполномоченного представителя в письменной форме 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, в соответствии с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенном в приложении № 10 настоящего Порядка;

6) распечатывает на бумажном носителе краткое руководство по обеспечению безопасности использования неквалифицированной электронной подписи и средств неквалифицированной электронной подписи и под расписку выдает его владельцу сертификата или его уполномоченному представителю.

Указанное руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенное в приложении № 10 настоящего Порядка, может быть направлено владельцу сертификата по электронной почте в форме электронного документа, при этом владелец сертификата подтверждает факт его получения, подписывая указанный электронный документ своей электронной подписью и направляя его в Удостоверяющий центр, либо направляя по электронной почте уведомление о прочтении, подписанное электронной подписью владельца сертификата. Получение Удостоверяющим центром указанного уведомления о прочтении является фактом, подтверждающим получение указанного электронного документа владельцем сертификата;

7) по согласованию с владельцем сертификата или его уполномоченным представителем направляет владельцу сертификата или записывает на носитель информации, предоставленный заявителем, документацию в форме электронных документов, в том числе содержащую:

руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенное в приложении № 10 настоящего Порядка, содержащее информацию о 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;

инструкцию по использованию средства электронной подписи, входящую в состав эксплуатационной документации на средство электронной подписи (по желанию владельца сертификата и при наличии в Удостоверяющем центре документации на средство электронной подписи, которое использует владелец сертификата);

8) вносит в реестр сертификатов Удостоверяющего центра информацию о выданном сертификате и сведения о владельце сертификата.

6.5.8. Срок создания и выдачи Удостоверяющим центром сертификата заявителя.

6.5.8.1. Срок создания и выдачи Удостоверяющим центром сертификата заявителя с момента получения Удостоверяющим центром заявления на создание и выдачу сертификата, а также надлежаще оформленных документов и сведений, представленных заявителем в Удостоверяющий центр для получения сертификата, не может превышать 30 (тридцати) дней со дня получения Удостоверяющим центром заявления на создание и выдачу сертификата, если иное не определено договором оказания услуг или дополнительным соглашением, заключаемым с заявителем.

6.5.8.2. В случае, если заявитель, после получения от Удостоверяющего центра уведомления о необходимости предоставления документов либо их надлежащим образом заверенные копий и сведений, необходимых для создания и выдачи сертификата, не представил их, Удостоверяющий центр по истечении 30 (тридцати) дней со дня получения Удостоверяющим центром соответствующего заявления на создание и выдачу сертификата отказывает в создании и выдаче сертификата и направляет соответствующее уведомление заявителю.

6.5.8.3. Выдача сертификатов, созданных Удостоверяющим центром, осуществляется при условии выполнения Стороной, присоединившейся к Порядку, своих обязанностей.

6.5.8.4. Удостоверяющий центр не оказывает услуг по срочному выпуску сертификата, создание и выдача сертификата осуществляется в соответствии с требованиями Федерального закона «Об электронной подписи» и условиями, определенными настоящим Порядком.

6.6. Процедуры, осуществляемые при прекращении действия и аннулировании сертификата.

6.6.1. Основания прекращения действия или аннулирования сертификата.

6.6.1.1. Сертификат прекращения свое действие:

в связи с истечением установленного срока действия сертификата;

на основании заявления владельца сертификата, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

в случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам;

в иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными

правовыми актами, настоящим Порядком или соглашением (договором оказания услуг Удостоверяющего центра) с владельцем сертификата.

6.6.1.2. Удостоверяющий центр признает сертификат аннулированным, если в следующих случаях:

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

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

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

6.6.2. Порядок действий Удостоверяющего центра при прекращении действия (аннулировании) сертификата.

6.6.2.1. Порядок подачи и приема заявления о прекращении действия сертификата

6.6.2.1.1. Порядок подачи в Удостоверяющий центр заявления о прекращении действия сертификата.

6.6.2.1.1.1. Заявитель имеет право предоставить в Удостоверяющий центр заявление о прекращении действия сертификата как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца сертификата или усиленной неквалифицированной подписью заявителя, сертификат ключа проверки которой был получен ранее в Удостоверяющем центре.

6.6.2.1.1.2. Заявление о прекращении действия сертификата направляется заявителем в Удостоверяющий центр в случае:

принятия Стороной, присоединившейся к Порядку, решения о прекращении действия сертификата владельца сертификата;

договорные отношения, определенные настоящим Порядком, прекращаются по инициативе Стороны, присоединившейся к Порядку, в соответствии с пунктом 2.1.7 настоящего Порядка;

изменились сведения о владельце сертификата, в результате которых сведения, внесенные в сертификат, перестали быть достоверными;

прекращения полномочий владельца сертификата;

нарушена конфиденциальность ключа электронной подписи владельца сертификата.

6.6.2.1.1.3. Требования к заявлению о прекращении действия сертификата.

Заявление о прекращении действия сертификата оформляется по форме, приведенной в приложении № 8 или приложения № 9 к настоящему Порядку, и должно соответствовать следующим требованиям:

1) В случае, если заявителем является юридическое лицо, заявление должно быть оформлено на бланке организации (при наличии) и заверено печатью юридического лица, а также содержать:

сведения о сертификате, действие которого прекращается;

реквизиты (дата и номер письма);

собственноручную подпись владельца сертификата.

2) В случае, если заявителем является физическое лицо, заявление должно содержать:

сведения о сертификате, действие которого прекращается;

собственноручную подпись физического лица, являющегося владельцем сертификата, и дату подписания заявления.

6.6.2.1.2. Порядок приема Удостоверяющим центром заявления о прекращении действия сертификата.

6.6.2.1.2.1. После поступления заявления о прекращении действия сертификата и его регистрации в Удостоверяющем центре осуществляется:

проверка заявления на соответствие требованиям, указанным в пункте 6.6.2.1.1.3 настоящего Порядка;

проверка соответствия сведений, указанных в заявлении, и сведений, которые имеются в Удостоверяющем центре о владельце сертификата и выданном ему сертификате;

проверка полномочий владельца сертификата и (или) лица, обратившегося с заявлением о прекращении действия сертификата.

6.6.2.1.2.2. Проверка полномочий владельца сертификата и (или) лица, обратившегося с заявлением о прекращении действия сертификата, и удостоверение его личности и осуществляются в порядке, предусмотренном для процедуры создания и выдачи сертификата, приведенной в пункте 6.5 настоящего Порядка, с соблюдением следующих условий:

1) с заявлением о прекращении действия сертификата, владельцем которого является физическое лицо, имеет право обращаться указанное физическое лицо, либо лицо, действующее от имени владельца сертификата на основании нотариальной доверенности на совершение действий, связанных с прекращением действия сертификата владельца сертификата.

Полномочия вышеуказанного лица подтверждаются на основании основного документа, удостоверяющего личность, или его нотариально заверенной копии, либо заверенной в Удостоверяющем центре при предоставлении основного документа, удостоверяющего личность;

2) с заявлением о прекращении действия сертификата, владельцем которого является юридическое лицо или уполномоченный представитель юридического лица, имеет право обращаться физическое лицо, имеющее право действовать от имени этого юридического лица

без доверенности, либо уполномоченный представитель юридического лица, действующий на основании доверенности или распорядительного акта юридического лица, подписанного руководителем юридического лица.

Полномочия физического лица, имеющего право действовать от имени этого юридического лица без доверенности, подтверждаются Удостоверяющим центром с использованием актуальных сведений, полученных Удостоверяющим центром из государственных информационных ресурсов. Полномочия физического лица, действующего на основании доверенности или распорядительного акта юридического лица, подтверждаются при предоставлении вышеуказанных документов либо их надлежаще заверенных копий, а также при предоставлении основного документа, удостоверяющего личность, либо его надлежаще заверенной копии.

6.6.2.1.2.3. В случае, если заявление не соответствует условиям и требованиям в соответствии с пунктом 6.6.2.1 настоящего Порядка, в том числе в случае, если сертификат, сведения о котором указаны в заявлении о прекращении действия сертификата, не выдавался Удостоверяющим центром, либо сведения, указанные в заявлении, не соответствуют сведениям о владельце сертификата, либо не подтверждены полномочия владельца сертификата и (или) лица, обратившегося с заявлением о прекращении действия сертификата, Удостоверяющий центр отказывает в проведении процедуры прекращения действия сертификата и направляет соответствующее уведомление заявителю в течение 1 (одного) рабочего дня со дня получения сведений из государственных информационных ресурсов, в случае, если полномочия лица, обращающегося для прекращения действия сертификата, не подтверждены, но не позднее 3 (трех) рабочих дней со дня получения заявления о прекращении действия сертификата.

6.6.2.2. Порядок внесения информации о прекращении действия или аннулировании сертификата в реестр сертификатов.

6.6.2.2.1. После проверки заявления и полномочий владельца сертификата и (или) лица, обратившегося для прекращения действия сертификата, Удостоверяющий центр:

выполняет процедуру прекращения действия сертификата;

направляет в форме электронного документа соответствующее уведомление владельцу сертификата;

вносит информацию о прекращении действия сертификата в реестр сертификатов Удостоверяющего центра.

6.6.2.2.2. Информация о прекращении действия и аннулировании сертификата вносится Удостоверяющим центром в реестр сертификатов Удостоверяющего центра в течение 12 (двенадцати) часов с момента наступления обстоятельств, указанных в пункте 6.6.1 настоящего Порядка, или в течение 12 (двенадцати) часов с момента, когда Удостоверяющему

центру стало известно или должно было стать известно о наступлении таких обстоятельств.

6.6.2.2.3. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов Удостоверяющего центра.

6.6.2.2.4. Информация о прекращении действия и аннулировании сертификатов в течение 1 (одного) рабочего дня включается Удостоверяющим центром в список отозванных сертификатов, который подписывается электронной подписью, основанной на сертификате Удостоверяющего центра, и публикуется на сайте Удостоверяющего центра. Период публикации списка отозванных сертификатов составляет 24 (двадцать четыре) часа.

6.6.2.2.5. Информация о адресах публикации списка отозванных сертификатов указывается в сертификатах, созданных Удостоверяющим центром, и включается в расширение «Точка распределения списка отзыва» («CRL Distribution Point») сертификата.

6.6.2.2.6. Оповещение участников электронного взаимодействия о факте прекращения действия сертификата осуществляется Удостоверяющим центром путем опубликования первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения о сертификате, который аннулирован или действие которого прекращено, и изданного не ранее времени наступления произошедшего случая. Временем оповещения о прекращении действия сертификата является время издания указанного списка отозванных сертификатов, хранящееся в поле «Действителен с» («thisUpdate») списка отозванных сертификатов.

6.6.2.2.7. В случае прекращения действия сертификата по истечению срока его действия временем прекращения действия сертификата является время, хранящееся в поле «Действителен по» («NotAfter») сертификата. В этом случае информация о сертификате, действие которого прекращено, в список отозванных сертификатов не заносится.

6.6.2.2.8. В случае внеплановой смены ключа электронной подписи Удостоверяющего центра в связи с нарушением его конфиденциальности временем прекращения действия сертификата Удостоверяющего центра является время нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, при этом прекращение действия сертификата Удостоверяющего центра осуществляется уполномоченным федеральным органом. Информация о прекращении действия сертификата Удостоверяющего центра включается в список отозванных сертификатов, который публикуется головным удостоверяющим центром.

6.6.2.3. В случае аннулирования в соответствии с пунктом 6.6.1.2 настоящего Порядка сертификата, выданного Удостоверяющим центром, Удостоверяющий центр уведомляет владельца сертификата не менее чем за 1 (один) рабочий день до внесения в реестр сертификатов Удостоверяющего центра информации об аннулировании сертификата путем направления документа на бумажном носителе или электронного документа, подписанного усиленной квалифицированной подписью уполномоченного лица Удостоверяющего центра.

Использование аннулированного сертификата ключа проверки электронной подписи не влечет юридических последствий, за исключением тех, которые связаны с его аннулированием.

6.7. Порядок ведения реестра сертификатов Удостоверяющего центра.

6.7.1. Формирование и ведение реестра сертификатов Удостоверяющего центра.

6.7.1.1. Формирование и ведение реестра сертификатов осуществляется Удостоверяющим центром в соответствии с Федеральным законом «Об электронной подписи», иными принимаемыми в соответствии с Федеральным законом «Об электронной подписи» и Федеральным законом «Об информации, информационных технологиях и о защите информации» нормативными правовыми актами и настоящим Порядком.

6.7.1.2. Формирование реестра сертификатов включает в себя внесение сертификатов, выданных Удостоверяющим центром, в реестр сертификатов.

6.7.1.3. 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.

6.7.1.4. Хранение информации, содержащейся в реестре сертификатов, осуществляется Удостоверяющим центром в форме, позволяющей проверить ее целостность и достоверность.

6.7.1.5. Удостоверяющий центр обеспечивает защиту информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

6.7.1.6. Формирование и ведение реестра сертификатов осуществляется Удостоверяющим центром с соблюдением требований к мерам и способам защиты информации, обеспечивающих предотвращение несанкционированного доступа к нему.

6.7.1.7. В целях обеспечения целостности информации, в том числе предотвращения утраты сведений о сертификатах, содержащихся в реестре сертификатов, Удостоверяющий центр осуществляет резервной копирование баз данных, обрабатываемых с использованием сертифицированных средств Удостоверяющего центра, а также реестра сертификатов.

6.7.1.8. Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов.

6.7.1.9. Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, к реестру сертификатов в любое время в течение срока деятельности Удостоверяющего центра.

6.7.1.10. Удостоверяющий центр предоставляет безвозмездно любому лицу по его обращению сведения, содержащиеся в реестре сертификатов, в том числе информацию об

аннулировании сертификата. Указанная информация предоставляется в форме выписки из реестра сертификатов и направляется обратившемуся лицу как в форме документа на бумажном носителе с использованием почтового отправления, так и с в форме электронного документа использованием информационно-телекоммуникационных сетей, в том числе с использованием электронной почты (по выбору лица, обратившегося за получением информации из реестра сертификатов).

Срок предоставления Удостоверяющим центром запрошенной заявителем информации, содержащейся в реестре сертификатов, не превышает 7 (семи) дней со дня получения запроса от заявителя, в случае, если Удостоверяющий центр направляет запрошенную информацию в форме документа на бумажном носителе с использованием почтового отправления, и 24 (двадцати четырех) часов для направления выписки посредством информационно-телекоммуникационных сетей, в том числе с использованием электронной почты.

6.7.1.11. В процессе реализации функций Удостоверяющего центра и исполнения обязанностей Удостоверяющий центр осуществляет также формирование и ведение:

1) реестра Пользователей УЦ, который в том числе содержит:

информацию о Пользователях УЦ, владельцах сертификатов, выданных им сертификатах, в том числе прекративших действие и аннулированных сертификатах;

реестр списка отозванных сертификатов в электронном виде за все время деятельности Удостоверяющего центра.

Реестр Пользователей УЦ ведется в электронном виде с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации;

2) журнала учета сертификатов ключей проверки электронной подписи, соответствующего форме журнала поэкземплярного учета, приведенной в приложении № 1 Инструкции ФАПСИ № 152, в том числе содержащего информацию о серийном номере сертификата, выдаче сертификата, прекращении его действия, основания выдачи или прекращении его действия, о лице, получившем и выдавшем сертификат. Журнал учета сертификатов ключей проверки электронной подписи может вестись как в электронном, так и бумажном виде.

6.7.1.12. Информация, внесенная в реестр сертификатов, подлежит хранению в течение всего срока деятельности Удостоверяющего центра.

6.7.1.13. В случае принятия решения о прекращении своей деятельности Удостоверяющий центр обязан передать реестр сертификатов лицу, к которому перешли функции удостоверяющего центра.

6.7.2. Формы ведения реестра сертификатов.

6.7.2.1. Реестр сертификатов Удостоверяющего центра включает реестр сертификатов юридических лиц и реестр сертификатов физических лиц.

6.7.2.2. Реестр сертификатов юридических лиц состоит из следующих разделов:

сертификаты, выданные юридическим лицам;

сертификаты, выданные юридическим лицам, прекратившие свое действие;

аннулированные сертификаты, выданные юридическим лицам.

6.7.2.2.1. Раздел «сертификаты, выданные юридическим лицам» содержит следующие обязательные поля:

1) уникальный номер сертификата;

2) даты начала и окончания действия сертификата;

3) наименование и место нахождения;

4) ограничения использования сертификата (если такие ограничения устанавливаются).

6.7.2.2.2. Раздел «сертификаты, выданные юридическим лицам, прекратившие свое действие» содержит следующие обязательные поля:

1) уникальный номер сертификата;

2) даты начала и окончания действия сертификата;

3) наименование и место нахождения;

4) дата прекращения действия сертификата;

5) основание прекращения действия сертификата.

6.7.2.2.3. Раздел «аннулированные сертификаты, выданные юридическим лицам» содержит следующие обязательные поля:

1) уникальный номер сертификата;

2) даты начала и окончания действия сертификата;

3) наименование и место нахождения;

4) дата аннулирования сертификата;

5) основание аннулирования сертификата.

6.7.2.3. Реестр сертификатов физических лиц состоит из следующих разделов:

сертификаты, выданные физическим лицам;

сертификаты, выданные физическим лицам, прекратившие свое действие;

аннулированные сертификаты, выданные физическим лицам.

6.7.2.3.1. Раздел «сертификаты, выданные физическим лицам» содержит следующие обязательные поля:

1) уникальный номер сертификата;

2) даты начала и окончания действия сертификата;

3) фамилия, имя и отчество (если имеется) владельца сертификата;

4) ограничения использования сертификата (если такие ограничения устанавливаются).

6.7.2.3.2. Раздел «сертификаты, выданные физическим лицам, прекратившие свое действие» содержит следующие обязательные поля:

1) уникальный номер сертификата;

2) даты начала и окончания действия сертификата;

3) фамилия, имя и отчество (если имеется) владельца сертификата;

4) дата прекращения действия сертификата;

5) основание прекращения действия сертификата.

6.7.2.3.3. Раздел «аннулированные сертификаты, выданные физическим лицам» содержит следующие обязательные поля:

1) уникальный номер сертификата;

2) даты начала и окончания действия сертификата;

3) фамилия, имя и отчество (если имеется) владельца сертификата;

4) дата аннулирования сертификата;

5) основание аннулирования сертификата.

6.7.3. Сроки внесения информации о прекращении действия или аннулировании сертификата в реестр сертификатов.

6.7.3.1. Информация о выданных Удостоверяющим центром сертификатах вносится в реестр сертификатов одновременно с их выдачей, но не позднее не позднее даты начала действия сертификата, указанной в сертификате.

6.7.3.2. Информация о прекращении действия и аннулировании сертификата вносится Удостоверяющим центром в реестр сертификатов Удостоверяющего центра в течение 12 (двенадцати) часов с момента наступления обстоятельств, указанных в пункте 6.6.1 настоящего Порядка, или в течение 12 (двенадцати) часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

6.7.3.3. Информация об аннулировании сертификата вносится Удостоверяющим центров в реестр сертификатов не позднее 1 (одного) рабочего дня со дня вступления в законную силу решения суда, явившегося основанием для аннулирования, а также при аннулировании Удостоверяющим центром сертификатов по основаниям, указанным в пунктах 1 и 2 части 6.1 статьи 14 Федерального закона «Об электронной подписи»:

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

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

6.7.3.4. В случае аннулирования в соответствии с пунктом 6.6.1.2 настоящего Порядка сертификата, выданного Удостоверяющим центром, Удостоверяющий центр уведомляет

владельца сертификата не менее чем за 1 (один) рабочий день до внесения в реестр сертификатов Удостоверяющего центра информации об аннулировании сертификата путем направления документа на бумажном носителе или электронного документа, подписанного усиленной квалифицированной подписью уполномоченного лица Удостоверяющего центра.

6.8. Обеспечение доступа к реестру сертификатов

6.8.1. Доступ к реестру сертификатов предоставляется по индивидуальному запросу, направленному на адрес ca@tcinet.ru.

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.

7.1.1. Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, содержащее информацию об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, приведено в приложении № 10 к настоящему Порядку.

7.1.2. Удостоверяющий центр осуществляет информирование Стороны, присоединившейся к Порядку, в том числе владельцев сертификатов, 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 следующими способами:

1) Удостоверяющий центр информирует всех участников электронного взаимодействия 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 путем размещения настоящего Порядка, а также руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи, которое приведено в приложении № 10 к настоящему Порядку, отдельным документом в электронной форме на сайте Удостоверяющего центра;

2) Сторона, присоединившаяся к Порядку, обязана ознакомиться с настоящим Порядком и всеми приложениями к нему, в том числе с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, о чем

подтверждает путем подписания Заявления по форме, приведенной в приложении № 1 или приложении № 2 к настоящему Порядку;

3) заявитель, при оформлении Заявления по форме, приведенной в приложении № 1 или приложении № 2 к настоящему Порядку предоставляет также согласие на обработку персональных данных, которое собственноручно подписывает лицо, указанное в заявлении на создается создание и выдачу сертификата, и, в том числе, подтверждает, что с настоящим Порядком и всеми приложениями к нему, в том числе с Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, ознакомлен;

4) Удостоверяющий центр оказывает техническую поддержку Пользователей УЦ и осуществляет предоставление консультаций по вопросам использования электронной подписи и средств электронной подписи, в том числе по вопросам обеспечения безопасности при использовании электронной подписи и средств электронной подписи.

7.2. Выдача по обращению заявителя средств электронной подписи.

7.2.1. Средства электронной подписи, используемые заявителем, должны соответствовать требованиям частью 4 статьи 6 и статьи 12 Федерального закона «Об электронной подписи», Требованиями к средствам электронной подписи, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796.

7.2.2. Выдача Удостоверяющим центром сертифицированных по требованиям безопасности средств электронной подписи заключается в:

консультировании Пользователей УЦ по вопросам получения по доверенным каналам распространения от производителей данных средств, обеспечивающих возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

выдаче средств электронной подписи, содержащих ключ электронной подписи и ключ проверки электронной подписи;

выдаче лицензий на право использования средств электронной подписи на возмездной основе.

7.2.3. Выдача и распространение сертифицированных средств электронной подписи и эксплуатационной документации к ним осуществляется Удостоверяющим центром на основании положений, приведенных в пункте 2.2.1 настоящего Порядка, в соответствии с требованиями Инструкция ФАПСИ № 152. Факт выдачи заявителям сертифицированных средств электронной подписи и эксплуатационной документации к ним учитывается в соответствующих журналах поэкземплярного учета Удостоверяющего центра.

7.2.4. Если лицензионным соглашением, условия которой определил правообладатель (производитель) средства электронной подписи, правообладателем предоставлена возможность бесплатного использования средства электронной подписи без необходимости

приобретения права использования продукта на условиях простой (неисключительной) лицензии, либо использования без установки ключа (лицензионного номера), либо предоставлена возможность его использования в рамках ограниченного периода времени в целях демонстрации программного продукта и ознакомления пользователя с его возможностями, Удостоверяющий центр имеет право, в рамках лицензионного соглашения, безвозмездно передать заявителю средство электронной подписи, которое есть в наличии в Удостоверяющем центре, и которое соответствует требованиям, указанным в пункте 7.2.1 настоящего Порядка, либо предоставить заявителю информацию о сайте правообладателя (производителя) в сети Интернет, в том числе информацию, содержащую условия лицензионного соглашения и информацию (при её наличии) о возможности ознакомления с программным продуктом, соответствующим требованиям к сертифицированным средствам электронной подписи.

7.2.5. Порядок использования средств электронной подписи определяются эксплуатационной документацией на средство электронной подписи и лицензионным соглашением, условия которой определяет правообладатель.

7.3. Обеспечение актуальности информации, содержащейся в реестре сертификатов, а также ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

7.3.1. Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов, а также защиту информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности

7.3.2. Актуальность информации, содержащейся в реестре сертификатов, обеспечивается путем соблюдения порядка формирования и ведения реестра сертификатов в соответствии с пунктом 6.6 настоящего Порядка.

7.3.3. Защита информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается путем реализации комплекса организационных и технических мер по обеспечению информационной безопасности инфраструктуры Удостоверяющего центра, обеспечению защиты информации, обрабатываемой с использованием средств Удостоверяющего центра, которые в том числе включают меры по защите информации, содержащейся в реестре сертификатов.

7.3.4. Мероприятия по обеспечению защиты информации, при её обработке с использованием средств Удостоверяющего центра, осуществляются в соответствии требованиями норм действующего законодательства.

7.4. Обеспечение доступности реестра сертификатов в информационно-телекоммуникационной сети «Интернет».

7.4.1. Удостоверяющий центр в соответствии с пунктом 3 части 2 статьи 13 и частью 3 статьи 15 Федерального закона «Об электронной подписи» обеспечивает безвозмездный круглосуточный доступ к реестру сертификатов, опубликованному на сайте Удостоверяющего центра, при обращении к нему любого лица с использованием сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра сертификатов, проводимых Удостоверяющим центром в соответствии с пунктом 6.8 настоящего Порядка.

7.4.2. Удостоверяющий центр обеспечивает доступность и целостность информации, опубликованной на сайте Удостоверяющего центра, в том числе реестра сертификатов, сертификатов Удостоверяющего центра, списка отозванных сертификатов.

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

7.5.1. Порядок обеспечения конфиденциальности ключей электронных подписей уполномоченных лиц Удостоверяющего центра и ключа электронной подписи Удостоверяющего центра.

7.5.1.1. Конфиденциальность ключей электронных подписей уполномоченных лиц Удостоверяющего центра, а также ключа электронной подписи Удостоверяющего центра, обеспечивается путем реализации комплекса организационных и технических мер по обеспечению информационной безопасности инфраструктуры Удостоверяющего центра, обеспечению защиты информации, обрабатываемой с использованием средств Удостоверяющего центра.

7.5.1.2. Хранение и использование ключей электронной подписи Удостоверяющего центра и ключей электронной подписи уполномоченных лиц Удостоверяющего центра осуществляется в соответствии с требованиями с Инструкции ФАПСИ № 152, Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 02 марта 2001 г. № 28, в форме, позволяющей обеспечить целостность и конфиденциальность ключей электронной подписи Удостоверяющего центра.

7.5.1.3. Средства Удостоверяющего центра, с использованием которых осуществляется использование и хранение ключей электронной подписи Удостоверяющего центра и ключей электронной подписи уполномоченных лиц Удостоверяющего центра, имеют документ, подтверждающий оценку соответствия по требованиям безопасности информации и соответствуют Требованиям к средствам электронной подписи и Требованиями к средствам удостоверяющего центра, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796.

7.5.1.4. Ключи электронной подписи Удостоверяющего центра и уполномоченных лиц Удостоверяющего центра выводятся из эксплуатации при окончании срока их действия. Временное их хранение не осуществляется.

7.5.2. Порядок обеспечения конфиденциальности ключей электронных подписей заявителей.

7.5.2.1. Конфиденциальность ключей электронных подписей заявителей обеспечивается Удостоверяющим центром в период времени получения носителя ключевой информации от заявителя или его уполномоченного представителя и записи на него ключей электронной подписи, созданных Удостоверяющим центром, до момента передачи ключевого носителя заявителю или его уполномоченному представителю, при этом создание и запись ключа электронной подписи на ключевой носитель, представленный заявителем или его уполномоченным представителем осуществляется Удостоверяющим центром только в случае личного прибытия заявителя или его уполномоченного представителя в Удостоверяющий центр и в его присутствии.

7.5.2.2. После создания Удостоверяющим центром ключа электронных подписи заявителя и его записи на носитель ключевой информации, представленный непосредственно перед созданием ключа электронных подписи заявителем или его уполномоченным представителем, данный носитель ключевой информации, в том числе содержащий ключ электронной подписи, указанный ключевой носитель выдается заявителю или его уполномоченному представителю под расписку, при этом вносится запись в соответствующий журнал учета Удостоверяющего центра о выдаче ключа электронной подписи и соответствующего ему сертификата, с которой заявитель или его уполномоченный представитель должен быть ознакомлен под расписку.

7.5.2.3. Создание ключей электронной подписи заявителя осуществляется с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации.

7.5.2.4. Удостоверяющий центр не осуществляет хранение (в том числе временное хранение) ключей электронной подписи, а также носителей ключевой информации, содержащих ключи электронной подписи заявителя (владельца сертификата).

7.5.2.5. В случае, если заявитель направил в Удостоверяющий в электронном виде ключ электронной подписи по информационно-телекоммуникационной сети или иными способами, не гарантирующими обеспечение конфиденциальности ключа электронной подписи, такой ключ считается скомпрометированным в связи нарушением конфиденциальность ключа электронной подписи, при этом заявитель обязан провести процедуру его внеплановой смены. В случае наличия действующего сертификата, соответствующего указанному ключу электронной подписи, такой сертификат прекращает

действие, при этом владелец сертификата обязан обратится в Удостоверяющий центр с заявлением о прекращении его действия.

7.5.2.6. Владелец сертификата, получивший сертификат в Удостоверяющем центре обеспечивает конфиденциальность ключей электронных подписей и обязан:

хранить в тайне ключ электронной подписи, принимать все возможные меры для предотвращения его утраты, раскрытия, искажения и несанкционированного использования;

не допускать использование принадлежащих ему ключей электронных подписей без своего согласия;

уведомлять Удостоверяющий центр и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

не использовать ключ электронной подписи, если ему стало известно, что этот ключ используется или использовался ранее другими лицами;

не использовать ключ электронной подписи и немедленно обратиться в Удостоверяющий центр, выдавший сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена.

7.6. Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре сертификатов.

7.6.1. Удостоверяющий центр предоставляет безвозмездно любому лицу доступ к информации, содержащейся в реестре сертификатов Удостоверяющего центра, включая информацию о прекращении действия сертификата или об аннулировании сертификата путем публикации реестра сертификатов на сайте Удостоверяющего центра в форме электронного документа, который доступен для загрузки с использованием сети Интернет.

7.6.2. Актуальность и доступность реестра сертификатов, опубликованного на сайте Удостоверяющего центра в сети Интернет обеспечивается Удостоверяющим центром в соответствии с пунктом 7.3 и 7.2 настоящего Порядка соответственно.

7.6.3. Удостоверяющий центр предоставляет безвозмездно любому лицу по его обращению сведения, содержащиеся в реестре сертификатов, в том числе информацию об аннулировании сертификата. Указанная информация предоставляется в форме выписки из реестра сертификатов в соответствии с пунктом 6.7.1.10 настоящего Порядка.

7.6.4. Удостоверяющий центр предоставляет безвозмездно любому лицу доступ к информации о прекращении действия сертификата или об аннулировании сертификата, путем публикации актуального перечня прекративших свое действие (аннулированных) сертификатов в виде электронного документа (списка отозванных сертификатов),

включающий в себя список серийных номеров сертификатов, которые аннулированы или действие которых было прекращено.

7.6.5. Адреса публикации списка отозванных сертификатов Удостоверяющего центра указывается в сертификатах, созданных Удостоверяющим центром.

7.6.6. Внесение информации о прекращении действия или аннулировании сертификата в реестр сертификатов осуществляется Удостоверяющим центром в соответствии с пунктом 6.6.2.2 настоящего Порядка.

8. Прочие положения

8.1. Прекращение деятельности Удостоверяющего центра.

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

В случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты прекращения деятельности этого удостоверяющего центра. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть уничтожена. В случае прекращения деятельности удостоверяющего центра с переходом его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть передана лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность.

8.2. Политика конфиденциальности.

8.2.1. Типы конфиденциальной информации.

К конфиденциальной информации, обрабатываемой в Удостоверяющем центре, относится:

1) информация, обрабатываемая с использованием средств Удостоверяющего центра:

ключи электронной подписи Удостоверяющего центра и ключи электронной подписи уполномоченных лиц Удостоверяющего центра;

сведения о мерах и способах защиты инфраструктуры Удостоверяющего центра, включая идентифицирующую и аутентифицирующую информацию, информацию о среде

функционирования технических и программных средств Удостоверяющего центра, средств защиты информации и шифровальных (криптографических) средств;

техническая и эксплуатационная документация Удостоверяющего центра, в том числе содержащая информация о настройках средств Удостоверяющего центра, средств защиты информации, средств межсетевого экранирования, средств криптографической защиты информации;

2) информация, содержащая персональные данные, за исключением:

сведений, включаемых в сертификат, выданный Удостоверяющим центром;

информации, содержащейся в реестре сертификатов;

общедоступной информации и информации, включенной в общедоступные источники персональных данных.

3) ключ электронной подписи является конфиденциальной информацией лица, являющегося владельцем соответствующего сертификата, выданного ему Удостоверяющим центром. Удостоверяющий центр не осуществляет хранение ключей электронных подписей владельцев сертификатов, в том числе их временное хранение. Ключи электронной подписи, создаваемые Удостоверяющим центром при личном присутствии заявителя или его уполномоченного представителя, непосредственно сразу после их изготовления передаются лично заявители или его уполномоченному представителю под расписку.

8.2.2. Типы информации, не являющейся конфиденциальной.

Удостоверяющий центр осуществляет обработку следующей информации, которая не является конфиденциальной:

1) информация, подлежащая в соответствии с законодательством Российской Федерации размещению в сети Интернет, доступ к которой не ограничен, в том числе информация, являющаяся общедоступной информацией в соответствии со статьей 7 Федерального закона «Об информации, информационных технологиях и о защите информации» или информация, включенная в общедоступные источники персональных данных в соответствии со статьей 8 Федерального закона «О персональных данных», а также информация, с письменного согласия субъекта персональных данных, включенная в общедоступные источники персональных данных;

2) информация, включаемая в сертификаты, выдаваемые Удостоверяющим центром, информация, содержащейся в реестре сертификатов, а также информация, включаемая в списки отозванных сертификатов Удостоверяющего центра;

3) информация, содержащаяся в настоящем Порядке.

8.2.3. Типы информации, не подлежащей публикации.

Не подлежит публикации следующая информация о заявителях и владельцах сертификатов:

1) сведения, содержащиеся в договорах на оказание услуг, заключаемых заявителем с Удостоверяющим центром, заявлениях, доверенностях, согласии на обработку персональных данных и иных документах, предоставляемых заявителем в Удостоверяющий центр, за исключением информации не являющейся конфиденциальной, указанной в пункте 8.2.2 настоящего Порядка.

8.2.4. Обеспечение конфиденциальности.

Сведения, относящиеся к конфиденциальной информации в соответствии с действующим законодательством Российской Федерации и настоящим Порядком, полученные Удостоверяющим центром или Стороной, присоединившейся к Порядку, в целях оказания или получения услуг в соответствии с настоящим Порядком, не подлежат разглашению, распространению и передаче третьим лицам, если иное не оговорено особо, а также в случаях, предусмотренных законодательством Российской Федерации, настоящим Порядком, договором оказания услуг Удостоверяющего центра или соглашением Сторон.

9. Приложения

Приложение № 1

к Порядку реализации функций удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет»

(Форма заявления на создание и выдачу сертификата ключа проверки электронной подписи **для юридических лиц**) [1]

Общество с ограниченной ответственностью
«Технический центр Интернет»

_____ № _____

_____

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

в лице _____,

(должность, фамилия, имя, отчество)

действующего на основании _____,

в соответствии со статьей 428 Гражданского кодекса Российской Федерации полностью и безусловно присоединяется к Порядку реализации функций Удостоверяющего центра и исполнения его обязанностей (далее – Порядок), опубликованному на сайте Удостоверяющего центра ООО «ТЦИ» в информационно-телекоммуникационной сети «Интернет» по адресу https://ca.tcinet.ru, гарантирует, что

уполномоченные лица _____,

(сокращенное наименование организации)

регистрирующиеся в Удостоверяющем центре ООО «ТЦИ», с Порядком и приложениями к нему, в том числе с руководством по обеспечению безопасности использования электронной

[1] Заявление подается в Удостоверяющий центр в двух экземплярах. После регистрации Заявления в Удостоверяющем центре один экземпляр предоставляется заявителю

подписи и средств электронной подписи, ознакомлены и обязуются соблюдать все его положения,

просит создать и выдать своему уполномоченному представителю сертификат ключа проверки электронной подписи, содержащий следующую информацию:

Наименование юридического лица[1]	
Наименование населенного пункта	
Название улицы, номер дома	
Область	
Страна	
Фамилия	
Имя Отчество	
Адрес электронной почты	
Ключ электронной подписи и ключ проверки электронной подписи	□ *Создать с использованием средств Удостоверяющего центра* □ *Создан с использованием средств электронной подписи заявителя.*

Приложение: Согласие лица, на имя которого создается сертификат, на обработку персональных данных[2];

Запрос на создание сертификата в электронном и (или) бумажном виде[3]

_____ _____ / _____ /

(должность) (подпись и Ф.И.О.)

М.П.

(заполняется уполномоченным лицом Удостоверяющего центра)

Заявление зарегистрировано в реестре Удостоверяющего центра, подтверждает присоединение

_____,

(сокращенное наименование организации)

---

[1] Рекомендуется указывать сокращенное наименование юридического лица (если имеется).

[2] Не предоставляется в случае, если данное согласие ранее предоставлялось, либо если создается сертификат, используемый для автоматического подписания электронной подписью в информационной системе.

[3] Предоставляется в случае самостоятельного создания заявителем ключа электронной подписи и ключа проверки электронной подписи с использованием средств электронной подписи заявителя.

к Порядку реализации функций удостоверяющего центра и исполнения его обязанностей.

Регистрационный № _____ от «_____» _____ 20___ г.

Уполномоченное лицо Удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет» _____ / _____ /

(подпись) (расшифровка подписи)

М.П.

Приложение
к заявлению на создание и выдачу сертификата ключа проверки
электронной подписи **для юридических лиц**
(Форма согласия на обработку персональных данных)

_____

(Фамилия, Имя, Отчество лица, на имя которого изготавливается сертификат, серия и номер паспорта, кем и когда выдан)

_____

(адрес места регистрации и проживания)

в соответствии со статьей 9 Федерального закона «О персональных данных» даю согласие оператору персональных данных – Обществу с ограниченной ответственностью «Технический центр Интернет», расположенному по адресу: 127083, г. Москва, улица 8 Марта, дом 1, строение 12, офис Э. 7, ПМ. XL К. 23-32, на автоматизированную, а также без использования средств автоматизации, обработку своих персональных данных, включающих: фамилию, имя, отчество, адрес регистрации (места жительства), серию, номер, дату и место выдачи основного документа, удостоверяющего личность, пол, дату и место рождения, гражданство, страховой номер индивидуального лицевого счета (СНИЛС), адрес электронной почты, номер мобильного телефона, сведения о месте работы, должность.

Настоящее согласие предоставляется мной в целях получения услуг в соответствии с Порядком реализации функций удостоверяющего центра Общества с ограниченной ответственностью «Технический центр Интернет» (далее – Порядок), включения сведений в выдаваемый мне сертификат, а также в реестр сертификатов. Настоящим соглашаюсь на включение моих сведений, содержащихся в выдаваемом мне сертификате ключа проверки электронной подписи, в том числе включающих фамилию, имя, отчество, сведений о месте работы и занимаемой должности, СНИЛС, адрес электронной почты, в общедоступные источники персональных данных, которыми являются сертификат ключа проверки электронной подписи и реестр сертификатов удостоверяющего центра Общества с ограниченной ответственностью «Технический центр Интернет».

Настоящим предоставляю Обществу с ограниченной ответственностью «Технический центр Интернет» право осуществлять все действия (операции) со моими персональными данными, предусмотренные Порядком, включая сбор, запись, систематизацию, накопление, хранение, обновление, изменение, использование, передачу, предоставление, доступ, блокирование и уничтожение персональных данных.

Настоящее согласие на обработку персональных данных действует в течение всего срока осуществления Обществом с ограниченной ответственностью «Технический центр

Интернет» функций удостоверяющего центра и может быть отозвано на основании письменного заявления в произвольной форме.

В случае отзыва согласия на обработку персональных данных Общества с ограниченной ответственностью «Технический центр Интернет» имеет право не прекращать их обработку до окончания установленных нормативными правовыми актами Российской Федерации сроков хранения соответствующей информации или документов, при обработке которых использовалась усиленная неквалифицированная электронная подпись субъекта персональных данных, а также в случаях, предусмотренных статьей 6 Федерального закона «О персональных данных».

Подтверждаю, что с Порядком, опубликованным на сайте Удостоверяющего центра Общества с ограниченной ответственностью «Технический центр Интернет» в информационно-телекоммуникационной сети «Интернет» по адресу https://ca.tcinet.ru/, и приложениями к нему, в том числе с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, ознакомлен и обязуюсь соблюдать все его положения.

_____ _____ / _____ /

Дата (подпись и ФИО уполномоченного лица, на имя которого изготавливается сертификат).

Приложение № 2

к Порядку реализации функций удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет»

(Форма заявления на создание и выдачу сертификата ключа проверки электронной подписи

для физических лиц и индивидуальных предпринимателей)5

Общество с ограниченной ответственностью

«Технический центр Интернет»

Я, _____

(фамилия, имя, отчество)

_____

(серия и номер паспорта, кем и когда выдан)

в соответствии со статьей 428 Гражданского кодекса Российской Федерации полностью и безусловно присоединяюсь к Порядку реализации функций Удостоверяющего центра и исполнения его обязанностей (далее – Порядок), опубликованному на сайте Удостоверяющего центра ООО «ТЦИ» в информационно-телекоммуникационной сети «Интернет» по адресу https://ca.tcinet.ru,

регистрируясь в Удостоверяющем центре ООО «ТЦИ», с Порядком и приложениями к нему, в том числе с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, ознакомлен(а) и обязуюсь соблюдать все его положения,

прошу создать и выдать сертификат ключа проверки электронной подписи, содержащий следующую информацию:

Фамилия	
Имя Отчество	
Адрес электронной почты	
Ключ электронной подписи и ключ	□ *Создать с использованием средств*

[5] Заявление о присоединении к Порядку подается в Удостоверяющий центр в двух экземплярах. После регистрации Заявления в Удостоверяющем центре один экземпляр предоставляется заявителю

проверки электронной подписи	*Удостоверяющего центра* □ *Создан с использованием средств электронной подписи заявителя*
Приложение:	Согласие лица, на имя которого создается сертификат, на обработку персональных данных[6]; Запрос на создание сертификата в электронном и (или) бумажном виде[7]

_____ / _____ /

(подпись и ФИО лица, на имя которого изготавливается сертификат).

«____» _____20___ г.

(заполняется уполномоченным лицом Удостоверяющего центра)

Заявление зарегистрировано в реестре Удостоверяющего центра, подтверждает присоединение _____,

(ФИО лица, на имя которого изготавливается сертификат)

к Порядку реализации функций удостоверяющего центра и исполнения его обязанностей.

Регистрационный № _____ от «_____» _____ 20___ г.

Уполномоченное лицо Удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет» _____ / _____ /

(подпись) (расшифровка подписи)

М.П.

---

[6] Не предоставляется в случае, если данное согласие ранее предоставлялось, либо если создается сертификат, используемый для автоматического подписания электронной подписью в информационной системе.

[7] Предоставляется в случае самостоятельного создания заявителем ключа электронной подписи и ключа проверки электронной подписи с использованием средств электронной подписи заявителя.

Приложение
к заявлению на создание и выдачу сертификата ключа проверки
электронной подписи **для физических лиц**
(Форма согласия на обработку персональных данных)

_____

(Фамилия, Имя, Отчество лица, на имя которого изготавливается сертификат, серия и номер паспорта, кем и когда выдан)

_____

(адрес места регистрации и проживания)

в соответствии со статьей 9 Федерального закона «О персональных данных» даю согласие оператору персональных данных – Обществу с ограниченной ответственностью «Технический центр Интернет», расположенному по адресу: 127083, г. Москва, улица 8 Марта, дом 1, строение 12, офис Э. 7, ПМ. XL К. 23-32, на автоматизированную, а также без использования средств автоматизации, обработку своих персональных данных, включающих: фамилию, имя, отчество, адрес регистрации (места жительства), серию, номер, дату и место выдачи основного документа, удостоверяющего личность, пол, дату и место рождения, гражданство, страховой номер индивидуального лицевого счета (СНИЛС), адрес электронной почты, номер мобильного телефона, сведения о месте работы, должность.

Настоящее согласие предоставляется мной в целях получения услуг в соответствии с Порядком реализации функций удостоверяющего центра Общества с ограниченной ответственностью «Технический центр Интернет» (далее – Порядок), включения сведений в выдаваемый мне сертификат, а также в реестр сертификатов. Настоящим соглашаюсь на включение моих сведений, содержащихся в выдаваемом мне сертификате ключа проверки электронной подписи, в том числе включающих фамилию, имя, отчество, сведений о месте работы и занимаемой должности, СНИЛС, адрес электронной почты, в общедоступные источники персональных данных, которыми являются сертификат ключа проверки электронной подписи и реестр сертификатов удостоверяющего центра Общества с ограниченной ответственностью «Технический центр Интернет».

Настоящим предоставляю Обществу с ограниченной ответственностью «Технический центр Интернет» право осуществлять все действия (операции) с моими персональными данными, предусмотренные Порядком, включая сбор, запись, систематизацию, накопление, хранение, обновление, изменение, использование, передачу, предоставление, доступ, блокирование и уничтожение персональных данных.

Настоящее согласие на обработку персональных данных действует в течение всего срока осуществления Обществом с ограниченной ответственностью «Технический центр Интернет»

функций удостоверяющего центра и может быть отозвано на основании письменного заявления в произвольной форме.

В случае отзыва согласия на обработку персональных данных Общества с ограниченной ответственностью «Технический центр Интернет» имеет право не прекращать их обработку до окончания установленных нормативными правовыми актами Российской Федерации сроков хранения соответствующей информации или документов, при обработке которых использовалась усиленная неквалифицированная электронная подпись субъекта персональных данных, а также в случаях, предусмотренных статьей 6 Федерального закона «О персональных данных».

Подтверждаю, что с Порядком, опубликованным на сайте Общества с ограниченной ответственностью «Технический центр Интернет в информационно-телекоммуникационной сети «Интернет» по адресу https://ca.tcinet.ru/, и приложениями к нему, в том числе с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, ознакомлен и обязуюсь соблюдать все его положения.

_____ / _____ /

Дата

(подпись и ФИО уполномоченного лица, на имя которого изготавливается сертификат).

Приложение № 3

к Порядку реализации функций удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет

(Форма доверенности на получение сертификата ключа проверки электронной подписи) **для юридических лиц**

Доверенность

г. _____ «____» _____20___ г.

_____

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

в лице _____,

(должность)

_____,

(фамилия, имя, отчество)

действующего на основании _____,

уполномочивает _____

(фамилия, имя, отчество)

_____

(серия и номер паспорта, кем и когда выдан, код подразделения, адрес места регистрации и проживания)

предоставить в Общество с ограниченной ответственностью «Технический центр Интернет документы и сведения в соответствии с Порядком реализации функций удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет, необходимые для создания ключа электронной подписи, ключа проверки электронной подписи и сертификата ключа проверки электронной подписи;

получить средства электронной подписи, ключ электронной подписи, ключ проверки электронной подписи и сертификат ключа проверки электронной подписи, созданный для пользователя Удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет.

_____

(фамилия, имя, отчество Пользователя Удостоверяющего центра)

Представитель наделяется правом расписываться на копии сертификата ключа проверки электронной подписи на бумажном носителе и в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по «____» _____ 20____ г.

Подпись уполномоченного представителя _____ / _____ подтверждаю.

(Фамилия И.О.) (подпись)

_____ _____ / _____ /

(должность) (подпись) (расшифровка подписи)

М.П.

Приложение № 4

к Порядку реализации функций удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет

(Форма заявления на подтверждение действительности электронной подписи в электронном документе)

для юридических лиц

Общество с ограниченной ответственностью

«Технический центр Интернет»

№

_____

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

в лице _____,

(должность)

_____,

(фамилия, имя, отчество)

действующего на основании _____,

просит проверить действительность усиленной неквалифицированной электронной подписи, использованной для подписания электронного документа на основании следующих данных:

1. Серийный номер сертификата ключа проверки электронной подписи, выданного Удостоверяющим центром, с использованием которого необходимо осуществить проверку действительности электронной подписи в электронном документе: _____

2. Время[8] подписания электронного документа электронной подписью:

«_____:_____» «_____/_____/_____»;

Час минута день месяц год

3. Время, на момент наступления которого необходимо проверить подлинность электронной подписи (если момент подписания электронного документа не определен):

«_____:_____» «_____/_____/_____»

Час минута день месяц год

[8] Время и дата указываются с учетом часового пояса (по Московскому времени).

Приложение: 1. Сертификат ключа проверки электронной подписи, выданный удостоверяющим центром Общество с ограниченной ответственностью «Технический центр Интернет, с использованием которого необходимо проверить действительность электронной подписи в электронном документе (файл формата CMS / PKCS #7), на носителе информации – рег. № _____;

2. Электронный документ, подписанный электронной подписью, основанной на сертификате, выданным удостоверяющим центром Общество с ограниченной ответственностью «Технический центр Интернет, действительность которой необходимо проверить (в виде файла стандарта CMS / PKCS #7), на носителе информации – рег. № _____.

_____ _____ / _____ /

(должность) (подпись и Ф.И.О.)

Приложение № 5

к Порядку реализации функций удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет

(Форма заявления на проверку подлинности усиленной электронной подписи в электронном документе)

для физических лиц и индивидуальных предпринимателей

Общество с ограниченной ответственностью

«Технический центр Интернет»

Я, _____

(фамилия, имя, отчество)

прошу проверить действительность усиленной неквалифицированной электронной подписи, использованной для подписания электронного документа на основании следующих данных:

1. Серийный номер сертификата ключа проверки электронной подписи, выданного Удостоверяющим центром, с использованием которого необходимо осуществить проверку действительности электронной подписи в электронном документе: _____

2. Время[9] подписания электронной подписью электронного документа:

«_____:_____» «_____/_____/_____»;

Час минута день месяц год

3. Время, на момент наступления которого необходимо проверить подлинность электронной подписи (если момент подписания электронного документа не определен):

«_____:_____» «_____/_____/_____»

Час минута день месяц год

Приложение: 1. Сертификат ключа проверки электронной подписи, выданный удостоверяющим центром Общество с ограниченной ответственностью «Технический центр Интернет, с использованием которого необходимо проверить действительность электронной подписи в электронном документе (файл формата CMS / PKCS #7), на носителе информации – рег. № _____;

2. Электронный документ, подписанный электронной подписью, основанной

[9] Время и дата указываются с учетом часового пояса (по Московскому времени).

на сертификате, выданным удостоверяющим центром Общество с ограниченной ответственностью «Технический центр Интернет, действительность которой необходимо проверить (в виде файла стандарта CMS / PKCS #7), на носителе информации – рег. № _____.

_____ _____ / _____ /

(Ф.И.О заявителя) (подпись) (расшифровка подписи)

«____» _____ 20___

Приложение № 6

к Порядку реализации функций удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет

(Форма заявления на получение информации о статусе сертификата)

для юридических лиц

Общество с ограниченной ответственностью

«Технический центр Интернет»

_____ № _____

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

_____,

(фамилия, имя, отчество)

действующего на основании _____,

просит предоставить информацию о статусе сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата	
Наименование организации	

Период времени[10], на момент наступления которого требуется установить статус сертификата ключа проверки электронной подписи: с «_____» по «_____».

_____ _____ / _____ /

(должность) (подпись и Ф.И.О.)

[10] Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение № 7

к Порядку реализации функций удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет

(Форма заявления на получение информации о статусе сертификата)

для физических лиц и индивидуальных предпринимателей

Общество с ограниченной ответственностью

«Технический центр Интернет»

Я, _____

(фамилия, имя, отчество)

прошу предоставить информацию о статусе сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата	
Фамилия	
Имя Отчество	

Период времени[11], на момент наступления которого требуется установить статус сертификата ключа проверки электронной подписи: с «_____» по «_____».

_____ _____ / _____ /

(Ф.И.О заявителя) (подпись) (расшифровка подписи)

«____» _____ 20___

[11] Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение № 8

к Порядку реализации функций удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет (Форма заявления о прекращении действия сертификата ключа проверки электронной подписи)

для юридических лиц

Общество с ограниченной ответственностью

«Технический центр Интернет»

_____ № _____

_____

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

в лице _____,

(должность)

_____,

(фамилия, имя, отчество)

действующего на основании _____,

в связи с _____,

(причина прекращения действия сертификата)

просит прекратить действие сертификата ключа проверки электронной подписи, содержащего следующие данные[12]:

Серийный номер сертификата	
Наименование юридического лица	
Фамилия	
Имя Отчество	
_____ (должность)	_____ / _____ / (подпись и Ф.И.О.)

[12] Указываются сведения, содержащиеся в сертификате владельца сертификата

Приложение № 9

к Порядку реализации функций удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет

(Форма заявления о прекращении действия сертификата ключа проверки электронной подписи)

для физических лиц и индивидуальных предпринимателей

Общество с ограниченной ответственностью

«Технический центр Интернет»

Я, _____

(фамилия, имя, отчество)

в связи с _____,

(причина прекращения действия сертификата)

прошу прекратить действие сертификата ключа проверки электронной подписи, владельцем которого я являюсь, содержащего следующие данные:

Серийный номер сертификата	
Фамилия	
Имя Отчество	

_____ _____ / _____ /

(Ф.И.О заявителя) (подпись) (расшифровка подписи)

«____» _____ 20___

Приложение № 10

к Порядку реализации функций удостоверяющего центра Общество с ограниченной ответственностью «Технический центр Интернет

Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи

1. Общие принципы обеспечения информационной безопасности при организации электронного взаимодействия с использованием электронной подписи.

Организация электронного взаимодействия с использованием электронной подписи должна осуществляться с учетом требований федеральных законов «Об электронной подписи», «Об информации, информационных технологиях и о защите информации», Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 (далее также – Инструкция ФАПСИ № 152), других федеральных законов и нормативных правовых актов, осуществляющих правовое регулирование отношений в области обеспечения защиты информации и использования электронной подписи, руководящих документов ФСТЭК России и ФСБ России, эксплуатационной и технической документации на используемые средства электронной подписи, средства криптографической защиты информации (далее также – СКЗИ).

Если иное не установлено федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или решением о создании корпоративной информационной системы, порядок использования электронной подписи в корпоративной информационной системе может устанавливаться оператором этой системы или соглашением между участниками электронного взаимодействия в ней.

2. Риски, связанные с использованием электронных подписей и средств электронной подписи.

2.1. Виды рисков, связанных с использованием электронных подписей и средств электронной подписи.

В случае, если электронное взаимодействие с использованием электронной подписи осуществляется без учета требований нормативных правовых актов, регулирующих отношения в области использования электронных подписей, используется неквалифицированная электронная подпись или средства электронной подписи не сертифицированы на соответствие

требованиям безопасности информации, могут возникнуть или существенно возрасти риски, связанные с использованием электронной подписи, основными из которых могут являться:

риски, связанные с нарушением целостности электронного документа и возможностью отказа от него. Данные риски могут быть связаны с внесенными в электронный документ изменениями, произведенными после его подписания. Лицо, подписавшее электронный документ неквалифицированной электронной подписью, или лицо, осуществляющее проверку такой электронной подписи, может заявить о том, что содержание электронного документа было изменено после его подписания и электронный документ не соответствует тому документу, который был подписан неквалифицированной электронной подписью;

риски, связанные с проверкой принадлежности ключа электронной подписи, с помощью которой подписан электронный документ, владельцу сертификата ключа проверки электронной подписи (далее – владелец сертификата). Лицо, владеющее сертификатом ключа проверки электронной подписи и соответствующим ключом электронной подписи, которым был подписан электронный документ, может заявить о том, что неквалифицированная электронная подпись, содержащаяся в электронном документе, не принадлежит данному владельцу сертификата;

риски, связанные с признанием юридической силы электронного документа, подписанного неквалифицированной электронной подписью. Одна из сторон может заявить о том, что подписанный неквалифицированной электронной подписью документ не может порождать юридически значимых последствий или считаться достаточным доказательством в суде;

риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае, если порядок использования неквалифицированной электронной подписи и средств электронной подписи не соответствует требованиям нормативных правовых актов Российской Федерации, осуществляющих правовое регулирование отношений в использовании электронной подписи или не соответствует порядку использования неквалифицированной электронной подписи, определяемому соглашениями сторон, юридическая значимость подписанных такой электронной подписью документов может быть не признана одной из сторон участника электронного взаимодействия;

риски, связанные с нарушением конфиденциальности ключей электронной подписи (использование ключей электронной подписи без согласия владельца). В случае нарушения конфиденциальности ключей электронной подписи, в том числе компрометации ключей, несанкционированного доступа к ключевым носителям или средствам электронной подписи, участником электронного взаимодействия может быть принят в исполнение подписанный неквалифицированной электронной подписью документ, порождающий юридически значимые последствия;

риски, связанные с несовместимостью средств электронной подписи, используемых сторонами для организации электронного взаимодействия. Несовместимость средств электронной подписи, протоколов и форматов данных, используемых сторонами для организации электронного взаимодействия, может привести к невозможности проверки неквалифицированной электронной подписи документа или к её некорректной проверке;

риски, связанные с определением полномочий лица, подписавшего электронной подписью документ. В случае, если участниками электронного взаимодействия не определены лица, участвующие в электронном взаимодействии, полномочия данных лиц по подписанию электронных документов от имени участника электронного взаимодействия, а также в случае, если полномочия лица по подписанию электронных документов прекращены, одна из сторон может заявить, что полученный электронный документ содержит неквалифицированную электронную подпись лица, не уполномоченного на подписание данного документа и не может быть принят в исполнение;

риски, связанные с использованием сертификатов ключей проверки электронной подписи и ключей электронной подписи, прекративших своё действие. В случае использования для подписания электронных документов ключа электронной подписи, прекратившего своё действие на момент подписания, либо, если момент подписания электронного документа не определен, а также в случае использования сертификата ключа проверки электронной подписи, который стал недействующим на день проверки электронной подписи, сторона, получившая подписанный неквалифицированной электронной подписью документ, может заявить о непризнании такого электронного документа.

2.2. Меры по снижения вероятности возникновения рисков, связанных с использованием электронных подписей.

В целях снижения вероятности возникновения и реализации указанных рисков участникам электронного взаимодействия необходимо предусмотреть обеспечение комплекса правовых и организационно-технических мероприятий по обеспечению информационной безопасности при осуществлении электронного взаимодействия с использованием усиленной неквалифицированной электронной подписи (далее также – электронная подпись) и сертифицированных по требованиям безопасности информации средств электронной подписи, получивших подтверждение соответствия требованиям к средствам электронной подписи, установленным в соответствии с Федеральными законом «Об электронной подписи» (далее также – сертифицированные средства электронной подписи).

Электронное взаимодействие с использованием усиленной неквалифицированной электронной подписи и сертифицированных средств электронной подписи, осуществляемое с учетом требований Федерального закона «Об электронной подписи», других федеральных

законов, принимаемых в соответствии с ними нормативных правовых актов, регулирующих отношения в области использования электронных подписей, позволяет обеспечить:

неотказываемость от электронного документа, содержащего электронную подпись. Неквалифицированная электронная подпись позволяет определить лицо, подписавшее электронный документ;

целостность электронного документа. Неквалифицированная электронная подпись позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания.

В случае необходимости обеспечения конфиденциальности передаваемой информации ключи электронной подписи и СКЗИ могут использоваться для обеспечения защиты информации, в том числе при её передаче по информационно-телекоммуникационным сетям, а также для организации защищенных каналов связи с использованием шифровальных (криптографических) средств.

Использование неквалифицированной электронной подписи и сертифицированных средств электронной подписи позволяет:

установить факт изменения подписанного электронного документа после момента его подписания;

обеспечить практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки;

создать электронную подпись в формате, обеспечивающем возможность ее проверки всеми средствами электронной подписи.

При создании электронной подписи сертифицированные средства электронной подписи должны:

показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с использованием указанных средств, лицу, осуществляющему создание электронной подписи, содержание информации, подписание которой производится;

создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи

однозначно показывают, что неквалифицированная электронная подпись создана.

При проверке электронной подписи сертифицированные средства электронной подписи должны:

показывать содержание электронного документа, подписанного электронной подписью;

показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;

указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

Одной из составных частей инфраструктуры открытых ключей и системы криптографической защиты информации является удостоверяющий центр, выполняющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей (далее также – сертификат).

Удостоверяющий центр осуществляет свою деятельность в строгом соответствии с нормативными правовыми актами Российской Федерации, руководящими документами, эксплуатационной документацией на используемые средства, Порядком реализации функций удостоверяющего центра и исполнения его обязанностей (далее также – Порядок) и другими документами, регулирующими вопросы использования электронной подписи.

Сертификаты, изготавливаемые Удостоверяющим центром, заверяются усиленной неквалифицированной электронной подписью уполномоченного лица удостоверяющего центра, что подтверждает факт принадлежности ключа электронной подписи конкретному лицу участника электронного взаимодействия. Использование сертификатов позволяет участника электронного взаимодействия идентифицировать лицо, подписавшее электронной подписью документ, а также позволяет подтвердить целостность (неизменность) содержания подписанного электронного документа при проверке электронной подписи. Таким образом, при соблюдении требований информационной безопасности и соблюдения порядка использования усиленной неквалифицированной электронных подписей, практически исключаются риски, связанные использованием электронных подписей, в том числе риски, связанные с подтверждением юридической значимости электронных документов, подписанных усиленной неквалифицированной электронной подписью

3. Меры, необходимые для обеспечения безопасности при использовании электронных подписей.

3.1. Требования и рекомендации по обеспечению информационной безопасности при использовании средств электронной подписи.

В организации, эксплуатирующей средства электронной подписи (СКЗИ), должны быть предусмотрены организационные и организационно-технические мероприятия, направленные на обеспечение информационной безопасности при использовании средств электронной подписи и определяющие требования к ответственным лицам, автоматизированным рабочим местам пользователей СКЗИ (далее также - АРМ), системному и прикладному программному

обеспечению, условиям хранения и использования средств электронной подписи, ключей электронной подписи и ключевых носителей.

3.1.1. Требования и рекомендации по назначению ответственных лиц.

В организации должны быть определены лица, ответственные за осуществление электронного взаимодействии с использованием электронной подписи и имеющие доступ к ключевым носителям, а также лица, ответственные за организацию работ по защите информации и соблюдению условий хранения и использования ключей электронной подписи и средств электронной подписи.

К работе со средствами электронной подписи должны допускаться лица, прошедшие соответствующее обучение и ознакомленные с инструкцией ФАПСИ №152, другими нормативными правовыми актами и руководящими документами, в том числе внутренними организационными документами и инструкциями по защите информации при использовании электронной подписи, а также эксплуатационной документацией на используемые средства электронной подписи.

В организации, эксплуатирующей СКЗИ, должно быть назначено лицо, выполняющее функции администратора информационной безопасности, на которого возлагаются задачи организации работ по защите информации, подготовки соответствующих инструкций, обучения и инструктажа пользователей СКЗИ, ведению журналов учета СКЗИ, настройке системного, прикладного программного обеспечения, СКЗИ и средств защиты от несанкционированного доступа, устанавливаемого на АРМ пользователей СКЗИ, контролю за соблюдением требований по безопасности, а также взаимодействия с удостоверяющим центром по вопросам использования электронной подписи.

3.1.2. Требования и рекомендации к помещениям и размещению технических средств АРМ.

Помещения, в которых расположены АРМ, предназначенные для работы со средствами электронной подписи (далее – спецпомещения), должны соответствовать требованиям инструкции ФАПСИ №152. Должен быть исключен бесконтрольный допуск лиц, не допущенных к работе в указанных спецпомещениях. В случае необходимости присутствия посторонних лиц в спецпомещениях должен быть обеспечен контроль за их действиями.

Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Размещение АРМ должно производиться с учетом схемы контролируемой зоны и исключать возможность просмотра посторонними лицами работ, осуществляемых на АРМ.

Спецпомещения рекомендуется оснащать охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.

3.1.3. Требования и рекомендации к АРМ пользователей СКЗИ.

Не допускается оставлять без контроля АРМ при включенном питании и подключенными ключевыми носителями. Перед уходом пользователь СЗКИ должен выключить АРМ либо заблокировать рабочую станцию с использованием средств защиты информации от несанкционированного доступа или с использованием средств операционной системы. Рекомендуется настроить автоматическое включение экранной заставки, защищенной паролем.

На АРМ пользователей рекомендуется установить сертифицированные средства защиты информации от несанкционированного доступа, а также средства антивирусной защиты.

В целях исключения возможности несанкционированного изменения аппаратной части системного блока администратору рекомендуется предусмотреть опечатывание системного блока АРМ.

Необходимо предусмотреть организацию парольной защиты при включении АРМ и загрузке операционной системы с использованием средств защиты информации (средств доверенной загрузки), либо средств BIOS и средств операционной системы, также рекомендуется определить установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске, отключить возможность загрузки с внешних съемных дисков, исключить возможность нестандартных видов загрузки операционной системы.

3.1.4. Требования и рекомендации по настройке системного и прикладного программного обеспечения.

На технических средствах АРМ с установленными средствами электронной подписи необходимо использовать только лицензионное программное обеспечение, полученное из доверенных источников. Не допускается использовать нестандартные, измененные или отладочные версии операционной системы.

Не допускается установка на АРМ средств разработки и отладки программного обеспечения. Необходимо исключить возможность установки средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам, а также вредоносного программного обеспечения, позволяющего получать привилегии администратора.

Рекомендуется ограничить права пользователя АРМ по самостоятельной установке программного обеспечения и настроить возможность выполнения пользователем АРМ только тех приложений, которые разрешены администратором информационной безопасности.

Необходимо регулярно отслеживать и устанавливать обновления безопасности для операционной системы, программного обеспечения АРМ, регулярно осуществлять обновление антивирусных баз.

3.1.5. Требования к настройкам операционной системы, установленной на АРМ пользователя.

До начала использования средств электронной подписи администратор информационной безопасности должен произвести настройку операционной системы, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль настроек в соответствии со следующими рекомендациями:

правом установки и настройки операционной системы и средств электронной подписи должен обладать только администратор безопасности;

в целях возможности разграничения прав доступа рекомендуется использовать средства, входящие в состав средств защиты информации;

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

все привилегии группы Everyone должны быть удалены;

необходимо исключить использование режима автоматического входа пользователя в операционную систему при ее загрузке без ввода пароля;

рекомендуется переименовать стандартную учетную запись администратора;

рекомендуется отключить учетная запись для гостевого входа;

исключить возможность удаленного управления, администрирования и модификации операционной системы и её настроек, системного реестра, для всех, включая группу администраторов;

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

должно быть исключено или ограничено использование пользователями сервиса планировщика задач. При использовании данного сервиса состав запускаемого программного обеспечения на АРМ согласовывается с администратором информационной безопасности;

рекомендуется организовать удаление временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы средств электронной подписи. Если это невыполнимо, то операционная система должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

должны быть отключены средства удаленного администрирования, в случае если такое подключение осуществляется без использования защищенных каналов связи;

должны быть установлены ограничения на доступ пользователей к системному реестру путем настройки прав доступа к системному реестру;

на все директории (папки), содержащие системные файлы и программы из комплекта СКЗИ, должны быть установлены права доступа, запрещающие запись всем пользователям, кроме пользователя, имеющего права администратора, создателя (владельца) и права системы;

необходимо обеспечить ведение журналов аудита в операционной системе;

настройка параметров системного реестра производится в соответствии с эксплуатационной документацией на средства электронной подписи.

3.1.6. Требования и рекомендации при организации парольной защиты.

Рекомендуется разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, доступа к ключам электронной подписи), использовать правила формирования и хранения паролей в соответствии со следующими правилами:

длина пароля должна быть не менее 8 символов;

в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;

пользователь АРМ должен обеспечивать конфиденциальность паролей, не допускается хранить записанные пароли в легкодоступных местах;

периодичность смены пароля определяется принятой политикой безопасности (инструкцией по организации парольной защиты), но не должна превышать двух месяцев.

указанная политика должна применяться для всех учетных записей пользователей, зарегистрированных в операционной системе.

3.1.7. Требования к установке, настройке и использованию средств электронной подписи.

Установка и настройка средств электронной подписи (СКЗИ) должна выполняться администратором информационной безопасности либо лицом, ответственным за работоспособность АРМ и прошедшим соответствующее обучение.

Установка средств электронной подписи должна производиться только с дистрибутива, полученного по доверенному каналу, в соответствии с эксплуатационной документацией на средства электронной подписи.

При установке средств электронной подписи должен быть обеспечен контроль целостности устанавливаемого программного обеспечения.

Перед установкой средств электронной подписи необходимо произвести проверку операционной системы на отсутствие вредоносных программ с помощью антивирусных средств.

После завершения установки осуществляются настройка и контроль работоспособности средств электронной подписи.

Использование средств электронной подписи должно осуществляться в соответствии с эксплуатационной документацией и инструкциями на средства электронной подписи.

3.1.8. Требования обеспечения информационной безопасности при подключении АРМ к сетям связи общего пользования, в том числе к информационно-телекоммуникационной сети «Интернет».

Не рекомендуется подключать к сетям связи общего пользования АРМ пользователя при работе со средствами электронной подписи и носителями ключей электронной подписи. В случае необходимости подключения АРМ к сетям связи общего пользования такое подключение рекомендуется производить с использованием сертифицированного межсетевого экрана, настроенного в соответствии с требованиями эксплуатационной документации на средства межсетевого экранирования.

В случае подключения АРМ с установленными средствами электронной подписи к сетям связи общего пользования необходимо ограничить возможность запуска и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX и т.д.), полученных из сетей общего пользования. Не допускается открывать такие файлы без проведения соответствующих проверок антивирусными средствами на предмет содержания в них программных закладок и вредоносных программ.

3.2. Порядок обращения с носителями ключевой информации.

При использовании и хранении ключей электронной подписи должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации (ключевых носителей), содержащих ключи электронной подписи, который должен исключать возможность несанкционированного доступа к ним.

Для хранения ключевых носителей в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами.

В качестве ключевых носителей рекомендуется использовать учтенные в установленном порядке сертифицированные ключевые носители USB-ключи и смарт-карты.

При хранении и использовании ключей электронной подписи пользователю СКЗИ запрещается:

выполнять копирование ключа электронной подписи на иные ключевые носители без разрешения администратора информационной безопасности;

знакомить с содержанием ключевых носителей или передавать ключевые носители иным лицам;

устанавливать ключевой носитель в другие АРМ, не предназначенные для работы с ключевой информацией;

записывать на ключевой носитель постороннюю информацию;

использовать ранее использовавшиеся ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации с использованием сертифицированных средств электронной подписи либо средств, гарантирующих практическую невозможность восстановления информации с ключевых носителей.

Владелец ключа электронной подписи (владелец сертификата) обязан:

хранить в тайне ключ электронной подписи;

немедленно обратиться в удостоверяющий центр для приостановления действия сертификата ключа проверки электронной подписи или его отзыва в случае компрометации ключа электронной подписи или при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

не использовать ключ проверки электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который отозван или действие которого приостановлено.

3.3. Учет и контроль выполнения требований информационной безопасности и порядка использования средств электронной подписи.

Действия, связанные с хранением и эксплуатацией средств электронной подписи и ключей электронной подписи, должны фиксироваться в журналах поэкземплярного учета, ведение которого осуществляется администратором информационной безопасности в соответствии с Инструкцией ФАПСИ № 152.

Администратор информационной безопасности должен периодически, не реже одного раза в два месяца, проводить проверку установленного программного обеспечения, журналов аудита операционной системы и средств защиты информации на всех АРМ пользователей СКЗИ, осуществлять контроль за условиями использования и хранения ключевых носителей, а также проводить периодическое тестирование технических и программных средств защиты информации.

В случае обнаружения постороннего программного обеспечения, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией, назначенной руководителем организации, а также организованы работы по анализу и устранению выявленных нарушений.