МИНИСТЕРСТВО ФИНАНСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ КАЗНАЧЕЙСТВО
(КАЗНАЧЕЙСТВО РОССИИ)

ПРИКАЗ

12 декабря 2017 г. № 342

Москва

О внесении изменений в Регламент Удостоверяющего центра Федерального казначейства, утвержденный приказом Федерального казначейства от 31 июля 2015 г. № 197

В связи со служебной необходимостью п р и к а з ы в а ю:

1. Регламент Удостоверяющего центра Федерального казначейства, утвержденный приказом Федерального казначейства от 31 июля 2015 г. № 197 «Об утверждении Регламента Удостоверяющего центра Федерального казначейства» (в редакции приказа Федерального казначейства от 25 июля 2016 г. № 280), изложить в новой редакции согласно приложению к настоящему приказу.

2. Территориальным органам Федерального казначейства обеспечить уведомление лиц, с которыми заключены Договоры присоединения (Соглашения) к Регламенту Удостоверяющего центра Федерального казначейства, о соответствующих изменениях до вступления в силу настоящего приказа.

3. Настоящий приказ вступает в силу с 15 февраля 2018 года.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель Р.Е. Артюхин

Приложение к приказу
Федерального казначейства
от «12» декабря 2017 г. № 342

УТВЕРЖДЕН

Приказом
Федерального казначейства
от 31.07.2015 № 197

РЕГЛАМЕНТ
Удостоверяющего центра Федерального казначейства

1. Сокращения

№ п/п	Сокращение	Значение
1	УЦ	Удостоверяющий центр
2	Средство создания запроса	Средство создания КЭП, Запроса на сертификат, Заявления на сертификат
3	Сертификат	Квалифицированный сертификат ключа проверки электронной подписи
4	ИНН	Идентификационный номер налогоплательщика
5	ОГРН	Основной государственный регистрационный номер
6	ТОФК	Территориальный орган Федерального казначейства
7	ЭП	Электронная подпись
8	КЭП	Ключ электронной подписи
9	КПЭП	Ключ проверки электронной подписи
10	СНИЛС	Страховой номер индивидуального лицевого счета
11	САС	Список аннулированных сертификатов
12	АРМ	Автоматизированное рабочее место
13	Заявление на сертификат	Заявление на получение сертификата
14	Заявление на изменение статуса	Заявление на приостановление/возобновление/прекращение действия сертификата

№ п/п	Сокращение	Значение
	сертификата	
15	Заявление о статусе сертификата	Заявление на получение информации о статусе сертификата
16	Реестр сертификатов	Реестр выданных и аннулированных сертификатов
17	ЕГРЮЛ	Единый государственный реестр юридических лиц
18	ЕСИА	Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»

2. Термины и определения

Запрос на сертификат – файл, созданный с использованием средств ЭП, содержащий КПЭП и иную информацию о Заявителе и/или о получателе сертификата.

Заявитель – юридическое лицо или индивидуальный предприниматель, с которыми заключен Договор присоединения (Соглашение) к Регламенту Удостоверяющего центра Федерального казначейства.

Получатель сертификата – руководитель юридического лица, индивидуальный предприниматель или лицо, уполномоченное ими на подписание документов с использованием сертификата от имени Заявителя.

Уполномоченное лицо – лицо, уполномоченное Заявителем на представление документов и сведений, предусмотренных настоящим Регламентом.

Компрометация КЭП – ознакомление неуполномоченного лица (лиц) с КЭП; потеря ключевого носителя; нарушение правил хранения и уничтожения КЭП (после окончания срока действия); нарушение печати на сейфе с ключевыми носителями; случаи, когда невозможно достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Печать – печать с воспроизведением Государственного герба Российской Федерации или иная печать Заявителя, содержащая его

наименование и используемая для заверения подлинности подписи лица, имеющего право действовать от имени Заявителя в соответствии с гражданским законодательством Российской Федерации.

Список аннулированных сертификатов (CAC) – электронный документ, подписанный ЭП Федерального казначейства, представляющий собой список серийных номеров сертификатов, которые были аннулированы или действие которых было прекращено/приостановлено.

Копия документа, удостоверяющего личность – копия страниц паспорта гражданина Российской Федерации или иного документа, удостоверяющего личность, в соответствии с законодательством Российской Федерации, содержащая фамилию, имя, отчество (если имеется).

3. Общие положения

3.1. Регламент Удостоверяющего центра Федерального казначейства (далее – Регламент) определяет:

– порядок выдачи средства ЭП и Средства создания запроса;

– порядок создания, выдачи, смены, прекращения действия, аннулирования, приостановления и возобновления действия сертификатов;

– порядок предоставления информации о статусе сертификатов.

3.2. Настоящий Регламент разработан в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных), постановлением Правительства Российской Федерации от 1 декабря 2004 г. № 703 «О Федеральном казначействе» (в редакции постановления Правительства Российской Федерации от 13 апреля 2016 г. № 300), приказом Федеральной службы безопасности Российской Федерации от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

В настоящем Регламенте используются понятия, термины, сокращения, которые применяются в указанных выше нормативных правовых актах.

При возникновении вопросов, не урегулированных положениями Регламента, следует руководствоваться законодательством Российской Федерации.

3.3. Выдачу сертификатов осуществляет ТОФК по месту нахождения Заявителя, обособленного подразделения юридического лица.

Взаимодействие ТОФК и Заявителя осуществляется на основании заключенного Договора присоединения (Соглашения) к Регламенту Удостоверяющего центра Федерального казначейства[1] (далее – Соглашение).

3.4. Создание и выдача сертификата осуществляется при условии наличия у Заявителя:

– средства ЭП и Средства создания запроса;

– ключевого носителя, удовлетворяющего следующим требованиям:

– тип ключевого носителя включен в Перечень ключевых носителей, публикуемый на официальных сайтах ТОФК в разделе «Удостоверяющий центр»;

– ключевой носитель проинициализирован (отформатирован);

– на ключевом носителе имеется маркировка с учетным номером, присвоенным Заявителем.

3.5. Срок действия КЭП составляет максимально допустимый срок действия КЭП, установленный эксплуатационной документацией для используемого средства ЭП. Начало периода действия КЭП владельца сертификата исчисляется с даты и времени начала действия соответствующего сертификата.

3.6. Срок изготовления сертификата не должен превышать пяти рабочих дней с даты приема документов и сведений, представленных для создания сертификатов.

В случае превышения срока изготовления сертификата Заявитель, получатель сертификата, владелец сертификата информируется об этом в установленном порядке.

3.7. Информирование Заявителя, получателя сертификата, владельца сертификата производится в случаях, предусмотренных настоящим Регламентом, любым способом, удостоверяющим его получение, в том числе посредством доставки сообщения по электронной почте на адрес, указанный в Заявлении на сертификат и в сертификате.

До внесения информации об аннулировании сертификата в Реестр сертификатов ТОФК уведомляет Заявителя, владельца сертификата об аннулировании сертификата путем направления письма на бумажном носителе или в форме электронного документа, оформленного в соответствии с требованиями Инструкции по делопроизводству в ТОФК.

3.8. Информация об аннулированных, прекративших действие, приостановленных сертификатах размещается в виде САС на официальном сайте Федерального казначейства в информационно-телекоммуникационной

---

[1] Примерный образец представлен в приложении № 1 к настоящему Регламенту.

сети «Интернет» по адресу URL=http://crl.roskazna.ru/crl/ и актуализируется не реже двух раз в сутки.

4. Порядок выдачи средства ЭП и Средства создания запроса

4.1. Выдача средства ЭП, Средства создания запроса и эксплуатационной документации к ним производится во временное пользование по письменному обращению Заявителя с указанием фамилии, имени, отчества (при наличии) получающего лица в количестве соответствующему количеству получателей сертификатов, с приложением оптического носителя информации с возможностью однократной записи.

В случае расторжения Соглашения Заявитель возвращает ТОФК средство ЭП и эксплуатационную документацию к нему.

4.2. Выдача средства ЭП, Средства создания запроса и эксплуатационной документации к ним должна осуществляться не позднее трех рабочих дней с даты приема письменного обращения Заявителя и оптического носителя.

4.3. При выдаче средства ЭП и Средства создания запроса осуществляется идентификация лица, указанного в письменном обращении Заявителя, по документу, удостоверяющему личность.

4.4. Установка, настройка и эксплуатация средства ЭП, Средства создания запроса осуществляется Заявителем самостоятельно в соответствии с требованиями эксплуатационной документации к ним и законодательства Российской Федерации.

5. Порядок создания и выдачи сертификата

5.1. Заключение Соглашения осуществляется в соответствии с пунктом 3.3 настоящего Регламента.

5.2. Выдача средства ЭП и Средства создания запроса осуществляется в соответствии с пунктами 4.1–4.3 настоящего Регламента (при необходимости).

5.3. Создание КЭП и Запроса на сертификат производится получателем сертификата на АРМ Заявителя либо в присутствии Оператора УЦ на АРМ ТОФК.

Создание КЭП и Запроса на сертификат производится в условиях, исключающих нарушение конфиденциальности КЭП.

5.4. Формирование Заявления на сертификат.

Заявление на сертификат формируется Средством создания запроса или с использованием информационной системы «Удостоверяющий центр

Федерального казначейства» и при наличии технической возможности представляется посредством информационной системы «Удостоверяющий центр Федерального казначейства».

В случае отсутствия технической возможности Заявление на сертификат представляется на бумажном носителе.

5.5. Комплект документов и сведений, представляемых для создания сертификата (далее – Документы на создание сертификата):

– Заявление на сертификат;

– заверенная копия документа, удостоверяющего личность получателя сертификата[2];

– согласие получателя сертификата, уполномоченного лица на обработку персональных данных, содержащихся в копии документа, удостоверяющего личность, оформленное в соответствии с требованиями Закона о персональных данных;

– номер СНИЛС получателя сертификата[3];

– ИНН получателя сертификата;

– ОГРН юридического лица[4];

– ОГРН индивидуального предпринимателя;

– файл Запроса на сертификат на съемном носителе информации, не содержащем КЭП;

– документ или сведения, подтверждающие полномочия получателя сертификата, уполномоченного лица;

– документ или сведения (информация об официальном источнике опубликования и (или) общедоступных изданиях и информационных системах), подтверждающие полномочия лица, действующего от имени Заявителя.

Лицо, непосредственно представившее Документы на создание сертификата, в целях идентификации представляет оригинал документа, удостоверяющего его личность, с которого снимается копия, удостоверяемая подписями лица и Оператора УЦ.

С целью подтверждения сведений, указанных в абзацах 5 и 6 настоящего пункта, допускается представление страхового свидетельства государственного пенсионного страхования, свидетельства или уведомления о постановке на учет физического лица в налоговом органе, либо их заверенных копий.

---

[2] В случае представления Документов на создание сертификата непосредственно получателем сертификата копия документа, удостоверяющего личность, не представляется.

[3] Не представляется в случае получения сертификата, предназначенного для автоматического создания и (или) автоматической проверки электронных подписей в информационных системах, без указания фамилии, имени, отчества владельца сертификата.

[4] Представляется в случае получения сертификата юридического лица.

5.6. Прием и проверка Документов на создание сертификата.

При приеме Документов на создание сертификата осуществляется проверка:

– полноты комплекта Документов на создание сертификата;

– соответствия сведений, указанных в Заявлении на сертификат, сведениям в документах, указанных в пункте 5.5 настоящего Регламента;

– отсутствия в представленных Документах на создание сертификата исправлений, не заверенных в установленном порядке[5];

– заверения копий документов;

– соответствия значений полей электронной формы Запроса на сертификат значениям полей Заявления на сертификат;

– соответствия сведений, указанных в Документах на создание сертификата, информации, полученной с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие действующих и создаваемых информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме.

В случае отрицательного результата проверки Документы на создание сертификата возвращаются с мотивированным отказом в письменной форме.

В случае положительного результата проверки Документов на создание сертификата осуществляется создание сертификата.

5.7. Выдача сертификата.

Владельцу сертификата выдаются файл сертификата и Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи[6].

При получении сертификата владелец сертификата под расписку ознакамливается с информацией, содержащейся в сертификате.

Один экземпляр сертификата на бумажном носителе выдается владельцу сертификата.

При выдаче сертификата в ЕСИА направляются сведения о владельце сертификата в объеме, необходимом для регистрации в данной системе, и о полученном им сертификате (уникальный номер сертификата, даты начала и

---

[5] Исправления в Документах на создание сертификата на бумажном носителе оформляются путем зачеркивания тонкой чертой неправильного текста так, чтобы можно было прочитать зачеркнутое, и написания над зачеркнутым исправленного текста. Исправления в документе на бумажном носителе должны быть оговорены надписью «исправлено», подтверждено подписью тех же лиц, которые подписали документ, с проставлением даты исправления. Не допускается внесение изменений в Заявление на сертификат в части сведений, включенных в Запрос на сертификат.

[6] Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи представлено в приложении № 2 к настоящему Регламенту и выдается владельцу сертификата под подпись в соответствующем журнале.

окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра)[7].

6. Порядок смены сертификата

6.1. Смена сертификата осуществляется не ранее двадцати календарных дней до окончания срока его действия на основании обращения владельца сертификата по месту получения сертификата.

6.2. Процедура смены сертификата производится в порядке, предусмотренном пунктами 5.3–5.7 настоящего Регламента, при этом повторная выдача Руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи не производится.

В случае отсутствия изменений в ранее представленных подтверждающих документах их повторное представление не требуется.

7. Прекращение действия, аннулирование, приостановление и возобновление действия сертификата

7.1. Сертификат прекращает свое действие:

– по истечении срока действия;

– в случае прекращения осуществления Федеральным казначейством функций удостоверяющего центра без перехода его функций другим лицам;

– по инициативе ТОФК, в случае если стало известно об увольнении (отстранении от исполнения обязанностей) владельца сертификата, прекращении деятельности Заявителя или изменении его реквизитов, компрометации КЭП Оператора УЦ;

– по инициативе Заявителя на основании Заявления на изменение статуса сертификата[8]:

– в случае прекращения деятельности;

– в случае лишения владельца сертификата полномочий;

– в случае увольнения владельца сертификата;

– в случае изменения сведений, включенных в сертификат (при этом в течение пяти рабочих дней представляется соответствующее Заявление на изменение статуса сертификата с последующим осуществлением смены сертификата);

---

[7] По желанию владельца сертификата безвозмездно осуществляется его регистрация в ЕСИА.

[8] Образец представлен в приложении № 3 к настоящему Регламенту.

– в случае компрометации КЭП владельца сертификата;

– выхода из строя ключевого носителя, содержащего КЭП владельца сертификата, при отсутствии учтенных резервных ключевых носителей КЭП;

– в иных случаях по решению Заявителя.

Заявление на изменение статуса сертификата представляется в форме документа на бумажном носителе или в форме электронного документа[9].

В случае представления Заявления на изменение статуса сертификата уполномоченным лицом повторное представление документа, подтверждающего его полномочия, не требуется при наличии в ТОФК актуальной версии данного документа.

Заявление на изменение статуса сертификата проверяется на предмет соответствия реквизитов, указанных в Заявлении на изменение статуса сертификата, данным Реестра сертификатов.

В случае выявления несоответствия реквизитов, Заявление на изменение статуса сертификата возвращается с указанием причин отказа.

7.2. Аннулирование сертификата осуществляется в следующих случаях:

– не подтверждено, что владелец сертификата владеет КЭП, который соответствует КПЭП, указанному в таком сертификате;

– установлено, что содержащийся в таком сертификате КПЭП уже содержится в ином ранее созданном сертификате;

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

7.3. В течение двенадцати часов с момента наступления обстоятельств, указанных в пунктах 7.1 и 7.2 настоящего Регламента, или в течение двенадцати часов с момента, когда ТОФК стало известно или должно было стать известно о наступлении таких обстоятельств, соответствующая информация вносится в Реестр сертификатов, САС.

Действие сертификата прекращается с момента внесения записи об этом в Реестр сертификатов.

7.4. Приостановление действия сертификата осуществляется по инициативе Заявителя:

– в связи с длительным неисполнением обязанностей владельцем сертификата;

– в связи с возникновением разногласий между владельцем сертификата и ТОФК.

---

[9] При наличии технической возможности.

Приостановление действия сертификата производится на основании устного обращения владельца сертификата, в том числе по телефону[10], или посредством подачи Заявления на изменение статуса сертификата на бумажном носителе.

7.4.1. Приостановление действия сертификата по устному обращению владельца сертификата возможно исключительно при возникновении обстоятельств, требующих оперативного приостановления действия сертификата на период урегулирования возникших разногласий между владельцем сертификата и ТОФК.

При устном обращении владелец сертификата должен сообщить следующую информацию:

– фамилию, имя, отчество (если имеется) / наименование юридического лица владельца сертификата;

– уникальный номер сертификата;

– причину, по которой действие сертификата приостанавливается;

– ключевую фразу (кодовое слово).

Обращение в устной форме принимается к исполнению в случае совпадения информации, переданной в обращении, с информацией из Реестра сертификатов, и действие сертификата приостанавливается на срок, определенный в обращении, но не более чем на 10 рабочих дней.

Приостановление действия сертификата на основании устного обращения осуществляется в день обращения.

В срок, не превышающий 10 календарных дней с даты устного обращения, в ТОФК представляется Заявление на изменение статуса сертификата.

В случае непредставления Заявления на изменение статуса сертификата, в установленный срок, сертификат возобновляет действие, с информированием об этом владельца сертификата, Заявителя.

7.4.2. Приостановление действия сертификата на основании Заявления на изменение статуса сертификата осуществляется на срок не более 56 календарных дней и не менее 10 календарных дней.

В случае представления Заявления на изменение статуса сертификата уполномоченным лицом, повторное представление документа, подтверждающего его полномочия, не требуется при наличии в ТОФК актуальной версии данного документа.

При приеме Заявления на изменение статуса сертификата осуществляется:

---

[10] Телефонные обращения принимаются Операторами УЦ в соответствии с порядком, установленным ТОФК.

– идентификация лица, представившего Заявление на изменение статуса сертификата по документу, удостоверяющему личность;

– проверка корректности оформления и подписания Заявления на изменение статуса сертификата;

– проверка соответствия реквизитов, указанных в Заявлении на изменение статуса сертификата, данным Реестра сертификатов.

В случае отрицательного результата проверки Заявление на изменение статуса сертификата возвращается с указанием причины отказа.

В случае положительного результата проверки действие сертификата приостанавливается, о чем информируются Заявитель и владелец сертификата.

7.5. Возобновление действия сертификата осуществляется в отношении приостановленных сертификатов.

Возобновление действия приостановленного сертификата осуществляется на основании Заявления на изменение статуса сертификата и при условии, что срок, на который действие сертификата было приостановлено, не истек.

В случае представления Заявления на изменение статуса сертификата уполномоченным лицом, повторное представление документа, подтверждающего его полномочия, не требуется при наличии в ТОФК актуальной версии данного документа.

При приеме Заявления на изменение статуса сертификата осуществляется:

– идентификация лица, представившего Заявление на изменение статуса сертификата по документу, удостоверяющему личность;

– проверка корректности оформления и подписания Заявления на изменение статуса сертификата;

– проверка соответствия реквизитов, указанных в Заявлении на изменение статуса сертификата, данным Реестра сертификатов.

В случае отрицательной проверки, Заявление на изменение статуса сертификата отклоняется с указанием причин возврата.

В случае положительного результата проверки действие приостановленного сертификата возобновляется с информированием Заявителя и владельца сертификата.

Возобновление действия сертификата либо отказ в возобновлении действия сертификата, включая информирование, осуществляется в течение одного рабочего дня, следующего за днем принятия Заявления на изменение статуса сертификата.

8. Порядок предоставления информации о статусе сертификата

8.1. Информация о статусе сертификата предоставляется на основании Заявления о статусе сертификата[11], представленного на бумажном носителе.

Заявление о статусе сертификата проверяется на предмет соответствия реквизитов, указанных в Заявлении о статусе сертификата, данным Реестра сертификатов.

В случае положительного результата проверки информация о статусе сертификата формируется и направляется в виде Справки о статусе сертификата.

В случае отрицательного результата проверки Заявление о статусе сертификата возвращается с указанием причины отказа.

Справка о статусе сертификата должна содержать следующие сведения: уникальный номер, сведения о владельце сертификата, статус сертификата на запрошенный момент времени.

Представление Справки о статусе сертификата должно быть осуществлено не позднее 7 рабочих дней с даты официальной регистрации Заявления о статусе сертификата.

---

[11] Образец представлен в приложении № 4 к настоящему Регламенту.

Приложение № 1
к Регламенту
Удостоверяющего центра
Федерального казначейства,
утвержденному приказом
Федерального казначейства
от «31» июля 2015 г. № 197

ДОГОВОР ПРИСОЕДИНЕНИЯ (СОГЛАШЕНИЕ) № _____
К РЕГЛАМЕНТУ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
ФЕДЕРАЛЬНОГО КАЗНАЧЕЙСТВА

г. _____ «__» _____ 20__г.

_____, в лице _____, действующего на основании _____, именуемое в дальнейшем «Орган ФК», с одной стороны, и _____
(наименование юридического лица, ФИО индивидуального предпринимателя,

_____,
ФИО лица, действующего от имени юридического лица (индивидуального предпринимателя), документ,

_____,
подтверждающий его полномочия)

именуем____ в дальнейшем «Заявитель», с другой стороны, вместе именуемые «Сторонами», заключили настоящий договор (далее – Соглашение) о нижеследующем.

I. Предмет Соглашения

1.1. Предметом настоящего Соглашения является присоединение Заявителя в порядке статьи 428 Гражданского кодекса Российской Федерации к Регламенту Удостоверяющего центра Федерального казначейства (далее – Регламент).

II. Права, обязанности и ответственность Сторон

2.1. Права, обязанности и ответственность Сторон определяются Регламентом и настоящим Соглашением.

III. Заключительные положения

3.1. Настоящее Соглашение вступает в силу с даты его подписания Сторонами и действует до его расторжения по основаниям,

предусмотренным законодательством Российской Федерации, или по решению любой из Сторон, подписавших Соглашение, в одностороннем внесудебном порядке.

IV. Адреса и реквизиты Сторон

Орган Федерального казначейства: Заявитель:

Приложение № 2
к Регламенту
Удостоверяющего центра
Федерального казначейства,
утвержденному приказом
Федерального казначейства
от «31» июля 2015 г. № 197

Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

1. Общие положения

Настоящее руководство составлено в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и является средством официального информирования лиц, владеющих квалифицированной электронной подписью, об условиях, рисках и порядке использования квалифицированной электронной подписи и средств электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи.

При применении квалифицированной электронной подписи в информационных системах владельцу сертификата необходимо выполнять требования:

– Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13.06.2001 № 152, в части обращения со средствами криптографической защиты информации;

– Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 09.02.2005 № 66, в части эксплуатации средств криптографической защиты информации;

– эксплуатационной документации к средствам электронной подписи;

– приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

2. Требования по размещению

При размещении средств вычислительной техники с установленными на них средствами квалифицированной электронной подписи:

– должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства квалифицированной электронной подписи, посторонним лицам, не имеющим допуск к работе в

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

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

3. Требования по установке средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

3.1. При использовании средств квалифицированной электронной подписи должны выполняться следующие меры по защите информации от несанкционированного доступа:

3.1.1. Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

– длина пароля должна быть не менее 6 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, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);

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

– личный пароль пользователь не имеет права никому сообщать;

– периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

3.1.2. При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

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

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

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

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

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

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

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

– необходимо предусмотреть меры, максимально ограничивающие доступ к:

– системному реестру;

– файлам и каталогам;

– временным файлам;

– журналам системы;

– файлам подкачки;

– кэшируемой информации (пароли и т.п.);

– отладочной информации.

3.1.3. На средствах вычислительной техники необходимо:

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

– исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;

– регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

3.1.4. В случае подключения технических средств с установленными средствами квалифицированной электронной подписи к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

3.1.5. Необходимо организовать и использовать:

– систему аудита, организовать регулярный анализ результатов аудита.

– комплекс мероприятий по антивирусной защите.

3.2. Запрещается:

– осуществлять несанкционированное копирование ключевых носителей;

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации;

– использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;

– вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;

– записывать на ключевые носители постороннюю информацию;

– оставлять средства вычислительной техники с установленными средствами квалифицированной электронной подписи без контроля после ввода ключевой информации;

– использовать ключ электронной подписи и соответствующий сертификат ключа проверки электронной подписи, Заявление на изменение статуса которого подано в территориальный орган Федерального казначейства, в течение времени, исчисляемого с момента подачи Заявления на изменение статуса сертификата по момент официального информирования об изменении статуса сертификата, либо об отказе в изменении статуса;

– использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;

– удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки электронной подписи.

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

4.1. Меры защиты ключей квалифицированной электронной подписи

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

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

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи.

4.2. Обращение с ключевой информацией и ключевыми носителями

Недопустимо пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме открытых ключей).

Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными

средствами квалифицированной электронной подписи, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

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

Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

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

4.3. Обеспечение безопасности АРМ с установленными средствами квалифицированной электронной подписи

С целью контроля исходящего и входящего подозрительного трафика, технические средства с установленными средствами квалифицированной электронной подписи должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. На технических средствах, используемых для работы в информационных системах:

– на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 3;

– должно быть установлено только лицензионное программное обеспечение;

– должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;

– должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);

– должны регулярно устанавливаться обновления операционной системы;

– должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами квалифицированной электронной подписи и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в соответствующей информационной системе;

– должна быть активирована регистрация событий информационной безопасности;

– должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

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

Приложение № 3
к Регламенту
Удостоверяющего центра
Федерального казначейства,
утвержденному приказом
Федерального казначейства
от «31» июля 2015 г. № 197

Заявление
на изменение статуса
сертификата ключа проверки электронной подписи

_____ «__»_____ 20__г.
(наименование населенного пункта) *(дата)*

_____

_____
(полное наименование Заявителя)

в лице* _____
(ФИО лица, действующего от имени Заявителя)

действующего на основании* _____

_____

в связи с _____
(указать причину)

просит приостановить/возобновить/прекратить (*нужное подчеркнуть*) действие квалифицированного сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата _____
Фамилия, имя, отчество _____
Наименование организации _____
ОГРН, ИНН, ОГРНИП _____
СНИЛС _____
E-mail _____

с _____ по _____**

_____ « » 20 г. ***
(подпись) *(фамилия, инициалы владельца сертификата)*

_____ « » 20 г.
(подпись) *(фамилия, инициалы лица, действующего от имени Заявителя)*

Заполняется Оператором УЦ

№ транзакции _____ *Дата регистрации* _____

_____ /_____
(должность Оператора УЦ) *(подпись Оператора УЦ)* *(ФИО)*

№	*Действие*	*Дата, время*	*Код причины*	*Примечание*
1	*Сертификат прекратил действие*			
2	*Сертификат*			

	приостановлен			
3	*Сертификат возобновлен*			
4	*В прекращении действия отказано*			

* Не заполняется при обращении индивидуального предпринимателя.

** Заполняется в случае приостановления действия сертификата.

*** В случае увольнения владельца сертификата может не заполняться.

Приложение № 4
к Регламенту
Удостоверяющего центра
Федерального казначейства,
утвержденному приказом
Федерального казначейства
от «31» июля 2015 г. № 197

Заявление на получение информации о статусе сертификата ключа проверки электронной подписи

_____ «__»_____ 20__г.
(наименование населенного пункта) (дата)

_____

_____
(полное наименование Заявителя)

в лице* _____
(ФИО лица, действующего от имени Заявителя)

действующего на основании* _____

_____

в связи с _____
(причина проверки статуса сертификата)

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

Серийный номер сертификата _____
Фамилия, имя, отчество _____
Наименование организации _____
ОГРН, ИНН организации _____
СНИЛС _____

в период с __ часов __минут __.__.20__г. по __часов __ минут __.__.20__г.

Справку необходимо предоставить по адресу: _____

_____
(почтовый адрес получателя (включая индекс) либо e-mail)

_____ / _____ / _____
(лицо, действующее от имени Заявителя) *(подпись)* *(Фамилия И.О.)*

М.П. «__»_____ 20__г.

* Не заполняется при обращении индивидуального предпринимателя.