ЗАКОН

РЕСПУБЛИКИ ТАДЖИКИСТАН

Об электронной цифровой подписи

(в редакциии Закона от 21.07.2010г.№628,

от 25.03.2011г.№699)

Настоящий Закон регулирует общественные отношения в сфере создания и применения электронной цифровой подписи в процессе формирования и использования документов в электронной форме отображения с помощью автоматизированных информационных и телекоммуникационных систем и программнотехнических средств.

Глава 1. Общие положения

Статья 1. Сфера действия настоящего Закона

Положения настоящего Закона распространяются на электронные документы идентифицируемые посредством электронной цифровой подписи органов государственной власти Республики Таджикистан (кроме документов о контрразведывательной, разведывательной и оперативнорозыскной деятельности, использовании криптографических и оперативных мер защиты государственной тайны), а также физических и юридических лиц Республики Таджикистан, при совершении гражданско -правовых сделок и в других предусмотренных законодательством Республики Таджикистан случаях.

Целью настоящего Закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи В документе на бумажном носителе.

Действие настоящего Закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Статья 2. Основные понятия

В настоящем Законе используются следующие понятия:

- электронный документ - документ, в котором информация представлена в электронной цифровой форме;

- машинный носитель - магнитный диск, магнитная лента, лазерный диск и иные материальные носители, используемые для записи и хранения информации с помощью электронно-вычислительной техники;

- электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации, в электронном документе;

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

- закрытый ключ электронной цифровое подписи - последовательность символов, известная владельцу сертификата ключа подписи

- открытый ключ электронной цифровой подписи - последовательность символов электронной - цифровой подписи, доступная любому пользователю, предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе;

- сертификат средств электронной цифровой подписи - документ на бумажном носителе, выданный в соответствии; с правилами системы сертификатизации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;

- сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца-сертификата ключа подписи;

- сертификат открытого ключадокумент подтверждающий соответствие этого открытого ключа закрытому ключу, выданный центром регистрации открытых ключей владельцу закрытого ключа электронной цифровой подписи или его полномочному представителю;

- подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой, подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе;

- владелец сертификата ключа подписи,физическое лицо, на имя которого удостоверяющим центром выдан сертификат, ключа подписи и который владеет соответствующим закрытым ключом электронной цифровой подписи позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах;

- пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;

- информационная система общего пользования - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано;

- корпоративная информационная системаинформационная система ограниченного круга лиц, определяемой ее владельцем или соглашением участников этой информационной системы;

- электронные данные (электронное сообщение) - электронное представление любой информации, воспринимаемой электронной вычислительной машиной;

- центр сертификации открытых ключей электронно-цифровой подписи (далее - удостоверяющий центр)юридическое лицо, обладающее правомочиями на удостоверение соответствия открытого ключа электронной цифровой подписи закрытому, ключу электронной цифровой подписи на чье имя выдано регистрационное свидетельство (владелец свидетельства);

- уполномоченный орган - государственный орган, осуществляющий реализацию государственной политики в сфере обеспечения охраны государственных секретов и технической защиты информации Республики Таджикистан(в редакции Закона РТ от 21.07.2010г.№628);

- подписывающее лицо - физическое и юридическое лицо, правомерно владеющее, электронно-цифровой подписью и обладающее правом ее использования на электронном документе;

- проверка подлинности электронной цифровой подписи последовательность действий, при которой лицо, получившее электронное сообщение, подписанное электронной цифровой подписью, и открытый ключ подписавшего лица, может определить: было ли это сообщение подписано с использованием закрытого ключа, соответствующего открытому ключу подписавшего лица, и были ли изменены исходные данные после создания электронной цифровой подписи.

Статья 3. Законодательство Республики Таджикистан об электронной цифровой подписи

Законодательство Республики Таджикистан об электронно-цифровой подписи основывается на Конституции Республики Таджикистан и состоит из настоящего Закона, других нормативных правовых актов Республики Таджикистан, а также международных правовых актов, признанных Таджикистаном.

Статья 4. Субъекты правоотношений в сфере использования электронной цифровой подписи

Субъектами правоотношений в сфере обращения электронной цифровой подписи выступает государство в лице органов государственной власти, физические и юридические лица, а также зарубежные государства, международные организации, иностранные юридические лица и лица без гражданства.

Отношения между субъектами в сфере обращения электронных документов регулируются договорами в соответствии с порядком, установленном законодательством Республики Таджикистан.

Глава 2. Условия использования электронной цифровой подписи

Статья 5. Условия признания равнозначности электронной цифровой подписи, в электронном документе к собственноручной подписи на бумажном носителе

Электронная цифровая подпись в электронном документе юридически равнозначна собственноручной подписи в документе на бумажном носителе при одновременном выполнении следующих условий:

- сертификат ключа, электронной цифровой подписи, относящийся к этой электронной цифровой подписи не утратил силу;

- подтверждена подлинность электронной; цифровой подписи в электронном документе;

- электронная цифровая подпись используется в отношениях, в которых она имеет юридическое значение.

Пользователь информационной системы может быть обладателем любого количества сертификатов ключей подписей, имеющих одинаковое или различное юридическое значение, в зависимости от правоспособности их обладателя в отношениях, в которых они используются. Необходимые сведения, связанные с юридическим, значением использования каждой электронной цифровой подписи, приводятся в соответствующих сертификатах ключей подписей.

Статья 6. Средства электронной цифровой подписи

Создание ключей электронных цифровых подписей осуществляется для использования в информационной системе общего пользования ее участником или по его обращению удостоверяющим центром -корпоративной информационной системе в порядке, установленном в этой системе.

При создании ключей электронных цифровых подписей для использования в информационной системе общего пользования должны применяться только сертифицированные средства электронной цифровой подписи. Возмещение убытков, причиненных в связи с созданием ключей электронных

цифровых подписей не сертифицированными средствами электронной цифровой подписи, должно быть возложено на создателей и распространителей этих средств в соответствии с. законодательством Республики Таджикистан.

Использование не сертифицированных средств электронной цифровой подписи и созданных ими ключей электронных, цифровых подписей в корпоративных информационных системах Республики Таджикистан не допускается. Сертификация средств электронной цифровой подписи осуществляется в соответствии с законодательством Республики Таджикистан. Средства электронной цифровой подписи не являются средствами шифрования информации и подлежат обязательной сертификации в соответствии с законодательством Республики Таджикистан.

Средства электронной цифровой подписи должны обеспечить:

- уникальность создаваемых закрытых и открытых ключей;

- необходимую вычислительную сложность определения закрытого ключа и цифровой подписи;

- конфиденциальность закрытого ключа подписи;

- открытый ключ электронной цифровой подписи;

- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;

- наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;

- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

В случае необходимости, в сертификате ключа электронной цифровой подписи, на основании подтверждающих документов указываются должность (с указанием наименования и места нахождения организации, в которой установлена эта должность) и квалификация владельца сертификата ключа подписи, а по его заявлению в письменной форме иные сведения, подтверждаемые соответствующими документами.

Статья 7. Проверка подлинности электронной цифровой подписи

Проверка подлинности электронной цифровой подписи осуществляется сертифицированными средствами электронной цифровой подписи с использованием сертификата открытого ключа подписи составителя, подписавшего электронный документ.

Статья 8. Закрытые и открытые ключи электронной цифровой подписи

Закрытые и открытые ключи электронной цифровой подписи создаются физическими лицами.

Физическое лицо самостоятельно создает закрытые и открытые ключи с применением средств электронной цифровой подписи.

Создание закрытого- ключа и связанного с ним открытого ключа производится одновременно. Физическое лицо может быть владельцем любого количества закрытых и открытых ключей электронной цифровой подписи

Закрытый ключ электронной цифровой подписи хранится и используется исключительно его владельцем, чтобы исключить доступ к нему другого лица.

Открытый ключ электронной, цифровой подписи хранится в удостоверяющем центре и является доступным для всех субъектов электронного документооборота.

Глава 3. Удостоверяющий центр и сертификационные услуги по электронной цифровой подписи

Статья 9. Правовой статус удостоверяющего центра

Удостоверяющий центр является юридическим лицом, оказывающим услуги по сертификации открытых ключей электронной цифровой подписи и иные виды услуг, связанные с электронной цифровой подписью.

Лицензирование деятельности по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей осуществляется в соответствии с Законом Республики Таджикистан "О лицензировании отдельных видов деятельности".

Деятельность центров по сертификации открытых электронных ключей юридических лиц, созданных с корпоративными целями, и не предоставляющих услуги по сертификации электронных цифровых ключей третьим лицам не лицензируется.

Требования, предъявляемые к материальным и финансовым возможностям удостоверяющих центров, определяются Правительством Республики Таджикистан по представлению уполномоченного органа.

Государственная регистрация удостоверяющих центров осуществляется в соответствии с Законом Республики Таджикистан "О государственной регистрации юридических лиц и индивидуальных предпринимателей" (в редакции Закона РТ от 25.03.2011г.№699)

Статья 10. Осуществление деятельности удостоверяющего центра

Удостоверяющий центр осуществляет свою деятельность при наличии следующих условий:

- обладать соответствующими финансовыми, материальными, техническими и социальными ресурсами для обеспечения безопасности, надежности и непрерывности услуг по сертификации открытых ключей электронной цифровой подписи, а также для покрытия ущерба, который они могли бы нанести в связи с предоставлением данных услуг;

- сертифицировать открытый ключ, подписи уполномоченного лица центра, предназначенный для сертификации открытых ключей, в установленном законодательством порядке;

- обеспечивать надежную и оперативную регистрацию информации в реестре сертификатов открытых ключей, в частности, оперативное предоставление услуг по приостановлению действия, и отзыву сертификатов открытых ключей;

- обеспечивать возможность определения даты и времени выдачи, приостановления действия или отзыва сертификата открытого ключа;

- располагать персоналом, обладающим квалификацией, необходимой для предоставления услуг по сертификации открытых ключей;

- соблюдать требования законодательства и принимать необходимые меры по обеспечению безопасности и защите информации;

- хранить всю информацию о сертификате открытого ключа подписи не менее 3 лет с момента отзыва сертификата на случай возникновения спора;

- соответствовать другим специальным условиям, установленным уполномоченным органом.

Основные требования по обеспечению безопасности информационных и телекоммуникационных систем удостоверяющих центров, использованию ими средств криптографической и технической защиты информации устанавливаются уполномоченным органом.

Статья 11. Права и обязанности удостоверяющего центра

Удостоверяющий центр имеет право:

- создавать и выдавать сертификаты открытых ключей электронной цифровой подписи;

- приостанавливать и возобновлять действие сертификатов открытых ключей, а также имеет право на их отзыв с внесением соответствующих изменений в реестр сертификатов ключей подписей;

- оказывать на договорной, основе иные виды услуг, связанные с электронной подписью;

- может предоставлять участникам информационных систем иные, связанные с использованием электронных цифровых подписей, услуги.

Удостоверяющий центр обязан:

- убедиться в достоверности данных, указанных в заявке на сертификацию открытого ключа, на основании документов, подтверждающих указанные данные

- обеспечить соответствие информаций содержащейся в сертификате ключа информации, представленной владельцем сертификата, открытого ключа подписи;

- вести реестр сертификатов открытых ключей электронных цифровых подписей, обеспечивать его актуализацию и свободный доступ к нему, включить сертификат ключа в реестр сертификатов открытых ключей не позднее чем за один день до начала срока действия сертификата;

- проверять уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;

- обеспечить свободный доступ к реестру сертификатов ключей подписи;

- уведомить владельца сертификата закрытого ключа о ставших известными удостоверяющему центру фактах, указывающих на невозможность дальнейшего использования закрытого ключа, а также об отзыве сертификата закрытого ключа;

- предоставлять имеющуюся информацию, необходимую для подтверждения подлинности электронной цифровой подписи;

- осуществлять также и другие обязанности в соответствии с настоящим Законом и иными нормативными правовыми актами Республики Таджикистан или предусмотренными соглашениями сторон.

Статья 12. Отношения между удостоверяющим центром и уполномоченным органом

Удостоверяющий центр до начала использования электронной цифровой подписи уполномоченным лицом удостоверяющего центра для заверения от имени удостоверяющего центра сертификатов ключей подписей обязан представить в уполномоченный орган Правительства Республики Таджикистан сертификат ключа подписи уполномоченного лица удостоверяющего центра в форме электронного документа, а также этот сертификат в форме документа на бумажном носителе с собственноручной подписью указанного уполномоченного лица, заверенный подписью руководителя и печатью удостоверяющего центра.

Уполномоченный орган ведет единый государственный реестр сертификатов ключей, подписей, которыми удостоверяющие центры, работающие с участниками информационных систем общего пользования, заверяют выдаваемые ими сертификаты ключей подписей, обеспечивает возможность свободного доступа к этому реестру и выдает сертификаты ключей подписей соответствующих, уполномоченных лиц удостоверяющих центров.

Электронные цифровые подписи уполномоченных лиц удостоверяющих центров могут использоваться только после включения их в единый государственный реестр, сертификатов, ключей, подписей. Использование этих электронных цифровых подписей для целей, не связанных с заверением сертификатов ключей подписей и сведений об их действии, не допускается.

Уполномоченный орган;

- осуществляет по обращениям физических и юридических лиц, органов государственной власти и органов местного самоуправления поселка и села подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;

- осуществляет в соответствии с Положением об уполномоченном органе иные полномочия по обеспечению настоящего Закона.

Статья 13. Прекращение деятельности удостоверяющего центра

Деятельность удостоверяющего центра, выдающего сертификаты ключей подписей для использования в информационных, системах общего пользования, может быть прекращена в порядке установленном Гражданским кодексом Республики Таджикистан.

В случае прекращения деятельности в качестве удостоверяющего центра юридическое лицо обязано в течение не менее двух месяцев до прекращения своей деятельности проинформировать об этом всех участников обслуживаемых, им систем электронного документооборота и уполномоченный орган.

Сведения об открытых ключах, принадлежащих участникам электронного документооборота, и иная информация удостоверяющего центра подлежат хранению в порядке, установленном законодательством Республики Таджикистан.

Глава 4. Сертификат ключа электронной цифровой подписи

Статья 14. Сертификат ключа электронной цифровой подписи

Сертификат ключа электронной цифровой подписи должен содержать следующие сведения:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;

- фамилия, имя и отчество или имя владельца сертификата ключа подписи или его псевдоним. В случае, использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи;

- открытый ключ электронной цифровой подписи;

- наименование средств электронной цифровой подписи, с которыми используется данный, открытый ключ электронной подписи;

- наименование и место нахождения удостоверяющего центра, выдавшего сертификат открытого ключа подписи;

- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

В случае необходимости, в сертификате ключа подписи на основании подтверждающих документов указываются должность (с указанием наименования и места нахождения организации, в которой установлена эта должность) и квалификация сертификата ключа подписи, а по его заявлению в письменной форме иные сведения, подтверждаемые соответствующими документами.

Сертификат ключа подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей подписей, не позднее чем за один день до начала срока действия сертификата ключа подписи.

Для проверки принадлежности электронной цифровой подписи соответствующей их владельцу, сертификат ключа подписи выдается пользователям с указанием даты и времени его выдачи, сведений о действии сертификата ключа подписи (действует, действие приостановлено, сроки приостановления его действия, аннулирован, дата и время аннулирования сертификата ключа подписи) и сведений о реестре сертификатов ключей подписей. В случае выдачи сертификата ключа подписи в форме документа на бумажном носителе этот сертификат оформляется на бланке удостоверяющего центра и заверяется собственноручной подписью уполномоченного лица и печатью удостоверяющего центра.

В случае выдачи сертификата ключа подписи и указанных дополнительных данных в форме электронного документа этот сертификат должен быть подписан электронной цифровой подписью уполномоченного лица удостоверяющего центра.

Статья 15. Срок и порядок хранения сертификата ключа подписи в удостоверяющем центре

Срок хранения сертификата ключа подписи в форме электронного документам на бумажном носителе в удостоверяющем центре определяется договором между удостоверяющим центром и владельцем сертификата ключа подписи. При этом обеспечивается доступ участников информационной системы в удостоверяющий центр для получения сертификата ключа подписи.

Срок хранения сертификата ключа подписи в форме электронного ключа на бумажном носителе в удостоверяющем центре после аннулирования сертификата ключа подписи должен быть установлен до трех лет.

По истечении указанного срока хранения сертификат ключа подписи исключается из реестра сертификатов ключей подписей и переводится в режим архивного хранения. Срок архивного хранения составляет три года. Порядок выдачи копий сертификатов ключей подписей в этот период устанавливается в соответствии с законодательством Республики Таджикистан.

Сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательством Республики Таджикистан.

Статья 16. Изготовление сертификата ключа подписи

Изготовление сертификата ключа подписи осуществляется на основании заявки участника информационной системы, которое содержит сведения, указанные в статье 14 настоящего Закона и необходимые для идентификации владельца сертификата ключа подписи и передачи ему сообщений. Заявка подписывается собственноручно владельцем сертификата ключа подписи. Содержащиеся в заявке сведения подтверждаются предъявлением соответствующих документов.

Статья 17. Сертификат открытого ключа

При создании сертификата открытого ключа электронной цифровой подписи удостоверяющий центр обязан проверить уникальность открытого ключа электронной цифровой подписи.

Сертификат открытого ключа должен также содержать следующие сведения:

- отдельный уникальный регистрационный номер сертификата открытого ключа;

- идентификационные данные удостоверяющего центра, выдавшего сертификат открытого ключа;

- фамилию и имя пользователя сертификата открытого ключа;

- другие идентификационные данные пользователя сертификата открытого ключа в зависимости от целей, для которых выдастся сертификат, а также информацию, необходимую для передачи ему сообщений;

- открытый ключ;

- даты начала и окончания срока действия сертификата открытого ключа;

- данные о криптографическом алгоритме электронной подписи;

- при необходимости ограничения по использованию сертификата открытого ключа или ограничения стоимости сделок, в которых он может использоваться;

- другие сведения, установленные уполномоченным органом.

Сертификат открытого ключ а подписывается электронной подписью уполномоченного лица удостоверяющего центра.

В случаях, установленных законодательством или соглашением сторон, удостоверяющий центр создает сертификат открытого ключа и в виде документа на бумажном носителе в двух экземплярах. В этом случае сертификат открытого ключа в виде документа на бумажном носителе подписывается собственноручными подписями владельца сертификата открытого ключа и уполномоченного лица удостоверяющего центра и заверяется печатью центра. Один экземпляр сертификата открытого ключа передается его владельцу, а другой хранится в удостоверяющем центре.

Удостоверяющий центр по согласованию с владельцем сертификата открытого ключа может указать в сертификате открытого ключа ограничения по

использованию данного сертификата, а также случаи, в которых он может использоваться.

По обращению владельца сертификата открытого ключа удостоверяющий центр может указать в сертификате открытого ключа и другие сведения, не предусмотренные частью 2 настоящей статьи, при условии, что они не противоречат законодательству, не представляют угрозу безопасности или общественному порядку, и только после предварительной проверки точности этих сведений.

Удостоверяющий центр вносит этот сертификат в свой реестр не позднее даты начала действия сертификата ключа подписи.

Реестр сертификатов открытых ключей должен содержать:

- действительные сертификаты открытых ключей;

- отозванные сертификаты открытых ключей;

- дату и время выдачи сертификатов открытых ключей;

- дату и время отзыва сертификатов открытых ключей;

- другую необходимую информацию.

В целях осуществления проверки подлинности цифровой подписи удостоверяющий центр открытых ключей обязан обеспечивать свободный доступ к реестру сертификатов открытых ключей, в том числе в режиме реального времени.

Статья 18. Сроки действия и хранения сертификата открытого ключа

Срок действия сертификата открытого ключа устанавливается удостоверяющим центром, и не может составлять более пяти лет.

Срок хранения сертификата, открыто го ключа, в форме электронного документа в удостоверяющем центре определяется договором между удостоверяющим центром и владельцем сертификата открытого ключа.

Статья 19. Приостановление и аннулирование сертификата открытого ключа

Удостоверяющий центр вправе приостанавливать действие сертификата открытого ключа подписи на срок не более двух рабочих дней по указанию владельца сертификата или его уполномоченного представителя если иное не предусмотрено по согласованию между уполномоченным органом и владельцем сертификата открытого ключ;

Удостоверяющий центр обязан аннулировать сертификат открытого ключа в следующих случаях:

- по истечении срока действия сертификата открытого ключа;

- по требованию владельца сертификата открытого ключа;

- при обнаружении недостоверности сведений, указанных в заявке на сертификацию открытого ключа или в сертификате открытого ключа;

- по решению уполномоченного органа;

- по истечении срока, на который было приостановлено действие сертификата открытого ключа;

- при внесении изменений в сертификат открытого ключа;

- в случае смерти владельца сертификата открытого ключа или признания его недееспособным;

- в других установленных уполномоченным органом случаях согласно процедурам обеспечения безопасности и сертификации открытых ключей.

В случае аннулирования сертификата открытого ключа удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты и времени аннулирования сертификата открытого ключа, за исключением случаев аннулирования сертификата открытого ключа по истечении срока его действия, а также извещает об этом владельца сертификата открытого ключа и полномочное лицо (орган), от которого получено указание об аннулировании сертификата открытого ключа.

Статья 20. Обязательства владельца сертификата открытого ключа

Владелец сертификата открытого ключа обязан:

а) обеспечить необходимые условия для исключения доступа другого лица к своему закрытому ключу;

б) не использовать для создания электронной цифровой подписи закрытый ключ при имеющихся основаниях полагать, что нарушена конфиденциальность закрытого ключа;

в) незамедлительно требовать приостановление действия или отзыв сертификата открытого ключа в случае:

- утери закрытого ключа;

- имеющегося основание полагать, что нарушена конфиденциальность закрытого ключа;

- несоответствия содержащейся в сертификате открытого ключа информации действительности;

- своевременно уведомлять удостоверяющий центр о каких либо изменениях информации, содержащейся в сертификате открытого ключа;

г) выполнять другие обязанности, установленные настоящим Законом и договором с удостоверяющим центром.

Глава 5. Особенности использования электронной

цифровой подписи

Статья 21. Использование электронной цифровой подписи в сфере государственного управления

Органы государственной власти Республики Таджикистан, а также организации, участвующие в документообороте с указанными органами, используют для подписания своих электронных документов электронные цифровые подписи уполномоченных лиц указанных органов, организаций.

Сертификаты ключей электронных цифровых подписей уполномоченных лиц органов государственной власти включаются в реестр сертификатов ключей электронных цифровых подписей, который ведется уполномоченным органом, и выдаются пользователям сертификатов ключей электронных цифровых подписей из этого реестра в порядке, установленном настоящим Законом, для удостоверяющих центров.

Порядок организации и выдачи сертификатов ключей электронных цифровых подписей уполномоченных лиц органов государственной власти устанавливается нормативными правовыми актами соответствующих органов.

Статья 22. Использование электронной цифровой подписи в корпоративной информационной системе

Корпоративная информационная система, предоставляющая участникам информационной системы общего пользования услуги удостоверяющего центра корпоративной информационной системы, должна соответствовать требованиям, установленным настоящим Законом для информационных систем общего пользования.

Порядок использования электронных цифровых подписей в корпоративной информационной системе устанавливается решением владельца корпоративной информационной системы или соглашением участников этой системы.

Содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов ключей подписей, порядок хранения аннулированных сертификатов ключей подписей, случаи утраты указанными сертификатами юридической силы в корпоративной информационной системе регламентируются решением владельца этой системы или соглашением участников корпоративной информационной системы.

Статья 23. Признание иностранного сертификата ключа подписи

Признание иностранных сертификатов ключей электронной цифровой подписи осуществляется в соответствии с действующим законодательством Республики Таджикистан и международными договорами, признанными Таджикистаном.

Международные договоры Республики Таджикистан применяются к отношениям указанным в части первой настоящей статьи, непосредственно, кроме случаев, когда из международного договора следует, что для его применения требуется издание внутригосударственного акта.

Если международным договором Республики Таджикистан установлены иные правила, чем те, которые предусмотрены настоящим Законом, применяются правила международного договора.

Глава 6. Заключительные положения

Статья 24. Ответственность за нарушение настоящего Закона

Физические и юридические лица, виновные в нарушении настоящего Закона, несут ответственность в соответствии с законодательством Республики Таджикистан.

Статья 25. Порядок введения в действие настоящего Закона

Настоящий Закон ввести в действие после его официального опубликования.

Президент

Республики Таджикистан Э.Рахмонов

г. Душанбе

30 июля 2007 года № 320

ПОСТАНОВЛЕНИЕ МАДЖЛИСИ НАМОЯНДАГОН

МАДЖЛИСИ ОЛИ РЕСПУБЛИКИ ТАДЖИКИСТАН

О принятии Закона Республики Таджикистан

"Об электронной цифровой подписи"

Маджлиси намояндагон Маджлиси Оли Республики Таджикистан постановляет:

Принять Закон Республики Таджикистан "Об электронной цифровой подписи".

Председатель Маджлиси намояидагон

Маджлиси Оли Республики Таджикистан С.Хайруллоев

г. Душанбе,

28 июня 2007 года №708

ПОСТАНОВЛЕНИЕ МАДЖЛИСИ МИЛЛИ

МАДЖЛИСИ ОЛИ РЕСПУБЛИКИ ТАДЖИКИСТАН

О Законе Республики Таджикистан "Об электронной цифровой подписи"

Рассмотрев Закон Республики Таджикистан "Об электронной цифре подписи", Маджлиси милли Маджлиси Оли Республики Таджикистан постановляет:

Одобрить Закон Республики Таджикистан "Об электронной подписи".

Председатель Маджлиси милли

Маджлиси Оли Республики Таджикистан М.Убайдуллоев

г.Душанбе,

19 июля 2007 года №391