**Об электронной цифровой подписи**

**Проект федерального закона**

Одобрен на заседании Правительства 22.03.01

Вносится Правительством Российской Федерации

Проект

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

Об электронной цифровой подписи

**Глава I. Общие положения**

**Статья 1. Цель и сфера применения настоящего Федерального закона**

1. Целью настоящего Федерального закона является обеспечение правовых условий для использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается юридически равнозначной собственноручной подписи человека (гражданина или индивидуального органа юридического лица) в документе на бумажном носителе.

2. Действие настоящего Федерального закона распространяется на отношения, возникающие в связи с использованием электронной цифровой подписи гражданами, организациями, государственными органами и органами местного самоуправления.

**Статья 2.Правовое регулирование отношений в области использования электронной цифровой подписи**

Правовое регулирование отношений в области использования электронной цифровой подписи осуществляется в соответствии с настоящим Федеральным законом, Федеральным законом "Об информации, информатизации и защите информации", другими федеральными законами, принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, а в случаях регулирования этих отношений договором - также по соглашению сторон.

**Статья 3. Понятия, используемые в настоящем Федеральном законе**

В настоящем Федеральном законе используются следующие понятия:

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

электронная цифровая подпись (ЭЦП) - реквизит электронного документа, защищенный от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП, позволяющий установить отсутствие утраты, искажения или подделки содержащейся в электронном документе информации, а также обладателя электронной цифровой подписи;

обладатель электронной цифровой подписи - лицо, на имя которого зарегистрировано право использования электронной цифровой подписи и который обладает соответствующим закрытым ключом ЭЦП, позволяющим с помощью средств ЭЦП создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);

средства ЭЦП - аппаратные и/или программные средства, реализующие хотя бы одну из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи;

подтверждение с использованием открытого ключа подлинности электронной цифровой подписи, содержащейся в электронном документе; создание закрытых и открытых ключей ЭЦП;

закрытый ключ ЭЦП - уникальная последовательность символов, известная обладателю электронной цифровой подписи и предназначенная для создания им с использованием средств ЭЦП электронной цифровой подписи в электронных документах;

отрытый ключ ЭЦП - уникальная последовательность символов, доступная любому пользователю информационной системы, предназначенная для подтверждения с использованием средств ЭЦП подлинности электронной цифровой подписи в электронном документе;

сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, идентифицирующий обладателя электронной цифровой подписи, включающий открытый ключ ЭЦП и выдаваемый удостоверяющим центром пользователю информационной системы для обеспечения возможности подтверждения подлинности электронной цифровой подписи;

подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат подтверждения сертифицированным средством ЭЦП с использованием сертификата ключа подписи принадлежности содержащейся в электронном документе электронной цифровой подписи ее обладателю и отсутствия искажения и подделки подписанного данной электронной цифровой подписью электронного документа;

информационная система общего пользования - информационная система, пользование которой основано на публичном договоре;

корпоративная информационная система - система, пользователями которой может быть только ограниченный круг лиц, определенный владельцем или соглашением участников корпоративной информационной системы.

**Глава II. Условия использования электронной цифровой подписи**

**Статья 4. Юридическое значение электронной цифровой подписи**

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

сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует);

подтверждена подлинность электронной цифровой подписи в электронном документе;

электронная цифровая подпись использована в отношениях, в которых имеет юридическое значение.

2. Пользователь информационной системы может быть обладателем любого количества электронных цифровых 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 5. Использование средств ЭЦП**

1. Создание ключей электронной цифровой подписи осуществляется:

для использования в информационной системе общего пользования - пользователем или по его обращению - удостоверяющим центром;

для использования в корпоративной информационной системе - в порядке, установленном в этой системе.

2. При создании ключей ЭЦП для использования в информационной системе общего пользования должны применяться только сертифицированные средства ЭЦП. Возмещение убытков и вреда, возникших в связи с созданием ключей ЭЦП несертифицированными средствами ЭЦП, может быть возложено на создателей и распространителей таких ключей.

3. В корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления использование несертифицированных средств ЭЦП и созданных ими ключей ЭЦП не допускается.

4. Сертификация средств ЭЦП осуществляется в соответствии с законодательством Российской Федерации о сертификации продукции и услуг.

**Статья 6. Сертификат ключа подписи**

1. Сертификат ключа подписи должен содержать следующие сведения:

уникальный номер сертификата ключа подписи, дату начала и дату окончания срока его действия;

фамилию, имя и отчество обладателя электронной цифровой подписи;

открытый ключ ЭЦП;

наименование средства ЭЦП, с которым используется данный открытый ключ ЭЦП;

наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;

правоотношения, в которых электронная цифровая подпись имеет юридическое значение.

2. В случае необходимости, связанной с юридическим значением электронной цифровой подписи, в сертификате ключа подписи на основании подтверждающих документов указываются должность, наименование и местонахождение организации, наименование квалификации обладателя электронной цифровой подписи, по его письменному заявлению - иные сведения, подтверждаемые соответствующими документами.

3. Сертификат ключа подписи должен быть внесен удостоверяющим центром в виде электронного документа в реестр сертификатов не позднее даты начала срока действия сертификата.

4. Сертификат ключа подписи выдается пользователям с указанием даты и времени его выдачи, сведений о действии сертификата - действует, действие приостановлено (начало и конец периода приостановления), аннулирован (дата и время аннулирования) - и данных о реестре сертификатов, позволяющих провести проверку действительности данного сертификата ключа подписи. В случае выдачи сертификата ключа подписи на бумажном носителе, он оформляется на бланке удостоверяющего центра и заверяется собственноручной подписью уполномоченного лица и печатью организации. В случае выдачи сертификата ключа подписи в форме электронного документа, он должен быть подписан электронной цифровой подписью уполномоченного лица удостоверяющего центра.

**Статья 7. Срок и порядок хранения сертификата ключа подписи в удостоверяющем центре**

1. Срок хранения сертификата ключа подписи в удостоверяющем центре после его аннулирования должен быть не менее установленного законодательством срока исковой давности для правоотношений, указанных в сертификате ключа подписи. При этом обеспечивается доступ пользователей информационной системы для получения сертификата ключа подписи.

2. По истечении указанного срока хранения сертификат ключа подписи исключается из реестра и переводится в режим архивного хранения. Срок архивного хранения составляет 5 лет. Порядок выдачи копий сертификатов ключей подписей в этот период устанавливается в соответствии с законодательством Российской Федерации.

**Глава III. Удостоверяющие центры**

**Статья 8. Правовой статус удостоверяющих центров**

1. Удостоверяющим центром, выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, может быть коммерческая организация. Деятельность удостоверяющего центра подлежит лицензированию в соответствии с законодательством Российской Федерации о лицензировании отдельных видов деятельности. Указанная организация при оформлении лицензии должна представить обоснование своей способности нести гражданскую ответственность в размере, не менее чем в 1 тысячу раз превышающем максимальный предел цены сделки, который данный центр может указывать в сертификате ключа подписи.

2. Правовой статус удостоверяющего центра, обеспечивающего деятельность корпоративной информационной системы, определяется владельцем или соглашением участников этой системы.

**Статья 9. Деятельность удостоверяющих центров**

1. Удостоверяющий центр:

регистрирует электронные цифровые подписи;

создает по обращению пользователей закрытые и открытые ключи ЭЦП;

приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;

ведет реестр сертификатов ключей подписей, обеспечивает актуальность реестра и возможность свободного доступа пользователей к реестру;

выдает сертификаты ключей подписей на бумажных носителях и в виде электронных документов с информацией об их действительности;

проводит по обращениям пользователей подтверждение подлинности (действительности) электронной цифровой подписи в электронном документе в отношении зарегистрированных им электронных цифровых подписей;

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

2. Регистрация каждой электронной цифровой подписи осуществляется на основе заявления, содержащего сведения, указанные в пунктах 1 и 2 статьи6 настоящего Федерального закона, а также сведения, необходимые для идентификации обладателя подписи и передачи ему сообщений. Заявление подписывается собственноручной подписью обладателя электронной цифровой подписи, содержащиеся в нем сведения подтверждаются предъявлением соответствующих документов. При регистрации проверяется уникальность открытых ключей ЭЦП в реестре и архиве удостоверяющего центра.

3. При регистрации удостоверяющим центром оформляются на бумажных носителях два экземпляра сертификата ключа подписи, которые заверяются собственноручными подписями обладателя электронной цифровой подписи и уполномоченного лица удостоверяющего центра и печатью удостоверяющего центра. Один экземпляр выдается обладателю электронной цифровой подписи, второй остается в удостоверяющем центре.

4. Услуги по выдаче действующих сертификатов ключей зарегистрированных удостоверяющим центром подписей с информацией об их действии в виде электронных документов оказываются пользователям безвозмездно.

**Статья 10. Отношения удостоверяющих центров с уполномоченным федеральным органом исполнительной власти**

1. Удостоверяющий центр обязан до начала использования электронной цифровой подписи уполномоченного центром лица для заверения от имени центра сертификатов ключей подписей представить в уполномоченный федеральный орган исполнительной власти на бумажном носителе сертификат ключа подписи уполномоченного лица с его собственноручной подписью, заверенный подписью руководителя организации и печатью организации.

2. Уполномоченный федеральный орган исполнительной власти ведет единый государственный реестр сертификатов ключей подписей, которыми удостоверяющие центры, работающие с пользователями информационных систем общего пользования, заверяют выдаваемые ими сертификаты ключей подписей, обеспечивает возможность свободного доступа к этому реестру и выдает эти сертификаты ключей подписей, заверенные электронными цифровыми подписями соответствующих уполномоченных лиц.

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

4. Уполномоченный федеральный орган исполнительной власти:

имеет право контролировать правильность использования электронных цифровых подписей, указанных в настоящей статье;

проводит по обращениям граждан, организаций и органов государственной власти Российской Федерации, субъектов Российской Федерации и органов местного самоуправления подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;

осуществляет в соответствии с положением о нем иные полномочия по обеспечению действия настоящего Федерального закона.

**Статья 11. Обязанности удостоверяющего центра по отношению к обладателю электронной цифровой подписи**

Удостоверяющий центр, проводя регистрацию электронной цифровой подписи, принимает на себя следующие обязанности по отношению к обладателю электронной цифровой подписи:

внести сертификат в реестр сертификатов ключей подписей;

обеспечивать свободную выдачу сертификата ключа подписи обратившимся к нему пользователям;

приостанавливать действие сертификата ключа подписи по обращению ее обладателя;

уведомлять обладателя электронной цифровой подписи об известных удостоверяющему центру фактах, которые существенным образом сказываются на возможности дальнейшего использования сертификата ключа подписи;

иные обязанности, установленные нормативными правовыми актами или соглашением сторон.

**Статья 12. Обязанности обладателя электронной цифровой подписи**

Обладатель электронной цифровой подписи обязан:

не использовать для электронной цифровой подписи открытые и закрытые ключи, если ему известно, что эти ключи где-либо используются или использовались ранее;

хранить в тайне закрытый ключ ЭЦП;

немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа нарушена;

использовать электронную цифровую подпись в правоотношениях, указанных в сертификате ключа подписи, в соответствии с ее юридическим значением.

**Статья 13. Приостановление действия сертификата ключа подписи**

1. Действие сертификата ключа подписи может быть приостановлено удостоверяющим центром по указанию лиц или органов, имеющих такое право в силу закона или договора, а в корпоративной информационной системе также в силу установленных правил пользования ею.

2. Период времени от поступления в удостоверяющий центр указания о приостановлении действия сертификата ключа до внесения соответствующей информации в реестр должен устанавливаться в соответствии с общим правилом. По специальной договоренности между удостоверяющим центром и обладателем электронной цифровой подписи в отношении его подписи этот период может быть сокращен.

3. Действие сертификата по указанию полномочного лица или органа приостанавливается на срок, исчисляемый днями, если иное не установлено нормативными правовыми актами или договором. Удостоверяющий центр возобновляет действие сертификата ключа подписи по указанию правомочного лица или органа. Если по истечении указанного срока приостановления не поступает указания о возобновлении действия сертификата, он подлежит аннулированию.

4. Получив указание полномочного лица или органа о приостановлении действия сертификата ключа подписи, удостоверяющий центр оповещает об этом пользователей открытого ключа подписи путем включения в реестр соответствующей информации с указанием времени, даты и срока приостановления действия сертификата, а также извещает об этом обладателя электронной цифровой подписи и лицо (орган), от которого получено указание о приостановлении.

**Статья 14. Аннулирование сертификата ключа подписи**

1. Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его:

по истечении срока его действия;

при утрате силы сертификата соответствующих средств ЭЦП;

в случае, если удостоверяющему центру стало достоверно известно о прекращении действия документа, на основе которого оформлен сертификат ключа подписи;

по письменному (на бумажном носителе) заявлению обладателя электронной цифровой подписи;

в иных случаях, установленных законом или договором.

2. Аннулируя сертификат ключа подписи, удостоверяющий центр оповещает об этом пользователей открытого ключа ЭЦП путем включения в реестр соответствующей информации с указанием времени и даты, а также извещает об этом обладателя электронной цифровой подписи и лицо (орган), давшее указание об аннулировании.

**Статья 15. Прекращение деятельности удостоверяющего центра**

1. Деятельность удостоверяющего центра, выдающего сертификаты ключей подписей для использования в информационных системах общего пользования, может быть прекращена в порядке, установленном гражданским законодательством. Кроме установленных гражданским законодательством процедур ликвидации, организация, принимающая решение о прекращении деятельности обязана обеспечить информирование об этом пользователей, в том числе персонально - всех обладателей зарегистрированных электронных цифровых подписей, и принять меры по передаче с согласия указанных обладателей электронных цифровых подписей обязанностей по оказанию услуг удостоверяющего центра другой организации в порядке правопреемства.

2. Если обязанности удостоверяющего центра перед обладателем электронной цифровой подписи не передаются другой организации в порядке правопреемства, соответствующий сертификат аннулируется и передается на хранение в соответствии со статьей 7 настоящего Федерального закона уполномоченному федеральному органу исполнительной власти.

3. Деятельность удостоверяющего центра, обеспечивающего корпоративную информационную систему, прекращается по решению владельца или договоренности участников системы в связи с передачей его обязанностей другому удостоверяющему центру или в связи с ликвидацией корпоративной информационной системы.

**Глава IV. Особенности использования электронной цифровой подписи в отдельных случаях**

**Статья 16. Использование электронной цифровой подписи в сфере государственного управления**

1. Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, а также организации, участвующие в электронном документообороте с этими органами, используют для заверения электронных документов названных органов и организаций электронные цифровые подписи уполномоченных ими лиц.

2. Сертификаты ключей подписей уполномоченных лиц федеральных органов государственной власти включаются в реестр, ведущийся уполномоченным федеральным органом исполнительной власти, и выдаются пользователям из этого реестра в порядке, установленном настоящим Федеральным законом для удостоверяющих центров.

3. Порядок организации выдачи сертификатов ключей подписей уполномоченных лиц органов государственной власти субъектов Российской Федерации и органов местного самоуправления устанавливается актами соответствующих органов власти субъектов Российской Федерации.

**Статья 17. Использование электронной цифровой подписи в корпоративных информационных системах**

1. Если корпоративная информационная система доступна для пользователей информационной системы общего пользования или корпоративная информационная система предоставляет своим пользователям доступ в информационную систему общего пользования, она должна соответствовать требованиям, установленным настоящим Федеральным законом для систем общего пользования.

2. Использование электронных цифровых подписей в корпоративных информационных системах регламентируется решением владельца системы, соглашением между участниками системы или между владельцем системы и пользователями (клиентами).

3. В корпоративных информационных системах содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов, хранения аннулированных сертификатов, вопросы утраты сертификатами силы регулируются внутренними нормативными правовыми актами или договором.

**Статья 18. Признание иностранных сертификатов ключей подписей**

Иностранный сертификат ключа подписи, удостоверенный в соответствии с законодательством страны, где он зарегистрирован, признается на территории Российской Федерации с учетом выполнения установленных законодательством Российской Федерации процедур признания юридического значения иностранных документов.

**Статья 19. Случаи замещения печатей**

1. Содержание документа на бумажном носителе, имеющего печать и преобразованного в форму электронного документа, в соответствии с нормативными правовыми актами или договоренностью сторон может заверяться электронной цифровой подписью уполномоченного лица.

2. В случаях, установленных нормативными правовыми актами или договоренностью сторон, электронная цифровая подпись, сертификат которой содержит необходимые в данных правоотношениях сведения о правомочиях своего обладателя, признается юридически равнозначной собственноручной подписи лица, заверенной печатью.

**Глава V. Заключительные и переходные положения**

**Статья 20. Приведение нормативных правовых актов в соответствие с настоящим Федеральным законом**

1. Нормативные правовые акты Российской Федерации подлежат приведению в соответствие с настоящим Федеральным законом в трехмесячный срок со дня вступления в силу настоящего Федерального закона.

2. Учредительные документы организаций, осуществляющих деятельность удостоверяющих центров для информационных систем общего пользования, подлежат приведению в соответствие с настоящим Федеральным законом до 1 июля 2002 года.

**Статья 21. Переходные положения**

Удостоверяющие центры, создаваемые после вступления в силу настоящего Федерального закона, но до начала ведения уполномоченным федеральным органом исполнительной власти реестра сертификатов ключей подписей, должны отвечать всем требованиям настоящего Федерального закона, кроме предварительного, до начала использования, представления сертификатов ключей подписей своих уполномоченных лиц уполномоченному федеральному органу исполнительной власти. Соответствующие сертификаты должны быть представлены указанному органу не позже 1 января 2002 года.

Президент Российской Федерации

(датировано 26.03.2001)