ЗАКОН РЕСПУБЛИКИ ТАДЖИКИСТАН
ОБ ЭЛЕКТРОННОМ ДОКУМЕНТЕ И ЭЛЕКТРОННОЙ ПОДПИСИ

Принят Постановлением МН МОРТ
от 15 февраля 2023 года, №973
Одобрить Постановлением ММ МОРТ
от 15 марта 2023 года, №374

Настоящий Закон устанавливает правовые и организационные основы, порядок оборота и использования электронных документов, а также создания и применения электронной подписи в процессе формирования и использования электронных документов.

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Основные понятия

В настоящем Законе используются следующие основные понятия:

1) **электронный документ** - информация, которая представлена в электронной форме;

2) **электронная форма** - совокупность технологий, позволяющие создавать, получать и обмениваться информацией путем применения электронной подписи;

3) **информационная система** - система, участники которой обмениваются информацией в электронной форме путем использования электронных подписей;

4) **корпоративная информационная система** - информационная система, в которой участниками электронного взаимодействия является определенный круг лиц;

5) **информационная система общего пользования** - информационная система, в которой участниками электронного взаимодействия является неопределенный круг лиц;

6) **участники информационной системы (участники электронного документооборота)** - физические лица, индивидуальные предприниматели, юридические лица, государственные органы, которые применяют электронные подписи при осуществлении своих прав и законных интересов;

7) **электронный документооборот (оборот электронных документов)** - составление, использование, хранение и обмен электронными документами, осуществляемое посредством информационнокоммуникационных технологий;

8) **простая электронная подпись** - информация, дающая возможность определить участника электронного документооборота и его волю в действиях и сделках (договорах);

9) **усиленная электронная подпись** - реквизит электронного документа, который формируется путем использования ключа усиленной электронной подписи и направленный на защиту электронного документа от подделки;

10) **защищенная электронная подпись (электронная цифровая подпись)** - реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи, и позволяющий идентифицировать владельца сертификата ключа подписи, установить отсутствие искажения информации в электронном документе и направленный на защиту электронного документа от несанкционированного исправления;

11) **средства защищенной электронной подписи** - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

а) создание электронной подписи в электронном документе с использованием закрытого ключа электронной подписи;

б) подтверждение подлинности электронной подписи в электронном документе с использованием открытого ключа электронной подписи;

в) создание закрытых и открытых ключей электронных подписей;

12) **закрытый ключ защищенной электронной подписи** - последовательность символов, известная владельцу сертификата ключа подписи;

13) **открытый ключ защищенной электронной подписи** - последовательность символов электронной подписи, доступная любому пользователю, предназначенная для подтверждения подлинности электронной подписи в электронном документе;

14) **сертификат средств защищенной электронной подписи** - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств защищенной электронной подписи установленным требованиям;

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

16) **сертификат ключа усиленной электронной подписи** - документ на бумажном носителе или электронный документ с защищенной электронной подписью уполномоченного лица, выдавшего усиленную электронную подпись, которые включают в себя открытый ключ усиленной электронной подписи и которые выдаются уполномоченным лицом участнику информационной системы для подтверждения подлинности усиленной электронной подписи и идентификации владельца сертификата ключа подписи.

17) **подтверждение подлинности защищенной электронной подписи в электронном документе** - положительный результат проверки соответствующим сертифицированным средством защищенной электронной подписи с использованием сертификата ключа защищенной электронной подписи принадлежности защищенной электронной подписи в электронном документе владельцу сертификата ключа защищенной электронной подписи и об отсутствии искажений в подписанном электронном документе;

18) **подписант (подписант электронного документа)** - участник информационной системы, использующий электронную подпись при подписании электронного документа;

19) **владелец сертификата ключа защищенной электронной подписи** - физическое лицо, индивидуальный предприниматель, законный представитель юридического лица, на имя которого удостоверяющим центром выдан сертификат ключа защищенной электронной подписи и который владеет соответствующим закрытым ключом защищенной электронной подписи, позволяющим с помощью средств защищенной электронной подписи использовать свою электронную подпись в электронных документах;

20) **пользователь сертификата ключа защищенной электронной подписи** - участник информационного электронного обмена, использующий полученные в удостоверяющем центре сведения о сертификате ключа защищенной электронной подписи в ходе проверки принадлежности защищенной электронной подписи владельцу сертификата ключа защищенной электронной подписи;

21) **центр сертификации открытых ключей электронной подписи (далее - удостоверяющий центр)** - юридическое лицо, обладающее соответствующими правами на удостоверение соответствия открытого ключа защищенной электронной подписи закрытому ключу защищенной электронной подписи, на чье имя выдано регистрационное свидетельство (владелец свидетельства);

22) **проверка подлинности защищенной электронной подписи** - последовательность действий, в ходе которых проверяется информация о соответствии открытого ключа защищенной электронной подписи участника электронного документооборота закрытому ключу защищенной электронной подписи;

23) **электронный архив** - база архивных электронных документов.

Статья 2. Законодательство Республики Таджикистан об электронном документе и электронной подписи

Законодательство Республики Таджикистан об электронном документе и электронной 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 3. Сфера действия настоящего Закона

1. Положения настоящего Закона распространяются на:

1) электронные документы государственных органов (кроме документов о контрразведывательной, разведывательной и оперативно - розыскной деятельности, использование криптографических и оперативных мер защиты государственной тайны), физических и юридических лиц Республики Таджикистан при совершении ими гражданско - правовых сделок, а также в других случаях, предусмотренных законодательством Республики Таджикистан;

2) электронные подписи, которые были созданы в порядке, предусмотренном настоящим Законом.

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

ГЛАВА 2. ГОСУДАРСТВЕННЫЙ НАДЗОР В СФЕРЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРТА И ЭЛЕКТРОННОЙ ПОДПИСИ

Статья 4. Уполномоченные органы по государственному надзору в сфере электронного документооборота и электронной подписи

Уполномоченный орган по государственному надзору в сфере электронного документооборота (далее - **уполномоченный орган в сфере электронного документооборота**) и уполномоченный орган по государственному надзору в сфере электронной подписи (далее- **уполномоченный орган в сфере электронной подписи**) определяются Правительством Республики Таджикистан.

Статья 5. Полномочия уполномоченного органа в сфере электронного документооборота

К полномочиям уполномоченного органа в сфере электронного документооборота относятся:

1) реализация государственной политики в сфере электронного документооборота;

2) разработка прогнозов, стратегий, концепций и программ в сфере электронного документооборота и координация деятельности соответствующих государственных органов по их реализации;

3) утверждение типовых правил в сфере электронного документооборота;

4) установление правил архивирования и хранения электронных документов;

5) осуществление других полномочий, предусмотренных законодательством Республики Таджикистан.

Статья 6. Полномочия уполномоченного органа в сфере электронной подписи

К полномочиям уполномоченного органа в сфере электронной подписи относятся:

1) реализация государственной политики в сфере электронной подписи;

2) разработка нормативных правовых актов Республики Таджикистан в сфере электронной подписи, в том числе разработка нормативных правовых актов для обеспечения взаимосвязи между реестрами сертификатов ключей защищенных электронных подписей различных удостоверяющих центров, а также возможности использования особого хранения закрытых ключей защищенной электронной подписи при получении защищенной электронной подписи и использовании личных данных заявителей, существующих в государственных органах;

3) оказание практической и методической помощи государственным органам и иным участникам электронного документооборота;

4) утверждение Типового положения удостоверяющего центра;

5) утверждение правил выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром, удостоверяющими центрами государственных органов;

6) утверждение правил взаимодействия удостоверяющих центров Республики Таджикистан с удостоверяющими центрами и доверенными третьими сторонами иностранных государств;

7) утверждение правил проверки подлинности электронной подписи, в том числе подтверждение подлинности защищенной электронной подписи в электронном документе;

8) разработка и утверждение порядка приобретения и использования корневых сертификатов защищенных электронных подписей;

9) осуществление подтверждения подлинности защищенных электронных подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;

10) выдача лицензий удостоверяющим центрам и определение лицензионных требований и условий в порядке, установленном нормативными правовыми актами Республики Таджикистан;

11) проверка деятельности удостоверяющих центров в части соблюдения и выполнения ими лицензионных требований и условий в порядке, установленном нормативными правовыми актами Республики Таджикистан;

12) осуществление других полномочий, предусмотренных законодательством Республики Таджикистан.

ГЛАВА 3. УСЛОВИЯ ОБРАЩЕНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Статья 7. Сфера обращения электронных документов

1. Электронный документ может использоваться во всех сферах деятельности, где применяются программные и технические средства, необходимые для создания, обработки, хранения, передачи и приема информации.

2. С помощью электронных документов могут совершаться сделки (заключаться договоры), производиться расчеты, осуществляться переписка, передача документов и иной информации.

3. Ограничения на применение электронных документов могут быть установлены в случаях, предусмотренных законодательством Республики Таджикистан.

Статья 8. Виды и структура электронного документа

1. Электронные документы разделяются на защищенные и простые. Защищенный электронный документ подписывается защищенной электронной подписью. Простой электронный документ подписывается простой электронной подписью или усиленной электронной подписью.

2. Электронный документ состоит из общей и особенной частей. Общая часть электронного документа состоит из информации, составляющей содержание документа и сведений об адресате. Особенная часть электронного документа состоит из одной или нескольких защищенных электронных подписей.

Статья 9. Оригинал защищенного электронного документа

Оригинал защищенного электронного документа существует только в электронной форме, подписанный защищенной электронной подписью.

Статья 10. Юридическая сила электронного документа

1. Электронный документ признается подписанным только тогда, если при его подписании использована электронная подпись.

2. Электронный документ, подписанный защищенной электронной подписью (защищенный электронный документ), имеет равную юридическую силу с документом на бумажном носителе, подписанным собственноручной подписью.

3. Электронный документ, подписанный простой электронной подписью или усиленной электронной подписью (простой электронный документ), будет признаваться имеющим равную юридическую силу с документом на бумажном носителе в том случае, если это предусмотрено соглашением участников информационной системы или предусмотрено нормативными правовыми актами Республики Таджикистан.

4. В электронном документообороте с участием государственных органов используются только защищенные электронные документы.

Статья 11. Создание, оформление, хранение и оборот электронных документов

Правила создания, оформления, хранения и оборота электронных документов государственными органами, а также физическими и юридическими лицами устанавливаются согласно нормативным правовым актам Республики Таджикистан и договорам между участниками информационных систем.

Статья 12. Хранение и уничтожение электронных документов

1. Хранение электронных документов производится организациями, осуществляющими архивную деятельность, а также деятельность по хранению документированной информации, в соответствии с законодательством Республики Таджикистан.

2. Электронные документы хранятся в электронных архивах. Порядок создания электронных архивов, а также порядок хранения электронных документов в электронных архивах и их уничтожения, определяются Правительством Республики Таджикистан.

Статья 13. Защита электронного документа

Лица, занимающиеся созданием, обработкой, приемом, передачей и хранением электронных документов, должны использовать программные и технические средства, обеспечивающие необходимый уровень защиты этих документов от несанкционированных изменений.

Статья 14. Электронные документы, содержащие информацию, распространение которой запрещено или ограничено

Содержанием электронных документов может быть информация, являющаяся служебной или коммерческой тайной, а также иная информация, распространение которой запрещено или ограничено. Правила использования и меры защиты такой информации устанавливаются законодательством Республики Таджикистан.

Статья 15. Отправление и получение электронного документа

1. Временем отправления электронного документа считается момент, когда электронный документ выходит из информационной системы отправителя.

2. Временем получения электронного документа является момент, когда электронный документ поступает в информационную систему получателя.

3. Местом отправления и получения электронного документа признаются место жительство для физических лиц и юридический адрес других участников электронного документооборота.

Статья 16. Ответственность за содержание электронного документа

Ответственность за содержание электронного документа, оформленного в порядке, предусмотренном настоящим Законом, возлагается на подписанта электронного документа.

ГЛАВА 4. УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ

Статья 17. Использование электронной подписи

1. Электронная подпись используется при оформлении электронных документов, сделок (договоров), в случаях и в порядке, предусмотренных настоящим Законом и законодательством Республики Таджикистан.

2. Электронные подписи могут быть использованы как в корпоративной информационной системе, так и в информационной системе общего пользования в порядке, установленном настоящим Законом.

Статья 18. Виды электронных подписей

1. При оформлении документов и сделок (договоров) могут использоваться следующие электронные подписи:

1) простая электронная подпись;

2) усиленная электронная подпись;

3) защищенная электронная подпись.

2. Простая электронная подпись подтверждается комбинацией логина и пароля, кода подтверждения, по электронной почте, СМС сообщений, USSD командами, другими аналогичными способами и может быть использована только в случае, если соглашением участников информационной системы предусмотрена возможность ее использования. При использовании простой электронной подписи не применяются ключ проверки подписи, средства электронной подписи и сертификат ключа проверки подписи.

3. Усиленная электронная подпись подтверждается ключом электронной подписи. Ключ усиленной электронной подписи формируется самостоятельно субъектами, использующими усиленную электронную подпись во внутреннем документообороте или в корпоративной информационной системе. В усиленной электронной подписи должна быть указана информация о владельце электронной подписи и серии ключа. Правила сертификации защищенных электронных подписей, предусмотренных настоящим Законом, также распространяются на усиленные электронные подписи.

4. Использование простой электронной подписи, порядок выдачи и использования усиленной электронной подписи при внутреннем документообороте определенного субъекта, может быть оформлено нормативными правовыми актами должностного лица или иного уполномоченного органа управления данного субъекта. Порядок выдачи и использования усиленной электронной подписи в корпоративной информационной системе устанавливается соглашением участников корпоративной информационной системы. Субъекты корпоративной информационной системы должны обеспечить защиту усиленных электронных подписей и безопасность их использования.

5. Защищенная электронная подпись используется только при подписании защищенных электронных документов. Защищенный электронный документ и защищенная электронная подпись должны содержать информацию о владельце электронной подписи, номере сертификата и сроке его действия.

Статья 19. Условия признания равнозначности электронной подписи и собственноручной подписи

1. Простая электронная подпись и усиленная электронная подпись с собственноручной подписью равнозначны в случаях, предусмотренных соглашением участников информационной системы или нормативными правовыми актами Республики Таджикистан.

2. Защищенная электронная подпись юридически равнозначна собственноручной подписи при выполнении следующих условий, если:

1) срок действия сертификата ключа защищенной электронной подписи, относящийся к этой электронной подписи, не окончен;

2) подлинность защищенной электронной подписи подтверждена в электронном документе.

Статья 20. Количество электронных подписей участников информационной системы

Участники информационной системы вправе пользоваться неограниченным количеством электронных подписей.

Статья 21. Создание электронных подписей

1. Простые электронные подписи и усиленные электронные подписи создаются самостоятельно участниками информационной системы в порядке, установленном настоящим Законом.

2. При создании усиленной электронной подписи, субъекты, использующие данный вид подписи, должны обеспечить следующие требования:

1) наличие в своем штате соответствующих специалистов;

2) использование средств электронной подписи, сертифицированных в порядке, установленном настоящим Законом;

3) ведение реестра ключей усиленной электронной подписи.

4) хранение информации о сертификатах ключей усиленной электронной подписи. Порядок хранения сертификатов ключей защищенной электронной подписи, предусмотренный настоящим Законом относительно удостоверяющих центров, применяется также к субъектам, создающими такие ключи усиленной электронной подписи;

5) проверку подлинности ключа усиленной электронной подписи;

6) использование усиленной электронной подписи только во внутреннем электронном документообороте или в документообороте между участниками корпоративной системы.

3. Защищенные электронные подписи создаются удостоверяющими центрами на основании заключенного договора с участником информационной системы.

ГЛАВА 5. ЗАЩИЩЕННАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ

Статья 22. Ключи защищенной электронной подписи

1. При использовании защищенной электронной подписи используются открытый и закрытый ключи.

2. Открытый ключ защищенной электронной подписи хранится в удостоверяющем центре и является доступным для всех участников информационной системы. Закрытый ключ электронной подписи хранится и используется исключительно его владельцем, без доступа к нему других лиц.

Статья 23. Создания ключей защищенной электронной подписи

1. На территории Республики Таджикистан ключи защищенной электронной подписи создаются удостоверяющими центрами на основании соответствующих договоров, заключенных с участниками информационной системы.

2. При создании ключей защищенных электронных подписей, их дальнейшей защиты и проверки подлинности сертификата ключей защищенной электронной подписи должны применяться только сертифицированные средства электронной подписи.

3. Возмещение убытков, причиненных в связи с созданием ключей защищенных электронных подписей посредством несертифицированных средств электронной подписи, производится удостоверяющими центрами, создавшими ключи защищенных электронных подписей в соответствии с законодательством Республики Таджикистан.

Статья 24. Сертификат ключа защищенной электронной подписи

1. При создании защищенного электронного ключа владельцу защищенной электронной подписи выдается сертификат ключа защищенной электронной подписи.

2. Сертификат ключа защищенной электронной подписи должен содержать следующие сведения:

1) уникальный регистрационный номер сертификата ключа защищенной электронной подписи;

2) даты начала и окончания срока действия сертификата ключа защищенной электронной подписи, находящегося в реестре удостоверяющего центра;

3) фамилию, имя и отчество (при наличии) владельца сертификата ключа защищенной электронной подписи;

4) открытый ключ защищенной электронной подписи;

5) наименование средств защищенной электронной подписи, в которых используется данный открытый ключ защищенной электронной подписи;

6) сведения об удостоверяющем центре, выдавшим сертификат открытого ключа защищенной электронной подписи, включая его наименование, место нахождения и серию лицензии.

3. Сертификат ключа защищенной электронной подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей защищенной электронной

подписи не позднее, чем за один день до начала срока действия сертификата ключа защищенной электронной подписи.

4. В случае выдачи сертификата ключа защищенной электронной подписи в форме документа на бумажном носителе, данный сертификат оформляется на бланке удостоверяющего центра и заверяется собственноручной подписью уполномоченного лица и печатью удостоверяющего центра.

5. В случае выдачи сертификата ключа подписи и указанных дополнительных данных в форме электронного документа, данный сертификат должен быть подтвержден защищенной электронной подписью уполномоченного лица удостоверяющего центра.

Статья 25. Приостановление и аннулирование действия сертификата защищенной электронной подписи

1. Удостоверяющий центр обязан приостановить действие сертификата ключа защищенной электронной подписи на срок, указанным владельцем защищенной электронной подписи.

2. Удостоверяющий центр обязан аннулировать сертификат защищенной электронной подписи в следующих случаях:

1) по истечении срока действия сертификата защищенной электронной подписи;

2) по требованию владельца защищенной электронной подписи;

3) при обнаружении недостоверности сведений, указанных в заявке на получение сертификата защищенной электронной подписи;

4) по решению уполномоченного органа в сфере электронной подписи;

5) при внесении изменений в сертификат защищенного электронного ключа;

6) в случае смерти владельца защищенного электронного ключа или признания его недееспособным.

3. В случае приостановления или аннулирования сертификата ключа защищенной электронной подписи, удостоверяющий центр вносит в реестр сертификатов ключей защищенной электронной подписи соответствующую информацию с указанием даты и времени приостановления или аннулирования сертификата ключа защищенной электронной подписи, а также извещает об этом владельца защищенной электронной подписи или иное лицо, от которого получено указание о приостановлении или аннулировании сертификата ключа защищенной электронной подписи.

Статья 26. Обязательства владельца сертификата ключа защищенной электронной подписи

Владелец сертификата ключа защищенной электронной подписи обязан:

1) не допускать доступа других лиц к своему закрытому ключу электронной подписи;

2) не использовать для создания защищенной электронной подписи закрытый ключ, если имеются основания полагать, что нарушена конфиденциальность закрытого ключа;

3) незамедлительно требовать приостановления или аннулирования сертификата ключа защищенной электронной подписи в случае утери закрытого ключа или если имеются основания полагать, что нарушена конфиденциальность закрытого ключа;

4) своевременно уведомлять удостоверяющий центр о каких-либо изменениях в личной информации, содержащейся в сертификате ключа защищенной электронной подписи;

5) выполнять другие обязанности, предусмотренные настоящим Законом, и договором, заключенным с удостоверяющим центром.

Статья 27. Срок и порядок хранения сертификата ключа защищенной электронной подписи в удостоверяющем центре

1. Срок хранения сертификата ключа защищенной электронной подписи в форме электронного документа или на бумажном носителе в удостоверяющем центре определяется согласно договору, заключенному между удостоверяющим центром и владельцем сертификата ключа защищенной электронной подписи.

2. По истечении указанного срока хранения, сертификат ключа защищенной электронной подписи исключается из реестра сертификатов ключей подписей и переводится в режим архивного хранения.

3. Срок архивного хранения составляет пять лет. Порядок выдачи копий сертификатов ключей подписей в период их хранения устанавливается в соответствии с законодательством Республики Таджикистан.

Статья 28. Проверка подлинности электронной подписи

1. Проверка подлинности защищенной электронной подписи осуществляется посредством обращения лиц и пользователей сертификата ключа защищенной электронной подписи в удостоверяющий центр с предоставлением информации о сертификате открытого ключа защищенной электронной подписи.

2. Удостоверяющие центры обязаны обеспечить доступ лиц к базе сертификатов ключей защищенных электронных подписей на своих интернет- сайтах.

3. Правила доступа к базе сертификатов ключей защищенных электронных подписей определяются удостоверяющими центрами и должны быть доступны на их интернет-сайте.

Статья 29. Средства защищенной электронной подписи и их сертификация

1. Средства защищенной электронной подписи должны обеспечивать:

1) уникальность создаваемых закрытых и открытых ключей;

2) необходимую вычислительную сложность определения закрытого ключа и защищенной электронной подписи;

3) конфиденциальность закрытого ключа защищенной электронной подписи;

4) защиту открытого ключа защищенной электронной подписи.

2. Средства защищенной электронной подписи в соответствии с законодательством Республики Таджикистан подлежат обязательной сертификации. Защищенным средствам электронной подписи выдается сертификат защищенного средства электронной подписи.

3. Использование несертифицированных средств защищенной электронной подписи и созданных ими ключей защищенных электронных подписей не допускается.

ГЛАВА 6. УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Статья 30. Правовой статус удостоверяющего центра

1. Удостоверяющий центр является юридическим лицом, предоставляющим услуги по выдаче сертификатов ключей защищенных электронных подписей, а также услуги, связанные с использованием защищенных электронных подписей, и подтверждением подлинности защищенности электронных подписей.

2. Удостоверяющие центры могут быть созданы в виде государственных и негосударственных (частных) удостоверяющих центров. Государственные удостоверяющие центры оказывают услуги, связанные с защищенными электронными подписями, государственным органам, государственным учреждениям и государственным предприятиям. Государственные удостоверяющие центры могут оказывать услуги также иным хозяйствующим субъектам. Негосударственные (частные) удостоверяющие центры оказывают услуги, связанные с защищенными электронными подписями, хозяйствующим субъектам, кроме государственных органов, государственных учреждений и государственных предприятий.

3. Государственная регистрация удостоверяющих центров осуществляется в соответствии с законодательством Республики Таджикистан.

4. Требования, предъявляемые к удостоверяющим центрам, определяются Правительством Республики Таджикистан по представлению уполномоченного органа в сфере электронной подписи.

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

Статья 31. Лицензирование деятельности удостоверяющих центров

1. Деятельность по выдаче сертификатов ключей защищенных электронных подписей, оказанию услуг, связанных с использованием защищенных электронных подписей, и подтверждению подлинности защищенности электронных подписей подлежит лицензированию в соответствии с законодательством Республики Таджикистан.

2. Деятельность хозяйствующих субъектов, направленная на создание и использование простых электронных подписей и усиленных электронных подписей, не будет признаваться как деятельность удостоверяющего центра в соответствии с настоящим Законом и не подлежит лицензированию.

Статья 32. Условия для осуществления деятельности удостоверяющим центром

Удостоверяющий центр осуществляет свою деятельность при наличии следующих условий:

1) наличие соответствующих финансовых, материальных, технических и социальных ресурсов, необходимых для обеспечения безопасности, надежности и непрерывности оказания услуг по сертификации ключей защищенной электронной подписи, а также для покрытия ущерба, который может быть нанесен в связи с предоставлением данных услуг;

2) наличие сертифицированного ключа подписи уполномоченного лица удостоверяющего центра, назначенного для сертификации ключей защищенных электронных подписей, в установленном законодательством порядке;

3) обеспечение надежной и оперативной регистрации информации в реестре сертификатов ключей, включая своевременное предоставление услуг по приостановлению действия и аннулированию сертификатов ключей защищенных электронных подписей;

4) обеспечение возможности определить дату и время выдачи, приостановления или аннулирования сертификата ключа защищенной электронной подписи;

5) наличие персонала, обладающего соответствующей квалификацией, необходимой для предоставления услуг по сертификации ключей защищенных электронных подписей;

6) обеспечение безопасности защищенных электронных подписей;

7) хранение информации о сертификате ключа защищенной электронной подписи в порядке, предусмотренном настоящим Законом;

8) соответствие другим специальным условиям, установленным уполномоченным органом в сфере электронной подписи.

Статья 33. Права и обязанности удостоверяющего центра

1. Удостоверяющий центр имеет право:

1) создавать и выдавать сертификаты ключей защищенной электронной подписи;

2) приостанавливать действие сертификатов ключей защищенных электронных подписей, возобновлять, аннулировать, вносить соответствующие изменения в реестр сертификатов ключей защищенных электронных подписей;

3) оказывать на договорной основе иные виды услуг, связанные с защищенными электронными подписями.

2. Удостоверяющий центр обязан:

1) убедиться в достоверности данных, указанных в заявке на сертификацию ключа защищенной электронной подписи, на основании документов, подтверждающих указанные данные;

2) обеспечить соответствие информации, содержащейся в сертификате ключа защищенной электронной подписи и информации, представленной владельцем сертификата ключа защищенной электронной подписи;

3) вести реестр сертификатов ключей защищенных электронных подписей, обеспечивать его актуализацию и свободный доступ к нему, включать необходимые данные о сертификате ключа в реестр сертификатов ключей защищенных электронных подписей не позднее, чем за один день до начала срока действия сертификата;

4) проверять уникальность ключей защищенных электронных подписей в реестре сертификатов ключей защищенных электронных подписей и архиве удостоверяющего центра;

5) уведомлять владельца сертификата закрытого ключа защищенной электронной подписи о ставших известными удостоверяющему центру фактах, указывающих на невозможность дальнейшего использования закрытого ключа защищенной электронной подписи, а также о приостановлении или аннулировании сертификата закрытого ключа защищенной электронной подписи;

6) предоставлять лицам имеющуюся информацию, необходимую для подтверждения подлинности защищенной электронной подписи;

7) осуществлять другие обязанности в соответствии с настоящим Законом, иными нормативными правовыми актами Республики Таджикистан, а также договором, заключенным между удостоверяющим центром и владельцем защищенной электронной подписи.

Статья 34. Прекращение деятельности удостоверяющего центра

1. Деятельность удостоверяющего центра может быть прекращена в порядке, установленном законодательством Республики Таджикистан.

2. В случае прекращения деятельности удостоверяющего центра путем его ликвидации, удостоверяющий центр обязан не менее чем за два месяца до прекращения своей деятельности проинформировать об этом всех обслуживаемых им владельцев защищенных электронных подписей.

3. Порядок использования информации удостоверяющего центра после прекращения его деятельности, определяется уполномоченным органом в сфере электронной подписи.

ГЛАВА 7. ПРИЗНАНИЕ ИНОСТРАННОГО СЕРТИФИКАТА КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ

Статья 35. Признание иностранного сертификата ключа электронной подписи

1. Признание иностранного сертификата ключа электронной подписи осуществляется в соответствии с действующим законодательством Республики Таджикистан и международными договорами, признанными Республикой Таджикистан.

2. Электронные подписи, созданные в соответствии с правом иностранного государства, в Республике Таджикистан признаются электронными подписями того вида, по признакам которого они отвечают в соответствии с настоящим Законом.

3. Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки подписи выдан в соответствии с правом иностранного государства.

4. Порядок признания электронных подписей, созданных в соответствии с правом иностранного государства, определяется уполномоченным органом в сфере электронной подписи.

ГЛАВА 8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Статья 36. Ответственность за несоблюдение требований настоящего Закона

Физические и юридические лица за несоблюдение требований настоящего Закона привлекаются к ответственности в порядке, установленном законодательством Республики Таджикистан.

Статья 37. О признании утратившими силу Закона Республики Таджикистан "Об электронном документе" и Закона Республики Таджикистан "Об электронной цифровой подписи"

Признать утратившими силу Закон Республики Таджикистан "Об электронном документе" от 10 мая 2002 года (Ахбори Маджлиси Оли Республики Таджикистан, 2002 г., №4, ч.1, ст. 308; 2005 г., №12, ст. 637; 2012 г., №12, ч.1, ст. 1002; 2013 г., №7, ст. 523; 2014 г., №12, ст. 828) и Закон Республики Таджикистан "Об электронной цифровой подписи" от 30 июля 2007 года (Ахбори Маджлиси Оли Республики Таджикистан, 2007 г., №7, ст. 682; 2010 г., №7, ст. 560; 2011 г., №3, ст. 166).

Статья 38. Порядок введения в действие настоящего Закона

Настоящий Закон ввести в действие после его официального опубликования.

Президент
Республики Таджикистан Эмомали Рахмон
г.Душанбе,
от 15 марта 2023 года №1965