Закон Об электронной подписи и электронном документе

Утратил силу

Глава I. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Цель и сфера применения настоящего закона

(1) Настоящий закон устанавливает правовой режим электронной подписи и электронного документа, включая основные требования относительно их действительности и основные требования к сертификационным услугам.

(2) Настоящий закон не ограничивает порядок использования документов.

(3) Признание электронной подписи и электронного документа за пределами Республики Молдова регламентируется международными договорами, одной из сторон которых является Республика Молдова. Если международным договором, одной из сторон которого является Республика Молдова, устанавливаются иные нормы, чем те, которые предусмотрены в настоящем законе, применяются нормы международного договора.

Статья 2. Основные понятия

Для целей настоящего закона используются следующие понятия:

добровольная аккредитация – разрешение, устанавливающее права и обязанности применительно к предоставлению сертификационных услуг, даваемое по запросу поставщика сертификационных услуг компетентным органом, ответственным за установление таких прав и обязанностей и осуществление надзора за их соблюдением, в случае, когда поставщик сертификационных услуг не управомочен пользоваться правами, возникающими из разрешения, до того, как он получил решение этого органа;

защищенный электронный архив – структурированное хранилище электронных документов, обеспечивающее их конфиденциальность, неотрекаемость и целостность и гарантирующее их доказательную силу во времени;

аутентичность электронного документа – качество электронного документа, состоящее в том, что он подписан лицом, обладающим подлинной электронной подписью и наделенным правом подписи;

сертификат открытого ключа – электронный документ, содержащий открытый ключ и подписанный электронной подписью поставщика сертификационных услуг, подтверждающий принадлежность открытого ключа владельцу сертификата открытого ключа и позволяющий идентифицировать данного владельца;

квалифицированный сертификат открытого ключа – сертификат открытого ключа, удовлетворяющий требованиям, предусмотренным статьей 31, и выдаваемый поставщиком сертификационных услуг, удовлетворяющим требованиям, предусмотренным статьей 26;

закрытый ключ – уникальная последовательность символов, сформированная при помощи устройства создания электронной подписи и предназначенная для создания электронной подписи;

открытый ключ – уникальная последовательность символов, сформированная при помощи устройства создания электронной подписи, соответствующая связанному с ним закрытому ключу и предназначенная для проверки подлинности электронной подписи;

электронный документооборот – совокупность процессов создания, обработки, отправки, получения, хранения, изменения и/или уничтожения электронных документов;

данные для создания электронной подписи – уникальные данные, такие как коды или закрытые ключи, которые используются подписывающим лицом для создания электронной подписи;

данные для проверки электронной подписи – данные, такие как коды или открытые ключи, которые используются в целях проверки электронной подписи;

устройство создания электронной подписи – конфигурированные программные и/или технические средства, используемые для реализации данных для создания электронной подписи;

защищенное устройство создания электронной подписи – устройство создания электронной подписи, удовлетворяющее требованиям, предусмотренным частями (3) и (4) статьи 8;

устройство проверки электронной подписи – конфигурированные программные и/или технические средства, используемые для реализации данных для проверки электронной подписи;

получатель электронного документа – физическое или юридическое лицо, которому адресован электронный документ, или иное лицо, которое в силу закона или договора получает электронный документ;

электронный документ – информация в электронной форме, создаваемая, структурируемая, обрабатываемая, хранимая и/или передаваемая с помощью компьютера или других электронных устройств, подписанная электронной подписью в соответствии с настоящим законом;

посредник в электронном документообороте – индивидуальный предприниматель или юридическое лицо, которые по поручению подписывающего лица и/или получателя электронного документа организуют и управляют системой электронного документооборота и/или предоставляют услуги, связанные с электронным документооборотом;

метка времени – атрибут электронного документа, посредством электронной подписи удостоверяющий, что информация существовала в определенный момент времени, с сохранением аутентичности и целостности электронного документа;

поставщик сертификационных услуг – индивидуальный предприниматель или юридическое лицо, предоставляющие сертификационные услуги;

поставщик регистрационных услуг – лицо, предоставляющее услуги по проверке личности заявителя, регистрации и отправке заявления о сертификации открытого ключа от имени лица, запрашивающего получение электронной подписи;

продукт для электронной подписи – программные или технические средства либо их соответствующие компоненты, которые предназначены для использования поставщиком сертификационных услуг в целях предоставления сертификационных услуг или предназначены для использования в целях создания или проверки электронных подписей;

Регистр представительских полномочий на основании электронной подписи – электронный регистр, в котором регистрируются представительские полномочия на основании электронной подписи, предоставляемые физическими или юридическими лицами иному лицу;

подписывающее лицо – лицо, обладающее устройством создания электронной подписи и действующее либо от своего собственного имени, либо от имени физического лица, юридического лица или субъекта, которое или которого оно представляет;

электронная подпись – данные в электронной форме, которые присоединены или логически связаны с другими электронными данными и которые используются в качестве способа аутентификации;

сертификационные услуги – услуги сертификации открытых ключей, проставления метки времени и иные услуги в области электронной подписи;

система электронного документооборота – организационно-техническая система, обеспечивающая осуществление электронного документооборота.

Глава II. ПРАВОВОЙ РЕЖИМ ЭЛЕКТРОННОЙ ПОДПИСИ

Статья 3. Принципы использования электронной подписи

Принципами использования электронной подписи являются:

a) свобода выбора и использования любого вида электронной подписи, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено нормативными актами либо соглашением сторон;

b) возможность выбора любой технологии и/или технических средств, позволяющих использовать конкретные виды электронных подписей в соответствии с положениями настоящего закона;

c) недопустимость ссылки на отсутствие юридической силы электронной подписи и/или подписанного ею электронного документа только на основании того, что такая электронная подпись создана не собственноручно, а с использованием устройства создания электронной подписи и/или продукта для электронной подписи.

Статья 4. Виды электронных подписей

(1) Видами электронных подписей, принципы и механизмы использования которых регулируются настоящим законом, являются:

a) простая электронная подпись;

b) усиленная неквалифицированная электронная подпись;

c) усиленная квалифицированная электронная подпись.

(2) Простой электронной подписью является электронная подпись, используемая в качестве способа аутентификации, без ссылки непосредственно на подписывающее лицо.

(3) Усиленной неквалифицированной электронной подписью является электронная подпись, которая удовлетворяет следующим требованиям:

a) ссылается непосредственно на подписывающее лицо;

b) достаточна для идентификации подписывающего лица;

c) создается с использованием средств, которые подписывающее лицо может держать под своим исключительным контролем; и

d) связана с данными, к которым она относится, таким образом, что любое последующее изменение данных является обнаружимым.

(4) Усиленной квалифицированной электронной подписью является электронная подпись, которая удовлетворяет всем требованиям усиленной неквалифицированной электронной подписи и к тому же:

a) основана на квалифицированном сертификате открытого ключа, выданном поставщиком сертификационных услуг, аккредитованным в области применения усиленной квалифицированной электронной подписи;

b) создана с использованием защищенного устройства создания электронной подписи независимо от его физического размещения и проверяется защищенным способом с использованием устройства проверки электронной подписи и/или продукта для электронной подписи, получивших подтверждение соответствия требованиям, предусмотренным настоящим законом.

(5) Электронные подписи, выданные на основании квалифицированных сертификатов поставщиков, зарегистрированных в других государствах, квалифицируются как усиленные квалифицированные подписи, обладающие аналогичной юридической силой с подписями, предусмотренными настоящим законом, в силу положений части (3) статьи 6 или вследствие соответствующего признания сертификата открытого ключа, выданного поставщиком услуг сертификации, проживающим либо находящимся в другом государстве.

Статья 5. Правовой режим использования электронной подписи

(1) Электронная подпись, вне зависимости от имеющейся степени защиты, имеет правовые последствия и допустима в качестве доказательства, в том числе в судопроизводстве, при том, что она:

a) имеет электронную форму; или

b) не основана на сертификате, выданном аккредитованным поставщиком сертификационных услуг; или

c) не основана на квалифицированном сертификате открытого ключа; или

d) не создана с использованием защищенного устройства создания электронной подписи.

(2) Усиленная квалифицированная электронная подпись имеет ту же юридическую силу, что и собственноручная подпись.

(3) Порядок обеспечения степени защиты усиленной квалифицированной электронной подписи с целью ее уравнения с собственноручной подписью на бумажном носителе определяется компетентным органом в соответствии с функциями, предусмотренными частью (1) статьи 36.

(4) Порядок применения электронных подписей должностными лицами юридических лиц публичного права устанавливается Правительством. Юридические лица частного права самостоятельно устанавливают порядок применения электронных подписей их представителями.

(5) Электронная подпись не является средством шифрования информации.

Статья 6. Признание иностранных электронных подписей

(1) Сертификат открытого ключа, выданный поставщиком сертификационных услуг, проживающим или находящимся в другом государстве, признается равнозначным с точки зрения правовых последствий сертификату открытого ключа, выданному поставщиком сертификационных услуг, проживающим или находящимся в Республике Молдова, если соблюдено одно из следующих условий:

a) поставщик сертификационных услуг, проживающий или находящийся в другом государстве, аккредитован согласно схеме аккредитации в соответствии с настоящим законом;

b) аккредитованный поставщик сертификационных услуг, проживающий или находящийся в Республике Молдова, гарантирует признание сертификата;

c) сертификат или поставщик сертификационных услуг, выдавший его, признаются на основе взаимности в соответствии с двусторонним или многосторонним соглашением между Республикой Молдова и другими государствами или международными организациями.

(2) Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на основании того, что сертификат открытого ключа выдан в соответствии с правилами иностранного государства.

(3) В отступление от положений частей (1) и (2) электронные подписи, признанные квалифицированными в соответствии с положениями законодательства Европейского Союза, созданные с использованием квалифицированного сертификата открытого ключа, выданного поставщиком доверительных услуг из государства–члена Европейского Союза, обладают аналогичной юридической силой с усиленными квалифицированными электронными подписями, созданными в соответствии с положениями настоящего закона.

(4) Порядок признания квалифицированных электронных подписей, созданных с использованием квалифицированного сертификата открытого ключа, выданного поставщиком доверительных услуг из государства–члена Европейского Союза, устанавливается Правительством.

(5) В отношении устройства проверки электронной подписи, используемого для проверки электронной подписи в смысле части (3), должно иметься подтверждение соответствия требованиям, предусмотренным настоящим законом, выданное органом, в компетенцию которого входит осуществление контроля в сфере применения электронной подписи.

Статья 7. Закрытый и открытый ключи

(1) Закрытый и открытый ключи, используемые для создания усиленной неквалифицированной электронной подписи, создаются физическим лицом. Они могут создаваться третьими лицами с выраженного согласия соответствующего физического лица, при условии обеспечения невозможности их копирования.

(2) Закрытый и открытый ключи, используемые для создания усиленной квалифицированной электронной подписи, создаются поставщиком сертификационных услуг с использованием защищенного устройства создания электронной подписи. В случае использования защищенного устройства создания электронной подписи на базе SIM-карты поставщик сертификационных услуг обеспечивает физическому лицу инициирование процедуры создания закрытого и открытого ключей.

(3) Создание закрытого ключа и связанного с ним открытого ключа производится одновременно.

(4) Физическое лицо может быть владельцем любого количества закрытых и открытых ключей.

(5) Закрытый ключ хранится и используется исключительно его владельцем таким образом, чтобы исключить доступ к нему другого лица.

(6) Открытый ключ сертифицируется поставщиком сертификационных услуг и является доступным для всех.

Статья 8. Создание электронной подписи

(1) Создание электронной подписи осуществляется посредством устройства создания электронной подписи и/или продукта для электронной подписи, с использованием данных для создания электронной подписи.

(2) При создании простой электронной подписи стороны основываются на положениях заключенного соглашения.

(3) При создании усиленной неквалифицированной электронной подписи и усиленной квалифицированной электронной подписи устройство создания электронной подписи и/или продукт для электронной подписи должны:

a) обеспечить возможность отображения содержания электронного документа, подписанного электронной подписью, или однозначно ссылаться на подписываемый документ;

b) создавать электронную подпись только после подтверждения подписывающим лицом операции по созданию электронной подписи;

c) однозначно подтверждать создание электронной подписи.

(4) Защищенные устройства создания электронной подписи должны, с применением соответствующих технических средств и процедур, обеспечивать, как минимум, что:

a) данные для создания электронной подписи могут появиться только однажды, а их конфиденциальность обеспечена в соответствии с настоящим законом;

b) данные для создания электронной подписи не могут быть вычислены, а электронная подпись защищена от любой возможной подделки с использованием доступной на тот момент технологии;

c) данные для создания электронной подписи надежно защищены законным подписывающим лицом от использования другими лицами.

(5) Защищенные устройства создания электронной подписи не должны изменять данные, подлежащие подписанию, или препятствовать тому, чтобы такие данные были предоставлены подписывающему лицу до начала процесса подписи.

Статья 9. Проверка подлинности электронной подписи

(1) Проверка подлинности электронной подписи осуществляется при помощи устройства проверки электронной подписи и/или продукта для электронной подписи, с использованием данных для проверки электронной подписи.

(2) При проверке простой электронной подписи стороны основываются на положениях заключенного соглашения, которое должно предусматривать порядок подтверждения целостности подписанного электронного документа.

(3) При проверке усиленной неквалифицированной электронной подписи и усиленной квалифицированной электронной подписи устройство проверки электронной подписи и/или продукт для электронной подписи должны:

a) обеспечить возможность отображения содержания электронного документа, подписанного электронной подписью, или однозначно ссылаться на подписываемый документ;

b) отображать факт изменения электронного документа, подписанного электронной подписью;

c) ссылаться на подписывающее лицо.

(4) При защищенной проверке усиленной неквалифицированной электронной подписи и усиленной квалифицированной электронной подписи с достаточной степенью надежности должно обеспечиваться, что:

a) данные для проверки электронной подписи соответствуют данным, отображаемым лицу, проверяющему электронную подпись;

b) электронная подпись проверяется надежно, результат проверки и идентичность подписывающего лица правильно отображаются;

c) аутентичность и действительность сертификата открытого ключа, требуемого во время проверки электронной подписи, надежно проверены;

d) содержание сертификата открытого ключа четко отображается; и

e) любые изменения, касающиеся безопасности электронной подписи, являются обнаружимыми.

Статья 10. Использование простой электронной подписи

(1) Электронный документ считается подписанным простой электронной подписью при выполнении одного из следующих условий:

a) простая электронная подпись содержится в самом электронном документе или логически связана с электронным документом;

b) данные для создания простой электронной подписи применяются в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и/или отправка электронного документа, и в электронном документе содержится информация, идентифицирующая лицо, от имени которого был создан и отправлен электронный документ.

(2) Нормативные акты и/или соглашение сторон, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать, в частности:

a) способ определения лица, от имени которого подписан электронный документ, по его простой электронной подписи;

b) обязанность лица, создающего и/или использующего данные для создания простой электронной подписи, обеспечить их конфиденциальность.

Статья 11. Ограничения на использование некоторых видов электронных подписей

(1) Не допускается использование простой электронной подписи и усиленной неквалифицированной электронной подписи для:

a) подписания электронных документов, содержащих сведения, составляющие государственную тайну;

b) подписания юридическими лицами публичного права электронных документов в правоотношениях юридических лиц публичного права с физическими лицами и юридическими лицами частного права.

(2) В отступление от положений пункта a) части (1) допускается подписание электронных документов, содержащих сведения, составляющие государственную тайну, усиленной неквалифицированной электронной подписью лицами, идентичность и статус которых в соответствии с Законом о государственной тайне № 245/2008 составляют государственную тайну, из состава Службы информации и безопасности, Национального центра по борьбе с коррупцией и Министерства внутренних дел в рамках электронного документооборота в этих структурах.

(3) Не допускается использование электронных подписей, признанных на основании части (3) статьи 6:

a) при подписании электронных документов, содержащих сведения, отнесенные к государственной тайне;

b) при подписании электронных документов, изданных органами публичной власти и публичными учреждениями Республики Молдова или в их отношении, если невозможны проверка и техническое подтверждение соответствующих электронных подписей с территории Республики Молдова с использованием ресурсов, доступных соответствующим органам публичной власти и публичным учреждениям.

Статья 12. Регистр представительских полномочий на основании электронной подписи

(1) Регистр представительских полномочий на основании электронной подписи содержит данные об уполномоченных лицах, представляемых лицах, роль и цель полномочий, дату предоставления полномочий, срок полномочий, другую информацию относительно предоставления, изменения или отзыва полномочий. Полномочия, требующие нотариальной формы удостоверения, регистрируются в Регистре представительских полномочий на основании электронной подписи с соблюдением нотариального законодательства.

(2) Любое изменение в Регистре представительских полномочий на основании электронной подписи относительно делегирования полномочий может осуществляться исключительно лицом, предоставляющим данные полномочия.

(3) Владелец и держатель Регистра представительских полномочий на основании электронной подписи, а также порядок его создания и обновления определяются Правительством.

Глава III. ПРАВОВОЙ РЕЖИМ ЭЛЕКТРОННОГО ДОКУМЕНТА И ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Статья 13. Правовой режим использования электронного документа

(1) Электронный документ, подписанный усиленной квалифицированной электронной подписью, признается равнозначным аналогичному документу на бумажном носителе, подписанному собственноручной подписью.

(2) Электронный документ, подписанный простой электронной подписью или усиленной неквалифицированной электронной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью, только в случаях, прямо установленных нормативными актами или соглашением сторон по применению электронной

подписи, с соблюдением требований, предусмотренных частью (1) статьи 16.

(3) Нормативные акты или соглашение сторон по применению электронной подписи, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью или усиленной неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи и обязанности сторон в отношении конфиденциальности и материальной ответственности.

(4) Если согласно законодательству требуется, чтобы документ был оформлен письменно либо представлен на бумажном носителе подписанным собственноручной подписью, то электронный документ считается соответствующим этому требованию.

(5) Если согласно законодательству требуется, чтобы документ на бумажном носителе был заверен печатью, то электронный документ считается соответствующим этому требованию.

(6) Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан весь пакет.

(7) Порядок использования электронных документов в судопроизводстве регламентируется процессуальным законодательством.

(8) Электронный документ признается доказательством, равным по своей значимости письменным или вещественным доказательствам. Электронный документ не может быть отклонен в качестве доказательства по причине его электронной формы.

(9) Если законодательством предусмотрена государственная регистрация документа, то электронный документ подлежит регистрации.

(10) Все одинаковые экземпляры одного электронного документа считаются его оригиналами и имеют одинаковую юридическую силу.

(11) В случае, когда одним лицом создаются одинаковые по содержанию электронный документ и документ на бумажном носителе, оба документа признаются самостоятельными документами и оригиналами.

(12) Копией электронного документа признается представление (отображение) электронного документа на бумажном носителе в форме, доступной для восприятия. Копия электронного документа заверяется в порядке, установленном законодательством для заверения копий документов на бумажном носителе, и должна содержать отметку о том, что она является копией электронного документа.

Статья 14. Области и цель использования электронного документа
(1) Электронный документ может использоваться физическими и юридическими лицами во всех сферах деятельности, в которых возможно применение программных и технических средств, позволяющих создавать, обрабатывать, отправлять, принимать, хранить, изменять и/или уничтожать информацию в электронной форме.

(2) Электронный документ может использоваться для передачи информации, осуществления переписки, при совершении юридически значимых действий, а также в качестве документа, отражающего факты экономической жизни.

Статья 15. Требования, предъявляемые к электронному документу
Электронный документ должен соответствовать следующим основным требованиям:

a) создаваться, обрабатываться, отправляться, приниматься, храниться, изменяться и/или уничтожаться с помощью программных и/или технических средств;

b) содержать, для подтверждения его аутентичности, одну или несколько электронных подписей, соответствующих условиям и требованиям, предусмотренным настоящим законом;

c) создаваться и использоваться способом и в форме, которые позволяют идентифицировать подписывающее лицо;

d) быть отображенным в форме, доступной для восприятия;

e) быть доступным для неоднократного использования.

Статья 16. Аутентичность электронного документа
(1) Электронный документ является аутентичным, если он соответствует следующим совокупным требованиям:

a) подписан лицом, уполномоченным в установленном порядке подписывать собственноручной подписью подобный документ на бумажном носителе;

b) подписан подлинной электронной подписью подписывающего лица, указанного в документе.

(2) Проверка аутентичности электронного документа осуществляется путем проверки, с использованием устройства проверки электронной подписи и/или продукта для электронной подписи, подлинности этой электронной подписи.

Статья 17. Организация электронного документооборота

(1) Электронный документооборот организуется в соответствии с положениями настоящего закона и с правилами, установленными собственником системы электронного документооборота, а также с договорами, заключаемыми между субъектами электронного документооборота.

(2) Электронный документооборот может включать:

a) создание и обработку электронного документа;

b) отправку и получение электронного документа;

c) проверку аутентичности электронного документа;

d) подтверждение получения электронного документа;

e) учет электронных документов;

f) хранение, изменение и/или уничтожение электронного документа;

g) создание дополнительных экземпляров электронного документа;

h) создание и заверение бумажных копий электронного документа;

i) проставление метки времени.

(3) Порядок создания, обработки, отправки, получения, хранения, изменения и/или уничтожения электронного документа в системах электронного документооборота юридических лиц публичного права устанавливается Правительством, а в системах электронного документооборота юридических лиц частного права – собственниками систем.

Статья 18. Посредник в электронном документообороте

(1) В организации и осуществлении электронного документооборота могут участвовать посредники в соответствии с положениями настоящего закона и с

правилами, установленными собственником системы электронного документооборота.

(2) Посредник в электронном документообороте обязан:

a) располагать программными и/или техническими средствами и оборудованием, обеспечивающими надежность и безопасность используемых информационных систем;

b) располагать персоналом, обладающим необходимыми знаниями и опытом в области информационных технологий и/или информационной безопасности;

c) обеспечивать условия точного определения времени и источника отправки электронного документа, а также времени его получения и электронного адреса получателя;

d) обеспечивать защиту и хранение электронных документов;

e) хранить электронные документы в соответствии с договором, заключенным с пользователями системы электронного документооборота.

Статья 19. Создание электронного документа

(1) Электронный документ создается подписывающим его лицом и включает информацию, составляющую содержание электронного документа, и электронную подпись подписывающего лица.

(2) Создание электронного документа завершается применением электронной подписи подписывающим лицом, с проставлением, при необходимости, метки времени.

Статья 20. Отправка и получение электронного документа

(1) Электронный документ может отправляться и приниматься с помощью информационных и телекоммуникационных систем и/или материальных носителей.

(2) Электронный документ отправляется в форме, позволяющей получателю электронного документа хранить и использовать его.

(3) В случае, когда подписывающим лицом и получателем электронного документа не согласовано иное, электронный документ считается отправленным, если он:

a) отправлен подписывающим лицом или посредником в электронном документообороте, действующим от его имени, или информационной системой,

используемой подписывающим лицом;

b) адресован надлежащим образом или направлен в указанную получателем информационную систему;

c) представлен в форме, доступной для обработки в указанной получателем информационной системе;

d) поступает в информационную систему, находящуюся вне контроля подписывающего лица или посредника в электронном документообороте, который отправляет электронный документ от его имени.

(4) В случае, когда подписывающим лицом и получателем электронного документа не согласовано иное, электронный документ считается принятым получателем, если он:

a) поступает в информационную систему, из которой получатель способен извлекать электронные документы;

b) поступает в указанную получателем информационную систему в форме, доступной для его использования в данной системе.

(5) Электронный документ считается неотправленным, если получатель знал или должен был знать о том, что:

a) лицо, представленное в документе как подписывающее лицо, в действительности не является таковым;

b) подписывающее лицо не является инициатором отправки электронного документа;

c) электронный документ принят получателем в измененном виде или без электронной подписи.

(6) Электронный документ считается неполученным, если лицо, получившее его, в действительности не является надлежащим получателем электронного документа.

Статья 21. Момент отправки и получения электронного документа

(1) Если подписывающим лицом и получателем электронного документа не согласовано иное, моментом отправки электронного документа считается момент поступления электронного документа в информационную систему, находящуюся вне контроля подписывающего лица или посредника в электронном документообороте, который отправляет электронный документ от

его имени.

(2) Если подписывающим лицом и получателем электронного документа не согласовано иное, моментом получения электронного документа считается момент поступления электронного документа в указанную получателем информационную систему. Если получатель электронного документа не указал информационную систему, электронный документ считается полученным им с момента поступления в информационную систему получателя, а в случае отсутствия таковой – с момента его извлечения получателем из информационной системы, посредством которой электронный документ был отправлен.

(3) Момент отправки электронного документа в информационные системы может быть подтвержден, при необходимости, проставлением метки времени в соответствующем электронном документе.

(4) Если соглашением подписывающего лица и получателя электронного документа предусмотрена необходимость подтверждения получения электронного документа, данный документ считается полученным с момента отправления получателем подтверждения о его получении, с проставлением, при необходимости, метки времени.

Статья 22. Учет электронных документов

(1) Учет электронных документов физических и/или юридических лиц осуществляется в соответствии с законодательством путем ведения электронных и/или бумажных регистров.

(2) Технология ведения электронных регистров должна включать программно-технологические процедуры заполнения и администрирования электронных регистров, а также средства хранения электронных документов.

Статья 23. Хранение электронных документов

(1) Субъекты электронного документооборота обязаны хранить оригиналы электронных документов на материальных носителях в форме, позволяющей проверять их аутентичность.

(2) Срок хранения электронных документов идентичен сроку, предусмотренному законодательством для подобных документов на бумажном носителе.

(3) Субъекты электронного документооборота могут обеспечивать хранение электронных документов, пользуясь услугами посредника в электронном документообороте, при условии соблюдения положений настоящего закона.

(4) Для архивного хранения электронных документов используется электронный архив. Правительство устанавливает категории электронных документов, для хранения которых используется защищенный электронный архив.

Статья 24. Защита электронного документа

(1) Электронный документ пользуется юридической защитой, равной защите аналогичного документа на бумажном носителе.

(2) Информация, составляющая содержание электронного документа, используется и защищается в соответствии с законодательством в зависимости от ее статуса и степени защиты.

(3) Создание, обработка, отправка, получение, хранение, изменение и/или уничтожение электронного документа должны отвечать требованиям безопасности, установленным Правительством для систем электронного документооборота юридических лиц публичного права. Для систем электронного документооборота юридических лиц частного права требования безопасности устанавливаются собственниками систем.

(4) В процессе создания, обработки, отправки, получения, хранения, изменения и/или уничтожения электронного документа должна сохраняться информация, позволяющая установить происхождение, принадлежность и назначение электронного документа, а также дату его создания, отправки и получения.

Глава IV. СЕРТИФИКАЦИОННЫЕ УСЛУГИ

Статья 25. Поставщик сертификационных услуг

(1) Поставщики сертификационных услуг в области применения простой электронной подписи и усиленной неквалифицированной электронной подписи пользуются правом на прохождение процедуры аккредитации. Поставщики сертификационных услуг в области применения усиленной квалифицированной электронной подписи подлежат обязательной аккредитации в соответствии с положениями настоящего закона.

(2) Поставщики сертификационных услуг организуются иерархически. На вершине иерархии находится поставщик сертификационных услуг высшего уровня.

(3) Поставщики сертификационных услуг в области применения простой электронной подписи и усиленной неквалифицированной электронной подписи организуют иерархию самостоятельно.

(4) Поставщики сертификационных услуг в области применения простой электронной подписи образуют один иерархический уровень. Поставщики сертификационных услуг в области применения усиленной неквалифицированной электронной подписи образуют два иерархических уровня, в том числе высший.

(5) Деятельность поставщиков сертификационных услуг в области применения усиленной квалифицированной электронной подписи, в том числе их иерархия, организуется в установленном Правительством порядке в соответствии с положениями настоящего закона.

(6) Учет аккредитованных поставщиков сертификационных услуг осуществляется компетентным органом в рамках Регистра учета поставщиков сертификационных услуг, постоянно обновляемого и общедоступного.

(7) Регистрация в Регистре учета поставщиков сертификационных услуг производится компетентным органом в день их аккредитации.

Статья 26. Аккредитация поставщика сертификационных услуг

(1) Аккредитация поставщика сертификационных услуг осуществляется компетентным органом на основании его заявки. Аккредитация поставщика сертификационных услуг является бесплатной и осуществляется на срок пять лет, если в заявке на аккредитацию не указан более короткий срок.

(1-1) В части, не урегулированной настоящим законом, порядок запроса, предоставления, приостановления и отзыва сертификата об аккредитации поставщика сертификационных услуг определяется Законом о регулировании предпринимательской деятельности путем разрешения № 160/2011.

(2) Аккредитация в области применения усиленной квалифицированной электронной подписи предоставляется поставщику сертификационных услуг, удовлетворяющему следующим требованиям:

a) наличие финансовых ресурсов (банковская гарантия или страховой полис) в сумме не менее 300 тысяч леев на случай необходимости возмещения ущерба, причиненного третьим лицам вследствие их доверия к информации, указанной в сертификате открытого ключа, выданном поставщиком сертификационных услуг, или к информации из регистра сертификатов, выданных поставщиком сертификационных услуг;

b) наличие для предоставления сертификационных услуг персонала с высшим образованием в области информационных технологий и/или информационной безопасности, обладающего соответствующим уровнем управленческих и

экспертных знаний и опыта в области технологии электронных подписей;

c) обеспечение безопасности, надежности и непрерывности предоставляемых сертификационных услуг;

d) обеспечение регистрации информации в регистре сертификатов открытых ключей, в частности оперативное предоставление услуги по приостановлению действия и отзыву сертификата открытого ключа;

e) обеспечение возможности определения точной даты и времени выдачи, приостановления действия или отзыва сертификата открытого ключа;

f) проверка в соответствии с законодательством идентичности лица, которому выдается квалифицированный сертификат открытого ключа;

g) использование систем и продуктов, которые защищены от изменений и обеспечивают техническую и криптографическую безопасность поддерживаемых ими функций;

h) создание условий для предотвращения подделки сертификатов и, в случае, когда поставщик сертификационных услуг генерирует данные для создания электронной подписи, – гарантирование конфиденциальности в процессе генерации таких данных;

i) использование систем, которые не хранят и не копируют данные для создания электронной подписи лиц, которым поставщик сертификационных услуг предоставлял услуги по управлению ключами;

j) использование надежных систем для хранения сертификатов в пригодной для проверки форме, так чтобы:

– только авторизованные лица могли вводить и изменять данные;

– аутентичность информации могла быть проверена;

– сертификаты могли быть общедоступными для ознакомления;

– любые технические изменения, нарушающие требования безопасности, были очевидны оператору.

(3) Поставщики сертификационных услуг в области применения усиленной квалифицированной электронной подписи представляют на бумажном носителе, в электронной форме или посредством единого окна для выдачи разрешительных документов заявку на аккредитацию с приложением документов, которые подтверждают соответствие требованиям, указанным в

части (2), а именно подтверждают:

a) наличие финансовых ресурсов на случай необходимости возмещения ущерба;

b) наличие внутренних правил об обеспечении деятельности поставщика сертификационных услуг в соответствии с положениями настоящего закона;

c) соответствие используемых систем и продуктов требованиям настоящего закона;

d) образование и квалификацию должностных лиц, чьи функциональные обязанности непосредственно связаны с предоставлением сертификационных услуг;

e) назначение лиц, ответственных за деятельность поставщика сертификационных услуг, и лиц, уполномоченных подписывать сертификаты открытых ключей, а также личность данных лиц;

f) порядок синхронизации со Всемирным координированным временем (UTC);

g) право на импорт, экспорт, разработку, производство и реализацию специальных технических средств, предназначенных для негласного получения информации, а также право на предоставление услуг в области крипто-графической и технической защиты информации, кроме деятельности органов публичной власти, наделенных таким правом согласно закону (лицензия).

(4) Документы, указанные в пункте a) части (3), представляются в оригинале. Документы, указанные в пунктах b)–g) части (3), представляются в оригинале и копии, оригинал возвращается после сверки с копией в момент его представления.

(5) При подаче заявки на аккредитацию поставщик сертификационных услуг в области применения простой электронной подписи и усиленной неквалифицированной электронной подписи обязан представить в установленном компетентным органом формате информацию относительно используемых процедур безопасности и сертификации, а также свои идентификационные данные.

(6) В течение 30 календарных дней компетентный орган на основании представленных документов принимает решение об аккредитации поставщика сертификационных услуг или об отказе в его аккредитации.

(7) В случае принятия решения об аккредитации компетентный орган в течение 10 календарных дней с момента принятия решения об аккредитации уведомляет поставщика сертификационных услуг о принятом решении и выдает

свидетельство об аккредитации установленного образца и в соответствии с нормативными актами в области электронной подписи регистрирует аккредитованного поставщика в Регистре учета поставщиков сертификационных услуг.

(8) В случае принятия решения об отказе в аккредитации компетентный орган в течение 10 календарных дней с момента принятия решения об отказе письменно уведомляет поставщика сертификационных услуг о принятом решении с указанием причин отказа.

(9) Основанием для отказа в аккредитации является несоответствие поставщика сертификационных услуг требованиям, указанным в части (2), или представление недостоверных сведений в прилагаемых к заявке на аккредитацию документах.

(10) Отказ в аккредитации не может выступать препятствием для повторной подачи документов для аккредитации после устранения причин, послуживших основанием для отказа в аккредитации.

(11) Решение об отказе в аккредитации может быть обжаловано в установленном порядке в судебную инстанцию.

(12) Поставщик сертификационных услуг считается аккредитованным со дня выдачи свидетельства об аккредитации.

(13) В случае повреждения или утраты свидетельства об аккредитации поставщику сертификационных услуг на основании поданного им заявления выдается в течение пяти рабочих дней дубликат свидетельства.

(14) Информация о поставщиках сертификационных услуг, которые аккредитованы, а также о тех, аккредитация которых отозвана, публикуется компетентным органом на его официальной веб-странице.

(15) После получения свидетельства об аккредитации для предоставления сертификационных услуг в области применения усиленной квалифицированной электронной подписи открытый ключ поставщика сертификационных услуг сертифицируется поставщиком сертификационных услуг высшего уровня в соответствии с положением, утвержденным компетентным органом.

(16) Аккредитация считается предоставленной или, по обстоятельствам, продленной, если компетентный орган не отвечает заявителю в срок, установленный законом для ее предоставления или продления.

(17) По истечении срока аккредитации и при отсутствии письменного уведомления от компетентного органа аккредитация считается продленной на тот же срок.

(18) Аккредитованные поставщики сертификационных услуг в области применения простой электронной подписи и усиленной неквалифицированной электронной подписи обязаны не позднее чем за 10 календарных дней уведомить компетентный орган о любом намерении изменения процедур безопасности и сертификации, с указанием даты и времени, когда изменение вступает в силу, и подтвердить в течение 24 часов произведенные изменения.

(19) В неотложных случаях, когда затрагивается безопасность сертификационных услуг, аккредитованные поставщики сертификационных услуг в области применения простой электронной подписи и усиленной неквалифицированной электронной подписи могут произвести изменения в процедурах безопасности и сертификации с последующим доведением в течение 24 часов до сведения компетентного органа произведенных изменений и обоснования принятого решения.

(20) Аккредитованный поставщик сертификационных услуг обязан обеспечить соблюдение требований, на соответствие которым он аккредитован, в течение всего срока его аккредитации. В случае возникновения обстоятельств, делающих невозможным обеспечение соблюдения этих требований, поставщик сертификационных услуг обязан уведомить об этом компетентный орган в течение 24 часов.

(21) Поставщик сертификационных услуг высшего уровня в области применения усиленной квалифицированной электронной подписи не подлежит аккредитации в соответствии с положениями настоящего закона.

Статья 27. Деятельность поставщика сертификационных услуг

(1) Поставщик сертификационных услуг:

a) создает и выдает сертификаты открытых ключей;

b) приостанавливает и отзывает сертификаты открытых ключей, возобновляет действие приостановленных сертификатов;

c) ведет регистр сертификатов открытых ключей, обеспечивает его обновление и открытый доступ к нему; и/или

d) предоставляет на договорной основе иные услуги, связанные с электронной подписью.

(2) Деятельность поставщика сертификационных услуг представляет собой деятельность в области криптографической и технической защиты информации и подлежит лицензированию лицензирующим органом в соответствии с законодательством о регулировании предпринимательской деятельности путем лицензирования.

Статья 28. Обязанности поставщика сертификационных услуг

(1) Поставщик сертификационных услуг обязан:

a) проверить достоверность данных, указанных в заявке на сертификацию открытого ключа, на основании документов, подтверждающих указанные данные;

b) обеспечить соответствие информации, содержащейся в сертификате открытого ключа, информации, представленной владельцем сертификата открытого ключа;

c) включить сертификат открытого ключа в регистр сертификатов открытых ключей не позднее даты и времени начала действия сертификата;

d) обеспечивать доступ к регистру сертификатов открытых ключей с соблюдением положений статьи 43;

e) приостанавливать или отзывать сертификат открытого ключа в случаях, предусмотренных законом, и вносить в установленные сроки соответствующую запись в регистр сертификатов открытых ключей;

f) возмещать ущерб, причиненный любому юридическому или физическому лицу вследствие разумного доверия к информации, указанной в сертификате открытого ключа, выданном поставщиком сертификационных услуг, в случае пропуска регистрации отзыва сертификата;

g) уведомлять владельца сертификата открытого ключа о ставших известными поставщику сертификационных услуг фактах, указывающих на невозможность дальнейшего использования закрытого ключа, а также об отзыве сертификата открытого ключа;

h) представлять информацию, необходимую для подтверждения подлинности электронной подписи;

i) запрашивать выдачу дубликата в случае утраты или повреждения свидетельства об аккредитации;

j) осуществлять иные обязанности, установленные настоящим законом.

(2) Аккредитованный поставщик сертификационных услуг в области применения усиленной квалифицированной электронной подписи обязан кроме того:

a) сертифицировать в установленном законодательством порядке открытый ключ аккредитованного поставщика сертификационных услуг в области применения усиленной квалифицированной электронной подписи, предназначенный для сертификации открытых ключей;

b) осуществлять запись в течение установленного периода времени в соответствии со статьей 31 всей относящейся к квалифицированному сертификату открытого ключа информации, в частности для цели его представления в качестве доказательства сертификации в суде. Такая запись может производиться электронными средствами;

c) до вступления в договорные отношения с лицом, запрашивающим сертификат в целях поддержки своей электронной подписи, информировать данное лицо посредством надежных средств связи о точных сроках и условиях использования сертификата, включая ограничения на его использование, о наличии системы аккредитации и процедур обжалования и разрешения споров. Такая информация, которая может быть передана в электронном виде, должна быть сообщена в письменной форме и на легко понятном языке. Определенные части этой информации также должны быть доступны по запросу третьим лицам, пользующимся сертификатом;

d) хранить всю информацию о сертификате открытого ключа, прилагаемом к усиленной квалифицированной электронной подписи, не менее 15 лет со дня отзыва или истечения срока действия сертификата на случай возникновения спора.

(3) Поставщик сертификационных услуг, аккредитованный в сфере применения усиленной квалифицированной электронной подписи на этапе выдачи квалифицированного сертификата, проверяет соответствующими средствами и согласно применимой нормативной базе личность и, при необходимости, специфические признаки лица, которому выдается квалифицированный сертификат. Указанная информация проверяется либо напрямую поставщиком сертификационных услуг, аккредитованным в сфере применения усиленной квалифицированной электронной подписи, либо через поставщика регистрационных услуг. Проверка осуществляется одним из следующих способов:

a) в физическом присутствии лица;

b) дистанционно, с использованием электронных средств идентификации, для чего до выдачи квалифицированного сертификата было обеспечено физическое присутствие лица;

c) посредством сертификата усиленной квалифицированной электронной подписи;

d) использованием других методов идентификации, признанных на национальном уровне, которые обеспечивают уровень доверия, равнозначный с точки зрения надежности физическому присутствию.

Признанные методы дистанционной идентификации лица устанавливаются Правительством.

Статья 29. Заявка на сертификацию открытого ключа

(1) Заявка на сертификацию открытого ключа подается поставщику сертификационных услуг в электронной форме, подписанная электронной подписью, и/или в форме документа на бумажном носителе, подписанного собственноручной подписью. Заявка на сертификацию открытого ключа подписывается заявителем электронной подписи или поставщиком регистрационных услуг. В случае подписания поставщиком регистрационных услуг он обеспечивает проверку личности заявителя в соответствии с методами, предусмотренными применимыми нормативными актами, или в соответствии с процедурой, согласованной с поставщиком сертификационных услуг.

(11) К поставщикам регистрационных услуг, которые могут подавать заявки от имени лица, запрашивающего получение электронной подписи, относятся:

a) лица, уполномоченные поставщиком сертификационных услуг, либо те, с кем поставщик сертификационных услуг заключил соглашение, дающее им полномочия по установлению личности лица, запрашивающего получение электронной подписи, в порядке, установленном таким соглашением;

b) лица, которые в соответствии с законом обладают компетенцией:

- по приему и регистрации заявлений о выдаче и/или по выдаче актов гражданского состояния либо удостоверяющих личность документов из национальной паспортной системы;

- по оказанию нотариальных услуг в соответствии с Законом о нотариате № 1453/2002.

(2) Заявка на сертификацию открытого ключа должна содержать:

a) фамилию, имя заявителя и номер документа, удостоверяющего личность;

b) другие идентификационные данные заявителя в зависимости от цели, для которой выдается сертификат открытого ключа, а также сведения, необходимые для связи с заявителем.

Статья 30. Рассмотрение заявки на сертификацию открытого ключа

(1) Заявка на сертификацию открытого ключа рассматривается поставщиком сертификационных услуг в течение трех рабочих дней с даты регистрации заявки, если сторонами не установлено иное.

(2) На основании решения о сертификации открытого ключа поставщик сертификационных услуг создает и выдает сертификат открытого ключа.

(3) Решение об отказе в сертификации открытого ключа принимается поставщиком сертификационных услуг в случае:

a) нарушения положений настоящего закона;

b) нарушения в процессе подготовки или подачи заявки на сертификацию прав третьих лиц;

c) представления в заявке на сертификацию информации, не соответствующей действительности.

(4) Решение об отказе в сертификации открытого ключа может быть обжаловано в установленном порядке в судебную инстанцию.

(5) Решение об отказе в сертификации открытого ключа не лишает заявителя права на подачу новой заявки после устранения всех допущенных нарушений.

Статья 31. Сертификат открытого ключа

(1) При создании сертификата открытого ключа поставщик сертификационных услуг обязан проверить уникальность открытого ключа.

(2) Сертификат открытого ключа должен содержать:

a) уникальный регистрационный номер сертификата открытого ключа;

b) идентификационные данные поставщика сертификационных услуг, выдавшего сертификат открытого ключа;

c) идентификационные данные и другие данные владельца сертификата открытого ключа в зависимости от цели, для которой выдается сертификат, а

также сведения, необходимые для связи с ним;

d) открытый ключ;

e) дату и время начала и окончания действия сертификата открытого ключа;

f) данные о криптографическом алгоритме электронной подписи;

g) ограничения на использование сертификата открытого ключа и/или пределы стоимости сделок, в которых он может использоваться, если таковые применяются;

h) иные сведения, предусмотренные законодательством.

(3) Квалифицированный сертификат открытого ключа выдается аккредитованным поставщиком сертификационных услуг и должен дополнительно содержать:

a) указание о том, что сертификат выдан в качестве квалифицированного сертификата открытого ключа;

b) информацию, при необходимости, о специфических особенностях подписывающего лица в зависимости от цели, для которой предназначен сертификат;

c) данные для проверки электронной подписи, соответствующие данным для создания электронной подписи, находящимся под контролем подписывающего лица.

(4) В качестве идентификационных данных владельца сертификата открытого ключа пользователя выступают фамилия, имя и идентификационный номер физического лица (IDNP) и/или псевдоним – в случае использования, а в сертификате открытого ключа поставщика сертификационных услуг – наименование поставщика и идентификационный номер юридического лица (IDNO).

(5) В случае простой электронной подписи и усиленной неквалифицированной электронной подписи структура сертификата открытого ключа определяется в соответствии с положениями настоящего закона поставщиком сертификационных услуг. В случае усиленной квалифицированной электронной подписи структура сертификата открытого ключа определяется в соответствии с положениями настоящего закона компетентным органом.

(6) Сертификат открытого ключа подписывается электронной подписью поставщика сертификационных услуг, соответствующей виду запрашиваемого

сертификата.

(7) В случаях, установленных законодательством или соглашением сторон, поставщик сертификационных услуг создает сертификат открытого ключа и в форме документа на бумажном носителе в двух экземплярах. Сертификат открытого ключа в форме документа на бумажном носителе подписывается собственноручными подписями владельца сертификата открытого ключа и уполномоченного лица поставщика сертификационных услуг и заверяется печатью поставщика сертификационных услуг. Один экземпляр сертификата открытого ключа передается его владельцу, а другой хранится у поставщика сертификационных услуг.

(8) Поставщик сертификационных услуг по согласованию с владельцем сертификата открытого ключа может указать в сертификате открытого ключа случаи, в которых он может использоваться, а также ограничения на использование данного сертификата.

(9) По обращению владельца сертификата открытого ключа поставщик сертификационных услуг может указать в сертификате открытого ключа и другие, не предусмотренные частями (2) и (3), сведения, при условии, что они не противоречат законодательству, не представляют угрозу национальной безопасности или общественному порядку, и только после предварительной проверки точности этих сведений.

(10) Поставщик сертификационных услуг вносит сертификат в регистр сертификатов открытых ключей не позднее даты и времени начала действия сертификата.

Статья 32. Сроки действия и хранения сертификата открытого ключа

(1) Срок действия сертификата открытого ключа поставщика сертификационных услуг высшего уровня составляет 20 лет, срок действия сертификата открытого ключа поставщика сертификационных услуг второго уровня составляет 10 лет, срок действия сертификата открытого ключа пользователя устанавливается поставщиком сертификационных услуг, но не может составлять более пяти лет в зависимости от потенциала технических средств по созданию электронной подписи.

(2) Поставщик сертификационных услуг обязан хранить сертификат открытого ключа не менее 15 лет с даты отзыва или истечения срока действия сертификата.

Статья 33. Приостановление действия и отзыв сертификата открытого ключа

(1) Поставщик сертификационных услуг приостанавливает действие сертификата открытого ключа по требованию владельца сертификата открытого ключа.

(2) Поставщик сертификационных услуг отзывает сертификат открытого ключа:

a) по требованию владельца сертификата открытого ключа;

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

c) при нарушении конфиденциальности закрытого ключа (компрометация закрытого ключа);

d) по истечении срока, на который было приостановлено действие сертификата открытого ключа, в отсутствие заявки со стороны владельца сертификата открытого ключа на восстановление его действия;

e) при внесении изменений в сертификат открытого ключа;

f) в случае смерти владельца сертификата открытого ключа или установления в отношении владельца меры судебной охраны (временная охрана, попечительство или опека);

g) по обращению компетентного органа в случае нарушения настоящего закона.

(3) При получении информации о необходимости отзыва сертификата открытого ключа поставщик сертификационных услуг обязан в течение трех рабочих часов внести соответствующие записи в регистр сертификатов открытых ключей.

(4) Поставщик сертификационных услуг обязан уведомить владельца сертификата открытого ключа о причинах отзыва его сертификата.

Статья 34. Обязанности владельца сертификата открытого ключа

Владелец сертификата открытого ключа обязан:

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

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

c) незамедлительно требовать приостановления действия или отзыва сертификата открытого ключа в случае:

– утери закрытого ключа;

– наличия оснований полагать, что нарушена конфиденциальность закрытого ключа;

– несоответствия действительности информации, содержащейся в сертификате открытого ключа;

d) уведомлять в течение 24 часов поставщика сертификационных услуг о любых изменениях сведений, содержащихся в сертификате открытого ключа;

e) выполнять иные обязанности, предусмотренные настоящим законом и соглашением с поставщиком сертификационных услуг.

Статья 35. Регистр сертификатов открытых ключей

(1) Поставщик сертификационных услуг обязан вести регистр сертификатов открытых ключей.

(2) Регистр сертификатов открытых ключей должен содержать:

a) действительные сертификаты открытых ключей;

b) отозванные и приостановленные сертификаты открытых ключей;

c) дату и время выдачи сертификатов открытых ключей;

d) дату и время отзыва сертификатов открытых ключей;

e) иную необходимую информацию в соответствии с нормативными актами в области электронной подписи.

(3) В целях осуществления проверки подлинности электронной подписи поставщик сертификационных услуг обязан обеспечить доступ к регистру сертификатов открытых ключей, в том числе в режиме реального времени.

Глава V. НАДЗОР И КОНТРОЛЬ

Статья 36. Функции органов публичной власти в области применения электронной подписи

(1) Компетентным органом, ответственным за разработку и реализацию государственной политики и контроль в области применения всех видов электронных подписей, является Служба информации и безопасности, которая выполняет следующие функции:

a) осуществляет аккредитацию, в том числе добровольную, поставщиков сертификационных услуг;

b) выполняет функции поставщика сертификационных услуг высшего уровня для аккредитованных поставщиков сертификационных услуг в области применения усиленной квалифицированной электронной подписи;

c) обеспечивает ведение, обновление и открытый доступ к данным Регистра учета поставщиков сертификационных услуг;

d) разрабатывает и утверждает посредством нормативных актов требования в области применения всех видов электронных подписей;

e) осуществляет надзор и контроль за соблюдением требований при предоставлении сертификационных услуг в области применения всех видов электронных подписей;

f) участвует в разработке и утверждении технических регламентов и стандартов в области электронной подписи;

g) оказывает по запросу методическую и практическую помощь по вопросам применения механизмов электронной подписи;

h) осуществляет международное сотрудничество в области электронной подписи.

(2) Правительство определяет государственный орган или учреждение, ответственные за предоставление услуги единого источника синхронизации со Всемирным координированным временем (UTC).

Статья 37. Контроль в области применения электронной подписи

(1) Компетентный орган контролирует соблюдение требований, установленных настоящим законом, при предоставлении сертификационных услуг аккредитованными поставщиками и при предоставлении или продлении аккредитации.

(2) Контроль осуществляется комиссией по контролю в области электронной подписи (далее – Комиссия) на основании положения, утвержденного компетентным органом.

(3) Комиссия создается в рамках компетентного органа на основании приказа руководителя данного органа о проведении контроля.

(4) Персональный состав Комиссии определяется для каждого случая отдельно.

(5) Комиссия вправе:

a) иметь свободный доступ к документальным материалам на бумажных или электронных носителях, необходимым для проведения работ, связанных с предоставлением сертификационных услуг, а также к программным дистрибутивам, установленным приложениям и техническим средствам;

b) получать полную информацию об условиях и порядке эксплуатации программных и технических средств;

c) получать от ответственных лиц и персонала поставщика сертификационных услуг информацию в отношении предоставления сертификационных услуг, связанную с предметом контроля;

d) иметь доступ в помещения поставщика сертификационных услуг в течение рабочего дня (на период осуществления контроля).

(6) Комиссия не вправе осуществлять контроль без предъявления приказа о проведении контроля и без предъявления документов, удостоверяющих личность членов Комиссии.

(7) При проведении контроля соответствия условиям, предусмотренным настоящим законом, Комиссия руководствуется следующими принципами:

a) законность и соблюдение установленной законом компетенции;

b) недопущение применения не предусмотренных законом санкций;

c) толкование сомнений, возникающих при применении законодательства, в пользу поставщика сертификационных услуг;

d) осуществление контроля за счет государства;

e) выдача предписаний об устранении выявленных в результате контроля нарушений;

f) право поставщика сертификационных услуг на обжалование действий компетентного органа, в том числе в судебную инстанцию.

(8) Плановые проверки соблюдения поставщиком сертификационных услуг обязательств, предусмотренных настоящим законом, проводятся компетентным органом не чаще одного раза в течение календарного года с привлечением при необходимости представителей регулирующих и контролирующих органов согласно компетенции.

(9) Планы проверок, разработанные компетентным органом и утвержденные в установленном порядке, не позднее чем за пять рабочих дней до начала этих проверок согласовываются в отношении сроков проведения с руководством поставщика сертификационных услуг.

(10) Внеплановые проверки проводятся по решению компетентного органа только на основании:

a) выявления и подтверждения компетентным органом фактов нарушения настоящего закона; и/или

b) поступления в адрес компетентного органа обоснованных письменных заявлений и жалоб относительно нарушений и ненадлежащего исполнения поставщиком сертификационных услуг обязанностей, предусмотренных настоящим законом.

(11) Поставщик сертификационных услуг информируется о проведении внеплановой проверки в день ее начала.

(12) Повторные проверки проводятся только с целью проверки выполнения предписаний об устранении нарушений настоящего закона, указанных в акте предыдущей проверки (плановой или внеплановой). Повторная проверка считается составной частью предыдущей проверки.

(13) Проверка проводится строго в установленные приказом о проведении контроля сроки.

(14) Срок проведения плановой и внеплановой проверки не может превышать 10 рабочих дней, а повторной – пяти рабочих дней. В случае внеплановой проверки десятидневный срок может быть продлен еще на 10 дней руководителем компетентного органа на основании мотивированного решения, доведенного до сведения проверяемого поставщика сертификационных услуг, которое может быть обжаловано поставщиком сертификационных услуг.

(15) При проведении проверки соблюдения обязанностей, предусмотренных настоящим законом, поставщик сертификационных услуг предоставляет сведения и документы, относящиеся к цели проверки, и не препятствует ее проведению.

(16) По результатам проверки составляется акт в двух экземплярах, один из которых не позднее пяти рабочих дней после завершения проверки направляется/вручается поставщику сертификационных услуг, а второй хранится у компетентного органа. В случае несогласия с результатами проведенной проверки поставщик сертификационных услуг в течение 10

рабочих дней со дня получения акта проверки может представить в письменном виде обоснование несогласия, приложив соответствующие документы.

(17) В случае выявления нарушений обязанностей, предусмотренных настоящим законом, компетентный орган на основании акта проверки выдает предписание об устранении нарушений, содержащее рекомендации по устранению всех выявленных нарушений, а также предупреждение о возможном приостановлении или отзыве аккредитации в случае неустранения в установленный срок выявленных нарушений.

(18) Минимальный срок, устанавливаемый компетентным органом для устранения выявленных нарушений, составляет 10 рабочих дней, максимальный – 30 рабочих дней после получения предписания, направленного/врученного вместе с актом проверки.

(19) В исключительных случаях, а также по официальному обращению поставщика сертификационных услуг срок для устранения нарушений может быть продлен не более чем на 20 рабочих дней.

(20) Аккредитованный поставщик сертификационных услуг, получивший предписание об устранении нарушений обязанностей, предусмотренных настоящим законом, обязан в установленный в предписании срок представить компетентному органу информацию об устранении нарушений.

(21) При установлении признаков компрометации закрытых ключей аккредитованного поставщика сертификационных услуг, в случае нарушения обязанностей, предусмотренных настоящим законом, а также в случае неустранения в установленный срок недостоверных данных в сертификатах открытых ключей компетентный орган вправе применить меры по приостановлению или отзыву аккредитации поставщика сертификационных услуг в соответствии с настоящим законом.

(22) Информация о результатах проверки публикуется компетентным органом на его официальной веб-странице.

(23) Поставщик сертификационных услуг вправе обратиться с письменной жалобой на допущенные Комиссией нарушения положений настоящего закона в компетентный орган или обжаловать ее действия в судебную инстанцию.

Статья 38. Приостановление и возобновление аккредитации

(1) Аккредитация может быть приостановлена в соответствии с законодательством о регулировании предпринимательской деятельности.

(2) Основанием для осуществления предусмотренных законом мер по приостановлению аккредитации является:

a) заявление поставщика сертификационных услуг о приостановлении аккредитации;

b) нарушение поставщиком сертификационных услуг обязанностей, предусмотренных настоящим законом;

c) недействительность предусмотренных в пункте a) части (2) статьи 26 банковской гарантии или страхового полиса поставщика сертификационных услуг в области применения усиленной квалифицированной электронной подписи;

d) невыполнение поставщиком сертификационных услуг предписания об устранении выявленных в ходе проведенной Комиссией проверки нарушений обязанностей, предусмотренных настоящим законом.

(3) Решение о приостановлении аккредитации доводится до сведения поставщика сертификационных услуг в течение трех рабочих дней после его принятия. Срок приостановления аккредитации не может превышать двух месяцев, если нормативными актами в области электронной подписи не предусмотрено иное.

(4) Поставщик сертификационных услуг обязан письменно уведомить компетентный орган об устранении обстоятельств, повлекших приостановление аккредитации.

(5) Решение о возобновлении аккредитации принимается компетентным органом на основании решения судебной инстанции, вынесшей решение о приостановлении аккредитации, в течение трех рабочих дней со дня получения извещения. Решение доводится до сведения поставщика сертификационных услуг в течение трех рабочих дней со дня его принятия.

(6) Срок действия аккредитации не продлевается на время ее приостановления.

Статья 39. Отзыв аккредитации

(1) Аккредитация может быть отозвана в соответствии с законодательством о регулировании предпринимательской деятельности.

(2) Основанием для осуществления предусмотренных законом мер по отзыву аккредитации является:

a) заявление поставщика сертификационных услуг о прекращении деятельности, поданное за 30 календарных дней до планируемого прекращения деятельности;

b) решение об аннулировании государственной регистрации юридического лица, в рамках которого действует поставщик сертификационных услуг;

c) выявление недостоверных данных в документах, представленных компетентному органу;

d) установление факта передачи свидетельства об аккредитации или его копии другому лицу для осуществления аккредитуемого вида деятельности;

e) неустранение в установленный срок обстоятельств, повлекших приостановление аккредитации;

f) повторное невыполнение предписаний об устранении нарушений обязанностей, предусмотренных настоящим законом.

(3) Запись о дате и номере решения об отзыве аккредитации вносится в Регистр учета поставщиков сертификационных услуг не позднее следующего рабочего дня после принятия решения.

(4) Все сертификаты открытых ключей, выданные поставщиком сертификационных услуг в области применения усиленной квалифицированной электронной подписи, прекратившим деятельность, отзываются и передаются на хранение другому поставщику сертификационных услуг в области применения усиленной квалифицированной электронной подписи в порядке, установленном компетентным органом, за счет прекращающего деятельность поставщика сертификационных услуг.

(5) Поставщик сертификационных услуг обязан в течение 10 рабочих дней со дня принятия решения об отзыве аккредитации сдать в компетентный орган отозванное свидетельство об аккредитации.

Глава VI. ОТВЕТСТВЕННОСТЬ

Статья 40. Ответственность физических и юридических лиц, подпадающих под действие настоящего закона

(1) Физические и юридические лица несут установленную законодательством ответственность за нарушение положений настоящего закона.

(2) Посредник в электронном документообороте несет установленную законодательством ответственность за неисполнение либо ненадлежащее исполнение обязанностей, предусмотренных настоящим законом, за ненадлежащее качество предоставляемых услуг, а также за ущерб, причиненный указанными действиями и/или бездействием.

(3) Лица, осуществляющие незаконный доступ к информации, содержащейся в электронных документах, несут, по обстоятельствам, гражданскую, правонарушительную или уголовную ответственность в соответствии с законодательством.

(4) Споры, возникающие в рамках электронного документооборота, а также связанные с использованием электронных документов и применением электронной подписи, разрешаются субъектами электронного документооборота в соответствии с законодательством и заключенными между ними договорами.

Статья 41. Ответственность поставщика сертификационных услуг

(1) Поставщик сертификационных услуг несет, по обстоятельствам, гражданскую, правонарушительную или уголовную ответственность в соответствии с законодательством.

(2) Поставщик сертификационных услуг несет гражданскую ответственность за ущерб, причиненный неисполнением обязанностей, предусмотренных настоящим законом, за исключением случаев, когда поставщик сертификационных услуг представит соответствующие доказательства того, что он не мог предотвратить причинение ущерба.

(3) Поставщик сертификационных услуг не несет гражданской ответственности за ущерб, причиненный в связи с использованием сертификата открытого ключа с нарушением ограничений на использование сертификата или пределов стоимости сделок, в которых он может использоваться.

Статья 42. Ответственность владельца сертификата открытого ключа

(1) Владелец сертификата открытого ключа несет, по обстоятельствам, гражданскую, правонарушительную или уголовную ответственность в соответствии с законодательством.

(2) Владелец сертификата открытого ключа несет гражданскую ответственность за ущерб, причиненный:

а) неисполнением или ненадлежащим исполнением обязанностей, предусмотренных настоящим законом;

b) подписанием электронных документов с использованием его закрытого ключа, в том числе в период от обращения за приостановлением действия или отзывом сертификата открытого ключа до внесения в установленный срок соответствующей отметки в регистр сертификатов открытых ключей, за исключением случаев, когда владелец сертификата открытого ключа представит соответствующие доказательства того, что электронный документ был подписан другим лицом.

Глава VII. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 43. Защита персональных данных

(1) Поставщики сертификационных услуг обеспечивают в процессе предоставления сертификационных услуг соблюдение законодательства о защите персональных данных.

Глава VIII. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Статья 44. Заключительные положения

(1) Настоящий закон вступает в силу по истечении шести месяцев со дня опубликования.

(2) В день вступления в силу настоящего закона признается утратившим силу Закон об электронном документе и цифровой подписи № 264-XV от 15 июля 2004 года (Официальный монитор Республики Молдова, 2004 г., № 132–137, ст. 710).

(3) Положения части (1) статьи 5 в части, касающейся судопроизводства, вступают в силу с 1 января 2016 года.

(4) Правительству в 12-месячный срок со дня опубликования настоящего закона:

a) представить предложения по приведению действующего законодательства в соответствие с настоящим законом;

b) привести свои нормативные акты в соответствие с настоящим законом;

c) разработать и утвердить нормативные акты, необходимые для реализации настоящего закона.

(5) Сертификаты открытых ключей, выданные на основании Закона об электронном документе и цифровой подписи № 264-XV от 15 июля 2004 года, действительны до истечения срока их действия.

(6) Центры сертификации открытых ключей, созданные на основании Закона об электронном документе и цифровой подписи № 264-XV от 15 июля 2004 года, обязаны в 18-месячный срок со дня опубликования настоящего закона пройти процедуру аккредитации в соответствии с положениями настоящего закона.

Закон действующий. Актуальность проверена 03.09.2021