Закон Об электронной идентификации и доверительных услугах

Глава I. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Цель и сфера применения закона

(1) Настоящий закон направлен на обеспечение надлежащего уровня функционирования национального рынка в области безопасности электронных средств идентификации и доверительных услуг, а также устанавливает основную нормативную базу для использования электронных подписей, электронных печатей, электронных меток времени, электронных документов, зарегистрированных услуг электронного распространения и услуг сертификации для аутентификации веб-страниц.

(2) Настоящий закон не ограничивает порядок использования документов.

Статья 2. Основные понятия

Для целей настоящего закона следующие понятия означают:

аутентификация – электронная процедура, позволяющая подтвердить электронную идентификацию физических и/или юридических лиц либо происхождение и целостность данных в электронной форме;

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

сертификат открытого ключа – электронный документ, содержащий открытый ключ, к которому применена электронная подпись или электронная печать поставщика доверительных услуг, который позволяет идентифицировать владельца сертификата открытого ключа и подтверждает принадлежность открытого ключа данному владельцу;

квалифицированный сертификат открытого ключа – сертификат открытого ключа, отвечающий требованиям, предусмотренным статьей 13, и который выдается поставщиком доверительных услуг, отвечающим требованиям, предусмотренным статьей 8;

сертификат электронной подписи – электронное удостоверение, связывающее данные валидации электронной подписи с физическим лицом и

подтверждающее имя данного лица;

сертификат электронной печати – электронное сертифицирование, связывающее данные валидации электронной печати с юридическим лицом и подтверждающее наименование данного лица;

квалифицированный сертификат электронной подписи – сертификат электронной подписи, выдаваемый квалифицированным поставщиком доверительных услуг и отвечающий требованиям, предусмотренным статьей 25;

квалифицированный сертификат электронной печати – сертификат электронной печати, выдаваемый квалифицированным поставщиком доверительных услуг и отвечающий требованиям, предусмотренным статьей 25;

создатель электронной печати – юридическое лицо, создающее электронную печать;

сертификат аутентификации веб-страницы – электронное сертифицирование, позволяющее аутентифицировать веб-страницу и связывающее соответствующую веб-страницу с физическим или юридическим лицом, которому выдан сертификат;

квалифицированный сертификат аутентификации веб-страницы – сертификат для аутентификации веб-страницы, выдаваемый квалифицированным поставщиком доверительных услуг и отвечающий требованиям, предусмотренным статьей 34;

открытый ключ – уникальная цифровая последовательность, сформированная при помощи устройства создания электронных подписей или электронных печатей, и которая соответствует связанному с ней закрытому ключу и предназначена для использования при проверке подлинности электронной подписи;

закрытый ключ – уникальная цифровая последовательность, сформированная при помощи устройства создания электронных подписей или электронных печатей, и которая предназначена для использования при создании электронных подписей или электронных печатей;

персональные идентификационные данные – набор данных, позволяющих установить личность физического лица либо идентификационные данные юридического лица или личность физического лица, представляющего юридическое лицо;

данные для создания электронных подписей или электронных печатей – уникальные данные, используемые подписантом или создателем электронной печати для создания электронной подписи или электронной печати;

данные для валидации – данные, используемые для валидации электронной подписи или электронной печати;

данные для проверки электронных подписей или электронных печатей – данные, используемые в целях проверки электронной подписи или электронной печати;

устройство создания электронных подписей или электронных печатей – конфигурированное программное или аппаратное обеспечение, используемое для создания электронных подписей или электронных печатей;

устройство создания квалифицированных электронных подписей или электронных печатей – устройство создания электронных подписей или электронных печатей, отвечающее требованиям, предусмотренным статьей 27;

устройство проверки электронных подписей или электронных печатей – конфигурированное программное или аппаратное обеспечение, используемое для применения данных проверки электронной подписи или электронной печати;

электронный документ – содержание в электронной форме, в частности в форме текста или звуковой, визуальной или аудиовизуальной записи, к которому применена электронная подпись или электронная печать;

электронная идентификация – процесс использования персональных идентификационных данных в электронной форме, однозначно представляющих физическое или юридическое лицо либо физическое лицо, представляющее юридическое лицо;

посредник в электронном документообороте – индивидуальный предприниматель или юридическое лицо, которое от имени подписанта или создателя электронной печати и/или получателя электронного документа организует и администрирует систему электронного документооборота и/или оказывает услуги, связанные с электронным документооборотом;

электронное средство идентификации – материальные и/или нематериальные элементы, содержащие персональные идентификационные данные и используемые для целей аутентификации в рамках услуг, доступных в режиме онлайн;

электронная метка времени – данные в электронной форме, которые соотносят другие данные в электронной форме с определенным моментом времени, устанавливая доказательство того, что последние данные существовали в соответствующий момент времени;

квалифицированная электронная метка времени – электронная метка времени, отвечающая требованиям, предусмотренным статьей 31;

поставщик доверительных услуг – индивидуальный предприниматель или юридическое лицо, предоставляющее одну или несколько доверительных услуг в качестве квалифицированного поставщика доверительных услуг или неквалифицированного поставщика доверительных услуг;

квалифицированный поставщик доверительных услуг – поставщик доверительных услуг, предоставляющий одну или несколько квалифицированных доверительных услуг, который имеет статус квалифицированного поставщика доверительных услуг, присвоенный органом надзора и контроля;

продукт – аппаратное и/или программное обеспечение или их отдельные компоненты, предназначенные для использования при предоставлении доверительных услуг;

электронная подпись – данные в электронной форме, прикрепленные к другим данным в электронной форме или логически связанные с другими данными в электронной форме, и которые используются в качестве способа аутентификации;

усиленная электронная подпись – электронная подпись, отвечающая требованиям, предусмотренным статьей 23;

квалифицированная электронная подпись – усиленная электронная подпись, созданная при помощи устройства создания квалифицированной электронной подписи и основанная на квалифицированном сертификате электронной подписи;

подписант – физическое лицо, создающее электронную подпись;

доверительная услуга – электронная услуга, предоставляемая как правило за вознаграждение, состоящая из одного или нескольких нижеперечисленных действий:

а) создание, проверка и подтверждение действительности электронных подписей, электронных печатей или электронных меток времени,

зарегистрированных услуг электронного распространения и сертификатов, относящихся к этим услугам;

b) создание, проверка и валидация сертификатов аутентификации веб-страницы;

c) хранение электронных подписей, электронных печатей или сертификатов, относящихся к этим услугам;

квалифицированная доверительная услуга – доверительная услуга, отвечающая требованиям, изложенным в настоящем законе;

электронная печать – данные в электронной форме, прикрепленные к другим данным в электронной форме или логически связанные с другими данными в электронной форме для обеспечения происхождения и целостности последних;

усиленная электронная печать – электронная печать, отвечающая требованиям, предусмотренным статьей 23;

квалифицированная электронная печать – усиленная электронная печать, созданная при помощи устройства создания квалифицированных электронных печатей и основанная на сертификате квалифицированной электронной печати;

зарегистрированная услуга электронного распространения – услуга, позволяющая передавать данные между третьими лицами с помощью электронных средств и предоставляющая доказательства обработки переданных данных, в том числе относящихся к передаче и получению данных, и которая защищает переданные данные от риска потери, кражи, повреждения или любого несанкционированного изменения;

квалифицированная зарегистрированная услуга электронного распространения – зарегистрированная услуга электронного распространения, отвечающая требованиям, предусмотренным статьей 33;

владелец сертификата открытого ключа – физическое или юридическое лицо либо физическое лицо, представляющее юридическое лицо, которое пользуется доверительными услугами;

орган надзора и контроля – центральный административный орган, наделенный в соответствии с настоящим законом полномочиями по надзору и контролю в области электронной идентификации и доверительных услуг;

валидация – процесс проверки и подтверждения действительности электронной подписи или электронной печати.

Статья 3. Взаимное признание

(1) Признание сертификатов открытых ключей за пределами Республики Молдова регулируется международными соглашениями, стороной которых является Республика Молдова. В случае если международные соглашения, стороной которых является Республика Молдова, устанавливают иные нормы, чем предусмотренные настоящим законом, применяются правила международных соглашений.

(2) Сертификат открытого ключа, выданный поставщиком доверительных услуг, проживающим или находящимся в другом государстве, признается эквивалентным с точки зрения юридических последствий, сертификату открытого ключа, выданному поставщиком доверительных услуг, проживающим или находящимся в Республике Молдова, если выполняется хотя бы одно из следующих условий:

a) поставщик доверительных услуг, проживающий или находящийся в другом государстве, был аккредитован в режиме аккредитации в соответствии с положениями настоящего закона;

b) квалифицированный поставщик доверительных услуг, проживающий или находящийся в Республике Молдова, гарантирует признание соответствующего сертификата;

c) сертификат открытого ключа или выдавший его поставщик доверительных услуг признан посредством применения двустороннего или многостороннего соглашения между Республикой Молдова и другими государствами или международными организациями на основе взаимности.

(3) Доверительные услуги и электронные документы не могут считаться не имеющими юридической силы только на основании того, что сертификат открытого ключа выдан в соответствии с правилами другого государства, если таковой был признан согласно условиям, указанным в части (2).

(4) В отступление от положений частей (1) и (2) квалифицированный сертификат открытого ключа, выданный поставщиком доверительных услуг государства–члена Европейского Союза, признается эквивалентным, с точки зрения его правовых последствий, сертификату открытого ключа, выданному поставщиком доверительных услуг, проживающим или находящимся в Республике Молдова.

(5) Порядок признания квалифицированного сертификата открытого ключа, выданного поставщиком доверительных услуг в государстве–члене Европейского Союза, определяется Правительством.

(6) Устройство проверки электронной подписи или электронной печати, используемое для проверки электронных подписей или электронных печатей в значении части (4), должно иметь подтверждение соответствия требованиям, предусмотренным настоящим законом, выданное органом надзора и контроля.

Глава II. ЭЛЕКТРОННАЯ ИДЕНТИФИКАЦИЯ И ДОВЕРИТЕЛЬНЫЕ УСЛУГИ

Часть 1. Общая информация об электронной идентификации и доверительных услугах

Статья 4. Доступность для лиц с особыми потребностями

По возможности, предоставляемые доверительные услуги и продукты, используемые для предоставления этих услуг, предназначенные для конечного пользователя, должны быть доступны лицам с особыми потребностями.

Статья 5. Идентификация лиц в информационных системах

(1) Идентификация лиц в информационных системах не может быть ограничена идентификационными данными или другими идентифицирующими их данными.

(2) В случае, если запрашивается идентификация с использованием квалифицированных доверительных услуг, используются квалифицированные доверительные услуги, предусмотренные настоящим законом.

Статья 6. Поставщик доверительных услуг

(1) Поставщики доверительных услуг могут быть квалифицированными или неквалифицированными.

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

(3) Неквалифицированные поставщики доверительных услуг устанавливают иерархию самостоятельно.

(4) Порядок организации и осуществления деятельности квалифицированных поставщиков доверительных услуг, включая их иерархию, устанавливается Правительством в соответствии с положениями настоящего закона.

(5) Учет квалифицированных поставщиков доверительных услуг ведется органом надзора и контроля в Регистре учета квалифицированных поставщиков доверительных услуг, который постоянно обновляется и доступ к которому

является открытым.

(6) Внесение в Регистр учета квалифицированных поставщиков доверительных услуг осуществляется органом надзора и контроля в день аккредитации соответствующих поставщиков.

Статья 7. Заявка на аккредитацию
Для целей аккредитации поставщик доверительных услуг представляет следующие документы:

a) заявка на аккредитацию в соответствии с образцом, установленным органом надзора и контроля;

b) банковская гарантия или страховой полис на сумму 300 000 леев;

c) регламент работы поставщика доверительных услуг;

d) копия приказа о назначении сотрудников поставщика доверительных услуг и лиц, уполномоченных подписывать сертификаты открытых ключей, а также копии удостоверяющих их личность документов;

e) копии документов, подтверждающих образование и квалификацию должностных лиц, участвующих в предоставлении услуг по сертификации;

f) схематический план расположения помещений и порядок доступа в помещения с особым режимом;

g) акт, регламентирующий хранение резервных копий регистра учета сертификатов открытых ключей;

h) порядок синхронизации со всемирным координированным временем (UTC).

Статья 8. Аккредитация поставщика доверительных услуг
(1) Поставщик доверительных услуг получает статус квалифицированного поставщика доверительных услуг после прохождения процедуры аккредитации.

(2) Квалифицированные поставщики доверительных услуг подлежат процедуре аккредитации в соответствии с положениями настоящего закона.

(3) Аккредитация поставщика доверительных услуг осуществляется органом надзора и контроля на основании поданного заявления. Аккредитация поставщика доверительных услуг является бесплатной и предоставляется на пятилетний срок, если в заявлении на аккредитацию не указан более короткий срок.

(4) Орган надзора и контроля на основании представленных документов в тридцатидневный срок принимает решение об аккредитации поставщика доверительных услуг или об отказе в аккредитации.

(5) Поставщик доверительных услуг считается квалифицированным со дня выдачи сертификата аккредитации.

(6) Порядок и подробные требования, касающиеся порядка подачи заявки, выдачи, приостановления и отзыва сертификата аккредитации квалифицированного поставщика доверительных услуг, устанавливаются Правительством.

(7) Порядок подачи заявки, выдачи, приостановления и отзыва сертификата аккредитации поставщика квалифицированных доверительных услуг установлен Законом о регулировании предпринимательской деятельности путем разрешения № 160/2011 в части, нерегулируемой настоящим законом.

(8) Информация о квалифицированных поставщиках доверительных услуг и тех, у кого аккредитация отозвана, публикуется органом надзора и контроля на своей официальной веб-странице.

(9) Квалифицированные поставщики доверительных услуг обязаны в течение всего периода аккредитации обеспечивать соблюдение требований, в соответствии с которыми они были аккредитованы. В случае возникновения обстоятельств, не позволяющих обеспечить соблюдение соответствующих требований, квалифицированный поставщик доверительных услуг уведомляет об этом орган надзора и контроля в течение 24 часов.

(10) Неквалифицированные поставщики доверительных услуг обязаны уведомить орган надзора и контроля в десятидневный срок об изменении процедур обеспечения безопасности и/или сертификации с указанием даты и времени, когда изменения вступили или вступят в силу.

(11) Квалифицированный поставщик доверительных услуг высшего уровня не подлежит аккредитации в соответствии с положениями настоящего закона.

Статья 9. Деятельность поставщика доверительных услуг

(1) Поставщик доверительных услуг:

a) создает и выдает сертификаты открытых ключей;

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

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

d) предоставляет на договорной основе доверительные услуги.

(2) Деятельность поставщика доверительных услуг представляет собой деятельность в области криптографической и технической защиты информации и подлежит лицензированию в соответствии с законодательством в области регулирования предпринимательской деятельности путем лицензирования.

Статья 10. Обязанности поставщика доверительных услуг

(1) Поставщик доверительных услуг обязан:

a) проверять подлинность данных, указанных в заявлении на сертификацию открытого ключа, на основании документов, подтверждающих соответствующие данные;

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

c) вносить сертификат открытого ключа в регистр сертификатов открытых ключей не позднее даты и времени начала течения срока действия соответствующего сертификата;

d) обеспечивать доступ к регистру сертификатов открытых ключей с соблюдением положений статьи 52;

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

f) возмещать ущерб, причиненный субъектам или физическим лицам вследствие их разумного доверия к данным, содержащимся в сертификате открытого ключа, выданном поставщиком доверительных услуг, в случае упущения им регистрации отзыва сертификата;

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

h) представлять информацию, необходимую для аутентификации доверительных услуг.

(2) Дополнительно к обязанностям, предусмотренным в части (1), квалифицированный поставщик доверительных услуг обязан:

1) сертифицировать в установленном законодательством порядке свой открытый ключ, предназначенный для сертификации открытых ключей;

2) информировать орган надзора и контроля об изменениях в предоставлении квалифицированных доверительных услуг и о намерении прекратить данную деятельность;

3) использовать безопасные системы хранения предоставленных ему данных в пригодной для проверки форме таким образом, чтобы:

a) данные были доступны общественности в исследовательских целях только при условии получения согласия лица, к которому относятся данные;

b) вводить и/или изменять сохраненные данные могли только авторизованные лица;

c) аутентификация данных могла контролироваться;

4) проверять с помощью соответствующих средств и в соответствии с законодательством личность и, при необходимости, специфические признаки физического или юридического лица, которому выдается квалифицированный сертификат. Указанная информация проверяется либо напрямую квалифицированным поставщиком доверительных услуг, либо через третью сторону:

a) в физическом присутствии лица или уполномоченного представителя юридического лица; или

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

c) посредством сертификата открытого ключа, квалифицированной электронной подписи или квалифицированной электронной печати; или

d) с использованием других методов идентификации, признанных на национальном уровне, которые обеспечивают уровень доверия, равнозначный с точки зрения надежности физическому присутствию. Альтернативные методы дистанционной идентификации лица устанавливаются Правительством;

5) принимать надлежащие меры против подделки и кражи данных;

6) регистрировать в течение установленного срока в соответствии со статьей 13 всю необходимую информацию, относящуюся к квалифицированному сертификату открытого ключа, в частности для целей предоставления доказательств сертификации в суде. Записи могут производиться с помощью электронных средств;

7) до вступления в договорные отношения с лицом, запрашивающим сертификат в целях поддержки своей доверительной услуги, информировать данное лицо посредством надежных средств связи о точных сроках и условиях использования сертификата, включая ограничения, наложенные на использование данного сертификата, о наличии системы аккредитации и процедур обжалования и разрешения споров. Информация, передаваемая в электронном виде, должна сообщаться в виде текста на легко понятном языке. Определенные части такой информации должны быть предоставлены по запросу третьим лицам, пользующимся сертификатом открытого ключа;

8) требовать выдачи дубликата сертификата аккредитации в случае его утери или повреждения;

9) производить запись и сохранять доступной в течение 15 лет, в том числе после прекращения деятельности, всю соответствующую информацию, касающуюся выданных и принятых данных, в частности для предоставления доказательств в судопроизводстве и в целях обеспечения непрерывности услуги. Данные записи могут производиться в электронном формате.

Статья 11. Заявка на сертификацию открытого ключа

(1) Заявка на сертификацию открытого ключа подается в электронной форме, подписанной электронной подписью или заверенной электронной печатью, и/или в форме документа на бумажном носителе, подписанного собственноручно заявителем.

(2) Заявка на сертификацию открытого ключа должна содержать:

a) идентификационные данные заявителя;

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

Статья 12. Рассмотрение заявки на сертификацию открытого ключа

(1) Заявка на сертификацию открытого ключа рассматривается поставщиком доверительных услуг в течение пяти рабочих дней со дня регистрации запроса,

если стороны не договорились об ином.

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

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

a) подачи заявки на сертификацию открытого ключа в нарушение положений статьи 11;

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

c) предоставления в заявке на сертификацию открытого ключа недостоверной информации.

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

(5) Решение об отказе в сертификации открытого ключа не лишает заявителя права подать новую заявку после устранения всех допущенных нарушений.

Статья 13. Сертификат открытого ключа

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

(2) Сертификат открытого ключа должен содержать:

a) единый регистрационный номер сертификата открытого ключа;

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

c) идентификационные и другие данные владельца сертификата открытого ключа в зависимости от цели, для которой выдан сертификат, а также сведения, необходимые для связи с ним;

d) открытый ключ;

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

f) данные об используемом криптографическом алгоритме;

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

h) иные сведения, предусмотренные законодательством.

(3) Квалифицированный сертификат открытого ключа выдается квалифицированным поставщиком доверительных услуг и должен дополнительно содержать:

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

b) данные проверки электронной подписи или электронной печати, соответствующие данным создания электронной подписи или электронной печати, проверенным владельцем сертификата открытого ключа, если сертификат выдан для электронных подписей или электронных печатей.

(4) В случае неквалифицированных доверительных услуг структура сертификата открытого ключа определяется поставщиком доверительных услуг в соответствии с положениями настоящего закона. В случае квалифицированных доверительных услуг структура сертификата открытого ключа определяется органом надзора и контроля в соответствии с положениями настоящего закона.

(5) Сертификат открытого ключа подписывается электронной подписью или заверяется электронной печатью поставщика доверительных услуг в соответствии с типом запрашиваемого сертификата.

(6) В случаях, установленных законом, или по соглашению сторон поставщик доверительных услуг создает сертификат открытого ключа также в форме документа на бумажном носителе в двух экземплярах. Сертификат открытого ключа в форме документа на бумажном носителе подписывается собственноручно владельцем сертификата открытого ключа и уполномоченным лицом поставщика доверительных услуг. Один экземпляр сертификата открытого ключа передается владельцу, а другой хранится у поставщика доверительных услуг.

(7) Поставщик доверительных услуг по согласованию с владельцем сертификата открытого ключа может указать в сертификате открытого ключа случаи, в которых может использоваться данный сертификат, а также ограничения на его использование.

(8) По обращению владельца сертификата открытого ключа поставщик доверительных услуг может также указать в сертификате открытого ключа и

другие сведения, помимо указанных в частях (2) и (3), при условии, что они не противоречат законодательству и не представляют угрозу для национальной безопасности или общественного порядка, а также только после предварительной проверки точности этих сведений.

(9) Поставщик доверительных услуг вносит сертификат открытого ключа в регистр сертификатов открытых ключей не позднее даты и времени начала течения срока действия сертификата.

Статья 14. Закрытый и открытый ключи

(1) Закрытый и открытый ключи, используемые для создания доверительных услуг, создаются физическим или юридическим лицом. Таковые могут создаваться третьими лицами с выраженного согласия соответствующего лица, при условии исключения возможности копирования этих ключей.

(2) Закрытый ключ и связанный с ним открытый ключ создаются одновременно.

(3) Физическое или юридическое лицо может владеть неограниченным количеством закрытых и открытых ключей.

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

(5) Открытый ключ сертифицируется поставщиком доверительных услуг и доступен для всех.

Статья 15. Срок действия и срок хранения сертификата открытого ключа

(1) Срок действия сертификата открытого ключа поставщика доверительных услуг высшего уровня составляет 20 лет, а срок действия сертификата открытого ключа поставщика доверительных услуг второго уровня – десять лет. Срок действия сертификата открытого ключа пользователя определяется поставщиком доверительных услуг, но не может превышать пяти лет, в зависимости от потенциала технических средств по созданию электронной подписи.

(2) Поставщик доверительных услуг обязан хранить сертификат открытого ключа не менее 15 лет со дня отзыва или истечения срока действия данного сертификата.

Статья 16. Приостановление действия и отзыв сертификата открытого ключа

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

(2) Поставщик доверительных услуг отзывает сертификат открытого ключа:

a) по запросу владельца сертификата открытого ключа;

b) по запросу руководителя юридического лица, в котором осуществляет деятельность владелец сертификата открытого ключа, в случае сертификатов, выданных владельцам для представительства юридического лица;

c) при обнаружении недостоверности сведений в заявке на сертификацию открытого ключа или в сертификате открытого ключа;

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

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

f) при внесении изменений в информацию, содержащуюся в сертификате открытого ключа;

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

h) по обращению органа надзора и контроля в случае нарушения положений настоящего закона.

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

(4) Поставщик доверительных услуг обязан уведомить владельца сертификата открытого ключа о причинах отзыва его сертификата, за исключением случая, когда процедура отзыва была инициирована самим владельцем.

Статья 17. Обязанности владельца сертификата открытого ключа

Владелец сертификата открытого ключа обязан:

1) обеспечивать необходимые условия для исключения доступа другого лица к его закрытому ключу;

2) не использовать закрытый ключ для доверительных услуг при имеющихся основаниях полагать, что нарушена конфиденциальность закрытого ключа;

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

a) утери закрытого ключа;

b) наличия оснований предполагать, что нарушена конфиденциальность закрытого ключа;

c) содержания в сертификате открытого ключа недостоверных сведений;

4) уведомлять в течение 24 часов поставщика доверительных услуг об изменениях в информации, содержащейся в сертификате открытого ключа;

5) выполнять другие обязанности, предусмотренные настоящим законом и соглашением, заключенным с поставщиком доверительных услуг.

Статья 18. Регистр сертификатов открытых ключей

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

(2) Регистр сертификатов открытых ключей содержит:

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 информацию в соответствии с нормативными актами в области доверительных услуг.

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

Часть 2. Электронная подпись и электронная печать

Статья 19. Принципы использования электронной подписи и электронной печати

Принципами использования электронной подписи и электронной печати являются:

a) свобода выбора и использования любого вида электронной подписи или электронной печати, если нормативными актами либо соглашением сторон не предусмотрено использование конкретного вида электронных подписей или электронных печатей в соответствии с целями их использования;

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

c) недопустимость ссылки на отсутствие юридической силы электронной подписи или электронной печати и/или электронного документа, к которому она применена, только на том основании, что электронная подпись или электронная печать была создана при помощи устройства создания электронных подписей или электронных печатей и/или продукта.

Статья 20. Виды электронных подписей и электронных печатей

Электронные подписи и электронные печати, принципы и механизмы использования которых регулируются настоящим законом, могут быть:

a) усиленными;

b) квалифицированными.

Статья 21. Правовой режим использования электронной подписи и электронной печати

(1) Электронные подписи и электронные печати, вне зависимости от степени их защиты, имеют правовые последствия и допустимы в качестве доказательств, в том числе в судопроизводстве, при том, что они:

a) имеют электронную форму; или

b) не основаны на сертификате, выданном поставщиком доверительных услуг; или

c) не основаны на квалифицированном сертификате открытого ключа; или

d) не созданы при помощи устройства создания электронных подписей или электронных печатей.

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

(3) К квалифицированным электронным подписям и квалифицированным электронным печатям применяется презумпция целостности данных и правильности происхождения соответствующих данных, к которым относится квалифицированная электронная подпись или квалифицированная электронная печать.

(4) Порядок обеспечения степени защиты квалифицированной электронной подписи в целях ее приравнивания к собственноручной подписи на бумажном носителе определяется органом надзора и контроля в соответствии с частью (2) статьи 35.

(5) Порядок применения электронных подписей и электронных печатей работниками юридических лиц публичного права устанавливается Правительством. Юридические лица частного права самостоятельно определяют порядок применения электронных подписей и электронных печатей своими представителями.

(6) Электронные подписи и электронные печати не являются средствами шифрования информации.

Статья 22. Ограничения на использование некоторых видов электронных подписей или электронных печатей

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

a) применения к электронным документам, содержащим сведения, отнесенные к государственной тайне;

b) применения к электронным документам 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 усиленной электронной подписью электронных документов, содержащих сведения, отнесенные к государственной тайне, лицами, идентичность и статус которых составляют государственную тайну в соответствии с положениями Закона о государственной тайне № 245/2008, из состава Службы информации и безопасности, Национального центра по борьбе с коррупцией и Министерства внутренних дел в рамках их электронного документооборота.

Статья 23. Требования к усиленным электронным подписям и электронным печатям

Усиленные электронные подписи или электронные печати должны в совокупности отвечать следующим требованиям:

a) делать ссылку непосредственно на владельца;

b) позволять идентифицировать владельца;

c) создаваться с использованием данных для создания электронных подписей или данных для создания электронных печатей, которые подписант или создатель электронной печати может использовать с высокой степенью уверенности, под своим исключительным контролем;

d) быть связанными с данными, к которым они относятся таким образом, чтобы любое последующее изменение этих данных могло быть обнаружено.

Статья 24. Требования к квалифицированным электронным подписям и электронным печатям

Квалифицированные электронные подписи или электронные печати отвечают всем требованиям к усиленным электронным подписям или электронным печатям, а также дополнительно:

a) основываются на квалифицированном сертификате открытого ключа, выданном квалифицированным поставщиком доверительных услуг;

b) создаются при помощи устройства создания электронных подписей или электронных печатей и проверяются при помощи устройства проверки электронных подписей или электронных печатей и/или продукта, которые имеют подтверждение соответствия требованиям настоящего закона.

Статья 25. Требования к квалифицированным сертификатам электронных подписей или электронных печатей

(1) Квалифицированные сертификаты электронных подписей или электронных печатей содержат:

a) отметку в пригодной для автоматической обработки форме, что сертификат выдан в качестве квалифицированного сертификата электронных подписей или электронных печатей;

b) идентификационные данные квалифицированного поставщика доверительных услуг, выдающего квалифицированные сертификаты;

c) идентификационные и другие данные подписанта или создателя электронной печати;

d) данные валидации электронных подписей или электронных печатей, соответствующие данным для их создания;

e) дату и время начала течения срока действия сертификата и дату и время его окончания;

f) единый регистрационный номер сертификата;

g) данные проверки квалифицированного сертификата электронной подписи или электронной печати, соответствующие данным для их создания.

(2) Дополнительно к требованиям части (1) квалифицированные сертификаты электронных подписей или электронных печатей содержат:

a) квалифицированную электронную подпись или электронную печать квалифицированного поставщика доверительных услуг – эмитента; или

b) усиленную электронную подпись или усиленную электронную печать квалифицированного поставщика доверительных услуг – эмитента, проживающего или находящегося в другом государстве, в случае квалифицированных сертификатов электронных подписей или электронных печатей, признанных в соответствии со статьей 3; или

c) усиленную электронную подпись или усиленную электронную печать поставщика доверительных услуг высшего уровня – в случае квалифицированных сертификатов электронных подписей или электронных печатей аккредитованных поставщиков доверительных услуг.

Статья 26. Создание электронной подписи или электронной печати

(1) Создание электронной подписи или электронной печати осуществляется при помощи устройства создания электронных подписей или электронных печатей и/или продукта с использованием данных для создания электронной подписи или электронной печати.

(2) Генерация или управление данными для создания квалифицированной электронной подписи или квалифицированной электронной печати от имени подписанта или создателя электронной печати может осуществляться только квалифицированным поставщиком доверительных услуг с согласия владельца сертификата открытого ключа.

Статья 27. Требования к устройствам создания электронных подписей или электронных печатей

(1) Устройства создания усиленных или квалифицированных электронных подписей или электронных печатей должны обеспечивать с помощью соответствующих технических средств и процедур как минимум, что:

a) данные для создания электронных подписей или электронных печатей могут появиться только один раз, а их конфиденциальность обеспечивается в соответствии с настоящим законом;

b) данные о создании электронных подписей или электронных печатей не могут быть вычислены путем расчета, а электронная подпись или электронная печать защищены от возможных подделок с помощью технических средств, доступных на соответствующий момент;

c) данные для создания электронной подписи или электронной печати надежно защищены подписантом или создателем электронной подписи от использования другими лицами;

d) предоставляется возможность отображения содержания электронного документа, подписанного электронной подписью или заверенного электронной печатью, либо делается неотзываемая ссылка на данный документ;

e) электронная подпись или электронная печать создается только после подтверждения подписантом или создателем электронной печати операции по созданию электронных подписей или электронных печатей;

f) однозначно подтверждается создание электронной подписи или электронной печати.

(2) Генерирование или управление данными для создания электронных подписей или электронных печатей от имени подписанта или создателя электронной печати может осуществляться только квалифицированным поставщиком доверительных услуг.

(3) Усиленные или квалифицированные устройства создания электронных подписей или электронных печатей не должны изменять данные, к которым применена усиленная или квалифицированная электронная подпись либо усиленная или квалифицированная электронная печать, либо препятствовать предоставлению соответствующих данных подписанту или создателю электронной подписи до подписания или применения электронной печати.

Статья 28. Проверка подлинности электронной подписи или электронной печати

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

(2) При проверке усиленной электронной подписи или усиленной электронной печати, а также квалифицированной электронной подписи и квалифицированной электронной печати устройство для проверки электронных подписей или электронных печатей и/или продукт должны:

a) обеспечивать возможность отображения содержания электронного документа или однозначно делать ссылку на данный документ;

b) отображать факт изменения электронного документа;

c) ссылаться на подписанта или создателя электронной печати.

(3) При проверке усиленной электронной подписи или электронной печати, а также квалифицированной электронной подписи или квалифицированной электронной печати с достаточной степенью надежности должно обеспечиваться, что:

a) данные для проверки электронных подписей или электронных печатей соответствуют данным, отображаемым проверяющему электронную подпись или электронную печать лицу;

b) электронная подпись или электронная печать проверяется с достоверностью, а результат проверки и идентичность подписанта или создателя электронной печати отображаются правильно;

c) подлинность и действительность сертификата открытого ключа, требуемого во время проверки электронной подписи или электронной печати, достоверно проверены;

d) содержание сертификата открытого ключа четко отображается;

e) изменения, которые могут повлиять на безопасность электронной подписи или электронной печати, могут быть обнаружены.

Статья 29. Требования к валидации квалифицированной электронной подписи и квалифицированной электронной печати

Процесс валидации квалифицированной электронной подписи или электронной печати подтверждает их действительность при соблюдении следующих условий:

a) сертификат, лежащий в основе электронной подписи или электронной печати, на момент подписания или заверения печатью являлся квалифицированным сертификатом электронной подписи или электронной печати в соответствии со статьей 25;

b) квалифицированный сертификат был выдан квалифицированным поставщиком доверительных услуг и был действителен на момент применения электронной подписи или электронной печати;

c) данные валидации электронных подписей или электронных печатей соответствуют данным, предоставленным владельцем сертификата открытого ключа;

d) уникальный набор данных, представляющий подписанта или создателя электронной печати в сертификате, предоставлен владельцу сертификата открытого ключа правильно;

e) на использование псевдонима четко указывается владельцу сертификата открытого ключа в случае, если во время подписания использовался псевдоним;

f) электронная подпись или электронная печать была создана при помощи устройства создания квалифицированной электронной подписи или электронной печати;

g) целостность данных, к которым применена электронная подпись или электронная печать, не была нарушена;

h) требования, предусмотренные в статье 24, были выполнены на момент подписания.

Часть 3. Электронные метки времени

Статья 30. Правовые последствия электронных меток времени

(1) Электронная метка времени не может не иметь правовых последствий и быть допустимой в качестве доказательства в судопроизводстве только на основании того, что она существует в электронной форме или не отвечает требованиям, предъявляемым к квалифицированной электронной метке времени.

(2) К квалифицированной электронной метке времени применяется презумпция точности даты и времени, на которые она указывает, а также презумпция целостности данных, к которым относятся указанные дата и время.

Статья 31. Требования к электронным меткам времени

(1) Требования к усиленным электронным меткам времени устанавливаются поставщиками доверительных услуг.

(2) Квалифицированная электронная метка времени выдается квалифицированным поставщиком доверительных услуг и отвечает следующим требованиям:

a) обеспечивает связь между датой и временем и другими данными таким образом, чтобы разумно исключить возможность изменения данных без обнаружения;

b) основана на источнике точного определения времени, привязанном к всемирному координированному времени;

c) к ней применена квалифицированная электронная подпись или квалифицированная электронная печать квалифицированного поставщика доверительных услуг или усиленная электронная подпись либо усиленная электронная печать квалифицированного поставщика доверительных услуг – эмитента, проживающего или находящегося в другом государстве, в случае электронных меток времени, признанных в соответствии со статьей 3.

Часть 4. Зарегистрированная услуга электронного распространения и аутентификации веб-страниц

Статья 32. Правовые последствия зарегистрированной услуги электронного распространения

(1) Данные, переданные и полученные с использованием зарегистрированной услуги электронного распространения, не могут не иметь правовых последствий и быть допустимы в качестве доказательств в судебном процессе только на том основании, что они находятся в электронной форме или что они не отвечают требованиям, предъявляемым к квалифицированной зарегистрированной услуге электронного распространения.

(2) К данным, отправленным и полученным с помощью квалифицированной зарегистрированной услуги электронного распространения, применяется презумпция полноты данных, отправленных идентифицированным отправителем и полученных идентифицированным получателем, а также презумпция точности даты и времени отправки и принятия указанных данных зарегистрированной услугой электронного распространения.

Статья 33. Требования к квалифицированным зарегистрированным услугам электронного распространения

Квалифицированные зарегистрированные услуги электронного распространения отвечают следующим требованиям:

a) предоставляются одним или несколькими квалифицированными поставщиками доверительных услуг;

b) обеспечивают идентификацию отправителя;

c) обеспечивают идентификацию получателя до отправления данных;

d) отправка и принятие данных защищены электронной подписью или электронной печатью квалифицированного поставщика доверительных услуг таким образом, чтобы исключить возможность изменения данных без обнаружения;

e) изменение данных, необходимое для целей отправки или принятия данных, четко указывается отправителю и получателю данных;

f) дата и время отправки, принятия и изменения данных отмечается квалифицированной электронной меткой времени.

Статья 34. Требования к квалифицированным серти- фикатам аутентификации веб-страниц

Квалифицированные сертификаты аутентификации веб-страниц должны содержать:

a) отметку в доступной для автоматической формы обработки о том, что сертификат выдан в качестве квалифицированного сертификата для аутентификации веб-страницы;

b) идентификационные данные квалифицированного поставщика доверительных услуг, выдающего квалифицированные сертификаты;

c) идентификационные и другие данные владельца сертификата открытого ключа, а также информацию, необходимую для связи с владельцем;

d) дату и время начала течения срока действия сертификата и дату и время окончания этого срока;

e) имя домена (доменов), управляемого (управляемых) владельцем сертификата открытого ключа, которому был выдан сертификат;

f) единый регистрационный номер сертификата;

g) квалифицированную электронную подпись или электронную печать квалифицированного поставщика доверительных услуг – эмитента или усиленную электронную подпись или электронную печать квалифицированного поставщика доверительных услуг – эмитента, проживающего или находящегося в другом государстве, в случае квалифицированных сертификатов аутентификации веб-сайта, признанных в соответствии со статьей 3;

h) данные проверки квалифицированного сертификата аутентификации веб-страницы, соответствующие данным о ее создании.

Глава III. НАДЗОР И КОНТРОЛЬ

Статья 35. Орган надзора и контроля

(1) Органом надзора и контроля является Служба информации и безопасности Республики Молдова.

(2) Орган надзора и контроля исполняет следующие полномочия:

a) отвечает за разработку и реализацию государственной политики и осуществление контроля в области доверительных услуг;

b) осуществляет аккредитацию поставщиков доверительных услуг и отзывает соответствующий статус;

c) выполняет функции квалифицированного поставщика доверительных услуг высшего уровня для квалифицированных поставщиков доверительных услуг;

d) обеспечивает ведение, обновление и открытый доступ к данным Регистра учета поставщиков доверительных услуг;

e) ведет и публикует в защищенном виде безопасные списки, к которым применена электронная подпись или электронная печать органа надзора и контроля, содержащие сведения, в доступной для автоматической формы обработки, о квалифицированных поставщиках доверительных услуг и предоставляемых ими квалифицированных доверительных услугах;

f) разрабатывает и утверждает посредством нормативных актов требования в области доверительных услуг;

g) осуществляет надзор и контроль за соблюдением требований в отношении предоставления доверительных услуг;

h) участвует в разработке и утверждении технических регламентов и стандартов в области доверительных услуг;

i) оказывает по запросу методическую и практическую помощь в использовании доверительных услуг;

j) осуществляет надзор за квалифицированными поставщиками доверительных услуг в отношении качества и безопасности предоставляемых ими квалифицированных доверительных услуг, а также за выполнением требований, установленных настоящим законом;

k) приостанавливает или отзывает аккредитацию поставщика доверительных услуг, если он не отвечает требованиям в области доверительных услуг;

l) сотрудничает с национальным органом по защите персональных данных, в частности посредством его информирования без необоснованных задержек о результатах проверок квалифицированных поставщиков доверительных услуг в случае, если предполагается, что нарушены правила защиты персональных данных;

m) требует от поставщиков доверительных услуг устранить нарушения требований настоящего закона;

n) осуществляет международное сотрудничество в области доверительных услуг.

(3) Орган публичной власти или публичное учреждение, ответственное за предоставление услуги единого источника синхронизации со всемирным координированным временем (UTC), устанавливается Правительством.

Статья 36. Контроль в области доверительных услуг

(1) Контроль за соблюдением установленных настоящим законом требований в отношении предоставления доверительных услуг и аккредитации или продления срока аккредитации осуществляется органом надзора и контроля.

(2) Контроль осуществляется Комиссией по контролю за доверительными услугами (далее – Комиссия) на основании положения, утвержденного органом надзора и контроля.

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

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

(5) Комиссия вправе:

a) иметь свободный доступ к документальным материалам на бумажном носителе и в электронном формате, необходимым для осуществления видов деятельности, связанных с предоставлением доверительных услуг, а также доступ к системам распространения программных приложений, к установленным программным приложениям и аппаратным средствам;

b) получать полные сведения об условиях и порядке эксплуатации программных и аппаратных средств;

c) получать от ответственных лиц и персонала поставщика доверительных услуг сведения о предоставлении доверительных услуг, подлежащих контролю;

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

(6) Комиссия не вправе проводить проверки без представления приказа о проведении проверки и документов, удостоверяющих личность членов комиссии.

(7) При проведении проверок за соблюдением предусмотренных настоящим законом требований Комиссия принимает во внимание следующее:

a) законность и соблюдение установленных законом компетенций;

b) недопущение применения не установленных законом санкций;

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

d) осуществление контроля за счет государства;

e) выдача предписаний по устранению выявленных в результате контроля нарушений;

f) право поставщика доверительных услуг на обжалование действий органа надзора и контроля, в том числе в судебную инстанцию.

(8) Плановые проверки соблюдения квалифицированным поставщиком доверительных услуг требований и обязанностей, предусмотренных настоящим законом, проводятся органом надзора и контроля не чаще одного раза в течение календарного года с привлечением, при необходимости, представителей учреждений с регулирующими и контрольными функциями согласно компетенции.

(9) Планы проверок, разработанные органом надзора и контроля и утвержденные в установленном порядке, согласовываются в отношении сроков

проведения с руководством поставщика доверительных услуг не позднее чем за пять рабочих дней до начала данных проверок.

(10) Внеплановые проверки проводятся по решению органа надзора и контроля только на основании:

a) выявления и подтверждения органом надзора и контроля нарушений настоящего закона; и/или

b) поступления в адрес органа надзора и контроля обоснованных заявлений и жалоб в письменной форме относительно нарушений или ненадлежащего исполнения поставщиком доверительных услуг требований, предусмотренных настоящим законом.

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

(12) Повторные проверки проводятся только с целью проверки выполнения предписания об устранении нарушений настоящего закона, указанного в акте предыдущего контроля (планового или внепланового). Повторный контроль считается составной частью предыдущего контроля.

(13) Контроль осуществляется в строго установленные приказом сроки о проведении контроля.

(14) Срок проведения плановых проверок и внеплановых проверок не может превышать десяти рабочих дней, а повторных проверок – пяти рабочих дней. В случае внеплановых проверок десятидневный срок может быть продлен еще на десять дней руководителем органа надзора и контроля на основании мотивированного решения, доведенного до сведения проверяемого поставщика доверительных услуг, которое может быть обжаловано поставщиком доверительных услуг.

(15) При проведении проверки за соблюдением предусмотренных настоящим законом требований и обязанностей поставщик доверительных услуг представляет информацию и документы, относящиеся к цели проверки, и не препятствует ее осуществлению.

(16) По результатам проверки составляется акт в двух экземплярах, один из которых не позднее пяти рабочих дней после завершения проверки направляется/вручается поставщику доверительных услуг, а второй хранится в органе надзора и контроля. В случае несогласия с результатами проведенной проверки поставщик доверительных услуг в течение десяти рабочих дней со дня получения акта проверки может представить в письменном виде обоснование

несогласия, приложив соответствующие документы.

(17) В случае установления нарушения требований, предусмотренных настоящим законом, орган надзора и контроля на основании акта проверки выдает предписание об устранении этих нарушений, содержащее рекомендации по устранению всех установленных нарушений, а также предупреждение о возможном приостановлении или отзыве аккредитации в случае, если таковые не будут устранены в установленный срок.

(18) Срок устранения установленных нарушений составляет 15 рабочих дней, исчисляемых со дня, следующего за днем получения предписания, направленного/врученного вместе с актом проверки.

(19) Если поставщик доверительных услуг не устранил все установленные нарушения в установленный срок, по его официальному обращению срок для устранения нарушений продлевается на запрошенный поставщиком доверительных услуг период, но не более чем на 20 рабочих дней.

(20) Квалифицированный поставщик доверительных услуг, получивший предписание об устранении нарушения требований, предусмотренных настоящим законом, обязан в установленный предписанием срок представить органу надзора и контроля информацию об устранении нарушений.

(21) Информация о результатах проверки публикуется органом надзора и контроля на его официальной веб-странице.

(22) Поставщик доверительных услуг вправе обратиться с письменной жалобой на допущенные Комиссией нарушения положений настоящего закона в орган надзора и контроля или обжаловать ее действия в судебную инстанцию.

Статья 37. Приостановление и возобновление действия аккредитации

(1) Действие аккредитации приостанавливается в соответствии с законодательством в области регулирования предпринимательской деятельности.

(2) Основанием для реализации предусмотренных законом мер по приостановлению действия аккредитации являются:

a) заявление квалифицированного поставщика доверительных услуг о приостановлении действия аккредитации;

b) нарушение поставщиком доверительных услуг требований и обязанностей, предусмотренных настоящим законом;

c) выявление недостоверных данных в документах, представленных в орган надзора и контроля;

d) недействительность банковской гарантии или страхового полиса;

e) невыполнение поставщиком доверительных услуг предписания об устранении нарушения требований, предусмотренных настоящим законом, установленных в результате проведенной Комиссией проверки.

(3) Решение о приостановлении действия аккредитации доводится до сведения квалифицированного поставщика доверительных услуг в течение трех рабочих дней со дня его принятия. Срок приостановления действия аккредитации не может превышать двух месяцев.

(4) Поставщик квалифицированных доверительных услуг обязан письменно уведомить орган надзора и контроля об устранении обстоятельств, повлекших приостановление действия аккредитации.

(5) Решение о возобновлении действия аккредитации принимается органом надзора и контроля на основании решения судебной инстанции, вынесшей решение о приостановлении ее действия, или на основании решения вышестоящей судебной инстанции в течение трех рабочих дней со дня получения уведомления. Решение доводится до сведения поставщика доверительных услуг в течение трех рабочих дней со дня его принятия.

(6) Срок действия аккредитации не продлевается в период ее приостановления.

Статья 38. Отзыв аккредитации

(1) Аккредитация отзывается в соответствии с законодательством в области регулирования предпринимательской деятельности.

(2) Основанием для реализации предусмотренных законом мер по отзыву аккредитации являются:

a) заявка квалифицированного поставщика доверительных услуг о прекращении деятельности, поданная за 30 дней до планируемого прекращения деятельности;

b) решение об аннулировании государственной регистрации индивидуального предпринимателя или юридического лица, в рамках которого осуществляет деятельность поставщик доверительных услуг;

c) установление передачи сертификата аккредитации или его копии другому лицу для осуществления аккредитованного вида деятельности;

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

e) повторное невыполнение предписаний об устранении нарушения требований, установленных настоящим законом.

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

(4) Все сертификаты открытых ключей, выданные прекратившим деятельность квалифицированным поставщиком доверительных услуг, отзываются и передаются на хранение другому квалифицированному поставщику доверительных услуг в порядке, установленном органом надзора и контроля, за счет прекратившего деятельность поставщика доверительных услуг.

(5) Квалифицированный поставщик доверительных услуг обязан в течение десяти рабочих дней со дня принятия решения об отзыве аккредитации сдать в орган надзора и контроля отозванный сертификат аккредитации.

Статья 39. Требования к безопасности для поставщиков доверительных услуг

(1) Квалифицированные и неквалифицированные поставщики доверительных услуг применяют соответствующие технические и организационные меры для управления рисками в отношении безопасности доверительных услуг, которые они предоставляют.

(2) Квалифицированные и неквалифицированные поставщики доверительных услуг не позднее 24 часов с момента установления должны уведомить орган надзора и контроля о нарушении безопасности или утрате целостности, которое оказывает существенное влияние на предоставляемую доверительную услугу или хранящиеся у них персональные данные. В случае если нарушение безопасности или утрата целостности может оказать негативное влияние на физическое или юридическое лицо, которому была предоставлена услуга доверия, поставщик доверительных услуг уведомляет также соответствующее физическое или юридическое лицо о нарушении безопасности или утрате целостности без необоснованной задержки.

(3) Уведомленный орган надзора и контроля информирует общественность или требует сделать это от поставщика доверительных услуг, если считает, что раскрытие информации о нарушении безопасности или утрате целостности служит общественным интересам.

Статья 40. Правовой режим использования электронного документа

(1) Электронный документ, подписанный квалифицированной электронной подписью, приравнивается по своим последствиям к равнозначному подобному документу на бумажном носителе, подписанному собственноручной подписью.

(2) Электронный документ, подписанный другим типом электронной подписи, кроме квалифицированной, приравнивается по своим последствиям к подобному документу на бумажном носителе, подписанному собственноручной подписью, только в случаях, прямо установленных нормативными актами или соглашением сторон о применении электронных подписей или электронных печатей, с соблюдением требований, установленных в части (1) статьи 43.

(3) Нормативные акты или соглашение сторон о применении электронных подписей, устанавливающие случаи признания электронных документов, подписанных иным видом электронной подписи, чем квалифицированная электронная подпись, приравненные по своим последствиям к подобным документам на бумажном носителе, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи, а также обязанности сторон о конфиденциальности и материальной ответственности.

(4) В случае если в соответствии с законодательством требуется, чтобы документ был оформлен или представлен на бумажном носителе и подписан собственноручной подписью, электронный документ считается соответствующим этим требованиям.

(5) В случае если в соответствии с законодательством требуется, чтобы документ на бумажном носителе был заверен печатью, электронный документ считается соответствующим этому требованию.

(6) К нескольким связанным между собой электронным документам (пакет электронных документов) может применяться одна электронная подпись или одна электронная печать.

(7) Порядок использования электронных документов в рамках судопроизводства регулируется процессуальным законодательством.

(8) Электронный документ по своей доказательной силе приравнивается к письменным доказательствам или материальным средствам доказывания и не может быть отклонен в качестве доказательства только по причине его электронной формы.

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

(10) Все идентичные экземпляры электронного документа считаются оригиналами и имеют одинаковые правовые последствия.

(11) Если лицом создается электронный документ и идентичный по содержанию документ на бумажном носителе, подписанный собственноручной подписью, оба документа признаются самостоятельными и оригинальными.

(12) Копией электронного документа признается его представление (отображение) на бумажном носителе в доступной для восприятия форме. Копия электронного документа удостоверяется в порядке, предусмотренном законодательством для удостоверения копий документов на бумажном носителе, и содержит отметку о том, что она является копией электронного документа.

Глава IV. ПРАВОВОЙ РЕЖИМ ЭЛЕКТРОННОГО ДОКУМЕНТА И ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Статья 41. Области и цель использования электронного документа

(1) Электронный документ может использоваться физическими и юридическими лицами во всех сферах деятельности, в которых возможно использование программных и аппаратных средств, позволяющих создавать, обрабатывать, отправлять, принимать, хранить, изменять и/или уничтожать информацию в электронной форме.

(2) Электронный документ может использоваться для передачи информации, ведения переписки, составления юридических документов, а также в качестве документа, отражающего экономические факты.

Статья 42. Требования к электронному документу

Электронный документ должен отвечать следующим основным требованиям:

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

b) содержать для подтверждения подлинности документа одну или несколько электронных подписей или электронных печатей, отвечающих условиям и требованиям, установленным настоящим законом;

c) создаваться и использоваться способом и в форме, которые позволяют идентифицировать подписанта или создателя электронной печати;

d) отображаться в форме, доступной для восприятия;

e) быть доступным для неоднократного использования.

Статья 43. Подлинность электронного документа
(1) Электронный документ считается подлинным, если соответствует в совокупности следующим условиям:

a) электронная подпись или электронная печать применяется лицом, уполномоченным в установленном порядке подписывать собственноручной подписью эквивалентный документ на бумажном носителе;

b) электронный документ подписывается подлинной электронной подписью или заверяется подлинной электронной печатью подписанта или создателя электронной печати, указанного в документе.

(2) Проверка подлинности электронного документа осуществляется путем проверки электронной подписи или электронной печати при помощи устройств проверки электронных подписей или электронных печатей и/или продукта.

Статья 44. Организация электронного документооборота
(1) Электронный документооборот организуется в соответствии с положениями настоящего закона и правилами, установленными собственником системы электронного документооборота, а также в соответствии с договорами, заключенными между субъектами электронного документооборота.

(2) Электронный документооборот может включать:

a) создание и обработку электронных документов с применением электронной подписи или электронной печати;

b) отправку и получение электронных документов;

c) проверку подлинности электронных документов;

d) подтверждение получения электронных документов;

e) учет электронных документов;

f) хранение, изменение и/или уничтожение электронных документов;

g) создание дополнительных экземпляров электронных документов;

h) создание и заверение копий электронных документов на бумажном носителе;

i) проставление электронной метки времени.

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

Статья 45. Посредник в электронном документообороте

(1) В организации и осуществлении электронного документооборота могут участвовать посредники в соответствии с требованиями настоящего закона и с правилами, установленными собственником системы электронного документооборота.

(2) Посредник в электронном документообороте обязан:

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

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

c) обеспечивать необходимые условия для 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 46. Создание электронного документа

(1) Электронный документ включает информацию, составляющую содержание электронного документа, и электронную подпись или электронную печать подписанта или создателя электронной печати.

(2) Создание электронного документа завершается применением электронной подписи или электронной печати подписантом или создателем электронной печати и, при необходимости, проставлением электронной метки времени.

Статья 47. Отправка и получение электронного документа

(1) Электронный документ может отправляться и приниматься с помощью электронных информационно-коммуникационных систем и/или материальных носителей.

(2) Электронный документ отправляется способом, позволяющим получателю его хранить и использовать.

(3) В случае если подписант или создатель электронной печати и адресат электронного документа не условились об ином, электронный документ считается отправленным, если таковой:

a) отправлен подписантом или создателем электронной печати либо посредником в электронном документо-обороте, действующим от имени подписанта или создателя электронной печати, или через информационную систему, используемую подписантом или создателем электронной печати;

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

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

d) поступает в информационную систему, не контролируемую ни подписантом, ни создателем электронной печати, ни посредником в электронном документообороте, отправляющим электронный документ от имени подписанта или создателя электронной печати.

(4) В случае если подписант и адресат электронного документа не условились об ином, электронный документ считается принятым получателем, если таковой:

a) поступает в информационную систему, из которой получатель может 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, указанное в электронном документе в качестве подписанта, не является таковым;

b) подписант не является инициатором отправки электронного документа;

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

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

Статья 48. Момент отправки и получения электронного документа

(1) Если подписант или создатель электронной печати и получатель электронного документа не условились об ином, моментом отправки электронного документа считается момент его поступления в информационную систему, не контролируемую ни подписантом, ни создателем электронной печати, ни посредником в электронном документообороте, отправляющим электронный документ от имени подписанта или создателя электронной печати.

(2) Если подписант или создатель электронной печати и адресат электронного документа не условились об ином, моментом получения электронного документа считается момент его поступления в указанную получателем информационную систему. Если получатель электронного документа не указал соответствующую информационную систему, электронный документ считается полученным им с момента поступления в информационную систему получателя, а в случае отсутствия у получателя такой системы – с момента извлечения получателем электронного документа из информационной системы, посредством которой он был отправлен.

(3) Момент отправки электронного документа в информационной системе может быть подтвержден при необходимости проставлением электронной метки времени в соответствующем электронном документе.

(4) Если подписант или создатель электронной печати и получатель электронного документа условились о необходимости подтверждения получения электронного документа, моментом его получения считается момент отправления получателем подтверждения получения электронного документа с проставлением, при необходимости, электронной метки времени.

Статья 49. Учет электронных документов

(1) Учет электронных документов физических и/или юридических лиц осуществляется в соответствии с законодательством о регистрах.

(2) Ведение электронных регистров включает технологические и программные процедуры их заполнения и администрирования, а также средства хранения электронных документов.

Глава V. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ. ПРАВОВАЯ ОТВЕТСТВЕННОСТЬ

Статья 50. Хранение электронных документов

(1) Субъекты электронного документооборота обязаны хранить оригиналы электронных документов в форме, позволяющей проверять их подлинность.

(2) Срок хранения электронных документов идентичен сроку, предусмотренному законодательством для хранения равнозначных 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 51. Защита электронного документа

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

(2) Информация, составляющая содержание электронного документа, используется и защищается согласно законодательству 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. Требования безопасности для систем электронного документооборота юридических лиц частного права 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 и время его создания, отправки и получения.

Статья 52. Защита персональных данных

Поставщики доверительных услуг обеспечивают соблюдение законодательства в области защиты персональных данных в процессе предоставления доверительных услуг.

Статья 53. Ответственность физических и юридических лиц, подпадающих под действие настоящего закона

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

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

(3) Споры, возникающие в рамках электронного документооборота, а также связанные с использованием электронных документов и доверительных услуг, разрешаются субъектами электронного документооборота в соответствии с законодательством и заключенными договорами.

Статья 54. Ответственность поставщика доверительных услуг и бремя доказывания

(1) Поставщик доверительных услуг несет гражданско-правовую ответственность за ущерб, причиненный в результате невыполнения требований, предусмотренных настоящим законом, за исключением случаев, когда поставщик доверительных услуг представит соответствующие доказательства того, что он не мог предотвратить причинение ущерба.

(2) Бремя доказывания умысла или халатности неквалифицированного поставщика доверительных услуг лежит на физическом или юридическом лице, требующем компенсации за причиненный ущерб.

(3) К умыслу или халатности квалифицированного поставщика доверительных услуг применяется презумпция до тех пор, пока не будет доказано обратное.

(4) Поставщики доверительных услуг не несут ответственность за ущерб, причиненный в результате использования услуг, превышающих установленные ограничения, если поставщики соответствующим образом предварительно информируют клиентов об ограничениях на использование предоставляемых ими услуг.

Статья 55. Ответственность владельца сертификата открытого ключа

Владелец сертификата открытого ключа несет гражданско-правовую ответственность за ущерб, причиненный:

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

b) использованием доверительных услуг, включая период от подачи запроса о приостановлении действия или отзыве сертификата открытого ключа до внесения в установленный срок соответствующей записи в регистр сертификатов открытых ключей, если владелец сертификата не предоставит соответствующие доказательства того, что электронный документ подписан другим лицом.

Глава VI. ЗАКЛЮЧИТЕЛЬНЫЕ И ПЕРЕХОДНЫЕ ПОЛОЖЕНИЯ

Статья 56. Заключительные положения

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

(2) Со дня вступления в силу настоящего закона признать утратившим силу Закон об электронной подписи и электронном документе № 91/2014.

(3) Правительству в шестимесячный срок со дня опубликования настоящего закона:

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

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

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

Статья 57. Переходные положения

(1) Сертификаты открытых ключей, выданные на основании Закона об электронной подписи и электронном документе № 91/2014, действительны до истечения срока их действия.

(2) В двенадцатимесячный срок со дня вступления в силу настоящего закона поставщики услуг сертификации открытых ключей, аккредитованные на основании Закона об электронной подписи и электронном документе № 91/2014, обязаны пройти процедуру аккредитации в соответствии с положениями настоящего закона.

(3) Если поставщики услуг сертификации открытых ключей, аккредитованные на основании Закона об электронной подписи и электронном документе № 91/2014, не прошли процедуру аккредитации в соответствии с положениями настоящего закона в срок, установленный в части (2) настоящей статьи, их сертификат аккредитации отзывается.

Закон действующий. Актуальность проверена 03.09.2021