Принят на шестнадцатом
пленарном заседании
Межпарламентской Ассамблеи
государств - участников СНГ
(постановление № 16-10 от
9 декабря 2000 года

МОДЕЛЬНЫЙ ЗАКОН
Об электронной цифровой подписи

Глава 1. Общие положения

Статья 1. Цели и сфера применения настоящего Закона

Цель настоящего Закона - обеспечить правовые условия для использования электронных цифровых подписей, при соблюдении которых подпись признается достоверной. Настоящим Законом устанавливаются также права, обязанности и ответственность организаций, предоставляющих услуги по удостоверению электронных цифровых подписей.

Закон не распространяется на использование иных электронных аналогов собственноручной подписи, в том числе на оцифрованное изображение личной подписи, а также на использование средств криптозащиты электронного сообщения.

Использование электронной цифровой подписи регулируется настоящим Законом, иным национальным законодательством или соглашением сторон.

Статья 2. Понятия, используемые в настоящем Законе

Для целей настоящего Закона используются следующие понятия:

электронные данные (электронное сообщение) - цифровое представление любой информации, воспринимаемой ЭВМ;

электронная цифровая подпись - электронные данные, полученные в результате преобразования исходных электронных данных с использованием закрытого ключа подписи, которые с помощью соответствующей процедуры при использовании открытого ключа подписи позволяют:

- подтвердить неизмененность исходных данных после подписания их электронной цифровой подписью;
- установить, что электронная цифровая подпись создана с использованием закрытого ключа, соответствующего открытому;
- установить владельца регистрационного свидетельства на открытый ключ электронной цифровой подписи, при наличии такого свидетельства;

средство электронной цифровой подписи - совокупность программных и технических средств, реализующих функции создания и проверки подлинности электронной цифровой подписи;

закрытый ключ электронной цифровой подписи - электронные данные, используемые для создания электронной цифровой подписи, известные только подписывающему лицу;

открытый ключ электронной цифровой подписи - электронные данные, предназначенные для проверки подлинности электронной цифровой подписи и известные пользователю открытого ключа;

центр сертификации средств электронной цифровой подписи (далее - центр сертификации) - юридическое лицо, осуществляющее лицензируемую деятельность по выдаче сертификата на средства электронной цифровой подписи;

центр регистрации отрытого ключа электронной цифровой подписи (далее - центр регистрации) - юридическое лицо, обладающее

правомочиями на удостоверение соответствия открытого ключа электронной цифровой подписи закрытому ключу лица, на чье имя выдано регистрационное свидетельство (владелец свидетельства);

регистрационное свидетельство на открытый ключ электронной цифровой подписи (далее - регистрационное свидетельство, свидетельство) - документ, подтверждающий соответствие этого открытого ключа электронной цифровой подписи закрытому ключу, выданный центром регистрации открытых ключей владельцу закрытого ключа электронной цифровой подписи или его полномочному представителю;

владелец закрытого ключа электронной цифровой подписи -физическое или юридическое лицо, которое создает ключи электронной цифровой подписи с использованием принадлежащих ему на законном основании средств электронной цифровой подписи;

владелец регистрационного свидетельства на открытый ключ электронной цифровой подписи (далее - владелец свидетельства) - физическое или юридическое лицо, на имя которого выдано регистрационное свидетельство на открытый ключ электронной цифровой подписи, и которое владеет закрытым ключом, соответствующим открытому ключу, указанному в свидетельстве;

подписывающее лицо - физическое или юридическое лицо, создающее электронную цифровую подпись на электронных данных - владелец закрытого ключа электронной цифровой подписи или его представитель, которому доверен закрытый ключ электронной цифровой подписи;

пользователь открытого ключа электронной цифровой подписи - физическое или юридическое лицо, использующее открытый ключ электронной цифровой подписи;

операционное регистрационное свидетельство - регистрационное свидетельство на открытый ключ электронной цифровой подписи, содержащее информацию об ограничении использования электронной цифровой подписи, в том числе выданное на одну или несколько конкретных сделок;

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

печать времени - внесение в электронные данные, подписанные электронной цифровой подписью, связанное с электронной цифровой подписью обозначение даты, времени и лица, вносящего данное обозначение, осуществляемое уполномоченным лицом (в том числе центром регистрации) и заверенное его электронной цифровой подписью;

общедоступные (открытые) информационные системы - информационные системы, доступ к которым не ограничен законом;

персональные данные - информация (зафиксированная на материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним. К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие.

Статья 3. Правовой режим электронной цифровой подписи: общие положения

1. Закрытый ключ является собственностью лица, владеющего им на законном основании.

Лицо может иметь неограниченное количество закрытых ключей электронной цифровой подписи, полученных им на законных основаниях.

2. Создание ключей электронной цифровой подписи осуществляют собственники средств электронной цифровой подписи, если иной порядок

не установлен специальным законом.

3. Подписывающее лицо вправе передавать полномочия на подписание с помощью его электронной цифровой подписи уполномоченному надлежащим образом представителю.

4. Электронная цифровая подпись при соблюдении требований настоящего Закона, действующего законодательства и (или) в порядке, установленном соглашением сторон, равнозначна собственноручной подписи физического лица, в том числе полномочного представителя юридического лица, если:

- она прошла проверку на подлинность при помощи открытого ключа электронной цифровой подписи, имеющего регистрационное свидетельство аккредитованного центра регистрации, или в порядке, предусмотренном соглашением сторон;
- подписавшее лицо правомерно владеет закрытым ключом, используемым для создания электронной цифровой подписи;
- электронная цифровая подпись является действующей на момент подписания.

5. Регистрационное свидетельство, выданное юридическому лицу без указания имени должностного лица, уполномоченного на использование данного ключа, считается выданным на имя лица, которое в силу закона или учредительных документов юридического лица выступает от его имени.

6. Все экземпляры электронного сообщения, подписанного электронной цифровой подписью, имеют силу оригинала.

7. В случае нарушения положений настоящего Закона виновное лицо несет уголовную, гражданско-правовую и административную ответственность в соответствии с законодательством.

8. Ограничения использования электронной цифровой подписи устанавливаются в порядке, предусмотренном законодательством.

Статья 4. Использование средств электронной цифровой подписи

1. Средства электронной цифровой подписи не относятся к средствам шифрования.

2. Деятельность центров сертификации средств электронной цифровой подписи осуществляется на основании лицензии, выдаваемой государственным лицензирующим органом.

Использование электронной цифровой подписи подписывающим лицом и получателем открытого ключа электронной цифровой подписи осуществляется без лицензии.

3. Допускается использование средств электронной цифровой подписи, не имеющих сертификата, выданного центром сертификации средств электронной цифровой подписи. При этом владелец несертифицированных средств электронной цифровой подписи (владелец закрытого ключа) обязан заявить об отсутствии сертификата всем пользователям открытого ключа, создаваемого этим средством электронной цифровой подписи.

В противном случае владелец несертифицированных средств электронной цифровой подписи несет ответственность за убытки, понесенные пользователем соответствующего открытого ключа, вследствие использования несертифицированного средства электронной цифровой подписи.

Сертификация средств электронной цифровой подписи осуществляется в соответствии с национальным законодательством о сертификации товаров и услуг.

В случае использования заявленных несертифицированных средств электронной цифровой подписи риски убытков несут владелец закрытого ключа и получатель открытого ключа электронной цифровой подписи.

4. Несовершеннолетние граждане имеют право на приобретение средств электронной цифровой подписи, получение регистрационного свидетельства на открытый ключ электронной цифровой подписи и использование закрытого ключа электронной цифровой подписи во всех

случаях, за исключением предусмотренных действующим законодательством.

Статья 5. Срок хранения регистрационных свидетельств на открытые ключи электронной цифровой подписи

Срок хранения регистрационных свидетельств на открытые ключи электронной цифровой подписи в центрах регистрации может быть установлен действующим законодательством, но не должен быть менее пяти лет. Копия регистрационного свидетельства на открытый ключ электронной цифровой подписи хранится в центре регистрации вместе с открытым ключом.

Если регистрационное свидетельство аннулируется, оно вместе с открытым ключом электронной цифровой подписи поступает на архивное хранение. Срок их хранения устанавливается в соответствии с национальным архивным законодательством.

Статья 6. Права и обязанности владельца закрытого ключа и пользователя открытого ключа электронной цифровой подписи

1. Владелец закрытого ключа электронной цифровой подписи несет ответственность перед пользователем соответствующего открытого ключа за убытки, причиненные несанкционированным использованием закрытого ключа вследствие ненадлежащей охраны закрытого ключа.

2. Владелец закрытого ключа электронной цифровой подписи (владелец регистрационного свидетельства) обязан потребовать от выдавшего центра регистрации приостановить действие свидетельства или аннулировать его, если он узнал или должен был разумно предполагать о возможном нарушении режима ограничения доступа к закрытому ключу, соответствующему открытому ключу, указанному в свидетельстве.

3. Пользователь открытого ключа электронной цифровой подписи вправе обратиться в центр регистрации открытых ключей, выдавший регистрационное свидетельство на открытый ключ электронной цифровой подписи и указанный в этом свидетельстве, за подтверждением:

- принадлежности открытого ключа владельцу регистрационного свидетельства;
- подлинности электронной цифровой подписи.

4. Пользователь открытого ключа электронной цифровой подписи обязан в соответствии с национальным законодательством и международными соглашениями обеспечить защиту персональных данных, содержащихся в сообщении, подписанном электронной цифровой подписью.

Статья 7. Содержание регистрационного свидетельства на открытый ключ электронной цифровой подписи

1. Регистрационное свидетельство на открытый ключ электронной цифровой подписи должно содержать следующие обязательные сведения:

- наименование юридического лица или фамилию, имя и отчество физического лица (по желанию этого лица - псевдоним) - владельца закрытого ключа электронной цифровой подписи;
- номер регистрационного свидетельства открытого ключа электронной цифровой подписи, дату начала и дату окончания срока его действия;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми можно использовать данный открытый ключ электронной цифровой подписи;
- наименование и юридический адрес центра регистрации открытых ключей электронной цифровой подписи, выдавшего свидетельство;
- данные об ограничении вида или области применения электронной цифровой подписи (включая данные об операционном свидетельстве, указание на недостижение совершеннолетия владельцем свидетельства и

другие);

- данные о полномочиях представителя владельца регистрационного свидетельства, получившего свидетельство;

- данные, позволяющие идентифицировать общедоступный реестр владельцев свидетельств, в который внесено данное свидетельство, и место его опубликования (в том числе в общедоступных компьютерных сетях).

2. По согласованию с владельцем свидетельства, выраженному в письменной форме, центр регистрации может включать в регистрационное свидетельство открытого ключа электронной цифровой подписи иные данные (в том числе, паспортные данные владельца свидетельства либо иные сведения, позволяющие однозначно идентифицировать физическое лицо, а также ограничения ответственности, предусмотренные пунктом 1 статьи 16 настоящего Закона и другие).

Глава 2. Центры регистрации открытых ключей электронной цифровой подписи

Статья 8. Правовой статус центров регистрации открытых ключей электронной цифровой подписи

1. Центром регистрации может быть юридическое лицо, созданное в соответствии с национальным законодательством, а также обособленное подразделение юридического лица, выполняющее все или часть функций юридического лица. Регистрация открытых ключей электронной цифровой подписи может осуществляться в качестве единственного вида деятельности или наряду с иными видами деятельности юридического лица.

2. Деятельность по регистрации открытых ключей электронной цифровой подписи осуществляется в заявительном порядке (путем государственной аккредитации). Условия и порядок аккредитации центров регистрации и требования, предъявляемые к указанным юридическим лицам при получении аккредитации, устанавливаются правительством.

3. Центр регистрации должен располагать финансовыми ресурсами (в том числе, собственным капиталом, заемными средствами и др.), достаточными для осуществления деятельности, включая возможную имущественную ответственность перед лицами, полагающимися на выданные им свидетельства, за убытки, понесенные указанными лицами, вследствие недостоверности содержания свидетельства.

Размер указанных финансовых ресурсов, определяется национальным законодательством.

4. Центр регистрации обязан иметь свидетельство на принадлежащий ему открытый ключ электронной цифровой подписи, которым центр заверяет выдаваемые им свидетельства. Свидетельство на открытый ключ центра заверяется уполномоченным государственным органом. При этом уполномоченный орган обязан обеспечить, чтобы любое лицо по общедоступным телекоммуникационным каналам или иным образом имело возможность проверить любое из выданных данным органом свидетельств ключа подписи.

5. Уполномоченный государственный орган обязан вести единый государственный общедоступный реестр свидетельств регистрационных центров и обеспечить неограниченный доступ к этому реестру.

В общедоступный реестр свидетельств должны быть внесены следующие сведения: номер и дата аккредитации центра регистрации; наименование и юридический адрес государственного органа, уполномоченного удостоверять открытый ключ электронной цифровой подписи центра регистрации, выдавшего свидетельство; адрес центра регистрации; данные о заблокированных регистрационных свидетельствах; данные о прекращении деятельности какоголибо центра регистрации, а также приостановке или отзыве лицензий.

6. Любое лицо должно иметь возможность проверить подлинность свидетельства на открытый ключ электронной цифровой подписи центра

регистрации с использованием общедоступных телекоммуникационных каналов или иным образом.

Статья 9. Деятельность центров регистрации

1. Центр регистрации подтверждает факт принадлежности (на момент выдачи свидетельства) конкретного закрытого ключа электронной цифровой подписи и соответствующего ему открытого ключа конкретному пользователю путем выпуска соответствующего свидетельства открытого ключа электронной цифровой подписи.

2. Регистрация владельца закрытого ключа электронной цифровой подписи в центре производится на основании заявки, составленной в письменной форме. В заявке должны содержаться сведения о заявителе - юридическом лице или гражданине в объеме, необходимом для выполнения данным центром своих обязанностей. При этом центр вправе потребовать от заявителя подтверждения достоверности соответствующей информации.

3. При выпуске регистрационного свидетельства центр предоставляет следующие гарантии:

- достоверности сведений, содержащихся в свидетельстве; соответствия свидетельства требованиям настоящего Закона и иного национального законодательства, в том числе наличия в свидетельстве всей существенно важной для его надежности информации, предусмотренной настоящим Законом, или включения такой информации в свидетельство в виде отсылки;

- соответствия свидетельства требованиям аккредитации; принятия данного свидетельства владельцем открытого ключа; соответствия закрытого ключа электронной цифровой подписи открытому ключу, подтвержденного владельцем закрытого ключа при выдаче регистрационного свидетельства на открытый ключ электронной цифровой подписи;
наличия в центре всех сведений о получателе свидетельства, предусмотренных статьей 7 настоящего Закона;

4. По требованию владельца закрытого ключа или его полномочного представителя либо пользователя открытого ключа центр регистрации обязан снабжать печатью времени подписанные владельцем закрытого ключа электронные данные и проверять подлинность электронной цифровой подписи.

5. Любое соглашение, предусматривающее отказ центра от гарантий, установленных настоящей статьей, или ограничивающее их, является ничтожным.

6. Центр обязан вносить данные о владельце свидетельства с его согласия в общедоступный реестр свидетельств и обеспечить неограниченный доступ к этому реестру. Центр вправе самостоятельно осуществлять ведение данного реестра или обратиться к услугам иного лица, осуществляющего деятельность по ведению общедоступного реестра.

7. Центр регистрации обязан предоставить любому лицу возможность удостоверить принадлежность открытого ключа электронной цифровой подписи владельцу закрытого ключа (владельцу свидетельства) с использованием общедоступных телекоммуникационных каналов или иным образом.

Данное требование касается также информации об адресах центров регистрации, данных о заблокированных свидетельствах или прекращении либо приостановлении деятельности какого-либо центра регистрации.

8. Центр регистрации обязан выдавать и заверять бумажные копии сообщения, подписанного электронной цифровой подписью, на закрытый ключ которой данным центром выдано свидетельство, по требованию владельца закрытого ключа данной электронной цифровой подписи, пользователя соответствующего открытого ключа, а также уполномоченных государственных органов и судов. При этом в документе указывается место и дата заверения, а также средство проверки и соответствующее регистрационное свидетельство. Документ заверяется подписью должностного лица центра и его печатью.

Статья 10. Обязательства центра регистрации свидетельств при выпуске свидетельства

Если центр регистрации и владелец свидетельства не договорились об ином, центр при выпуске свидетельства принимает на себя следующие обязательства перед его владельцем, принявшим свидетельство:

- действовать надлежащим образом, в соответствии со статьями 12 и 13 настоящего Закона, для приостановления действия или аннулирования свидетельства;
- уведомить владельца в течение разумного срока о всех известных центру фактах, которые существенным образом сказываются на юридической силе выпущенного свидетельства.

Статья 11. Обязательства владельца при принятии свидетельства

1. Приняв свидетельство, выпущенное центром регистрации, владелец принимает на себя следующие обязательства:
- гарантировать достоверность информации, предоставляемой центром пользователю открытого ключа;
- законным образом владеть закрытым ключом, соответствующим открытому ключу, указанному в свидетельстве;
- обеспечить контроль использования закрытого ключа и предотвращение его раскрытия какому-либо лицу, не уполномоченному на создание электронной цифровой подписи.

2. Принятие свидетельства означает согласие владельца с содержанием свидетельства, которое должно быть выражено в письменной форме.

Статья 12. Приостановление действия свидетельства

1. Если иное не предусмотрено по согласованию между центром регистрации и владельцем свидетельства, центр, выпустивший свидетельство, прекращает его действие на срок не более двух рабочих дней по указанию владельца свидетельства или его уполномоченного представителя.

Центр регистрации также приостанавливает действие свидетельства по постановлению уполномоченного государственного органа или суда.

2. Немедленно после приостановления действия свидетельства центр регистрации публикует в реестре, указанном в свидетельстве, извещение о приостановлении действия последнего, а также извещает об этом владельца свидетельства.

3. Центр регистрации возобновляет действие свидетельства по заявлению лиц, указанных в пункте 1 настоящей статьи. Если по истечении указанного срока не поступает заявления о возобновлении действия свидетельства, последнее подлежит аннулированию.

Статья 13. Аннулирование свидетельства

1. Центр регистрации открытых ключей, выдавший регистрационное свидетельство, обязан аннулировать его по требованию указанного в нем владельца ключа электронной цифровой подписи либо его представителя, должным образом уполномоченного на аннулирование.

2. Центр регистрации открытого ключа аннулирует свидетельство в течение одного рабочего дня после получения письменного заявления владельца свидетельства или его уполномоченного представителя либо постановления уполномоченного государственного органа или суда.

3. Центр регистрации открытого ключа электронной цифровой подписи обязан аннулировать регистрационное свидетельство или приостановить его действие, независимо от согласия владельца ключа электронной цифровой подписи, указанного в свидетельстве, если центр регистрации:

- получил заверенную копию свидетельства о смерти владельца свидетельства либо подтверждения на основе иных доказательств его смерти;

- получил документы, подтверждающие реорганизацию или ликвидацию владельца свидетельства, являющегося юридическим лицом, либо иные доказательства факта его реорганизации или ликвидации;

- установил неисполнение или ненадлежащее исполнение владельцем свидетельства своих обязательств, предусмотренных статьей 11 настоящего Закона.

4. После того, как приостановление действия или аннулирование свидетельства вступит в силу, центр регистрации обязан незамедлительно уведомить владельца ключа, указанного свидетельстве.

Незамедлительно после аннулирования свидетельства центр регистрации публично извещает об этом и исключает данное свидетельство из реестра свидетельств, в котором оно находилось.

Статья 14. Прекращение деятельности центров регистрации открытого ключа электронной цифровой подписи

При принятии решения о прекращении своей деятельности центр регистрации открытого ключа электронной цифровой подписи обязан заблаговременно проинформировать орган, аккредитовавший данный центр, а также всех владельцев регистрационных свидетельств, выданных этим центром.

При принятии решения о прекращении деятельности центра: выданные им свидетельства аннулируются в соответствии с настоящим Законом, а открытые ключи электронной цифровой подписи, сведения о владельцах и иная документация центра передаются на хранение в государственный архив, о чем делается публичное уведомление пользователей открытых ключей; либо сведения о владельцах и иная документация центра передаются другому центру регистрации, о чем делается публичное уведомление пользователей открытых ключей.

Статья 15. Защита персональных данных

В соответствии с национальным законодательством или международными соглашениями по защите персональных данных центр регистрации обеспечивает защиту персональных данных владельца свидетельства, содержащихся в документах, представленных заявителем.

Указанные персональные данные не включаются в общедоступный реестр свидетельств.

Центр регистрации не вправе запрашивать персональные данные, не соответствующие цели выдачи свидетельства.

Раскрытие персональных данных владельцев свидетельства центром регистрации допускается только с их согласия либо по требованию правоохранительных органов при наличии судебного решения.

В том случае, когда владелец закрытого ключа электронной цифровой подписи регистрируется под псевдонимом, центр регистрации обязан сообщить правоохранительным органам по их законному требованию о тождественности псевдонима и владельца свидетельства, при этом центр регистрации обязан известить владельца свидетельства о раскрытии псевдонима, если национальным законодательством не предусмотрено иное.

Статья 16. Ответственность центров регистрации

1. Центр несет ответственность за убытки в объеме реального ущерба, понесенного лицом в результате доверия к представленным в сертификате данным, которые центр обязан проверить и подтвердить. Ответственность Центра не включает штрафные санкции, возмещение упущенной выгоды, возмещение морального вреда.

2. Если иное не предусмотрено законом или договором, центр несет ответственность, если не докажет, что надлежащее исполнение его обязанностей оказалось невозможным вследствие непреодолимой силы, то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств.

3. Центр не несет ответственности:

- за ущерб, понесенный в результате доверия к недействительной или подделанной цифровой подписи владельца, если центр выполнил все существенно важные требования настоящего Закона в отношении свидетельства цифровой подписи;
- за ущерб свыше суммы, указанной в свидетельстве в качестве установленного предела (ограничения) доверия, понесенный в результате доверия к представленным в сертификате данным, которые центр обязан проверить и подтвердить.

Глава 3. Порядок использования электронной цифровой подписи

Статья 17. Использование электронной цифровой подписи в сфере государственного управления

1. Электронная цифровая подпись применяется органами государственной власти и органами местного самоуправления при передаче по информационным системам и хранении в электронных базах данных любых документов, издаваемых данным органом в соответствии с его компетенцией.

2. Органы государственной власти и органы местного самоуправления, направляющие электронные данные, подписанные электронной цифровой подписью, обязаны иметь регистрационное свидетельство на открытый ключ электронной цифровой подписи, выданное в установленном порядке аккредитованным центром регистрации.

Органы государственной власти и органы местного самоуправления принимают электронные данные (сообщения), направленные в эти органы физическими и юридическими лицами и подписанные электронной цифровой подписью, только при наличии у этих лиц свидетельства о регистрации открытого ключа данной подписи, выданного аккредитованным центром регистрации в соответствии с настоящим Законом.

3. Условия и ограничения использования электронной цифровой подписи органами государственной власти и местного самоуправления устанавливаются национальным законом.

4. Для удостоверения подлинности электронной цифровой подписи должностных лиц органов государственной власти и органов местного самоуправления создаются государственные центры по удостоверению электронной цифровой подписи, выдающие регистрационные свидетельства на открытые ключи электронной цифровой подписи.

Законом могут быть установлены дополнительные функции центра, в том числе создание ключей электронной цифровой подписи должностным лицам, использующим электронную цифровую подпись по своему статусу, и предоставление открытых ключей получателям сообщений, подписанных электронной цифровой подписью.

Статья 18. Использование электронной цифровой подписи в открытых информационных системах

При предоставлении информации из общедоступных информационных систем (баз данных) владелец такой системы (базы данных) обязан заверить предоставляемую информацию электронной цифровой подписью, зарегистрированной в центре регистрации открытых ключей электронной цифровой подписи.

Субъект, получающий информацию из общедоступных информационных систем (баз данных), не обязан проверять ее достоверность с помощью открытого ключа владельца системы.

Статья 19. Использование электронной цифровой подписи в корпоративных информационных системах

Использование электронной цифровой подписи в корпоративных информационных системах регламентируется внутренними нормативными документами системы, соглашением между участниками системы или между владельцем системы и пользователями (клиентами).

Указанные нормативные документы или соглашения должны содержать положения о правах, обязанностях и ответственности лиц, использующих электронную цифровую подпись, а также о распределении рисков убытков при использовании недостоверной электронной цифровой подписи между участниками системы.

Глава 4. Заключительные положения

Статья 20. Признание иностранных свидетельств на открытый ключ электронной цифровой подписи

1. Электронная цифровая подпись, которая может быть проверена открытым ключом, имеющим иностранное свидетельство, выпущенное одной из стран Содружества Независимых Государств или государством, с которым есть договор о признании таких свидетельств или иной договор, обеспечивающий равноценную безопасность электронных сообщений, признается электронной цифровой подписью в соответствии с настоящим Законом.

2. Правом, применимым к правоотношениям, возникающим между центром регистрации и владельцем свидетельства, является материальное право страны, в которой было выдано регистрационное свидетельство.

Статья 21. Использование сообщения, подписанного электронной цифровой подписью, в качестве доказательства в судебных разбирательствах

В случае возникновения спора допускается представление суду данных, подписанных электронной цифровой подписью и заверенных центром регистрации в соответствии с настоящим Законом и изданными во исполнение настоящего Закона нормативными актами.

Статья 22. Ответственность за нарушение законодательства при использовании электронной цифровой подписи

1. Лица, неправомерно использующие электронную цифровую подпись другого лица, включая неправомерное получение закрытого ключа и (или) проставление электронной цифровой подписи другого лица без должных полномочий, несут уголовную, гражданско-правовую и административную ответственность в соответствии с национальным законодательством.

2. В случае причинения убытков в результате несоответствия средств электронной цифровой подписи заявленным изготовителем свойствам или нарушения установленной процедуры проверки средств электронной цифровой подписи, центр сертификации средств электронной цифровой подписи несет гражданско-правовую ответственность.

3. Неправомерный доступ к средствам электронной цифровой подписи, неправомерное создание и использование закрытых ключей электронной цифровой подписи влекут уголовную ответственность в соответствии с национальным законодательством.

4. В случае причинения убытков пользователю открытого ключа электронной цифровой подписи вследствие несанкционированного доступа к закрытому ключу электронной цифровой подписи по вине владельца закрытого ключа электронной цифровой подписи, последний обязан

возместить убытки.

5. Если владелец закрытого ключа электронной цифровой подписи передает открытый ключ электронной цифровой подписи по договору об использовании электронной цифровой подписи, получатель открытого ключа электронной цифровой подписи несет ответственность за выполнение условий хранения и использования открытого ключа, установленных договором.

Статья 23. Разрешение споров

Споры, вытекающие из правоотношений, связанных с использованием электронной цифровой подписи, а также признанием ее действительности подлежат разрешению в судебном порядке в соответствии с правилами подведомственности и подсудности, установленными национальным законодательством.