УДК 340.111.5(575.2)(04)

К ВОПРОСУ УНИФИКАЦИИ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ ПРИМЕНЕНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ

Х.А. Рустамова – аспирант

Развитие международной электронной коммерции требует унификации законодательного регулирования применения электронной подписи. В данной статье рассмотрены несоответствия Закона Кыргызской Республики "Об электронной цифровой подписи" унифицированным общеевропейским актам.

Ключевые слова: специфика компьютерных сетей; проблема глобальности; электронные компьютерные сети в современном мире.

Применение электронных цифровых подписей, электронный документооборот осуществляется посредством электронных компьютерных сетей, самой крупной и распространенной из которых является сеть Интернет. Специфика компьютерных сетей состоит, прежде всего, в том, что они носят трансграничный характер. Возникает вопрос о том, распространяется ли государственный суверенитет на компьютерные сети и обмен информацией в них. Совершенно очевидно, что попытки разрешения проблемных вопросов каждым из государств обособленно не будут иметь успеха.

Проблема глобальности и экстерриториальности, обусловленная распространенностью

электронных компьютерных сетей по всему миру и ограниченной территориальной компетенцией каждого отдельного государства, может быть решена путем активного международного сотрудничества в области сближения и унификации законодательства различных стран мира об использовании и функционировании электронных компьютерных сетей[1]. В иностранной юридической доктрине по вопросу регулирования применения электронной цифровой подписи преобладает точка зрения, согласно которой в связи с глобальным характером правого понятия электронной цифровой подписи и международным развитием электронной коммерции национальное право должно быть сведено к нескольким унифицированным законам, стать последовательно международным и прозрачным,[2] чтобы исключить неравноправие субъектов правоотношений. Это предопределяет роль и значение норм международного права в регламентации отношений в области применения электронных подписей. Этим обусловлено то внимание, которое уделяется правовому регулированию электронных цифровых подписей как законодателями отдельных государств, в том числе путем принятия международных соглашений, так и международными организациями, которые занимаются унификацией законодательства в данной области.

Значительными шагами в направлении унификации законодательного регулирования применения электронной подписи можно считать принятие Директивы об электронных подписях ЕС[3](далее – Директива ЕС) в 1999 г. и Модельного закона об электронных подписях ООН[4] (далее также – Модельный закон) в 2001 г.

Следует отметить, что Директива ЕС служит инструментом гармонизации права ЕС и является "обязательной для каждого государства – члена ЕС, которому она адресована, в отношении ожидаемого результата, но сохраняет за национальными властями свободу выбора форм и методов действия"[5]. Директива является нормативным актом. Принятие директивы порождает для государства ЕС обязанность привести их внутреннее право в соответствие с нормативными предписаниями директивы. Эти мероприятия государства должны осуществить в течение строго определенного времени: в директиве чётко устанавливается срок, к моменту окончания которого нормы национального права государств-членов должны быть гармонизированы согласно положениям директивы[6]. При этом, степень сближения правовых норм, действующих в государствах – членах ЕС, может быть различна. Часто положения директив, издаваемых ЕС, детально регламентируют соответствующие вопросы, и национальным парламентам (и другим правотворческим органам стран ЕС) остается лишь воспроизвести эти положения во внутреннем законодательстве. Однако в последние годы институты ЕС чаще придерживаются стратегии "минимальной гармонизации": в директивах закрепляются только общие, основные начала регулирования определенной сферы общественной жизни, а государства получают возможность развивать, дополнять эти правила с учетом особенностей страны[7].

В отличие от Директивы ЕС Модельный закон является законодательным актом типового характера, который содержит нормативные рекомендации, а также варианты возможных правовых решений, пояснения к ним, примеры. Смысл законотворческого моделирования заключается в том, чтобы собрать опыт разрешения конфликтов и споров и кодификации способов такого разрешения, относящийся к разным правовым системам и национальным юрисдикциям, а так-

---

[1] *Грибанов Д.В.* Правовое регулирование кибернетического пространства как совокупности информационных отношений: Автореф. дисс. … канд. юрид. наук. – Екатеринбург, 2003. – С. 6.

[2] *Соловяненко Н.И.* Правовое регулирование электронной торговли и электронной подписи (международный опыт и российская практика) // Хозяйство и право. – 2003. – №1. – С. 28.

[3] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures (Electronic Signatures Directive) // Official Journal of the European Communities L013, 19.01.00, p12; Digital Signature Directive 1999/93/EU (28.06.99) // Official Journal of the European Communities. – 1999. – № 28.

[4] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001. – New York: United Nations publication, 2002. Текст доступен на http://www.uncitral.org/english/documents/

[5] Ст. 189 Договора о ЕС 1992 г. .

[6] *Кашкин С.Ю.* Основы права Европейского союза. – М.: "Белые альвы", 1997. – С. 51.

[7] *Соловяненко Н.И.* Directive of the European Parliament and of the Council of on a Community framework for electronic signatures. Перевод нормативных положений Директивы. Комментарии // http://www.e-commerce.ru/biz_tech/implementation/legal/directive.html.

же юрисдикциям международных судебных органов. Модельные законы обычно гораздо более развернуты и подробны, чем законодательные акты, принимаемые в рамках национальных законодательств. Модельные законы не предусматривают прямого применения, они должны задавать рамки и общие направления развития национальных законодательств[1].

Законодательство КР не может развиваться без учета рекомендаций, содержащихся в вышеупомянутых актах, поскольку Кыргызстан является партнером многих государств, входящих в Европейский Союз. Следовательно, для успешного сотрудничества используемые в КР технологии и правовые формы должны соответствовать унифицированным общеевропейским требованиям либо не должны им противоречить, иначе могут возникнуть затруднения в реализации законодательных норм и неэффективности их применения.

Рассмотрим некоторые положения этих документов, которые могут быть учтены и использованы при приведении законодательства КР в соответствие с международными нормами.

Начать следует с определения терминов, содержащихся в них, поскольку для любого закона главные элементы — определения терминов (объектов закона), от них зависят и содержание, и применимость закона.

Директива ЕС об электронных подписях содержит два определения электронной подписи – электронная подпись и усиленная электронная подпись.

Под *электронной подписью* в Директиве ЕС понимается информация в электронной форме, которая прилагается или логически связана с иной электронной информацией и служит в качестве способа аутентификации (п. 1 ст. 2).

Под *усиленной электронной подписью* (англ. advanced electronic signature, букв. – "продвинутая" электронная подпись) в Директиве ЕС понимается электронная подпись, которая соответствует следующим требованиям (п. 2 ст. 2):

- однозначно (уникально) связана с подписывающим лицом;
- может служить идентификатором подписывающего лица;
- создана с использованием средств, которые могут находиться под единоличным контролем подписывающего лица;
- связана с информацией, к которой она относится, таким образом, что любое последующее изменение информации может быть установлено.

При соблюдении указанных требований Директива ЕС придает усиленной электронной подписи в электронном документообороте статус рукописной подписи.

Модельный закон об электронных подписях ООН также делит требования к электронной подписи на две части. Во-первых, дается определение электронной подписи, согласно которому документ считается подписанным в том случае, если метод подписания позволяет:

- *идентифицировать лицо,*
- *установить, что оно одобрило документ, и при этом*
- *надежность метода соответствует обстоятельствам и целям его применения* (appropriate to circumstances) (ст. 2).

Во-вторых, для признания юридической значимости конкретной подписи под конкретным документом Модельный закон формулирует условия, которые повторяют требования, предъявляемые к усиленной электронной подписи в директиве ЕС:

- *данные, представляющие собой электронную подпись, должны быть непосредственно связаны с лицом, подписавшим документ* (т.е. служить идентификатором подписывающего лица)*;*
- *подписание в тот момент, когда оно совершалось, было подконтрольно только подписывавшему лицу;*
- *любое изменение электронной подписи, сделанное после подписания, может быть выявлено* (это требование не касается изменений подписанного документа и не означает, что измененная подпись утрачивает юридическую силу, просто все изменения должны быть известны контрагенту)*;*
- *если по закону подпись требуется для подтверждения целостности подписанного документа, любое изменение в нем, сделанное после подписания, может быть выявлено* (п. 3 ст. 6).

По Закону Кыргызской Республики "Об электронной цифровой подписи" (Закон "Об ЭЦП") некоторым эквивалентом усиленной электронной подписи в европейском законодательстве является электронная цифровая подпись (ЭЦП), которая признается равнозначной собственноручной подписи. Следует отметить, что Закон "Об ЭЦП" касается только электронных цифровых, а не всех электронных подписей и ставит своей целью обеспечение правовых

[1] *Отставнов М.* Зайчик в шляпе //Компьютера. – 2000. – 11 апреля. – №13.

условий использования ЭЦП в процессах обмена электронными сообщениями, при соблюдении которых ЭЦП признается равнозначной собственноручной подписи (п. 1. ст. 1). Концепция закона базируется на понятии государственных гарантий правомерности использования ЭЦП. Иначе говоря, по сравнению с иными аналогами собственноручной подписи, только ЭЦП обеспечивает однозначное соответствие между электронным документом и лицом, его подписавшим[1].

Закон "Об ЭЦП" дает следующее определение. *Электронная цифровая подпись (ЭЦП) – последовательность символов, полученная в результате преобразования исходной информации с использованием закрытого ключа ЭЦП, которая позволяет пользователю открытого ключа ЭЦП установить целостность и неизменность этой информации, а также владельца закрытого ключа ЭЦП* (ст. 2). Это определение выгодно отличается от определений, данных в Директиве ЕС и Модельном законе тем, что не только содержит отсылку на то, что электронная цифровая подпись позволяет идентифицировать подписывающее лицо, но также содержит указание на процесс, с помощью которого такая идентификация производится. В данном случае указание на механизм создания и проверки электронных цифровых подписей создает более четкое правовое поле.

Директива ЕС и Модельный закон не ставят юридический статус электронно-цифровой подписи в зависимость от ее формата и не указывают на конкретное устройство или метод создания электронной цифровой подписи, т.е. остаются технологически нейтральными. Цель их требований состоит лишь в гарантировании достижения максимальной безопасности, что предусматривает также *сертификацию* электронных подписей. В правоотношении помимо двух сторон-контрагентов появляется третья сторона, призванная удостоверить, что подпись была совершена лицом, указанным в качестве подписавшего документ. В Директиве ЕС она названа лицом, оказывающим сертификационные услуги, в Модельном законе – сертифицирующим провайдером, в Законе "Об ЭЦП" – удостоверяющим центром. Причем, согласно общеевропейским актам, это может быть как юридическое, так и физическое лицо, по Закону "Об ЭЦП" – только юридическое, имеющее сертификат на принадлежащий ему ключ ЭЦП, выданный *уполномоченным государственным органом* (п. 5 ст. 8). Сертификат, естественно, является электронным, в противном случае он просто не впишется в технологию электронного обмена данными. В свою очередь, Директива ЕС предлагает систему создания "квалифицированных" сертификатов и устанавливает *добровольную аккредитацию* для тех, кто осуществляет такую сертификацию. При этом участникам электронного документооборота предоставляется возможность выбора между "квалифицированными" и "неквалифицированными" средствами на том основании, что уровень доверия, защиты и качества, требуемый от используемых средств и удостоверяющего центра, должен в значительной степени зависеть от того, что нужно заключающим сделку сторонам.[2] Директива ЕС устанавливает, что "государства-участники должны гарантировать, что усиленные электронные подписи, которые основаны на квалифицированном сертификате и созданы с помощью безопасного устройства электронной цифровой подписи" эквивалентны собственноручным подписям (п. 1 ст. 5). Однако в дальнейшем в статье указано, что "юридическая сила электронных подписей не должна отрицаться только на том основании, что они не основываются на квалифицированном сертификате или не созданы с помощью надежных средств электронной подписи" (п. 2 ст. 5).

Директива ЕС предусматривает, что пределы ответственности Центра могут быть установлены в сертификате (ст. 6). Согласно Закону "Об ЭЦП", удостоверяющий центр несет ответственность за убытки в объеме реального ущерба, который не включает штрафные санкции, возмещение упущенной выгоды и возмещение морального вреда. Если иное не предусмотрено законом или договором, удостоверяющий центр несет ответственность, если не докажет, что надлежащее исполнение его обязанностей оказалось невозможным вследствие непреодолимой силы. Удостоверяющий центр не несет ответственности за ущерб свыше суммы, указанной в сертификате ключа подписи в качестве установленного предела доверия (ст. 16), поскольку полная ответственность представляется неоправданной, так

[1] *Войниканис Е.А., Якушев М.В.* Информация. Собственность. Интернет: традиция и новеллы в современном праве. – М.: Волтерс Клувер, 2004. – С. 128–130.

[2] *Халиков Р.О.* Проблемы лицензирования и сертификации при использовании электронной цифровой подписи // Депонировано в ИНОИН РАН, рег. № 59117. – М., 2005.

как не соответствует степени возможной вины. Удостоверяющий центр должен отвечать только за ненадлежащее выполнение своих функций, а не за все убытки, величина которых зависит от множества иных факторов. Для обеспечения ответственности предусмотрено условие деятельности удостоверяющего центра – наличие у него определенных финансовых ресурсов.

Государства-участники ЕС сами вправе определить процедуру создания системы сертифицирующих провайдеров, но они не могут ограничивать число аккредитованных лиц, оказывающих сертификационные услуги (п. 2 ст. 3 Директивы ЕС) и оказание сертификационных услуг с территории другого государства-участника (п. 1 ст. 4). Модельный закон также устанавливает принципы недискриминации по территориальному признаку. При установлении юридической силы сертификата ключа подписи не должны принимать во внимание географическое место, где выдан сертификат, место нахождения предприятия, выдавшего сертификат (ст. 12 Модельного закона). Аналогичное по смыслу положение содержит и Модельный закон СНГ от 9 декабря 2000 г. "Об электронной цифровой подписи", согласно которому электронная подпись имеет юридическую силу, если может быть проверена открытым ключом, имеющим свидетельство, выпущенное одной из стран СНГ или государством, с которым есть договор о признании таких свидетельств[1]. В качестве главного основания сертификации Модельный закон об электронных подписях ООН выделяет сходство методов создания подписи: иностранная электронная подпись должна иметь то же юридическое значение, что и национальная, если технологии подписания эквивалентны по существу (п. 2 ст. 12). В отличие от Модельного закона, Директива ЕС устанавливает закрытый перечень случаев, при которых возможно признание юридической силы за иностранными электронными подписями:

- на взаимной основе признаются подписи, сделанные в государствах-участниках ЕС, поскольку они основываются на общих требованиях Директивы;
- если подпись сделана в государстве, не являющемся участником ЕС, но при этом соответствует требованиям Директивы, она может быть признана в государстве-участнике ЕС. В этом случае государство может устанавливать свои дополнительные требования к подписям;
- о признании подписей могут заключаться двусторонние и многосторонние соглашения между государствами с третьими странами или международными организациями (п. 1 ст. 7).

Закон "Об ЭЦП" признает электронную цифровую подпись, которая может быть проверена открытым ключом, имеющим иностранное свидетельство на открытый ключ ЭЦП, выданный государством, с которым есть международный договор Кыргызской Республики о признании таких свидетельств или иной международный договор КР, обеспечивающий равноценную безопасность электронных сообщений (ст. 20). Следует отметить, что на настоящий момент не было заключено ни одного подобного договора.

В целом, анализируя два документа двух международных организаций – Директиву об электронных подписях ЕС и Модельный закон об электронных подписях ООН, можно сделать вывод о разнице в подходах к регулированию, хотя некоторые детали в них и совпадают. Так, они дают тождественные определения понятию электронной подписи и создают одинаковую структуру правоотношений, но подход Директивы ЕС является более детализированным и более жестким. Директива устанавливает права, обязанности и ответственность сторон, критерии признания подписи обретают характер замкнутого перечня, делается упор на сертификацию подписей, хоть она и не является обязательной. Это обеспечивает унификацию норм государств-участников ЕС, но осложняет взаимодействие с другими государствами. Приняв директиву об использовании электронных подписей, ЕС не смог решить задачу включения своего информационно-правового пространства в общемировое.

Относительно несоответствий Закона Кыргызской Республики "Об электронной цифровой подписи" унифицированным общеевропейским актам следует отметить, что, во-первых, Директива ЕС и Модельный закон относятся ко всем электронным подписям, а не только к цифровой подписи, которая является предметом закона КР; во-вторых, при формировании понятий в вышеупомянутых актах исходным является не технологический, а информационный аспект, что, как представляется, связано с европейской концепцией информационного общества и нам, возможно, не очень подходит. Правоотноше-

[1] *Халиков Р.О.* Общая характеристика законодательства об электронной цифровой подписи в России и за рубежом // Вестник ТИСБИ. – 2005. – № 4. – С. 167–187.

ния по использования электронного документа и применению электронных подписей – новые правовые явления для нашего государства, еще не успела выработаться практика, не проанализированы проблемы и их решения. Поэтому неразумно пускать процесс построения таковых норм на самотек. Здесь просто необходим контроль со стороны государства, хотя бы на начальном этапе. Для Кыргызской Республики присоединение к международным стандартам в области электронных подписей немаловажно, чтобы стать равноправной участницей международных отношений с использованием электронных цифровых подписей, так как, и об этом уже говорилось выше, единство технологических и организационно-технических аспектов использования электронных подписей создает базу для их трансграничного признания. Но простое копирование общеевропейских правил может обернуться негативными последствиями, поскольку при создании правовых основ необходимо учитывать экономическую ситуацию и уровень развития правовой системы в Кыргызстане, которые значительно отличаются от существующих в европейских странах. Кыргызстану следует ориентироваться на европейское законодательство, но с учетом его национальной специфики, поскольку во многих европейских государствах оно является весьма либеральным.