ФЕДЕРАЛЬНАЯ СЛУЖБА ИСПОЛНЕНИЯ НАКАЗАНИЙ
ФЕДЕРАЛЬНОЕ КАЗЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
ВОРОНЕЖСКИЙ ИНСТИТУТ ФСИН РОССИИ

С. В. Щеголева

ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

Монография

ВОРОНЕЖ
2015

УДК 342.9 (075.8)
ББК 67.401
Щ32

Рецензенты:

доктор юридических наук, профессор *Ю.Н. Андреев;*
доктор технических наук, профессор *А.В. Кочегаров*

С.В. Щеголева

Щ32 Теоретические проблемы законодательного регулирования в сфере использования электронных подписей : монография / С.В. Щеголева ; ФКОУ ВПО Воронежский институт ФСИН России. – Воронеж : Издательско-полиграфический центр «Научная книга», 2015. – 124 с.

ISBN 978-5-4446-0732-9

Монография подготовлена на базе действующего законодательства и посвящена актуальным проблемным вопросам законодательного регулирования в сфере использования электронных подписей. В монографии обосновывается целостность, практическая и теоретическая значимость электронной подписи, затрагиваются проблемы использования документов в электронной форме отображения в государственном управлении и экономике, а так же пробелы в гармонизации иностранных законодательных актов с российскими, осуществляющих регулирование отношений в сфере электронных подписей и электронной торговли.

В работе проведен сравнительно-правовой анализ понятийного аппарата законодательства об электронной подписи; изучение нормативно определенных условий придания юридической силы электронным подписям. Результаты исследования могут быть использованы при подготовке учебных материалов и в процессе преподавания.

Для сотрудников государственных органов, практикующих юристов, преподавателей и студентов, курсантов, аспирантов юридических вузов и факультетов.

УДК 342.9 (075.8)
ББК 67.401

Издано в авторской редакции.

ISBN 978-5-4446-0732-9

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Повсеместное развитие телекоммуникаций и информационных технологий – одна из важных примет XXI века. В ряде стран, например в Японии и США, их уровень стал настолько высок, что можно говорить о начале перехода к информационному обществу.

Дальнейшее развитие телекоммуникационных технологий неизбежно станет локомотивом для прогресса всей информационной инфраструктуры, в том числе документооборота в электронной форме отображения, что для России с ее огромными территориями и сложной административной системой является решением многих проблем в государственном и корпоративном управлении.

Документ как отражение воли государственной власти существует тысячелетия. Но уже к середине прошлого века стало очевидным, что объемы деловых документов столь огромны, что их обработка и хранение без перехода на какой-то принципиально новый технологический уровень могут привести к быстрому информационному и управленческому коллапсу.

Данную проблему удалось постепенно решить с помощью вычислительной техники. Однако тут же возникла еще одна проблема – проблема надежного способа подтверждения подлинности электронного документа, которую для традиционного бумажного документа решили давно. В конечном итоге она нашла свое разрешение после разработки ряда математических алгоритмов, получивших обобщенное название «электронная подпись».

Потребность в обмене юридически значимыми документами в электронной форме отображения была столь высока, что многие страны поспешили принять специальные законы, регулирующие данные отношения, большинство из которых было ориентировано на сферу так называемой электронной торговли, открывавшей широкие перспективы для движения товаров, работ и услуг на новые рынки сбыта при снижении издержек.

Не осталась в стороне и Российская Федерация, приняв Федеральный закон «Об электронной подписи». Однако в тот период ни у России, ни у боль-

шинства других стран не было практического опыта построения систем подтверждения цифровой подписи как в организационном, так в юридическом плане. Многие национальные законы, в том числе и отечественный, создавались умозрительно, на основе еще более абстрактных моделей, разработанных международными организациями.

В Российской Федерации система юридически значимого электронного документооборота пока развита крайне слабо. Его активно используют в своих целях такие ведомства, как Федеральная налоговая служба, Федеральная таможенная служба, МВД РФ, а также банковский сектор. Такое положение дает шанс до начала повсеместного внедрения технологии цифровой подписи определить принципиальные пробелы в российской модели юридического обеспечения системы подтверждения цифровой подписи и устранить их.

Компьютерные технологии, проникая во все большее число сфер человеческой деятельности, приводят к существенным изменениям в мировом сообществе, которое вступает в новую стадию своего развития – информационную цивилизацию.

Настоящая работа посвящена осмыслению важного элемента информационной сферы – проблеме юридических аспектов организации электронного документооборота.

Основная цель данной работы – не только теоретико-практическое правовое осмысление актуальных вопросов организации и осуществления электронного документооборота на уровне современных требований, но и формирование у студентов и аспирантов вузов крайне необходимого минимального уровня практических знаний и навыков в данной области.

Монография состоит из введения, двух глав, включающих четыре параграфа, заключения, списка использованной литературы.

Первая глава «Актуальные теоретические проблемы законодательного регулирования в сфере использования электронных подписей» посвящена анализу комплекса проблем, связанных с правовой точки зрения с общим социаль-

ным и техническим прогрессом, существенный импульс для которого задала информационно-компьютерная революция. В ней исследуются задачи перевода документооборота на новые носители с возможностью передачи по каналам связи, обеспечения хранения и поиска документов в технических системах при сохранении главного свойства документа – его способности юридически значимо подтверждать волеизъявление управомоченных лиц, либо описанные в нем события и факты.

Во второй главе «Международно-правовое регулирование в сфере электронных подписей и электронной торговли» рассматриваются наиболее значимые положения Модельного закона «Об электронной цифровой подписи», Типового закона ЮНСИТРАЛ «Об электронной торговле», Модельного закона «Об электронной торговле», Типового закона ЮНСИТРАЛ «Об электронных подписях». Так же анализируются определения, изложенные в текстах актов международного уровня, и наиболее значимые нормы законодательства зарубежных стран в сфере использования электронных подписей с целью выработки четких дефиниций, однозначно определяющих сложные юридические понятия.

Глава 1

АКТУАЛЬНЫЕ ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

§ 1. Нормативное регулирование отношений в области использования электронной подписи

Формирование системы электронного документооборота в различных сферах государственной и экономической деятельности вызвало необходимость более детального регулирования отношений по использованию электронной подписи.

Данный комплекс проблем, которые автор хотел бы подвергнуть анализу с правовой точки зрения, связан с общим социальным и техническим прогрессом, существенный импульс для которого задала информационно-компьютерная революция. В основе этого глобального явления лежит объективная закономерность, подмеченная еще Г. Гегелем, а затем развитая марксистами, получившая название «закона перехода количества в качество». Усложнение производства, систем управления и многих иных процессов, именуемых научно-техническим прогрессом, к середине прошлого века дали огромный импульс для генерации все большего количества информации и человечество встало перед проблемой так называемого информационного коллапса, когда создаваемые сведения невозможно распределено хранить и, самое главное, к ним невозможно обеспечить быстрый доступ заинтересованных потребителей, которых, в свою очередь, становилось все больше.

С другой стороны, отсутствие возможности быстрого поиска и ознакомления с различными сведениями, в особенности с результатами научно-технических достижений, приводило к тому, что разные группы ученых параллельно друг с другом проводили одни и те же научные исследования, неоправданно удорожая конечный социально значимый результат.

С третьей стороны, возникавшие поневоле «кладези информации» в виде бюро научно-технической информации, банков нормативных правовых актов, государственных стандартов и т.п. не могли удовлетворить потребности всех желающих, что замедляло и удорожало как научные исследования, так и принятие управленческих решений на должном уровне.

Наконец, с четвертой стороны, бумажные документы не могли «размножаться» бесконечно, для них рано или поздно должно было закончиться сырье, то есть бумаги просто могло не хватить.

Автор, описывая вышеизложенное, просто зафиксировал некий этапный момент, с которым в той или иной мере столкнулись все развитые страны, и который необходимо было преодолевать путем качественного скачка на основе новых технологий. Проблема же информатизации, то есть передачи знаний, накопления и обработки различной информации управляющими подсистемами, не является новеллой именно XX в.

Один из основоположников науки информационного права в России В.А. Копылов выделяет пять этапов развития информационных отношений в обществе за всю историю цивилизации, назвав их обобщенно информационными революциями. По его мнению, первая информационная революция связана с изобретением письменности, в результате чего появилась возможность «фиксировать знания на материальном носителе, тем самым отчуждать их от производителя и передавать от поколения к поколению». Вторая информационная революция (середина XVI в.) вызвана изобретением книгопечатания, в результате которого появилась возможность тиражирования и активного распространения информации, возросла доступность людей к источникам знаний. Третья информационная революция (конец XIX в.) была обусловлена изобретением электричества, благодаря которому появились телеграф, телефон, радио, позволяющие оперативно передавать и накапливать информацию в значительных объемах. Четвертая информационная революция (середина XX в.) связана с изобретением вычислительной техники и появлением персонального компьютера,

созданием сетей связи и телекоммуникаций. Стало возможным накапливать, хранить, обрабатывать и передавать информацию в электронной форме. Пятая информационная революция, по мнению В.А. Копылова, проистекает сегодня, и связана она с формированием и развитием трансграничных глобальных информационно-телекоммуникационных сетей, охватывающих все страны и континенты [51].

Приведенную временно-событийную градацию автор полагает правильной, однако в ней в интересах данной работы необходимо сделать отдельные акценты. Так, телеграф, радио и телефон действительно позволили передавать информацию на значительные расстояния, однако о значительных объемах такой информации, а также о некоторых видах ее отображения при этом говорить не приходилось. В частности, по телеграфу практически невозможно передать многотомный труд, чертежи, фотографическое отображение, то есть информацию действительно значительного объема. Система телеграфа, радио и телефона, в сущности, это система передачи небольших отрезков оперативной информации, причем от конкретного источника к конкретному адресату. Жизнь же требовала передач существенных объемов сведений, причем в режиме «реального времени». При этом телеграф и радио не ставили проблемы достоверности передаваемой информации – и у источника, и у адресата она превращалась в бумажный документ, а идентификация определялась либо системой связи, либо возможностью (в случае сомнения) запросить оригинал сообщения. Даже факсимильная связь давала графическую копию исходного документа. Данная проблема возникла с появлением феномена «электронного документа», то есть документа, который подготовлен на электронно-вычислительной технике в некоем распространенном редакторе (специальной программе для подготовке текстовых документов).

«Электронный документ» как юридическая категория является одним из ключевых понятий, поэтому необходимо остановиться на ней несколько подробнее в самом начале работы.

Основную сложность представляет понятие «электронная форма».

Попробуем более подробно разобраться с данным термином. Во-первых, понятие «цифровой код» достаточно условно. Любой код – это представление информации в определенной системе счисления (например, русский алфавит правильно с математической точки зрения обозначается как тридцатитрехэлементный однозначный код). При этом, что мы используем для обозначения – цифры или какие-то другие знаки, – не имеет принципиального значения. На физическом уровне в компьютере осуществляется движение не цифр, а электрических сигналов с разными потенциалами (при этом меньший потенциал обозначается условно как « 0 » , а больший – как « 1 »). Приставка «электронный» также условна и предназначена для того, чтобы подчеркнуть, что во всем этом процессе участвует электрический ток. Но ведь он участвует и в передаче информации по телеграфу или телефону, однако мы воздерживаемся от использования данного дополнительного обозначения при описании этих видов связи. Наиболее принципиальным свойством «электронного документа» является то, что закодированную таким образом информацию мы можем хранить в неизменном виде неопределенно продолжительное время и каждый раз в том или ином редакторе получать одинаковый результат в виде текста или иного графического изображения. Ничего подобного ни телеграф, ни телефон, ни телевидение дать не могут – там сигнал генерируется, затем принимается, отображается и исчезает. К вопросу о том, чем отличается документ от иного отрезка информации, зафиксированного вышеописанным образом, автор вернется ниже.

Получив возможность фиксировать и хранить информацию в виде устойчивой последовательности электромагнитных сигналов и тем самым имитировать ее отображение иными способами, а также возможность копирования этой информации, ее передачи по каналам связи, преобразования в бумажную или иную форму, человечество действительно создало условия для решительных шагов во многих областях государственной, научной и общественной деятельности.

Не будет преувеличением сказать, что документ как юридическая категория является основой всей системы государственного управления. Причем документирование в системе управления делами государства сложилось многие века назад и с того времени шло только по нарастающей. В современных развитых государствах подавляющее большинство управленческих решений, а также оснований для их принятия должны быть документально оформлены. Это придает системе управления четкость и упорядоченность, снижает уровень противоречивости и спонтанности в ее деятельности. Хотя специалисты в области государственного управления чаще всего говорят об управленческой информации, но на самом деле подразумевают под ней именно документированную информацию. Не случайно Федеральный закон «Об информации, информатизации и защите информации», который задал существенный вектор в развитии системы документационного обеспечения деятельности органов государственной власти на основе новых информационных технологий, в качестве одного из базовых понятий ввел категорию «информационный ресурс», понимая под ней «отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)». К сожалению, действующий Федеральный закон «Об информации, информационных технологиях и защите информации» данное понятие в качестве легальной дефиниции не использует, однако оно продолжает широко применяться в текстах других нормативных правовых актов [11].

В качестве иллюстрации приведем перечень источников, объективно порождающих управленческую информацию, сформированный Г.В. Атаманчуком:

а) нормы законодательных и иных актов, управомочивающие государственные органы и государственных служащих на принятие определенных управленческих решений или совершение управленческих действий в обозначенном времени и направлении (решения и действия по исполнению законов и иных нормативных правовых актов);

б) обращения граждан в государственные органы по реализации своих законных интересов и субъективных прав (обслуживание и защита прав и свобод граждан);

в) обязательные указания вышестоящих государственных органов, подлежащие исполнению нижестоящими и обеспечивающие реальность государственного управления (директивная управленческая информация);

г) факты, отношения, выявляемые в процессах контроля, которые отражают состояние управляемых объектов, а также уровень функционирования управляющих компонентов (управленческая информация об обратных связях в процессах государственного управления);

д) проблемные, конфликтные, экстремальные и иные сложные ситуации, нуждающиеся в оперативном и активном сильном вмешательстве государственных органов и должностных лиц (управленческая информация о кризисных состояниях общественных процессов) [61].

Несложно заметить, что за исключением последней группы информации, все остальные информационные потоки должны быть документированы, в противном случае они не могут восприниматься в качестве норм права либо обязательных указаний, а также не могут вообще войти в государственный информационный оборот (обращения граждан по защите своих прав, факты, выявленные в процессе контроля и т.п.).

В движении информации в системе государственного управления в сравнении, скажем, с научной информацией, имеются свои особенности. Для научной информации главное – возможность заинтересованных лиц быть своевременно извещенным о достигнутом научном результате, а также, при необходимости, доступ к полному комплексу сведений об этом результате. Для информации, обращающейся в системе государственного управления, одним из основополагающих свойств является оперативность, то есть способность сведений быть доставленными заинтересованному субъекту как можно в более короткий срок, а также обеспечение возможности поиска всего комплекса сведений по

тому или иному вопросу также в возможно короткий срок. Это связано с тем, что государственное управление в достаточной степени динамичная система, а большинство обращающихся в ней сведений сохраняют свою ценность в течение относительно небольшого промежутка времени.

Несомненен и тот факт, что количество сведений, обращающихся между органами государственной власти, прямо пропорционально сложности их устройства, а также степени охвата государством тех или иных общественных отношений. В небольшой монархии позднего Средневековья документооборот осуществлялся в основном по линейному принципу: доклады суверену и указания от суверена. В современном государстве со сложно устроенной системой исполнительной власти основные информационные потоки протекают не по вертикальным линиям, а на внутриведомственном и межведомственном уровне, так как вышестоящим руководителям, как правило, докладывается согласованный результат. Для достижения такого результата требуется достаточно много времени и достаточно много различной информации.

В качестве примера возьмем подготовку такого акта, как постановление Правительства Российской Федерации. Как правило, за подготовку текста проекта отвечает одно ведомство, а согласование текста проводится со всеми административными ведомствами, на которые впоследствии будет возложена задача по исполнению предписаний данного акта. Помимо этого, если для его исполнения требуются дополнительные финансовые ресурсы, то текст постановления в обязательном порядке согласовывается с Минфином России. Согласование проводится путем обмена соответствующими документами, содержащими замечания, особые мнения, предложения по включению дополнительных норм и т.д. Данный процесс может занять достаточно длительное время, если осуществлять пересылку документов почтой, поэтому чаще всего документы доставляются нарочным, что требует увеличения штатной численности аппарата управления. Все еще более усложняется, если речь идет об актах закрытого характера, содержащих, скажем, сведения, составляющие государственную тайну.

Помимо указанного, следует учитывать еще ряд особенностей нашей страны. Первое – протяженность территории на девять часовых поясов. Второе – ее федеративное устройство и, следовательно, наличие органов государственной власти федерального уровня, уровня субъектов Федерации, а также органов местного самоуправления (автор впоследствии для экономии места для обозначения всех категорий сразу будет использовать понятие «органы публичной власти»). Рассмотрим данные особенности более подробно. Наличие технических средств связи, позволяющих передавать необходимые объемы достоверной информации из управляющего центра получателям сведений из числа органов публичной власти, в таких условиях является едва ли не решающим в обеспечении должного уровня управленческого воздействия. Аналогичная ситуация возникает и при направлении информации «снизу вверх». В противном случае от направления директивы до ее исполнения может пройти столько времени, что она попросту может оказаться ненужной, а сведения о состоянии управляемой подсистемы оказываются устаревшими. В данном случае основная нагрузка на принятие оперативных решений ложится на плечи непосредственных руководителей, что в условиях современного государства может привести к потере управляемости.

Не меньшая сложность возникает в данном случае и при организации ведомственного управления. Информационное взаимодействие федерального органа исполнительной власти с территориальными органами должно быть постоянным, а также подтвержденным документами. Существенные задержки в их движении приводят к замедлению в принятии решений и общей деградации управленческого цикла. То же самое касается и органов публичной власти субъектов Российской Федерации по управлению своими территориальными органами. Такие сложные в климатическом отношении и огромные по территории регионы, как Красноярский край, Хабаровский край, Республика Якутия, где даже авиационное сообщение не является бесперебойным, не могут эффективно управляться без наличия устойчивой связи и возможности быстро передавать служебные документы.

Для целей настоящего исследования, как автор указывал выше, необходимо более четко определиться с вопросом, чем документ отличается от отрезка информации, зафиксированного на материальном носителе. Здесь уместны два подхода: общий, определяющий свойства документа, и частный, определяющий задачи, выполняемые документом в системе государственного управления. Как полагает Г.В. Белов, у документа можно выделить информационные свойства и юридические свойства. К первому блоку свойств он относит следующие:

– дискретность в структуре информационного потока (то есть то, что документ является элементарной частицей информационного потока);

– автономность существования в пространстве и во времени (то есть обособленность конкретного документа от остальных, даже аналогичных документов);

– автоморфность, то есть аутентичность (самоподобность, самоидентифицируемость, связанная с наличием индивидуальности содержания, особенностей исполнения, реквизитов);

– потенциальность, то есть наличие в содержании скрытого или вложенного потенциала действия;

– интенциональность, то есть направленность на определенные цели и/или предметы деятельности;

– креативность, то есть способность запускать или поддерживать определенную содержанием деятельность людей (например, управленческую) или информационную технологию;

– адресность;

– своевременность, актуальность для конкретного момента времени;

– коммуникативность, то есть семантическую адекватность восприятия получателем (однозначность понимания и истолкования).

Ко второму блоку свойств документа Г.В. Белов относит:

– идентифицируемость;

– авторизованность;

– аутентичность;

– защищенность;

– юридическую силу;

– правовой режим [25].

Из приведенной совокупности информационных свойств для служебного документа (то есть документа, обращающегося в системе публичного управления) важным является его креативность, то есть способность быть основанием для будущих правомерных действий подчиненного субъекта. Однако Г.В. Белов опустил еще одно важное свойство документа, являющегося определяющим для множества из них: служебный документ – это практически единственно возможный способ фиксации уже осуществленных действий, оставление информационного юридически значимого следа о проделанной работе, о происшедших событиях и случившихся фактах, направленного в будущее. Это одновременно и информационная, и юридическая черта служебного документа.

По поводу второго блока свойств – юридических – у автора также имеется собственная позиция. Во-первых, Г.В. Белов использует термины, для которых в русском языке имеются полные аналоги и их использование позволило бы более просто взглянуть на проблему. Идентификация – это отождествление (от лат. *identificare* – отождествлять). Соответственно идентифицируемость – способность документа быть соотнесенным с конкретным источником. При этом Г.В. Белов не описывает, каким образом это достигается. Авторизованность – это, соответственно, соотносимость документа с конкретным автором либо подписантом. Аутентичность – это, видимо, в понимании Г.В. Белова возможность визуального установления подлинности документа. Защищенность, по нашему мнению, не есть изначально привнесенное свойство документа. Бумага обладает таким свойством естественным путем и при подготовке обычных документов о дополнительной защите никто не задумывается. Необходимость в дополнительной защите возникает по отношению к отдельным видам докумен-

тов – например, к векселям, банкнотам и т.п. Юридическая сила и правовой режим – это, на наш взгляд, свойства не собственно документа, а информации, в нем содержащейся (статус документа).

Как видно из вышеприведенного, несмотря на то, что документ как важнейший элемент в системе государственного управления присутствует тысячелетия, научные дискуссии о его свойствах продолжаются.

В современном государстве одной из важнейших потребностей является формализация документов, которая и помогает соотносить документы с источником. В системе государственного управления данный вопрос решается в настоящее время за счет издания государственных стандартов. В отношении исполнительно-распорядительной документации, на долю которой выпадает наибольший процент в общем количестве документов, обращающихся в системе публичной власти, в настоящее время действует ГОСТ Р 6.30-2003 «Требования к оформлению документов» [34]. Этот акт содержит 30 различных реквизитов для документа, интересный анализ которых провел в свое время А.А. Фатьянов, выделив из них наиболее значимые с юридической точки зрения. Наибольшее юридическое значение (применительно к переписке органов государственной власти), по его мнению, имеют следующие реквизиты: наименование органа государственной власти; дата подписания (регистрации) документа; регистрационный номер; текст документа; наименование должности лица, подписавшего документ; его подпись. В свою очередь, среди этих реквизитов наибольшую юридическую нагрузку несут текст документа и подпись должностного лица. В тексте документа заключено волеизъявление органа власти либо описан юридически значимый факт, которые удостоверены подписью соответствующего должностного лица. Все остальные реквизиты, в сущности, подтверждают, что текст документа и подпись должностного лица подлинны [70].

Таким образом, одной из основных теоретических проблем, которые необходимо было решить для совершенствования документационного обеспечения государственного управления, являлось решение задачи перевода доку-

ментооборота на новые носители с возможностью передачи по каналам связи, обеспечение хранения и поиска документов в технических системах при сохранении главного свойства документа – его способности юридически значимо подтверждать волеизъявление управомоченных лиц либо описанные в нем события и факты. Решение этой задачи было начато со второй половины 70-х гг. прошлого века и продолжается до сего времени.

§ 2. Основные проблемы использования документов в электронной форме отображения в государственном управлении и экономике

Документ представляет собой материальный след практической деятельности органов государственной власти и органов местного самоуправления. С помощью документов осуществляется весь традиционный управленческий цикл.

Используются документы и во внутрисистемной деятельности органов государственной власти и органов местного самоуправления.

Создание и движение документов в системе государственного и муниципального управления являются одной из технологических основ деятельности этих органов. Эффективность управления как раз зависит от четкости и слаженности работы элементов системы документооборота.

Революционные изменения в общественной жизни, которые предоставил информационный век, являются: взаимодействие бизнеса, граждан и государственных органов должно становиться прозрачным, что должно привести к значительному уменьшению коррупции; информационные обмены должны оптимизироваться настолько, что произойдет не просто экономия ресурсов и времени, а изменение принципов и традиций общественного производства, распределения и потребления. О перспективах электронной коммерции скажем ниже, а сейчас необходимо затронуть проблему электронного взаимодействия органов государственной власти с гражданами и их организациями, получившую название «электронного государства» («электронного правительства»).

И.Ю. Богдановская полагает, что термин «электронное государство» наиболее соответствует английскому термину e-government. Последнее в некоторых случаях переводится как «электронное правительство». Такой перевод допустим, но он сужает понятие, по существу сводя вопрос только к исполнительной власти. Между тем «электронное государство» касается всех трех ветвей власти – законодательной, исполнительной и судебной [32]. Достаточно эпохальным в данной сфере общественных отношений стало принятие США в 2002 г. закона «Об электронном государстве», где под данной категорией понимается использование органами государственной власти сети «Интернет» и других информационных технологий в сочетании с процессами внедрения этих технологий в целях расширения доступа общественности, агентств, других государственных структур к государственной информации и службам, а также повышение эффективности, оперативности, нововведений и общего качества работы.

Для обеспечения юридической значимости документов необходимо создать «инфраструктуру доверия», в которую должны войти:

– система доступных для граждан удостоверяющих центров;

– «электронный нотариат», удостоверяющий время совершения учетных записей;

– электронный архив, обеспечивающий хранение учетных данных и электронных документов;

– системы раскрытия информации;

– электронная «фельдпочта», в опоре на существующие массовые сети общего пользования обеспечивающая надежный электронный документооборот между системами государственного учета и гражданами и организациями;

– электронный каталог, представляющий собой общедоступный Реестр систем электронного государственного учета, открытых для электронного взаимодействия с гражданами и организациями» [40].

Для достижения указанных целей, необходимо решить следующие основные задачи:

– развитие и широкое применение в деятельности органов государственной власти средств обеспечения удаленного доступа организаций и граждан к информации о деятельности органов государственной власти, основанных на использовании современных информационно-коммуникационных технологий;

– предоставление государственных услуг с использованием многофункциональных центров и сети «Интернет» на основе создания единой инфраструктуры обеспечения межведомственного автоматизированного информационного взаимодействия и взаимодействия органов государственной власти с организациями и гражданами;

– создание защищенной системы межведомственного электронного документооборота;

– внедрение ведомственных информационных систем планирования и управленческой отчетности в рамках создания единой государственной системы контроля результативности деятельности органов государственной власти по обеспечению социально-экономического развития Российской Федерации;

– формирование нормативной правовой базы, регламентирующей порядок и процедуры сбора, хранения и предоставления сведений, содержащихся в государственных информационных системах, обмена информацией в электронной форме между государственными органами, организациями и гражданами, а также контроль за использованием государственных информационных систем.

Применительно к территории нашей страны удаленный доступ к государственным услугам (например, получение различного рода справочной информации, направление заявлений на выдачу заграничного паспорта, получение информации о наличии вакантных мест в органах занятости населения, направление документов на конкурс по замещению вакантных мест государственных служащих и многое, многое другое) является актуальнейшей задачей, существенным образом экономящей время граждан и их затраты на перевозку (соответственно происходит экономия энергоресурсов). Однако автор полагает, что хотя это и действительно важная задача, но главным в условиях демократии яв-

ляется все же не это, а повышение уровня открытости государства перед обществом. На взаимной связи, возникающей посредством информационного обмена, основывается доверие граждан к власти. Это могло бы остаться не реализованным принципом, если бы не имело под собой, помимо чисто декларативного характера, существенной материальной подоплеки. Дело в том, что рыночная экономика, как во многом самонастраивающийся механизм производства и товарного обмена, просто не может эффективно функционировать в условиях закрытости органов государства. Например, не имея достоверной информации о деятельности публичной администрации, не сможет нормально работать такой чуткий к политической конъюнктуре финансовый институт, как фондовая биржа. Следовательно, возникнет дисбаланс в притоке капиталов в перспективные производства и начнутся искажения в реализации стратегии экономического роста.

Немаловажным, если не важнейшим вопросом здесь является информирование заинтересованных субъектов и населения в целом об изменениях в законодательстве, появлении новых нормативных правовых актов, регулирующих те или иные отношения. К сожалению, не все граждане в состоянии приобретать дорогостоящие обновляемые базы правовой информации типа «Гарант» или выписывать «Собрание законодательства Российской Федерации». Да в этом, в сущности, во многих случаях отсутствует необходимость. Человека может интересовать конкретное положение конкретного акта, затрагивающее в данный момент времени его конкретные права (например, требования к лицам, претендующим на получение разрешения на занятие частной охранной деятельностью). Размещение таких требований в актуальном состоянии на сайте соответствующего административного ведомства в сети «Интернет» позволяет практически мгновенно получить необходимую информацию и принять решение. Размещение же этой информации на официальном сайте гарантирует достоверность представляемой информации (во всяком случае, это правило должно быть официально закреплено в соответствующем законодательстве).

Наконец, гражданин вправе знать «политическую кухню»: какие именно лица занимают высшие должности в органах государственной власти, какие вопросы развития страны данные органы решают в тот или иной момент времени (за исключением закрытых проблем). Гражданин может и должен участвовать в непосредственном обсуждении наиболее животрепещущих проблем путем высказывания своего мнения на блогах, при рейтинговом голосовании, организуемом как органами государственной власти, так и различного вида структурами, проводящими социологические опросы посредством сети «Интернет». Он должен также иметь возможность просмотреть в удобное для него время интервью руководителей государства, если по каким-либо причинам он пропустил эту возможность в новостных передачах по телевидению. Современные средства «Интернет» предоставляют такую возможность, а цена трафика постоянно снижается.

Среди более конкретных задач и являющихся важными, можно выделить те, которые касаются формирования межведомственной системы защищенного электронного документооборота, а также организации обмена информацией в электронной форме отображения между государственными органами и гражданами. Комментируя первую из них, автор полагает, что оптимальнее все же вести речь о формировании единого пространства для передачи электронных документов органов публичной власти. Формирование отдельно межведомственной сети передачи электронных документов и ведомственных сетей в защищенном варианте является неоправданной тратой государственных средств. Ведомственные защищенные сети, существующие автономно, необходимы далеко не всем даже федеральным органам исполнительной власти – это прерогатива так называемых «силовых» министерств и федеральных служб. Остальные органы государственной власти могли бы вполне обойтись единой защищенной системой обмена электронными документами, имея в ней свой ведомственный сегмент.

Организация обмена документами в электронной форме отображения между органами государственной власти и гражданами, причем в двухсторон-

нем порядке, является чрезвычайно перспективной задачей, однако, по мнению автора, на ее реализацию потребуется достаточно много времени. И дело здесь не только и не столько в технических сложностях – они как раз преодолимы, а в отсутствии должной компьютерной грамотности у большинства населения страны, позволяющей вести обмен электронными документами.

Обе из вышеуказанных задач связаны с проблемой внедрения и правового обеспечения использования электронной подписи. Выше мы упоминали, что собственноручная подпись является одним из основных реквизитов документа, придающих ему юридическое значение. Факт проставления собственноручной подписи есть подтверждение согласия лица с текстом документа. По этому поводу А.А. Фатьянов однозначно утверждает, что «любая простановка собственноручной подписи управомоченным субъектом в документе должна рассматриваться как волевой акт, документированная фиксация волеизъявления» [57].

Здесь есть и технический момент, связанный с бумагой как носителем информации. Зафиксированный на ней текст, в том числе и подпись, однозначно, то есть полностью увязываются с носителем. Любые умышленные изменения возможно обнаружить с помощью современных методов криминалистики. Поэтому бумажный документ стал поистине универсальным средством фиксации волеизъявления, прочно вошел в деловой юридический оборот и без него немыслима практика публичного управления.

С электронным файлом дела обстоят иначе. В текстовом редакторе возможно полностью или частично изменить его содержание, и ни о какой подлинности документа речи дальше идти не может. В том числе можно вставлять в любой файл и электронный образ любой собственноручной подписи. Поэтому для решения данной проблемы должно было быть найдено иное решение. И оно было найдено. В 1976 г. в статье двух математиков из Стенфордского университета (США) Уитфилда Диффи и Мартина Хэллмана была наиболее полно сформулирована идея цифровой подписи как законного средства подтверждения подлинности и авторства электронного документа. Изложенные авторами

принципы заложили основы электронной аутентификации, электронного заключения сделок и электронных денег.

Здесь необходимо снова вернуться к собственноручной подписи. Она является отражением почерка человека. Сам же почерк является отражением биологических особенностей человека (речь конечно же идет о так называемом выработанном почерке, то есть сформировавшемся способе нанесения знаков на бумагу). Поэтому можно сказать, что подпись является достаточно уникальным способом начертания знаков на бумаге и современные методы криминалистического анализа с высокой вероятностью позволяют установить ее подлинность. Самое же основное заключается в том, что подпись неотъемлема от конкретной личности.

Идеи Диффи и Хэллмана основаны на использования для формирования аналога собственноручной подписи некоего криптографического алгоритма, имеющего свои особенности. В течение всей истории криптографии используемые для зашифровывания, а затем для расшифровывания сообщений криптографические ключи должны были быть известными отправителям и получателям сообщений заранее. В данном случае задача несколько иная: какой-то компонент ключа или весь ключ в целом должен быть известен только одному пользователю. На основе данного ключа вырабатывается некий иной ключ, на основании которого идентифицируется владелец первого ключа и происходит проверка его электронной цифровой подписи. Однако при этом должна быть исключена возможность обнаружения (вычисления) первого ключа. Посредством первого (в дальнейшем автор будет использовать для него обозначение – закрытый ключ) ключа происходит выработка собственно электронной подписи, то есть происходит зашифровывание некоторой результирующей исходного текста. Это необходимо для того, чтобы при изменении первичного текста результирующая не совпала. Внести же изменения в зашифрованную результирующую (собственно ЭП) невозможно. Второй ключ (открытый) предназначен для проверки подлинности ЭП, так как он математически связан с закрытым

ключом, но связан таким образом, что по нему невозможно вычислить значение закрытого ключа.

Конечно, и обычную ключевую систему возможно использовать для формирования цифровой подписи. Стоит лишь договориться, что известный двум или более участникам информационного обмена криптографический ключ будет использоваться для формирования электронной подписи. Однако в этом случае снижается уровень определения подлинности сообщения в случае возникновения конфликтной ситуации.

Как полагает А.А. Фатьянов, участие в криптографическом преобразовании ключа, известного единственному субъекту, позволяет достичь нескольких юридически значимых целей:

– утверждать, что уникальная последовательность находится во власти одного физического лица;

– утверждать, что доступ к данному ключу иных лиц может быть осуществлен лишь по воле данного лица;

– утверждать, что бремя негативных правовых последствий, которые могут наступить в результате неправомерного использования данной последовательности третьим лицом для выработки подложной ЭП, должно быть возложено на ее законного обладателя, если он своевременно и должным образом не предупредил заинтересованных лиц об утере или компрометации закрытого ключа [56].

Поэтому для формирования электронного документооборота с использованием электронных подписей необходимо создавать довольно сложную инфраструктуру открытых ключей, то есть систему юридического соотнесения конкретных ключей с конкретными их обладателями. Как автор покажет в дальнейших разделах настоящего исследования, законодательные акты, регулирующие отношения в области использования ЭП, во многом направлены на установление таких систем для определенных блоков правоотношений. При этом инфраструктура открытых ключей (тех, которые вырабатываются на основе закрытых и предназначены для проверки ЭП) должна формироваться от-

дельно для системы государственного управления и для системы обмена электронными документами в бизнесе.

В качестве промежуточного вывода автор хотел бы отметить, что расширение информационного взаимодействия между органами публичной власти, гражданами и организациями в Российской Федерации, получившее название «электронного правительства», преследует довольно широкие цели, направленные прежде всего на повышение уровня открытости власти перед обществом, сокращении затрат на получение информации гражданами от государственных и муниципальных органов, а также обратной информации. В этой системе существенное место отводится движению юридически значимых документов, подлинность которых должна быть дополнительно подтверждена.

Компьютерные технологии и сформированные на их основе информационно-телекоммуникационные системы открыли широчайшие перспективы для совершенствования и расширения коммерческой деятельности. По мнению ряда исследователей, началом эпохи так называемой электронной коммерции можно считать 1960 г., когда компании American Airlines и IBM приступили к созданию системы автоматизации процедуры резервирования мест на авиарейсы. Данная система сделала воздушные перелеты более доступными для рядовых граждан, помогая им ориентироваться в тарифах и рейсах, число которых постоянно росло. За счет автоматизации процесса расчета тарифов при резервировании мест снижалась стоимость услуг. Эта система могла выполнять комплексное управление доходностью, позволяя авиакомпаниям добиваться максимальной прибыли за счет манипуляций с ценами с учетом наличия свободных мест. Следующим эпохальным событием (помимо введения системы кредитных пластиковых карт) явилось создание в 1994 г. Д. Бизосом компании Amazon – первого интернет-магазина. И в настоящее время этот магазин является самым крупным в мире [54].

В настоящее время электронная коммерция приобрела глобальный характер, получив свою постоянно расширяющуюся нишу в общем деловом обороте. В

зависимости от участников общественных отношений электронная коммерция подразделяется на следующие основные секторы коммерческого взаимодействия:

– B2B – между юридическими лицами;

– B2C – между юридическими и физическими лицами;

– B2G – между юридическими лицами и органами публичной власти;

– C2C – между физическими лицами;

– G2C – между органами публичной власти и физическими лицами.

Основными отношениями в секторе B2B в настоящее время являются: торгово-закупочные площадки; аутсорсинг (передача некоторых функций организации (бухгалтерский учет, реклама и т.д.) внешним исполнителям); электронные платежные системы; электронные биржи; электронные аукционы; доски объявлений; информационные бизнес-системы.

Основными отношениями в секторе B2C в настоящее время являются: торговые ряды; электронные витрины и каталоги; электронные магазины; электронные аукционы; интернет-страхование; системы телеработы; интернет-реклама; туристические и прочие услуги.

Основанными отношениями в секторе B2G в настоящее время являются: участие в электронных торгах по закупке продукции для государственных нужд; выполнение государственных заказов; предоставление налоговой, статистической, таможенной и другой отчетности.

Основными отношениями в секторе G2C (электронное правительство) являются: системы социального обслуживания (пенсии, пособия, льготы и т.п.); системы коммунального обслуживания; юридические и информационно-справочные службы; геоинформационные системы.

Основными отношениями в секторе C2C являются: выборы; участие в опросах общественного мнения; уплата налогов, сборов, штрафов; представление заявок, жалоб и обращений граждан.

Несложно заметить, что там, где для установления имущественных или иных юридически значимых отношений требуется документальное подтвер-

ждение взаимодействия, одним из самых действенных способов является направление электронных документов, заверенных электронной цифровой подписью. Поэтому можно утверждать, что использование электронной подписи в коммерческой деятельности также постоянно расширяется. Как представляется автору, в основе системы правового регулирования использования ЭП в государственном управлении и экономике должны лежать одни и те же принципы, однако при более детальном регулировании эти системы могут существенно отличаться друг от друга.

Однако это лишь сугубо научный анализ. Бурное развитие электронной коммерции основывается прежде всего на удобстве такого способа получения и обмена информацией, а также на экономии ресурсов, которые она за собой влечет. Построить сеть специализированных магазинов, приблизив таким образом товар к потребителю, а также содержать помещения, персонал, оптимальный товарный запас в каждой торговой точке является достаточно затратным делом. Помимо этого необходимо вывешивать рекламу, рассылать каталоги, участвовать в выставках-показах и т.п. Совсем иное дело – выставить подробное описание всего спектра товаров на собственном сайте в сети «Интернет» и заключать сделки по их поставке по средствам связи, имея всего лишь один большой склад и небольшую команду из квалифицированных менеджеров. С предложенными товарами могут ознакомиться лица, не только проживающие в данном городе или даже в данной стране, но и иностранные граждане, которые также могут сделать необходимый заказ. Поэтому самым сложным и дорогостоящим делом становится не содержание торговой сети, а создание системы доставки, где в действие вступают иные организации.

Теперь обратимся к потребителю. Вместо того, чтобы ехать в большой магазин и несколько часов проводить там в поисках товара с нужными характеристиками, гражданин предварительно дома через сеть «Интернет» изучает все модели необходимого ему товара, выбирает оптимальный по цене и характеристикам, а потом по желанию либо целенаправленно едет в магазин, либо зака-

зывает данный товар с доставкой на дом, вообще не затрачивая времени на его приобретение. Получив такую возможность в принципе, от нее уже не откажется никто и никогда.

Поставим вопрос более широко. Есть производственная фирма, которая закупает комплектующие и сырье для изготовления товаров. Имея доступ к электронным торговым площадкам через компьютерные телекоммуникации, данная организация может быть не слишком зависима от конкретных поставщиков, а выбрать необходимые материалы в полном ассортименте, имея полное представление о рыночной конъюнктуре, а также заключать сделки, при этом не затрачивая никаких средств на поездки к поставщикам, сбор информации о товаре и т.п. Налицо существенная экономия как трудовых, так и денежных ресурсов, ведущая к снижению себестоимости производимого товара и успеху на рынке его сбыта. При этом организация избавлена от необходимости поездок ее сотрудников в банк для передачи платежных поручений, от распечатки и представления в таком виде громоздких налоговых отчетов в государственные налоговые органы, а осуществляет направление данной информации в защищенном виде по средствам телекоммуникаций, обеспечивая с помощью ЭП их юридическую силу. Опять экономия трудовых и денежных ресурсов, при этом не только у данной организации, но и у банка, и у государственного органа.

Вряд ли кто-то сможет возразить по поводу того, что это выгодно. Во всяком случае, предоставление возможности гражданам заключать электронные сделки на приобретение и отчуждение ценных бумаг на фондовых биржах в США в свое время обеспечило десятикратное увеличение притока капитала и существенным образом стимулировало развитие бизнеса.

Автор еще не затронул серьезно проблему развития системы взаиморасчетов по пластиковым картам, существенным образом изменившую многие рынки сбыта товаров и продолжающую развиваться поныне.

Обратим внимание еще на одну систему, которая возникла благодаря системам электронной коммерции. Сведения о заключенных контрактах и отчеты

об их исполнении составляют разветвленную сеть общедоступных баз данных, интенсивно использующуюся не только государственными чиновниками, но и специалистами, работающими в сфере бизнеса, научно-технических исследований и т.п. Традиционная организация процесса государственных закупок в настоящее время крайне неэффективна. У сотрудников государственных учреждений, ответственных за закупки, нет полного представления о наличии товаров, ценах, поставщиках, которые присутствуют на рынке. Информационный обмен между поставщиками и покупателями затруднен. Наиболее эффективным способом организации торгово-закупочной деятельности государственных организаций является использование электронных торгово-закупочных площадок. Эти площадки способны обеспечить более эффективное взаимодействие между службами снабжения государственных учреждений и предприятиями-поставщиками» [38].

Как отмечает Е.Н. Филенко, в настоящее время в России получили распространение удостоверяющие центры, деятельность которых направлена на обеспечение работы системы обмена электронными версиями налоговой и финансовой отчетности по открытым каналам связи между территориальными инспекциями по налогам и сборам и налогоплательщиками, а также между кредитными организациями и Банком России [48]. То есть речь идет в основном о создании корпоративных государственных и полугосударственных систем обмена документами в электронной форме отображения. До настоящей системы, которую подразумевают нормы как Федерального закона «Об электронной подписи», так и вышеуказанной Федеральной целевой программы, пока далеко.

Пока реально функционирующим в общей системе удостоверяющих центров является только Федеральный удостоверяющий центр, функции которого на основании «Положения о Федеральном агентстве по информационным технологиям», утвержденного постановлением Правительства Российской Федерации от 30.06.2004 № 319 возложены на данное административное ведомство (ФАИТ организует ведение единого государственного реестра сертификатов

ключей подписей удостоверяющих центров и реестра сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, а также обеспечивает доступ к ним граждан, организаций, органов государственной власти и органов местного самоуправления) [29].

Следующим и теоретическим, и практическим вопросом, в отношении которого необходимо расширять правовое регулирование, является проблема признания иностранного сертификата ключа подписи. Как отмечают Е.В. Ильиных и М.Н. Козлова, порядок признания иностранного сертификата ключа подписи в действующем Федеральном законе « Об электронной подписи» имеет достаточно сложную процедуру. Процесс признания иностранного сертификата, удостоверенного в соответствии с законодательством иностранного государства, затруднен, поскольку соблюдение требований страны, где была создана электронная цифровая подпись, не устанавливает ее юридическое признание в России. При этом Закон не дает четкого ответа на вопрос, что должно быть объектом юридического признания – иностранный сертификат, выданный сертифицирующим органом другого государства как бумажный носитель, либо юридическое признание должно быть установлено в отношении электронной подписи, созданной в соответствии с правом другой страны» [15].

На самом деле это является существенной проблемой, из которой следует сразу несколько иных проблем. Во-первых, требуется гармонизация нашей национальной системы правового регулирования в сфере ЭП прежде всего с международными модельными актами, чтобы снизить уровень разночтений и тем самым приблизить наше законодательство к сложившимся мировым стандартам. Во-вторых, трансграничный обмен информацией подразумевает трансграничное совершение сделок в электронном виде, в противном случае отечественные предприниматели будут исключены из онлайновых сделок, а иностранные предприниматели будут ограничены в приобретении товаров отечественных производителей. В-третьих, отсутствие нормального решения в данном вопросе может отрицательно сказаться на некоторых временных этапах ра-

боты Российской Федерации в ВТО. В рамках данной работы автор намерен на основе анализа международных и зарубежных правовых актов сформировать свои предложения по данному вопросу.

В качестве резюме к данному разделу исследования автор хотел бы отметить следующее.

1. Получив возможность фиксировать и хранить информацию в виде устойчивой последовательности электромагнитных сигналов и тем самым имитировать ее отображение иными способами, а также возможность копирования этой информации, ее передачи по каналам связи, преобразования в бумажную или иную форму, человечество действительно создало условия для решительных шагов во многих областях государственной, научной и общественной деятельности.

2. Служебный документ – это практически единственно возможный способ фиксации уже осуществленных действий, оставление информационного юридически значимого следа о проделанной работе, о происшедших событиях и случившихся фактах, направленного в будущее.

3. Одной из основных теоретических проблем, которые необходимо было решить для совершенствования документационного обеспечения государственного управления, являлось решение задачи перевода документооборота на новые носители с возможностью передачи по каналам связи, обеспечение хранения и поиска документов в технических системах при сохранении главного свойства документа – его способности юридически значимо подтверждать волеизъявление управомоченных лиц либо описанные в нем события и факты.

4. В основе системы правового регулирования использования ЭП в государственном управлении и экономике должны лежать одни и те же принципы, однако при более детальном регулировании эти системы могут существенно отличаться друг от друга.

5. Система правового регулирования в сфере использования ЭП в Российской Федерации не может исчерпываться наличием одного только Федерально-

го закона «Об электронной подписи». Необходимо создать действительно систему нормативных правовых актов различного уровня, обеспечивающую, во-первых, действенность использования ЭП в административном и гражданском обороте, во-вторых, гармонизованную с международными правовыми актами и законодательством наиболее существенных торговых партнеров России, чтобы обеспечить возможность заключения сделок в электронном виде между юридическими лицами, находящимися под различной юрисдикцией, и тем самым расширить экономические связи, а также снизить затраты на обеспечение заключения различного рода разовых и пролонгируемых договоров.

Глава 2

ПРАВОВОЙ РЕЖИМ ЭЛЕКТРОННОГО ДОКУМЕНТА

§ 1. Международно-правовое регулирование в сфере электронных подписей и электронной торговли

Международное сообщество достаточно давно осознало необходимость унификации законодательства в сфере международной и межгосударственной торговли. Сначала оно шло путем заимствования наиболее выдающихся гражданских кодексов европейских стран другими странами, а в период после Второй мировой войны, по мере того, как Организация Объединенных Наций расширяла свою деятельность, появился даже специализированный орган ООН в виде Комиссии ООН по праву международной торговли, для которого была выбрана аббревиатура ЮНСИТРАЛ.

Как отмечает Х.А.Э. Фария, данная комиссия в конце 80-х гг. XX в. была уполномочена разработать единообразные частноправовые нормы в области электронной торговли. Первым документом в этом направлении стал Типовой закон ЮНСИТРАЛ об электронной торговле 1996 г., а затем, спустя 5 лет, Типовой закон ЮНСИТРАЛ об электронных подписях. Оба документа, в особенности Типовой закон об электронной торговле, оказались довольно успешными и служат на сегодняшний день широко принятой основой для международного правового согласования [56].

Однако данная работа ведется не только на уровне ЮНСИТРАЛ – существенную роль в данном вопросе играет и Европейская экономическая комиссия ООН, которая выработала Рекомендацию № 26 «Коммерческое использование соглашений об обмене для электронного обмена данными». В вводном комментарии к данному акту рабочая группа, подготовившая текст Рекомендации, отмечает следующее:

«ЭОД получает быстрое развитие в качестве эффективного средства ведения операций в международной торговле. Использование ЭОД для коммерческих и административных целей уже получило значительное распространение в целом ряде важнейших отраслей промышленности в Европе, Северной Америке, Австралии, Новой Зеландии и Азии.

Растущее использование ЭОД радикально трансформирует международную торговую практику, заменяя традиционную торговлю, основанную на применении бумаги, альтернативными электронными системами. Вместо направления и получения оригинальных письменных документов с подписью от руки участники торговых операций передают структурированные коммерческие данные от одной компьютерной системы к другой с помощью электронных средств, включая все более широкое использование электронных подписей.

Однако внутригосударственное и международное право предусматривает весьма различные нормы в отношении приемлемости замены бумажного документа электронным сообщением. Во многих конвенциях и соглашениях, касающихся международной торговли, возможное использование ЭОД не предусматривается. Это в значительной степени вызвано тем, что во время разработки этих международных конвенций и соглашений ЭОД просто не существовало и поэтому в них еще предстоит внести необходимые изменения. Многие национальные законы также порождают неясность в отношении действительности основанных на ЭОД операций или непоследовательны в своем подходе к новым технологиям. Аналогичным образом редко какие суды имели возможность вынести постановление относительно действительности электронных документов, сообщений или подписей.

С самого начала использования ЭОД эти виды ориентированных на правовые вопросы соглашений применялись компаниями в различных отраслях, в различных экономических или географических регионах и для различных уровней технологической сложности».

Оценка, прямо скажем, в достаточной степени нелицеприятная. Действительно, у обмена документами в электронной форме отображения, как автор частично показал в первом параграфе настоящего исследования, достаточно много проблем юридического и организационного свойства. Тем не менее унификация должна происходить и, хотя это длительный процесс, он в конечном итоге должен привести к желаемому результату – принятию в большинстве стран законодательных актов, которые содержали бы схожие нормы по основным позициям, позволяющие осуществлять беспрепятственный обмен сообщениями в электронной форме отображения, обладающими должной юридической силой для отношений, в которых они участвуют.

Хотя типовые законы ЮНСИТРАЛ являются актами рекомендательными, рамочными, содержащими модели соответствующих правовых норм национального законодательства, тем не менее целый ряд стран принял их в качестве основы для формирования законов, регулирующих рассматриваемые нами отношения. Как следует из статистических данных, опубликованных ЮНСИТРАЛ, национальное законодательство, основанное на Типовом законе «Об электронной торговле», было принято более чем в 60 странах мира, а основанное на Типовом законе «Об электронных подписях» – в 5 странах [94].

Правовой анализ вышеуказанных типовых законов, по мнению автора, имеет важное значение для совершенствования законодательного регулирования отношений в сфере электронной торговли и использования ЭП в Российской Федерации, а также для анализа подходов, предпринятых иностранными законодателями, поэтому автор намерен в рамках данного параграфа осуществить детальный анализ данных актов, а также модельных законов СНГ «Об электронной торговле» и «Об электронной подписи». Затем, основываясь на выводах, приступить к сравнительному анализу положений иностранного законодательства в сфере ЭП.

Прежде всего, следует отметить, что законодательство об электронной торговле и законодательство об ЭП соотносятся между собой как общее и частное. Говоря иначе, законодательство об ЭП является частным случаем в общем

регулировании отношений, касающихся электронной торговли. Поэтому начать анализ целесообразно с норм Типового закона ЮНСИТРАЛ «Об электронной торговле» [49].

Устанавливая сферу действия Типового закона «Об электронной торговле» (далее, для краткости – ТЗ ЭТ), ЮНСИТРАЛ указывает, что он применяется к любому виду информации в форме сообщения данных, используемых в контексте торговой деятельности. При этом в общих положениях текста закона устанавливается, что термин «торговая» следует толковать широко, с тем, чтобы он охватывал вопросы, вытекающие из всех отношений коммерческого характера, как договорных, так и недоговорных (это не только сделки на доставку и обмен товарами, но и дистрибьюторские отношения, коммерческое представительство, факторинг, лизинг и т.п.). То есть данный документ, инициаторы его создания хотели бы распространить практически на все экономические отношения.

В указанном смысле небезынтересна позиция А.В. Самигулиной, которая полагает, что «под электронной торговлей, как правило, понимаются сделки купли-продажи, совершенные с использованием средств электронного документооборота, или совокупность действий, направленных на заключение таких сделок. Одни специалисты считают понятия «электронная коммерция» и «электронная торговля» эквивалентными (равными по объему), другие специалисты полагают, что электронная коммерция – это любая форма бизнес-процесса, в котором взаимодействие между субъектами происходит электронным образом и сопровождается снабжением ресурсами или физической доставкой продукции. Электронная торговля, которая касается процесса продаж, является частью электронной коммерции и наиболее активно развивается в сети «Интернет».

Изложенное позволяет сделать вывод о необходимости скорейшего разрешения проблемы научной разработки и унификации терминологии в сети «Интернет», а также единообразного толкования основных понятий и институтов в рассматриваемой сфере.

При разработке и принятии Гражданского кодекса РФ законодатель принципиально отказался от использования термина «коммерция» для определения деятельности, направленной на извлечение прибыли. Для обозначения базового понятия в сфере имущественных и связанных с ними личных неимущественных отношений, на основе которого во многом и строится правовое регулирование, в российском гражданском законодательстве используется понятие «предпринимательская деятельность». Термин «экономическая деятельность» – в ч. 1 ст. 8 и в ст. 34 Конституции Российской Федерации. Следует отметить и то обстоятельство, что в ст. 3 Налогового кодекса РФ содержится термин «экономическая деятельность».

Анализ норм ст. 34 Конституции Российской Федерации позволяет сделать вывод, что, во-первых, понятия «предпринимательская деятельность» и «экономическая деятельность» различаются по своему объему, а во-вторых, понятие «экономическая деятельность» шире понятия «предпринимательская деятельность», ибо последняя рассматривается Конституцией Российской Федерации в качестве одного из видов экономической деятельности. Кроме того, Конституция Российской Федерации закрепляет за каждым гражданином России и иными лицами, законно находящимися на ее территории, право свободно вести экономическую деятельность и специально выделяет предпринимательскую деятельность в качестве главного ее вида.

По нашему мнению, необходимо закрепление в российском законодательстве термина «электронная экономическая деятельность», под которым следует понимать предпринимательскую деятельность, а также тесно связанную с ней не запрещенную законом экономическую деятельность, осуществляемую в электронной форме, т.е. с использованием современных коммуникационных средств, в том числе в информационной среде Интернет.

Вместо термина «электронная коммерция» целесообразно использовать понятие «электронная экономическая деятельность» (экономическая деятель-

ность, осуществляемая в электронной форме с использованием современных коммуникационных средств)».

Хотя данная позиция выглядит обоснованной, автор полагает, что введение в отечественное законодательство категории «электронная экономическая деятельность» привело бы к формированию излишне широкой сферы для такого закона и вошло бы в дисгармонию прежде всего с гражданским законодательством, которое уклоняется от ее использования. Учитывая, что данный акт, если он будет принят в нашей стране, будет содержать не только нормы гражданского права, но и нормы административного права и соответственно применяться в административно-правовых отношениях, целесообразно было бы просто четко определить те отношения, при регулировании которых он будет применяться, а не впадать в не имеющую перспективы научную полемику о содержании категории «экономическая деятельность». Категорию «электронная торговля» следует сохранить, чтобы обеспечить схожесть закона с международными актами и прежде всего с ТЗ ЭТ.

Разработчики рассматриваемого акта постарались свести к минимуму специальные дефиниции, используемые в его тексте, и оперируют по сути всего несколькими понятиями, самое основное из которых – «сообщение данных». Под данной категорией понимается «информация, сформированная, отправленная, полученная или хранимая с помощью электронных оптических или аналогичных средств, включая, но не ограничиваясь, электронный обмен данными, электронную почту, телеграмму, телекс или телефакс».

Анализ данного определения показывает, что здесь использованы все основные способы передачи информации, принятые в бизнес-среде при установлении непосредственной связи между отправителем и получателем сообщений. Таким образом, ТЗ ЭТ свое регулирование осуществляет далеко за пределами технологии собственно электронных сообщений.

В нем также используется дефиниция «электронный обмен данными», под которой понимается «электронная передача с одного компьютера на другой

информации с использованием согласованного стандарта структуры информации». Автор полагает данное определение примечательным, тем более что в отечественном законодательстве подобная дефиниция не сформулирована. Это краткое определение вполне объективно и однозначно описывает, что именно должно пониматься под электронным обменом данными: есть средства передачи и приема в виде компьютеров; способ передачи – электронный, а не путем физического переноса сведений, например с помощью флеш-накопителей; есть форма представления сведений в виде согласованного стандарта структуры информации, то есть типа файла, способа программного согласования компьютеров между собой и т.п. По мнению автора, данное определение без существенной корректировки может быть использовано при формировании российского законодательства об электронной торговле, которое постепенно начинается.

Далее в дефинициях ТЗ ЭТ описываются субъекты, которые могут участвовать в информационном обмене. Их три – инициатор сообщения, адресат сообщения и посредник в отношении конкретного сообщения. По сути, всех участников информационного обмена, возможно свести к этим трем категориям, что тоже может быть полезно отечественной системе правового регулирования в данной сфере.

Как и большинство типовых или модельных законов, ТЗ ЭТ не претендует на непосредственное занятие ниши национальных законов – это своего рода опорная конструкция для них. Поэтому в текст данного акта введена специальная статья, именуемая «Толкование». В ее рамках устанавливается, что при толковании настоящего Закона следует учитывать его международное происхождение и необходимость содействовать достижению единообразия в его применении и соблюдению добросовестности. Вопросы, которые относятся к предмету регулирования настоящего Закона и которые прямо в нем не разрешены, подлежат разрешению в соответствии с общими принципами, на которых основан данный Закон.

Из этих норм следует, что основная направленность норм ТЗ ЭТ – унификация национального законодательства, которая в данной сфере должна только приветствоваться, а также «соблюдение добросовестности», то есть общая гуманитарная посылка на правомерность отношений. Если говорить об общих принципах, на которых основан Закон, то они в тексте специально не сформулированы, что является в определенной мере недостатком, так как не позволяет опираться на конкретные положения. А выводить их приходится самостоятельно, а при таком подходе возможны существенные разночтения.

В ТЗ ЭТ изначально устанавливается соотношение императивных и диспозитивных норм – в соответствии с положениями ст. 4 все нормы, которые содержатся в главе III данного Закона, могут быть изменены сторонами соответствующих правоотношений. К их более детальному анализу автор вернется несколько позднее.

Следует отметить, что во всей структуре ТЗ ЭТ наибольшее юридическое значение имеют положения главы II, а из всех ее норм – положения ст. 5, согласно которым «информация на может быть лишена юридической силы, действительности или исковой силы на том лишь основании, что она имеет форму сообщения данных». Собственно говоря, это и есть центральное положение данного акта, а остальные положения направлены на его «обслуживание». Поэтому скорее ТЗ ЭТ описывает не электронную торговлю, а легитимирует электронный документ, устанавливая условия уравнивания его по юридической силе с традиционным бумажным документом. Учитывая сферу действия самой комиссии ООН, она естественным образом не могла подготовить акт более общего характера, чем затрагивающий сферу коммерции.

Позже, в 1998 г., ТЗ ЭТ был дополнен ст. 5 bis, согласно которой информация не может быть лишена юридической силы, действительности или исковой силы на том лишь основании, что она не содержится в сообщении данных, предназначенном для придания такой силы, но к которой просто содержится отсылка в этом сообщении данных. Таким образом были включены в докумен-

тальный оборот ссылки на иные документы и акты. Например, если в сообщении данных имеется отсылка к первоначальному договору, которым он дополняется, то такое дополнение будет иметь соответствующую юридическую силу.

Развивающим положения ст. 5 являются нормы ст. 6, в соответствии с которыми сообщение данных приравнивается к письменной форме документа с оговоркой, что содержащаяся в сообщении данных информация является доступной для последующей ссылки на нее. Это довольно сложное положение для комментирования. Речь здесь идет о том, что сообщение данных должно физически существовать на каком-то носителе, причем в том виде, в котором оно было передано и при этом не могло быть подвержено изменениям. Реализации данной нормы затруднительно достичь без дополнительного подтверждения подлинности электронного документа.

Далее устанавливается, что вышеуказанное положение применяется как в тех случаях, когда содержащееся в нем требование выражено в форме обязательства, так и в тех случаях, когда законодательство просто предусматривает наступление определенных последствий, если информация представлена в письменной форме.

Ст. 7 ТЗ ЭТ устанавливает общие требования к подписи в электронном документе. Как представляется автору, вряд ли эти положения распространимы на телексы и телефаксы, где образ первоначально проставленной подписи отображается. По логике разработчиков ТЗ ЭТ, если законодательство требует подписи лица, это требование считается выполненным в отношении сообщения данных, если:

(a) использован какой-либо способ для идентификации этого лица и указания на согласие этого лица с информацией, содержащейся в сообщении данных;

(b) этот способ является как надежным, так и соответствующим цели, для которой сообщение данных было сформировано или передано с учетом всех обстоятельств, включая любое соответствующее соглашение.

Приведенные положения содержат в себе четыре компонента, совокупное присутствие которых позволяет считать равнозначной по юридической силе подпись на бумажном документе и идентификацию лица, «подписавшего» электронный документ. Во-первых, способ идентификации конкретного физического лица, то есть однозначного установления личности. Во-вторых, подтверждение факта согласия данного лица с информацией, содержащейся в сообщении данных. В бумажном документе это достигается естественным путем – проставлением подписи лицом непосредственно после текста, а если текст расположен на нескольких листах – проставлением подписи на каждом предшествующем листе, либо объединением всех листов таким образом, чтобы часть из них невозможно было бы подменить. ТЗ ЭТ не описывает никаких способов, а лишь формулирует общие требования, оставляя все остальное на усмотрение законодателей конкретных государств. В-третьих, способ идентификации и подтверждения согласия лица с содержанием информации должен быть надежным, то есть исключать фальсификацию. В-четвертых, он должен быть соответствующим цели, для которой сообщение данных было сформировано. Последнее условие, по мнению автора, выглядит излишним, так как не несет в себе юридической нагрузки. Первых трех компонентов достаточно для экспертной оценки любого способа идентификации и подтверждения подлинности электронного документа.

Положения ст. 8 ТЗ ЭТ дополняют положения ст. 5 в части представления сообщения данных в качестве так называемого оригинала. Оригиналы документов, как правило, имеют большее доказательственное значение, чем заверенные копии, поэтому наличие условий для признания документа в электронной форме отображения (сообщения данных), сформулированных в ТЗ ЭТ, можно признать полезным. Автор хотел бы напомнить, что отличие оригинала от копии применительно к данной категории сведений регулирует и ГОСТ 6.10.4-84 « Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники», в отношении ко-

торого в информационных системах правовой информации Российской Федерации отсутствуют сведения, что он прекратил свое действие. В соответствии с данным актом подлинником (т.е. оригиналом) документа на машинном носителе признается первая по времени запись документа, содержащая указание на то, что документ является подлинником. Таким образом, отечественный ГОСТ определяет два условия для признания документа подлинником (оригиналом): временной фактор и прямое указание создателя на то, что это оригинал.

ТЗ ЭТ формулирует следующие условия:

(a) имеются надежные доказательства целостности информации с момента, когда она была впервые сформирована в ее окончательной форме в виде сообщения данных или иным образом; и

(b) в том случае, когда требуется представление информации, эта информация может быть продемонстрирована лицу, которому она должна быть представлена.

В данном случае речь идет о доказательствах целостности и возможности показа электронного документа.

Как представляется автору, в тот период, когда принимался отечественный ГОСТ, проблема целостности информации не являлась актуальной, так как компьютерные комплексы имелись только в органах государственного управления и государственных учреждениях и доступ к управлению ими посторонних лиц был исключен. В современный период эта проблема более чем актуальна, поэтому данное положение ТЗ ЭТ следует признать важным. Условие демонстрации информации в виде сообщения данных заинтересованному лицу, по мнению автора, является самоочевидным. А вот идея отечественного ГОСТа в отношении времени создания документа как условия признания его оригиналом является продуктивной и должна быть использована в качестве объективного условия.

В тексте ст. 8 ТЗ ЭТ имеется дополнительная норма, определяющая условия признания целостности сообщения данных, представляемого как оригинал:

(a) критерием оценки целостности является сохранение информации в полном и неизменном виде, без учета добавления любых индоссаментов и любых изменений, происходящих при нормальном процессе передачи, хранения и представления; и

(b) требуемая степень надежности оценивается с учетом цели, для которой информация была сформирована, и всех соответствующих обстоятельств.

Дополнительные условия не следовало представлять в качестве некоего комментария, а перенести в перечень основных. Дело в том, что они несколько по-иному прорисовывают понятие «оригинал». Во-первых, сообщение данных должно быть очищено от сопутствующей технологической информации; во-вторых, уровень защиты оригинального текста сообщения данных может варьироваться в зависимости от степени важности содержащихся в нем сведений: например, защита текста договора купли-продажи небольшой партии дешевого товара – это одна ситуация, а платежное поручение на перевод значительной денежной суммы – совершенно другая ситуация.

Из контекста положений ст. 8 следует, что все эти критерии должен устанавливать национальный законодатель. С данной посылкой следует согласиться, так как в разных странах существуют разные уровни угроз для обеспечения целостности электронных документов, зависящие от развитости информационной инфраструктуры, а также уровня подготовки потенциальных злоумышленников.

Ст. 9 ТЗ ЭТ формулирует критерии допустимости сообщений данных в качестве доказательств и их доказательственную силу, тем самым подводя итог предшествующим нормам:

(1) При любых процессуальных действиях никакие положения норм доказательственного права не должны применяться таким образом, чтобы отрицалась допустимость сообщения данных в качестве доказательства:

(a) на том лишь основании, что оно представляет собой сообщение данных; или

(b) если оно является наилучшим доказательством, которое, как этого можно разумно ожидать, может быть получено представляющим его лицом, на том основании, что оно не представлено в оригинальной форме.

(2) Информации в форме сообщения данных должна придаваться надлежащая доказательственная сила. При оценке доказательственной силы сообщения данных должна учитываться надежность способа, с помощью которого формировалось, хранилось или передавалось это сообщение данных, надежность способа, с помощью которого обеспечивалась целостность информации, способа, посредством которого идентифицировался его инициатор, и любой другой соответствующий фактор.

Подпункт (a) пункта (1) представляет собой императив, прямое требование законодательного акта и обязывает орган, рассматривающий спор, искать какие-то иные основания для исключения сообщения данных из совокупности доказательств, но не использовать для такого обоснования форму представления информации. В то же время, как следует из положений пункта (2), сообщение данных, не имеющее соответствующей защиты от внесения изменений, не может являться допустимым доказательством. Более того, данная норма обязывает отправителя (инициатора) принимать меры по защите, а органу, рассматривающему спор, предоставляет возможность ставить доказательственную силу сообщения данных в зависимость от надежности способа защиты и способа идентификации инициатора (то есть точного соотнесения с конкретным физическим или юридическим лицом).

Как было упомянуто выше, документ имеет своей целью перенесение информации в будущее, чтобы служить доказательством совершенных ранее действий или свершившихся фактов. Поэтому одним из важных условий является обеспечение его сохранности в течение определенного промежутка времени. По отношению к документам в бумажной форме отображения эта задача решается путем приобщения их к тематическим делам, которые по миновании прямой надобности сдаются в архивы и хранятся в течение сроков, определен-

ных соответствующими нормативными правовыми актами. В связи с тем, что правовая природа и цель создания бумажных документов и документов в электронной форме отображения одинакова, то для обеих категорий документов должны реализоваться одни и те же правила хранения. Ст. 10 ТЗ ЭТ формулирует общие условия хранения документов в электронной форме отображения (сообщений данных) следующим образом:

(a) информация, содержащаяся в сообщении данных, доступна для последующей ссылки на нее;

(b) сообщение данных сохраняется в том формате, в котором оно было сформировано, отправлено или получено, либо в таком формате, в котором может быть представлена точным образом сформированная, отправленная или полученная информация;

(c) сохраняется такая информации, при ее наличии, которая позволяет установить происхождение и назначение сообщения данных, а также дату и время его отправления или получения.

Вышеприведенные требования условно можно разбить на две подгруппы:

1) требования к сохранности и форме представления;

2) требования к идентификации сообщения данных.

Первая группа требований является очевидной и объективной. Сообщение данных должно храниться и быть представлено в таком виде, чтобы наиболее полно отражать его содержание. При этом подпункт (a), по мнению автора, сформулирован с интересным подтекстом: информация в форме сообщения данных должна храниться не на сменных носителях, а на соответствующих серверах, доступных для просмотра, то есть иметь адрес расположения, когда заинтересованные лица могут самостоятельно осуществлять к ней доступ. Это существенно меняет способ организации хранения электронных документов.

Вторая группа касается двух аспектов: традиционных атрибутов документа, согласно которым можно установить, от кого он исходит, кто и когда его

подписал, а также когда он передан и когда принят в рамках информационной системы.

Итак, глава II ТЗ ЭТ свое регулирование направила на императив признания юридической силы за документом в электронной форме отображения, в том числе путем отсылки, признание сообщения данных как письменной формы документа, а также на условия определения в электронном документе такого важного его атрибута как подпись, условия признания сообщения данных оригиналом документа, определение условий признания электронного документа как доказательства и допустимость его в таком качестве. Учитывая, что данные нормы являются основополагающими, в том или ином виде они в обязательном порядке должны быть включены в структуру национальных законов, регулирующих отношения в сфере электронного документооборота.

Как автор показал выше, положения главы III ТЗ ЭТ являются диспозитивными, то есть могут применяться сторонами соответствующих правоотношений как модель для установления непосредственных прав и обязанностей, а могут быть изменены по усмотрению сторон. При этом анализ данных норм показывает, что не все они являются таковыми, поэтому их диспозитивность можно признать в достаточной мере условной. Если же спроецировать ряд положений на сферу государственного управления, то их вполне возможно воспринимать в качестве императивных норм.

Действительность и юридическая сила сообщения данных в нормах данной главы признаются как общее правило, из которого возможны либо законодательные, либо договорные исключения. Так, в частности, п. (1) ст. 11 устанавливает, что в контексте заключения договоров, если стороны не договорились об ином, оферта и акцепт оферты могут производиться с использованием сообщений данных. В случае, когда при заключении договора используется сообщение данных, этот договор не может быть лишен действительности или исковой силы на том лишь основании, что для этой цели использовалось сообщение данных.

Говоря иначе, стороны гражданско-правового договора должны специально договориться о том, что они не будут использовать данный способ заключения сделки. Если предложение к совершению сделки (оферта) поступило в форме сообщения данных и было акцептовано таким же образом, то договор следует считать заключенным. Как мы видим, диспозитивное в данном случае заключается лишь в том, что стороны вправе договориться об ином способе заключения договора.

Следуя этой же логике, ТЗ ЭТ устанавливает в ст. 12, что в отношениях между инициатором и адресатом сообщения данных волеизъявление или другое заявление не может быть лишено юридической силы, действительности или исковой силы на том лишь основании, что оно имеет форму сообщения данных, оставляя при этом для национального законодателя определить исключения для данного общего правила. По мнению автора, общая норма сформулирована здесь излишне размыто. Все же не любое сообщение данных, содержащее волеизъявление субъекта, при облечении его в форму сообщения данных сохраняет должную действительность или юридическую силу. Это сообщение данных должно быть защищено и позволять однозначно идентифицировать его с конкретным субъектом (инициатором сообщения). Такая конкретизация здесь просто необходима.

Положения ст. 13 «Атрибуция (установление авторства) сообщения данных» выглядят еще более императивными. Части 1–3 данной статьи устанавливают варианты признания направленного электронного документа «сообщением данных инициатора». При обмене документами в электронной форме отображения нормативное регулирование данных отношений имеет принципиальное значение, так как позволяет установить и подтвердить факт происхождения информации от отправителя. При обмене бумажными документами для этого служат атрибуты документа, регистрационные номера, печати, различного рода реестры, по которым данная информация передается.

ТЗ ЭТ устанавливает, что сообщение данных считается сообщением данных инициатора, если оно было отправлено самим инициатором. Говоря иначе, оно должно быть отправлено с зарегистрированного в информационной системе компьютерного адреса инициатора. Однако в реальной жизни могут быть и иные ситуации, и закон приравнивает к первому случаю следующие:

– когда сообщение было отправлено лицом, которое имело полномочия действовать от имени инициатора в отношении этого сообщения данных; или

– когда сообщение было отправлено информационной системой, запрограммированной инициатором или от его имени функционировать в автоматическом режиме.

Очевидно, что данные факты должны быть юридически подтверждены определенными документами.

Устанавливает ТЗ ЭТ и некоторую совокупность прав адресата сообщения по признанию факта отправления сообщения данных инициатором, которая сводится к следующему правилу:

«В отношениях между инициатором и адресатом адресат имеет право считать, что сообщение данных является сообщением данных инициатора, и действовать исходя из этого предположения, если:

(a) для того чтобы установить, что сообщение данных является сообщением данных инициатора, адресат надлежащим образом применил процедуру, предварительно согласовованную с инициатором для этой цели; или

(b) сообщение данных, полученное адресатом, явилось результатом действий лица, отношения которого с инициатором или любым агентом инициатора дали такому лицу возможность доступа к способу, используемому инициатором для идентификации сообщений данных как своих собственных».

В данном случае речь уже идет о наличии письменных предварительных договоренностей о способах передачи и способах идентификации, то есть применение данных норм возможно только при заключении соответствующих договоров между инициатором и адресатом сообщений, в том числе и так называ-

емых договоров присоединения, когда потенциальный адресат заключает договор с организатором информационно-телекоммуникационной системы, в которую включен в том числе и инициатор сообщений.

В электронном обмене данными одним из самых существенных элементов, имеющих юридическое значение, является подтверждение факта получения документа в электронной форме отображения (сообщения данных). Как правило, именно с момента получения информации возникает собственно правоотношение. Именно поэтому в текст ТЗ ЭТ включена довольно большая группа норм, объединенных в ст. 14, которая регулирует отношения по подтверждению получения сообщений данных. Эти положения можно поделить на нормы общего и специального характера.

Прежде всех рассматривается случай, когда инициатор и адресат не договорились о способе подтверждения получаемых сообщений определенным способом или в определенной форме. В такой ситуации ТЗ ЭТ допускает подтверждение следующим путем:

– любого сообщения со стороны адресата, направленного автоматизированным или иным способом, или

– любых действий со стороны адресата, достаточных для того, чтобы показать инициатору, что сообщение данных было получено.

Затем рассматривается случай, когда инициатор не указал, что сообщение данных обусловливается получением подтверждения, и подтверждение не было получено им в течение оговоренного или согласованного срока, либо, если такой срок не был оговорен или согласован в течение разумного срока, инициатор:

– может направить адресату уведомление, указав в нем, что подтверждение получено не было, и установив разумный срок, к которому подтверждение должно быть получено;

– если подтверждение не получено в течение срока, установленного выше, может после уведомления об этом адресата считать сообщение данных неотправленным или осуществить любые другие права, которые он может иметь.

Существенным по своим юридическим последствиям правилом, сформулированным в рассматриваемой группе норм, является то, что «в случае, когда инициатор получает от адресата подтверждение получения, считается, что соответствующее сообщение данных было получено адресатом. Такая презумпция не предполагает, что отправленное сообщение данных соответствует полученному сообщению». Говоря иначе, факт подтверждения получения электронного документа не означает одновременного подтверждения его подлинности адресатом. Данное положение в обязательном порядке должно включаться в национальные законы, регулирующие общие правила оборота электронных документов.

Не менее важной является и ст. 15 ТЗ ЭТ, устанавливающая правила относительно времени и места отправления и получения сообщения данных. Во многих группах правоотношений время и место направления документа, а равно и электронного документа, могут иметь юридическое значение и порождать соответствующие правовые последствия.

В соответствии с ч. 1 данной статьи, если инициатор и адресат не договорились об ином, отправление сообщения данных происходит в момент, когда оно поступает в информационную систему, находящуюся вне контроля инициатора или лица, которое отправило сообщение данных от имени составителя. Примером такой системы может служить электронная почта в сети «Интернет», так как отправитель сообщения после не в состоянии произвольно изменить время направления файла и IP-адрес, с которого он был направлен.

Далее устанавливается, что если инициатор и адресат не договорились об ином, момент получения сообщения данных устанавливается следующим образом:

(а) если адресат указал информационную систему для цели получения таких сообщений данных, получение происходит:

– в момент, когда сообщение данных поступает в указанную информационную систему; или

– если сообщение данных направляется в информационную систему адресата, которая не является указанной информационной системой, в момент, когда сообщение данных извлекается адресатом из системы;

(b) если адресат не указал информационную систему, получение происходит в момент, когда сообщение данных поступает в какую-либо информационную систему адресата.

Перед нами три возможных случая подтверждения: (а) подтверждение факта поступления в информационную систему, определенную получателем; (б) извлечение сообщения адресатом из любой информационной системы; (в) поступление сообщения в информационную систему, принадлежащую адресату. Как представляется автору, указанные правила исчерпывающим образом определяют все должные варианты признания факта получения электронного документа получателем, в достаточной мере определены юридико-технически и могут быть в таком виде транслированы в соответствующее национальное законодательство.

Часть четвертая ст. 15 устанавливает правила определения места отправления и места получения электронного документа: если инициатор и адресат не договорились об ином, сообщение данных считается отправленным в месте нахождения коммерческого предприятия инициатора и считается полученным в месте нахождения коммерческого предприятия адресата. Приведены также варианты в отношении более сложных субъектов. Так, если инициатор или адресат имеют несколько коммерческих предприятий, местом нахождения коммерческого предприятия считается такое место, которое имеет наиболее тесное отношение к основной сделке, или – в случае отсутствия основной сделки – место нахождения основного коммерческого предприятия; если инициатор или адресат не имеют коммерческого предприятия, таковым считается их обычное место жительства.

Указанные правила, по мнению автора, также следует признать достаточно точно сформулированными и исчерпывающими по содержанию.

Подводя итог рассмотрению ТЗ ЭТ, автор хотел бы отметить, что он носит рамочный и, так сказать, технологический характер. Его нормы и структура могут стать основой для соответствующих национальных законов, так как описывают важные элементы в организации электронного документооборота между сторонами, имеющими одинаковый юридический статус и не подчиненными друг другу. Однако при этом необходимо заметить, что не все положения рассмотренного акта могут быть однозначно транслированы в соответствующий российский закон, если такой будет приниматься, из-за терминологических несоответствий и правовых неопределенностей, на которые автор обращал внимание.

Обратимся теперь к анализу Модельного закона «Об электронной торговле». Как следует из общих положений данного акта, целью Модельного закона является правовое обеспечение условий для электронной торговли на основе признания электронных сообщений, включая:

– закрепление прав и обязанностей лиц, осуществляющих электронную торговлю;

– определение правил совершения сделок с использованием электронных сообщений, подписанных аналогами собственноручной подписи;

– формирование правовой основы государственного регулирования и поддержки электронной торговли;

– защиту прав и законных интересов граждан и юридических лиц, участвующих в электронной торговле.

Следует обратить внимание на то, что в ТЗ ЭТ цель не определялась, а сфера определена предельно широко – любой вид информации в виде сообщения данных, используемый в коммерческой (торговой) деятельности. Модельный закон отходит от «технологичности » Типового закона и распространяет свое действие в том числе на формирование правовой основы регулирования данных отношений, а также на защиту прав и законных интересов граждан в данной сфере. Автор считает такой подход не совсем верным. Задача типового

или модельного закона – дать перечень наиболее общих правил, на основании которых национальные законодатели могли бы разработать национальные законы, позволяющие осуществлять электронный документооборот в сфере торговли между несколькими странами, а не вторгаться в исключительную прерогативу национального законодателя по построению соответствующей системы правового регулирования. Говоря иначе, типовой или модельный закон – это фундамент для национального закона, а его «здание» выстраивается самостоятельно.

Значительно больше в Модельном законе и дефиниций. Некоторые из них совпадают по значению с дефинициями ТЗ ЭТ. Так, близки к ним по содержанию категории «адресат», «информационный посредник», «отправитель электронного сообщения»), остальные понятия существенно изменены, а также сформулирован ряд новых понятий. Из указанного автор делает вывод о том, что разработчики Модельного закона были знакомы с содержанием ТЗ ЭТ и ряд его положений транслировали в этот акт. Однако в ряде случаев юридическая логика понятий существенно изменена. Так, в частности, п. 4 ст. 4 Модельного закона устанавливает, что «электронное сообщение, используемое в электронной торговле, не может быть отвергнуто только на том основании, что оно оформлено или получено посредством использования информационных систем или информационно-телекоммуникационных сетей». Центральная норма ТЗ ЭТ, как автор показал выше, делает акцент на форме представления информации. В приведенной норме также присутствует технологическая ошибка – электронное сообщение не может быть оформлено посредством информационных систем или сетей – оно формируется средством вычислительной техники, то есть компьютером, имеющим соответствующее программное обеспечение. Эта же ошибка заложена и в определение категории «электронное сообщение», которое представлено в тексте Модельного закона как «информация, подготовленная, отправленная, полученная и хранимая с помощью информационных систем, информационно-коммуникационной сети и электронных процедур».

Достаточно сложной для восприятия и весьма странной по содержанию представляется автору дефиниция Модельного закона «электронная операция сделки », определяемая как «совершение сторонами сделки отдельных действий по оформлению и совершению сделки субъектов и их информационных систем в электронной торговле». Со сторонами сделки вроде бы все ясно, но причем здесь субъекты и информационные системы – совершенно неясно. Тем не менее данное понятие включено в более общее, которое через него определяется. Так, «электронная процедура – порядок (правила, регламент) совершения электронных операций по сделке». Может быть, конечно, в ряде случаев и необходимо определять правила и порядок осуществления отдельных действий при заключении договоров в электронной форме, но сам по себе термин «электронная процедура» автору представляется лишенным должного смыслового наполнения. В свою очередь, это понятие входит в качестве элемента в одно из центральных для Модельного закона. Так, категория «электронный договор» определяется как «гражданско-правовой договор, осуществляемый на основе использования информационных систем, информационно-коммуникационной сети и электронных процедур». У автора здесь целый ряд вопросов: во-первых, почему речь идет только о гражданско-правовом договоре; во-вторых, использование информационных систем, информационно-коммуникационной сети и электронных процедур должно осуществляться при заключении такого договора совместно либо они могут использоваться поодиночке?

Одним словом, специальные термины, сформулированные в Модельном законе, с точки зрения юридической техники весьма далеки от совершенства.

Обратимся теперь к основным принципам правового регулирования в сфере электронной торговли, сформулированным в ст. 4 Модельного закона. В.А. Леушин и В.Д. Перевалов полагают, что принципы права – это руководящие идеи, характеризующие содержание права, его сущность и назначение в обществе. С одной стороны, они выражают закономерности права, а с другой – представляют собой наиболее общие нормы, которые действуют во всей сфере

правового регулирования и распространяются на всех субъектов. Эти нормы либо прямо сформулированы в законе, либо выводятся из общего смысла законов [60]. Необходимость формирования некоторой совокупности правовых принципов в текстах законов обусловлена также тем, что любой законодательный акт не в состоянии детально и подробно охватить все возможные варианты возникающих в сфере его действия правоотношений. Поэтому в тех случаях, когда в законе отсутствует соответствующая норма, следует исходить из принципов, в нем сформулированных. Данное суждение свидетельствует о том, что правовая нагрузка на нормы-принципы должна быть довольно высокой и они должны быть сформулированы четко и однозначно.

Часть 1 ст. 4 устанавливает, что «правовое регулирование в сфере электронной торговли основывается на принципах равенства ее участников, свободы договора, свободного перемещения товаров, услуг и финансовых средств на всей территории государства, беспрепятственного осуществления предпринимательской деятельности в рамках электронной торговли, а также на гарантиях судебной защиты прав участников электронной торговли». Здесь представлен набор основных конституционных гарантий для предпринимательской деятельности, который обычно формулируется в конституциях государств, признающих рыночную экономику. Включение или изъятие их из текста Модельного закона никак не повлияет на возможность их применения для конкретных отношений.

Часть 2 ст. 4 устанавливает, что «участники электронной торговли приобретают и реализуют права, исполняют обязанности в соответствии с законодательством и электронными договорами. Приобретение и осуществление участниками электронной торговли прав и обязанностей в области электронной торговли могут быть ограничены только национальным законодательством». Автор полагает, что участники рассматриваемых отношений могут приобретать права и обязанности не только посредством заключения договоров в электронной форме отображения, но и иных договоров, которые им

предшествуют, либо вообще их заменяют. Поэтому такое ограничение возможности вступать в правоотношения субъектам электронной коммерции недопустимо. Последнее предложение касается реализуемого, в частности, в России принципа ограничения гражданских прав только посредством норм федерального законодательства. Как модель для других стран данная норма может быть полезна.

Часть 3 ст. 4 устанавливает, что «участие в электронной торговле, если иное не установлено договором или законом, не может служить основанием для установления дополнительных требований, процедур или ограничений деятельности участников электронной торговли». Принцип в определенной мере спорный. Не следует забывать, что для электронной торговли используется определенная телекоммуникационная среда, от функционирования которой многое зависит. Ограничения и дополнительные требования для пользователей телекоммуникационных систем могут возникать не только на основании законов, но и подзаконных актов. Естественно, что такие требования будут влиять на участников электронной торговли.

Часть 4 ст. 4 устанавливает, что «электронное сообщение, используемое в электронной торговле, не может быть отвергнуто только на том основании, что оно оформлено или получено посредством использования информационных систем и информационно-коммуникационных сетей». По сути данный принцип есть перефразированная центральная норма ТЗ ЭТ, но видоизмененная не лучшим образом. Так, в статье 5 упомянутого Типового закона речь идет о признании юридической силы за документом в электронной форме отображения (сообщением данных), а в Модельном законе – о признании юридической силы (косвенно) за электронным документом, переданным посредством электронных телекоммуникаций. Это далеко не одно и то же. Получается, что электронный документ, переданный на каком-то носителе адресату непосредственно, a priori обладает юридической силой, равной бумажному документу. Вряд ли это возможно без применения соответствующих средств защиты информации.

Часть 5 ст. 4 является логическим развитием принципа, рассмотренного выше: «электронные сделки не могут быть признаны недействительными только на том основании, что они совершены и оформлены посредством использования информационных систем, информационно-коммуникационных сетей и электронных процедур, если иное не предусмотрено национальным законодательством». Здесь возникает следующий вопрос: если это «иное» предусмотрено национальным законодательством, то какой смысл в Модельном законе?

Часть 6 ст. 4 устанавливает следующий принцип: «нормативно-правовые акты в сфере правового регулирования электронной торговли не должны устанавливать каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий не установлена национальным законодательством в сфере информационной безопасности». Данное правило, по мнению автора, следует признать полезным, так как оно направлено на воспрепятствование ограничению конкуренции на рынке телекоммуникационных услуг.

Часть 7 ст. 4 устанавливает, что «участники электронной торговли должны все сведения о предлагаемых ими товарах (работах, услугах) предоставлять в форме, которая позволяет их адресату, не обладающему специальными знаниями, однозначно определить полученную информацию как относящуюся к электронной торговле и составить достоверное представление о правовом положении лица, осуществляющего электронную торговлю, о его товарах (работах, услугах), ценах на них и условиях их приобретения». Как полагает автор, данное положение, в целом весьма полезное для правового регулирования рассматриваемых правоотношений, не может рассматриваться как принцип. Это четкое императивное правило, но не более того.

Существенный научный интерес представляют нормы ст. 6 Модельного закона, содержащие общие требования к форме и порядку документирования при оформлении электронных сделок.

Часть 1 устанавливает, что «договор в электронной сделке оформляется как результат согласования условий договора сторонами и формирования его посредством обмена электронными сообщениями между сторонами сделки».

Конечно же, любой договор есть результат согласования его условий сторонами. Но неясно, почему текст договора предложено формировать путем обмена электронными сообщениями между сторонами сделки? Одна сторона направляет проект договора, другая сторона соглашается с его положениями полностью. Так бывает чаще всего и никакого «формирования» в данном случае не наблюдается.

Далее в части 1 устанавливается, что «при формировании электронного договора по соглашению сторон могут использоваться любые доступные сторонам или установленные законом или стандартом формы (форматы) электронного представления и оборота текстовой или иной информации (запись, файл, сайт, база данных, запись в базе данных) общепринятых или установленных нормативно-правовыми актами видов документов, применяемых в коммерческой деятельности (письмо, уведомление, учетная запись, предложение заключить договор (оферта), принятие предложения (акцепт), договор, соглашение, протокол и другие виды документов)». По мнению автора, данная норма Модельного закона излишне вторгается в сферу гражданского законодательства, меняя сложившуюся концепцию оформления заключаемых договоров. Задача здесь более простая: признать, что документ в электронной форме отображения (именно документ, со всеми атрибутами) по юридической силе равен документу, представленному на бумаге. Следовательно там где требуется заключение договора в письменной форме, его может заменить электронный документ при определенных условиях. Именно так следует понимать контекст ТЗ ЭТ. В данной же норме мы видим совершенно иное.

Далее в части 1 устанавливается, что «при формировании электронного сообщения используемые формы (форматы) его электронного представления и употребления должны обеспечивать достоверную передачу и получение сооб-

щения, его обработку, возможность проверки достоверности и целостности документа, хранение и поиск в информационной системе, а также обеспечивать идентификацию отправителя (создателя), время создания или получения, воспроизведение и однозначное восприятие его информации». Требование в достаточной мере обоснованное. В противном случае никакого электронного документооборота не получится.

Части 4, 5 и 7 ст. 6 устанавливают общие условия для цифровых подписей. В качестве электронной подписи в электронном сообщении признается любой способ фиксации и отображения выражения воли сторон сделки, который:

– установлен законом, иным нормативно-правовым актом или соглашением сторон и признается сторонами;

– позволяет идентифицировать лицо, подписавшее сообщение;

– содержит указание на то, что это лицо подтверждает (одобряет) информацию, содержащуюся в электронном сообщении;

– оправдан характером сделки, обеспечен ответственностью сторон сделки, а также соответствует цели, для которой электронное сообщение было подготовлено или передано.

Процедура подписания или установления (вписывания) электронной подписи в договор может функционально совмещаться с процедурами защиты электронного сообщения, обеспечивающими целостность, достоверность и неизменность его документированной информации перед другой стороной или третьими лицами.

При анализе данных, в целом верных, положений у автора возник резонный вопрос: зачем вновь формировать общее абстрактное правило, когда на деле совсем не много средств, позволяющих его реализовать, и эти средства в виде ЭП уже законодательно определены? Почему сразу не указать на необходимость применения ЭП? Так было бы проще и понятнее. Как представляется, разработчики Модельного закона здесь не слишком удачно скопировали ряд положений ст. 7 ТЗ ЭТ, хотя те в 1996 г. шли непроторенным путем, а к 2008 г., то есть к моменту принятия Модельного закона, в целом ряде государств-

участников СНГ были приняты законы об ЭП.

Часть 6 ст. 6 определяет условия для признания электронного документа в качестве подлинника. В целом эти нормы повторяют положения ст. 8 ТЗ ЭТ, однако опять же с существенным изъяном: ТЗ ЭТ требует наличия надежных доказательств целостности информации с момента, когда она была впервые сформирована в ее окончательной форме в виде сообщения данных, в ч. 6 ст. 6 Модельного закона более размыто говорится об обеспечении защиты сделки, целостности и неизменности содержащейся в ней информации с учетом характера сделки и т.п. Получается, что электронная сделка есть документ, хотя из дефиниций данного акта следует иное.

Интерес также представляют положения ст. 7 Модельного закона, являющиеся оригинальными по отношению к ТЗ ЭТ, в котором ничего подобного не содержится. Часть 1 данной статьи устанавливает следующее:

«В случаях, когда договор должен быть представлен в письменной форме или когда требуется оформление действий в письменной форме и предусматривается наступление определенных последствий в случае несоблюдения этой формы, то это требование считается выполненным путем представления электронного сообщения, если содержащаяся в нем информация является доступной для ее последующего использования.

Если иное не установлено национальным законодательством, электронное сообщение, реализующее факт взаимодействия и отношения сторон в сделках гражданско-правового значения при обмене информацией, является простой письменной формой, фиксирующей действия и отношения сторон в процессах оформления, заключения и реализации электронных сделок».

Автор говорил выше и акцентирует внимание еще раз на том, что электронное сообщение в виде файла без адекватной защиты содержащихся в нем сведений подвержено произвольным изменениям и не может приниматься в качестве доказательства факта возникновения тех или иных правоотношений. А о необходимости защиты в данных положениях не говорится.

Часть 2 этой же статьи содержит следующую норму, совершенно безотносительно к части 1: «Все экземпляры одного и того же электронного сообщения (подготовленные, полученные, переданные, хранимые), подписанные электронной подписью, имеют равное юридическое значение при условии обеспечения необходимой защиты информационных систем и среды хранения документов». Положение правильно во всех отношениях. Оно означает, что в случае применения ЭП (которое одновременно подтверждает факт волеизъявления субъекта и осуществляют своеобразную защиту файла от произвольных изменений) все экземпляры электронного документа имеют равную юридическую силу. Следовательно, среди них нет ни оригиналов, ни копий. Правда непонятно, причем здесь защита информационных систем и среды хранения документов. Видимо, разработчики Модельного закона не совсем понимают, что представляет собой ЭП и каково ее предназначение.

Положения части 3 ст. 7 сформулированы в Модельном законе следующим образом: «Копия электронного сообщения на бумажном носителе имеет юридическое значение, если она подписана собственноручной подписью обладателя электронной цифровой подписи или иного электронного аналога подписи, а также в случаях, если копия удостоверена лицом, имеющим право удостоверения в соответствии с порядком, установленным законом или иными нормативно-правовыми актами, а также соглашением сторон». Это действительно важная и нужная норма, устанавливающая соотношение между электронным документом и его бумажной копией и основные случаи удостоверения этой копии.

Положения части 4 рассматриваемой статьи, заключающиеся в том, что «электронные сообщения, подписанные электронной подписью или иным электронным аналогом подписи в порядке, определяемом законодательством, являются судебными доказательствами и при рассмотрении споров могут представляться в качестве судебных доказательств в порядке и на условиях, предусмот-

ренных национальным законодательством», напротив, представляются автору излишними, так как лишь констатируют факт, но никак не устанавливают условия признания электронных документов в качестве таких доказательств.

Остальные положения Модельного закона определяют примерные права и обязанности различных субъектов, участвующих в процедурах электронной торговли, и их анализ выходит за рамки настоящего исследования.

В качестве итога к рассмотрению основных положений Модельного закона «Об электронной торговле» автор отмечает, что данный акт является с юридико-технической точки зрения весьма далеким от совершенства. В его нормах присутствуют прямые и косвенные противоречия. Положения данного акта не опираются на доктрину. Хотя в ряде норм Модельного закона и можно обнаружить следы ключевых положений Типового закона ЮНСИТРАЛ «ОБ электронной торговле», однако концепцию данного акта Модельный закона не воспринял. В силу указанного он вряд ли может быть достойной основой для разработки соответствующего национального законодательства.

Теперь перейдем к анализу Типового закона ЮНСИТРАЛ «Об электронных подписях», принятого в Вене 05.07.2001. Действие данного акта также распространяется на торговую деятельность и, как автор говорил выше, является частным случаем ТЗ ЭТ.

Для акта, регулирующего столь сложные правоотношения, где право граничит с компьютерными технологиями, очень важным является не описание технологии юридическим языком, а формулирование условий, которым должны соответствовать те или иные способы защиты информации, чтобы электронный документ был по юридической силе равнозначен бумажному при одинаковом их использовании. Применительно к российскому Закону об ЭП, интересную мысль высказал С.И. Семилетов: «Большие надежны в обеспечении государственных гарантий применения свободного электронного документооборота возлагались на ФЗ «Об электронной подписи», однако этого не случилось. Существенными обстоятельствами, определившими декларативный ха-

рактер данного Закона, стали использование единственного способа организации электронной подписи, основанной на криптографии и паре связанных открытых и закрытых ключей, требующей развертывания инфрастуктуры удостоверяющих центров и, соответственно, отсутствие этих центров, а также отсутствие федеральных нормативно-правовых актов Правительства РФ в развитие данного Закона, особенно в части организации инфраструктуры удостоверяющих центров» [29]. Как должен поступить национальный законодатель – вопрос сложный, но международно-правовой акт в виде модели для национальных точно не должен фиксировать какую-то одну технологию.

Поэтому уже в определении цифровой подписи мы видим обобщенность подхода: «электронная подпись» означает данные в электронной форме, присоединяемые или логически ассоциируемые с сообщением данных, которые могут использоваться, чтобы идентифицировать подписавшего в отношении сообщения данных и указания на одобрение подписывающего лица информации, содержащейся в сообщении данных».

В определении цифровой подписи присутствуют три важных юридически значимых компонента: (а) неразрывная связь цифровой подписи с общением данных; (б) цифровая подпись должна идентифицировать лицо, подписавшее сообщение данных; (в) цифровая подпись должна подтверждать, что подписавшее лицо таким образом осуществило свое индивидуальное волеизъявление в виде одобрения.

Указанные идеи находят развитие и в других дефинициях. Так, категория «сертификат» означает сообщение данных или иную запись, подтверждающую связь между подписывающим лицом и данными для создания подписи. Категория «подписывающее лицо» означает лицо, которое владеет данными для создания подписи и действует либо от своего собственного имени, либо от имени лица, которое оно представляет. Категория «поставщик сертификационных услуг» означает лицо, которое выдает сертификаты и может оказывать другие услуги, касающиеся электронных подписей. Категория «полагающаяся сторо-

на» означает лицо, которое может действовать на основании сертификата или электронной подписи.

Типовой закон «Об электронных подписях» (далее – ТЗ ЭП) специально устанавливает в ст. 3 равный режим технологий подписи: «ничто в настоящем Законе, за исключением статьи 5, не должно применяться таким образом, чтобы исключать, ограничивать или умалять юридическую силу любого способа создания электронной подписи, который удовлетворяет требованиям, указанным в статье 6, или иным образом соответствует требованиям применимого права».

Статья 5 определяет, что из положений данного Закона могут быть сделаны изъятия или их действие может быть изменено по соглашению, если такое соглашение не будет являться недействительным или не имеющим силы в соответствии с применимым правом. Иными словами, она определяет диспозитивность большинства норм ТЗ ЭП.

Статья 6, именуемая «Соблюдение требования в отношении наличия подписи», непосредственно содержит набор требований, которые предъявляются к применяемой технологии электронной подписи. В частности, часть 1 устанавливает следующее: «Когда законодательство требует подписи лица, это требование выполняется в отношении сообщения данных, если используется электронная подпись, которая является настолько надежно, насколько соответствовала цели, для которой было сформировано или передано сообщение данных с учетом всех обстоятельств, включая любое соответствующее соглашение». Главная идея этой нормы – постановка надежности цифровой подписи как технологии от степени важности подписываемого сообщения. Действительно, использование цифровой подписи физическим лицом для приобретения малоценного контента – это одно, а подписание посредством цифровой подписи платежных документов на миллионы долларов – это совсем другое.

Далее, в части 3 рассматриваемой статьи формулируются требования, на основании которых электронная подпись считается надежной и удовлетворяющей требованиям части 1:

(a) данные для создания подписи, в том контексте, в котором они используются, связаны с подписывающим и никаким другим лицом;

(b) во время подписания данные для создания подписи находились под контролем подписывающего и никакого другого лица;

(c) любое изменение электронной подписи, сделанное после момента подписания, является обнаружимым; и

(d) в случае, когда одной из целей правового требования к подписи является предоставление гарантии целостности информации, к которой она относится, любое изменение данной информации, сделанное после момента подписания, является обнаружимым.

Совокупное решение этих вполне очевидных правовых задач представляет определенную технологическую сложность. Она заключается прежде всего в том, чтобы одновременно выполнить требования подпункта (a) и подпункта (b), то есть нужно одновременно иметь некоторый публичный сертификат цифровой подписи, созданный таким образом, чтобы он не раскрывал данные для создания цифровой подписи (главные из них – закрытый ключ).

В связи с указанным А.В. Юрасов отмечает, что «самое сложно выполнимое из этих условий – условие обеспечения гарантий невозможности восстановления закрытого ключа по открытому ключу и любому числу подписанных электронных документов. Лучший из предложенных на сегодня учеными способов его выполнения состоит в том, чтобы использовать такие процедуры подписания и проверки, что практическое восстановление закрытых ключей по ключам открытым требует решения известной сложно вычислительной задачи. Поскольку общеизвестно, что задача является сложной, и если ее не научились решать за обозримое время все математики мира во все предыдущие столетия (первые упоминания о задачах такого рода сделаны Аристотелем), то существует надежда, что ее не сумеют быстро решить и в ближайшем обозримом будущем. Практический результат последующих (после публикации статьи Диффи и Хэллмана) научных поисков таких задач оказался до некоторой сте-

пени парадоксальным: при всем многообразии известных сложных вычислительных задач практически применимой оказалась только одна (впоследствии она была дополнена еще двумя задачами). Это так называемая задача дискретного логарифмирования. Оказывается, что задача дискретного логарифмирования при правильном выборе указанных целых чисел настолько сложна, что позволяет надеяться на практическую невозможность восстановления числа **x** – индивидуального закрытого ключа по числу **b**, применяемому в качестве открытого ключа.

Чтобы говорить более определенно о практической невозможности решить эту вычислительную задачу, следует предварительно договориться о том, какие вычислительные ресурсы доступны тому, кто предположительно будет эту задачу решать. Поскольку давать конкретные оценки возможностей потенциальных вычислительных ресурсов будущего «взломщика» системы ЭП дело сложное, будем исходить из предположения, что он располагает полной информацией о наилучших известных мировой науке методах решения данной задачи.

Даже если допустить, что потенциальный взломщик ЭП располагает вычислительной системой, эквивалентной по мощности 1000 суперкомпьютеров, то на выполнение вычисленной объемом 10^{21} операций ему потребовалось бы не менее 30 лет непрерывной работы всей системы, что с практической точки зрения означает бессмысленность их выполнения. Поэтому ЭП со стандартной длиной ключа (64 бита), для расшифровки которой требуется выполнить более 10^{19} операций, обладает достаточно высоким уровнем защиты.

Однако 12 августа 2002 г. стало известно об успешном «вскрытии» зашифрованной 64-битным ключом информации. Произошло это в рамках научного проекта, известного под названием «Bovine». Проект был создан в 1997 г. и объединил к своему завершению более 331 тыс. человек, добровольно принявших участие в создании сети для распределенного решения этой задачи. Спустя 1757 дней (почти пять лет) после запуска проект, целью которого был

подбор 64-битного ключа методом перебора всех возможных кодовых комбинаций, завершил работу и показал возможность «взлома» системы ЭЦП.

Для увеличения надежности используются более длинные ключи шифрования. Современные цифровые процессоры позволяют за доли секунды вычислять и проверять электронные подписи с ключами в 512 бит, а стойкость большинства широко применяемых методов электронной подписи при такой длине ключей определяется необходимостью проведения более чем 10^{50} операций вычисления» [49].

Однако разработчики ТЗ ЭП ведут речь не только о криптографических качествах алгоритма цифровой подписи. Здесь важное место занимают организационные меры. Лицо, обладающее закрытым ключом электронной подписи, должно обеспечивать его секретность, то есть исключить возможность ознакомления с его содержанием и тем более его неправомерного использования третьими лицами. Реализация данного требования обладателем ключа подлежит доказыванию им при возникновении конфликтной ситуации.

Требования подпунктов (c) и (d) в большей мере обеспечиваются технологическими решениями, в том числе и криптографической стойкостью алгоритма цифровой подписи.

Учитывая масштабность потенциального применения ТЗ ЭП, разработчики сделали в рассматриваемой статье специальную оговорку, согласно которой сформулированные требования не ограничивают способности любого лица:

– устанавливать любым другим образом в целях удовлетворения указанных требований надежность электронной подписи; или

– представлять доказательства ненадежности электронной подписи.

Далее в ТЗ ЭП формулируется комплекс обязанностей субъектов отношений, связанных с использованием электронных подписей.

Обязанности лица, подписывающего сообщения данных электронной подписью, сформулированы в ст. 8 следующим образом:

«(1) В случае, когда данные для создания электронной подписи могут использоваться для создания подписи, которая имеет юридическую силу, каждое подписывающее лицо обязано:

(a) проявлять разумную осмотрительность для недопущения несанкционированного использования своих данных для создания подписи;

(b) без неоправданной задержки уведомлять любое лицо, которое, как разумно может ожидать подписывающее лицо, полагается на электронную подпись или оказывает услуги, опираясь на электронную подпись, если:

(i) подписывающее лицо знает, что данные для создания подписи были скомпрометированы;

(ii) обстоятельства, известные подписывающему лицу, порождают значительный риск того, что данные для создания подписи могли быть скомпрометированы;

(c) в случае, когда для поддержки электронной подписи используется сертификат, проявлять разумную осмотрительность для обеспечения точности и полноты всех существенных заверений, сделанных подписывающим лицом, которые имеют значение для сертификата в течение срока его использования или которые включатся в сертификат.

(2) Подписывающее лицо несет ответственность за невыполнение требований пункта (1).

Национальному законодателю в данном случае остается уточнить сроки уведомления (если это необходимо), а также определить вид юридической ответственности, наступающей в случае невыполнения этих требований.

Статья 9 определяет комплекс обязанностей поставщика сертификационных услуг (в системе понятий российского Закона об ЭП).

П – удостоверяющего центра). К числу основных обязанностей данного субъекта отношений относятся:

(a) действовать в соответствии с заверениями, сделанными им в отношении своих основных принципов деятельности и практики (здесь необходимо сразу дать пояснение: в частности, российское законодательство не предполагает юридической силы подобного рода деклараций – цели и задачи деятельности должны быть определены в каком-то правоустанавливающем документе – положении или уставе);

(b) проявлять разумную осмотрительность в целях обеспечения точности и полноты всех существенных заверений, сделанных им, которые имеют значение для сертификата в течение срока его использования или которые включатся в сертификат (по сути данная норма предполагает формулирование в национальном законодательстве требований к делопроизводству поставщика данных услуг);

(c) предоставлять разумным образом доступные средства, которые позволяют полагающейся стороне удостовериться из сертификата:

(i) в личности поставщика сертификационных услуг;

(ii) что подписывающее лицо, идентифицированное в сертификате, обладало контролем над данными для создания подписи в момент, когда был выдан сертификат;

(iii) что данные для создания подписи являлись действительными в момент, когда был выдан сертификат или до этого;

(d) предоставлять разумным образом доступные средства, которые позволяют полагающейся стороне удостовериться, когда это имеет значение, из сертификата или иным образом:

(i) в способе, используемом для идентификации подписывающего лица;

(ii) в любом ограничении цели использования или стоимостного размера, в отношении которых могут использоваться данные для создания подписи или сертификат;

(iii) что данные для создания подписи являются действительными и не были скомпрометированы;

(iv) использовать надежные системы, процедуры и людские ресурсы при осуществлении своих услуг.

Здесь мы одновременно видим требования к сертификату электронной подписи и к организации, которая взяла на себя функции поставщика сертификационных услуг. Данные нормы могут быть сравнительно легко конкретизированы в национальном законодательстве.

Отдельно выделяют качественные характеристики поставщика сертификационных услуг, которым он должен соответствовать (ст. 10): «При установлении того, являются ли надежными и в какой степени любые системы, процедуры или людские ресурсы поставщика сертификационных услуг, могут приниматься во внимание следующие факторы:

(a) финансовые и людские ресурсы, включая наличие активов;

(b) качество систем аппаратных и программных средств;

(c) процедуры обработки сертификатов, заявок на сертификаты и сохранения записей;

(d) доступность информации для подписывающих лиц, идентифицированных в сертификатах, а также для потенциальных полагающихся сторон;

(e) регулярность и степень проведения аудита независимым органом;

(f) наличие заявления государства, органа аккредитации или провайдера сертификационных услуг, касающегося соответствия с предшествующими факторами или их наличия».

Мы видим здесь совокупность достаточно жестких требований, предъявляемых к поставщику сертификационных услуг, которые должны быть конкретизированы в национальном законодательстве. Прежде всего речь идет о наличии финансовых активов, которые могут быть использованы для выплаты потерпевшей стороне в случае ошибок поставщика, повлекших имущественный ущерб. Второе важное условие – обязательное проведение внешнего аудита и определение глубины проверок. Третье – подтверждение органом государства или иным органом степени готовности поставщика

к выполнению возложенных на него задач (ситуация, близкая к лицензированию).

Для потребителя услуг («полагающейся стороны») прямые обязанности не определены. Констатируется только, что она несет правовые последствия своей неспособности:

(a) принимать разумные меры по проверке надежности электронной подписи; или

(b) в случае, когда электронная подпись поддерживается сертификатом, принимать разумные меры:

(i) для проверки действительности, приостановления или отзыва сертификата; и

(ii) по соблюдению любого ограничения в отношении сертификата.

Говоря иначе, если потребитель услуг осуществляет своевременные действия по проверке действительности цифровой подписи и действительности ее сертификата, то никаких негативных последствий для него не наступает.

Последняя важная группа норм, которую необходимо подвергнуть анализу при рассмотрении ТЗ ЭП, является признание иностранных сертификатов и электронных подписей. Наверное, не следовало бы создавать типовой закон, если не попытаться урегулировать данные отношения, ведь ЮНСИТРАЛ стремится прежде всего к развитию международной торговли. В последней, 12-й статье данного акта эти нормы сформулированы следующим образом:

«(1) При определении того, обладает ли – или в какой мере обладает – сертификат или электронная подпись юридической силой, не учитываются:

(a) место выдачи сертификата или создания или использования электронной подписи, или

(b) местонахождение коммерческого предприятия эмитента или подписавшего.

(2) Сертификат, выданный за пределами принимающего государства, обладает такой же юридической силой в принимающем государстве, как и серти-

фикат, выданный в принимающем государстве, если он обеспечивает по существу эквивалентный уровень надежности.

(3) Электронная подпись, созданная или используемая за пределами принимающего государства, обладает такой же юридической силой в принимающем государстве, как и электронная подпись, созданная или используемая в принимающем государстве, если она обеспечивает по существу эквивалентный уровень надежности.

(4) При определении того, обеспечивает ли сертификат или электронная подпись по существу эквивалентный уровень надежности для целей пункта (2) или (3), следует учитывать признанные международные стандарты и любые другие соответствующие факторы.

(5) В тех случаях, когда, независимо от положений пунктов (2), (3) и (4), стороны договариваются между собой об использовании определенных видов электронных подписей или сертификатов, такая договоренность признается достаточной для цели трансграничного признания, за исключением случаев, когда такая договоренность не будет действительной или не будет иметь силы согласно применимому праву».

Положения данной статьи предполагают, во-первых, развитие международных стандартов в области использования цифровых подписей, которые официально должны быть признаны государствами; во-вторых, дает возможность государствам устанавливать двусторонние или многосторонние отношения на основе договоров и соглашений по признанию юридической силы цифровых подписей.

На основании проведенного анализа автор может сделать вывод о том, что ТЗ ЭП по своему юридико-техническому уровню и форме регулирования соответствует своему предназначению. Он содержит вполне приемлемые для акта такого уровня нормы, позволяющие на их основе сформировать схожие по сути национальные законы, которые впоследствии могут быть применены для установления соответствующих межгосударственных отношений. Положения

данного акта также могут применяться международными коммерческими арбитражами.

Обратимся теперь к анализу Модельного закона «Об электронной цифровой подписи» принятого на 16-м пленарном заседании Межпарламентской ассамблеи государств – участников СНГ (постановление № 16-10 от 09.12.2000).

В качестве цели данного акта его разработчики выделяют обеспечение правовых условий для использования электронных подписей, при соблюдении которых подпись признается достоверной, а также права, обязанности и ответственность организаций, предоставляющих услуги по удостоверению электронных подписей. При этом действие Модельного закона 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.

Рассматриваемый акт содержит довольно значительное число специальных дефиниций, среди которых наиболее значимыми являются категории «электронные данные (электронное сообщение)» и «электронная подпись». Первая категория определяется довольно просто, как «цифровое представление любой информации, воспринимаемой ЭВМ». Вторая категория определяется развернуто, как «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».

Как можно заменить, ЭП здесь определяется через конечный результат выполняемой ей задачи. И только пара «открытый ключ - закрытый ключ» указывает на подстройку норм Модельного закона под определенный алгоритм выработки ЭП.

Категория «закрытый ключ электронной подписи» определяется как «электронные данные, используемые для создания электронной подписи, известные только подписывающему лицу». Соответственно категория «открытый ключ электронной цифровой подписи» определяется как «электронные данные, предназначенные для проверки подлинности электронной цифровой подписи и известные пользователю открытого ключа».

Важной для дальнейшего анализа является также категория, определяющая субъекта, отвечающего за удостоверение принадлежности ЭП определенному субъекту: «центр регистрации открытого ключа электронной цифровой подписи – юридическое лицо, обладающее правомочиями на удостоверение соответствия открытого ключа электронной цифровой подписи закрытому ключу лица, на чье имя выданное регистрационное свидетельство». Мы видим здесь, что в качестве такого субъекта может выступать только юридическое лицо, но не указано, что оно должно быть специализированным, что расширяет количество потенциальных субъектов, претендующих на реализацию данной задачи.

Документы, подтверждающие факт принадлежности открытого ключа конкретному субъекту, определяются в Модельном законе следующим образом:

– «регистрационное свидетельство на открытый ключ электронной цифровой подписи – документ, подтверждающий соответствие этого открытого ключа электронной цифровой подписи закрытому ключу, выданный Центром регистрации открытых ключей владельцу закрытого ключа электронной подписи или его полномочному представителю»;

– «операционное регистрационное свидетельство – регистрационное свидетельство на открытый ключ электронной подписи, содержащее информацию

об ограничении использования электронной подписи, в том числе выданное на одну или несколько конкретных сделок».

Наличие двух этих документов вызывает у автора определенные сомнения, так как ограничения на использование ЭП можно отражать в основном регистрационном свидетельстве, как это сделано в российском Законе об ЭП. Кстати говоря, сама категория «регистрационное свидетельство» по сравнению с отечественной категорией «сертификат» в большей степени отражает функциональное предназначение данного документа.

Далее следуют дефиниции, определяющие основных субъектов правоотношений по применению электронных подписей:

– «владелец закрытого ключа электронной 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 – физическое или юридическое лицо, на имя которого выдано регистрационное свидетельство на открытый ключ электронной 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 подписи»;

– «пользователь открытого ключа электронной подписи – физическое или юридическое лицо, использующее открытый ключ электронной подписи».

Проведём анализ. Во-первых, владелец закрытого ключа и владелец регистрационного свидетельства – это одно и то же лицо, поэтому вряд ли целесообразно их разделять. Во-вторых, и это самое важное – предоставляемая Модельным законом возможность легального владения закрытым ключом

юридическому лицу в корне меняет концепцию применения ЭП, резко отрывая данную систему подтверждения подлинности документа от бумажного документа, где собственноручная подпись несет юридическую функцию, о которой автор уже говорил выше. Из данного факта может проистекать много следствий, в том числе имеющих негативный характер. Например, совершив противоправное действие путем оформления какого-то документа ответственность несет то лицо, которое его подписало. Это может быть в том числе и уголовная ответственность. А она, как известно, на юридические лица не распространяется. Таким образом, применив ЭП юридического лица, различного рода махинаторы могут уйти от ответственности. Далее, бумажный документ, подписанный собственноручной подписью физического лица, и электронный документ, подписанный ЭП юридического лица, имея одно и то же содержание, становятся по юридической значимости между собой неэквивалентными, что кроме путаницы в деловой оборот ничего внести не может.

Попытка приспособления различного рода новых средств к давно сложившимся юридическим конструкциям, таким как документ и подпись в документе, – дело довольно сложное и порождающее различные суждения. Например, И.Л. Бачило и С.И. Семилетов полагают, что «тезис о признании равнозначности электронной подписи с собственноручной подписью физического лица в документе на бумажном носителе не выдерживает критики, поскольку, с одной стороны, данная статья не содержит условия о биометрической привязке ключа подписи к владельцу сертификата ключа подписи и соответствующей биометрической процедуры подписывания, а, с другой стороны, электронная цифровая подпись может передаваться доверенным третьим лицам или несанкционированно использоваться третьей стороной. По своей физической природе и сути электронная цифровая подпись в электронном документе, если быть точным, скорее является аналогом оттиска печати юридического (или, что реже, факсимиле физического) лица на бумажном

документе, которая в отличие от печати заверяет электронный документ в целом, а не только подпись должностного лица» [15].

Конечно, искусственное приспособление чего-либо к естественному процессу всегда есть только приближение, более грубое или менее грубое. И ЭП путем формулирования совокупности некоторых правовых условий искусственно сближается с собственноручной подписью. Основная задача юридического свойства здесь – исключить возможность использовать закрытый ключ ЭП третьими лицами против воли обладателя. Но ведь и собственноручную подпись физического лица, как это ни парадоксально, возможно использовать третьим лицам: в деловой практике как государственного управления, так и коммерческой, имеют место случаи, когда руководители оставляют своим доверенным сотрудникам чистые листы бумаги со своей собственноручной подписью, на которые затем наносится необходимая информация, и они приобретают статус документа.

Поэтому нельзя так однозначно утверждать, что «по своей физической природе и сути» ЭП является аналогом оттиска печати. ЭП – это вообще нечто особое, которое мы путем создания некоторой совокупности правил делаем юридическим аналогом другого. Но это другое, автор хотел бы подчеркнуть еще раз, – веками сложившаяся практика, где все естественным образом расставлено на свои места и любое смещение в сторону здесь – путь в никуда.

В нормах Модельного закона делается определенная попытка как-то разграничить подпись физического лица и «подпись» юридического лица. Пункт 4 ст. 3 устанавливает следующее:

«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 ак-

кредитованного Центра регистрации или в порядке, предусмотренном соглашением сторон;

– подписавшее лицо правомерно владеет закрытым ключом, используемым для создания электронной цифровой подписи;

– электронная подпись является действующей на момент подписания».

Пункт 5 той же статьи устанавливает:

«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».

Мы видим, что в любом случае ЭП все же «привязывается» к физическому лицу. Тогда возникает вопрос: зачем усложнять систему? Разумного объяснения для такого решения разработчиков Модельного закона автор не видит.

Одними из важнейших в Модельном законе являются нормы, устанавливающие статус и порядок деятельности центров регистрации открытых ключей ЭП. В связи с тем, что Модельный закон направлен на унификацию нормативного регулирования в данной сфере, эти нормы, по логике, должны создать единообразные правовые условия для деятельности таких субъектов для всех стран СНГ. Попробуем именно под этим углом зрения проанализировать нормы главы 2 данного акта.

Как следует из части 1 ст. 8, «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».

Часть 2 ст. 8 устанавливает, что «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».

Как полагает автор, такой административный механизм деятельности Центров регистрации (заявительный порядок) устанавливается для того, чтобы стимулировать занятие данной деятельностью тех или иных субъектов. Однако, в частности, в российских реалиях государственная аккредитация мало чем отличается от лицензирования, так как она подразумевает под собой экспертизу (проверку) готовности субъекта к выполнению определенных функций. Точно такая же экспертиза проводится и перед получением лицензии. Но лицензия дается на определенный срок, затем снова следует проверка готовности и выдача новой лицензии, а в отношении государственной аккредитации срока последующих проверок может быть не установлено.

Мнение автора по данному вопросу более радикальное: если мы хотим обеспечить действенность системы удостоверения подлинности ЭП, то данную деятельность необходимо лицензировать, причем условия для получения лицензии должны быть одинаковыми для всех стран СНГ. Только в этом случае возможно создание непротиворечивой и прозрачной системы, которая будет способствовать развитию электронной торговли [19].

1. Часть 4 ст. 8 устанавливает, что «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». При всей, казалось бы, прозрачности данного положения, в нем заложена та же ошибка, что и в отношении возможности использования ЭП юридическим лицом – должен подлежать регистрации не открытый ключ Центра, а открытые ключи должностных лиц, которые вправе удостоверять сертификаты

ключа подписи. В противном случае данная норма входит в противоречие с п. 8 ст. 9, согласно которому Центр регистрации «обязан выдавать и заверять бумажные копии сообщения, подписанного электронной цифровой подписью, на закрытый ключ которой выдано свидетельство, по требованию владельца закрытого ключа данной 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». Таким образом, если у Центра один ключ ЭП для заверения сертификатов и несколько должностных лиц, уполномоченных выдавать сертификаты в бумажной форме, то это нелогично.

Достаточно однозначно установлены Модельным законом пределы юридической ответственности центров регистрации. В соответствии с нормами ст. 16 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. В то же время при возникновении обстоятельств непреодолимой силы ответственность Центра не наступает только в случае, если иное не предусмотрено законом или договором. Ответственность Центра не наступает также 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.

Как представляется автору, Модельный закон в данном случае излишне вторгается в компетенцию национальных законодателей, устанавливая процитированные императивы, например, ответственность только за реальный ущерб. В отношении так называемого «предела доверия», ситуация и вовсе неясная, так как в иных нормах Модельного закона об этой юридической кон-

струкции никаких норм более не содержится. И вообще установление «предела доверия» автору представляется вредным, так как снижает уровень достоверности всей системы подтверждения подлинности ЭП.

Подводя итог краткому анализу наиболее значимых норм Модельного закона «Об электронной цифровой подписи», хотелось бы констатировать, что не все его нормы являются логичными и взаимоувязанными, ряд положений данного акта излишне вторгается в компетенцию национальных законодателей. Хотя структура Закона и может служить основой для структуры национальных законов, однако многие его положения необходимо существенно перерабатывать для того, чтобы они были встроены в национальные системы права.

В качестве заключения к данному параграфу хочется сказать, что в последние годы предпринимаются попытки принятия отечественного закона «Об электронной коммерции», для которого предлагаются различные названия, вплоть до «электронной экономической деятельности». Введение в отечественное законодательство такой категории привело бы к формированию излишне широкой сферы действия для такого акта и вошло бы в дисгармонию прежде всего с гражданским законодательством, которое уклоняется от ее использования. Учитывая, что данный акт, если он будет принят в нашей стране, будет содержать не только нормы гражданского права, но и нормы административного права и соответственно применяться в административно-правовых отношениях, целесообразно было бы просто четко определить те отношения, при регулировании которых он будет применяться, а не впадать в не имеющую перспективы научную полемику о содержании категории «экономическая деятельность». Категорию «электронная торговля» следует сохранить, чтобы обеспечить схожесть закона с международными актами и прежде всего с Типовым законом ЮНСИТРАЛ «Об электронной торговле».

§ 2. Сравнительно-правовой анализ понятийного аппарата законодательства об электронной подписи. Условия придания юридической силы электронным подписям

В теории права является общепризнанным, что язык нормативных правовых актов должен быть кратким, четким и определенным. Многословие, расплывчатость дают повод различному толкованию норм права, препятствуют их единообразному применению. Краткость и определенность формулировки достигаются с помощью различных приемов изложения норм права, использования специальных терминов, стандартных языковых оборотов. Терминология нормативных актов должна быть единой. Для достижения точности и определенности терминов, их единообразного понимания могут использоваться легальные дефиниции (дефинитивные нормы), в которых даются определение термина, его разъяснение, обязательное для адресатов нормативного акта. Это легальное определение может иногда существенно расходиться с обыденным или даже научным определением. Формализация понятий привносит в правовое регулирование большую точность и определенность» [69].

Еще римские юристы говорили, что любое юридическое определение несет в себе опасность. Поэтому определение должно наполнить конкретным юридическим смыслом термины, нередко взятые из повседневной речи. Оно должно исключать любую двусмысленность, делая ясным и достоверным толкование и применение той или иной нормы или группы норм права. Существуют следующие правила составления дефиниций:

– они должны отражать только существенные признаки обобщаемых явлений; эти признаки должны иметь правовое значение;

– они должны быть полными и отражать все обобщаемые явления;

– они должны быть адекватными, то есть иметь совпадающий объем с определяемым понятием;

– они не должны содержать противоречивых суждений;

– они не должны содержать термины, употребляемые в определяемом понятии (чтобы избежать тавтологии).

Обобщенно можно сказать, что выработка четких дефиниций в нормативном правовом акте не только делает его определенным, даже, можно сказать, эстетичным, но и экономит место в его нормах, подчас двумя-тремя словами заменяя целые группы предложений, которыми можно раскрыть то или иное понятие.

Для сферы электронного документооборота в целом и применения электронной подписи в частности дефиниции, тем более важны, так как они определяют многие новые для права понятия и создают единое понятийное пространство, которое должно действовать не только в одном государстве. Изучение этих понятий с целью классификации и выбора наиболее приемлемых категорий представляет, по мнению автора, существенный научный и практический интерес [94].

Чтобы представить картину из этих определений более целостной, автор хотел бы вновь оттолкнуться от определений, изложенных в текстах актов международного уровня – Типового закона ЮНСИТРАЛ «О цифровых подписях», Модельного закона государств-участниц СНГ «Об электронной цифровой подписи» и Директивы Европейского парламента и Совета 1999/93/ЕС от 13.12.1999 «О правовых основах Сообщества для электронных подписей». Затем автором будут анализироваться аналогичные дефиниции национальных законов, вызвавшие у него наибольший интерес.

Главное заключается в том, что для формирования электронной подписи мы используем определенные математические преобразования, выраженные в числовой форме.

ТЗ ЭП определяет «электронную подпись» как данные в электронной форме, присоединяемые или логически ассоциируемые с сообщением данных, которые могут использоваться, чтобы идентифицировать подписавшего в от-

ношении сообщения данных и указания на одобрение подписывающего лица информации, содержащейся в сообщении данных.

Директива ЕС определяет категорию «электронная подпись» как данные в электронной форме, которые присоединены или логически ассоциируются с другими электронными данными, и которые служат в качестве метода аутентификации.

Модельный закон СНГ определяет категорию «электронная цифровая подпись» как 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: (а) подтвердить неизмененность исходных данных после подписания их электронной цифровой подписью; (б) установить, что электронная цифровая подпись создана с использованием закрытого ключа, соответствующего открытому; (в) установить владельца регистрационного свидетельства на открытый ключ электронной цифровой подписи, при наличии такого свидетельства.

В одном из вопросов – идентификации источника сообщения – все три определения в той или иной степени схожи, то есть во всех трех случаях данная цель создания цифровой подписи прослеживается достаточно однозначно. При этом дефиниция Модельного закона в буквальном смысле содержит «техническое задание» на то, какие функции должна выполнять техническая система цифровой подписи.

Однако определения Директивы ЕС и Модельного закона страдают весьма существенным изъяном. Они, к сожалению, опускают главную правовую функцию подписи (соответственно и цифровой подписи) – служить подтверждением факта волеизъявления физического лица по отношению к информации, зафиксированной на том или ином носителе. Причем проставление подписи без оговорок по сложившейся правовой традиции воспринимается как согласие с содержанием данной информации. Отметим, что в ТЗ ЭП формула «ука-

зание на одобрение подписывающего лица» содержится, что, по мнению автора, ценно.

Здесь также уместно отметить, что один из самых мощных векторов в формировании современных правовых систем направлен на то, чтобы правомерное волеизъявление индивидов было максимально свободным. Это относится прежде всего к сфере гражданско-правового регулирования, но присутствует ныне и во многих институтах административного права, в рамках которых граждане вступают в административные отношения по своей воле. И если обычно презюмируется, что проставление собственноручной подписи в документе (пока не доказано обратное) свидетельствует об этом свободном волеизъявлении, то в отношении цифровой подписи, «оторванной» от руки человека, необходимо формирование некоторой дополнительной совокупности правовых условий, обеспечивающих подтверждение данного факта. Причем, как полагает автор, эти правовые условия должны быть предметом специализированного законодательного регулирования.

Если исходить из градации дефиниций на полные и неполные, то законодательно определить цифровую подпись через полную дефиницию в обозримом будущем вряд ли удастся, что связано с разной законодательной техникой и принципами построения нормативных правовых актов, применяемыми в разных странах. Помимо этого, сама категория «цифровая подпись» является сложной и отдельные грани ее свести в кратком определении более чем проблематично [92].

Исходя из вышеизложенного целесообразно либо использовать неполную дефиницию, в которую необходимо включать наиболее существенные признаки того или иного предмета или явления, либо формировать дефиницию-перечень, где по возможности перечислять все признаки или функции. Это более громоздко. Но, как автор покажет ниже, в отношении цифровой подписи в некоторых национальных законодательных актах применяется.

Однако в любом случае указание на то, что цифровая подпись является (должна являться) средством подтверждения факта свободного волеизъявления физического лица в документе, представляется автору самым существенным ее признаком как юридической категории.

В указанном смысле весьма примечательной и логичной выглядит соответствующая дефиниция, содержащаяся в Законе Туркменистана от 19.12.2000 «Об электронном документе», где цифровая подпись определяется как «аналог собственноручной подписи в виде набора символов (последовательности чисел), признаваемый в качестве официальной подписи отправителя электронного документа». Далее следуют иные функциональные характеристики данного средства:

– задача подтвердить принадлежность цифровой подписи конкретному владельцу;

– задача подтверждения факта, что цифровая подпись (а точнее, по мнению автора, ключи цифровой подписи) является действующей на момент подписания.

Совсем иначе выглядит категория «цифровая подпись» в интерпретации Закона Республики Беларусь от 01.01.2000 «Об электронном документе», где она определена как «набор символов, вырабатываемый средствами электронной цифровой подписи и являющийся неотъемлемой частью электронного документа».

В данной дефиниции одно понятие дается через другое понятие, что с точки зрения логики недопустимо. Помимо этого, вряд ли во всех случаях цифровая подпись является неотъемлемой частью документа – она может с ним логически ассоциироваться, и указание на такую связь содержится в целом ряде аналогичных определений.

На основании изложенного можно заключить, что дефиниция белорусского закона не отражает ни юридической сущности, ни предназначения цифровой подписи.

Следующее определение, в котором содержатся несколько нестандартные по отношению к модельному законодательству (в дальнейшем автор под данным обобщенным термином будет понимать одновременно и Типовой, и Модельный законы) положения, представлено в Законе Украины от 04.04.2001 «О платежных системах и переводе денег». Здесь цифровая подпись определяется как «совокупность данных, полученная в результате криптографического преобразования содержимого электронного документа, которая предоставляет возможность подтвердить его целостность и идентифицировать лицо, которое его подписало».

Наиболее примечательным элементом данной дефиниции является категория «криптографическое преобразование», а в целом данное определение в качестве легального признает только один, довольно узкий класс цифровых подписей, в которых они получаются посредством зашифровывания некоторого отрезка информации. Примерно так же подходят к определению сущности цифровой подписи и российские законодатели (электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе) [15].

В индийском Законе от 09.06.2000 «Об информационных технологиях» прямо устанавливается, что любой абонент вправе аутентифицировать электронную запись путем присоединения своей цифровой подписи; аутентификация электронной записи производится использованием асимметричной криптосистемы и хэш-функции, которая охватывает и преобразует первоначальную электронную запись в другую электронную запись).

Как справедливо указано в индийском законе, собственно криптографическому преобразованию предшествует формирование хэш-функции – резуль-

тата обобщенного анализа данных в электронном файле, который всегда одинаков по отношению к конкретному файлу. Изменение данных в файле должно изменять результат хэш-функции. Для того, чтобы злоумышленник не смог это реализовать, результат хэш-функции зашифровывается. Собственно, тогда и получается цифровая подпись в понимании российского и индийского законодателей.

Однако вернемся к вопросу о том, насколько важным в определении цифровой подписи является упоминание о криптографическом преобразовании. С точки зрения формулирования общих правовых условий использования цифровых подписей не имеет значения, будет ли признан алгоритм выработки цифровой подписи криптографическим преобразованием, либо нет.

Но у данной проблемы имеется иная составляющая. Криптографические алгоритмы длительное время использовались в целях обеспечения обороны и безопасности государств, проводящих суверенную внешнюю политику. Поэтому шифры как собственно криптоалгоритмы, принципы из создания и правила использования в течение многих веков тщательно скрывались. А так называемая «открытая» криптография насчитывает от силы четыре-пять десятилетий, обязана своим появлением компьютерным и производным от них технологиям и пробивала себе дорогу достаточно сложным путем. Еще в прошлом десятилетии в США велась острая дискуссия по поводу возможности экспорта компьютерных и телефонных криптосистем повышенной сложности. В конечном итоге победила точка зрения, которая в наиболее концентрированном виде нашла отражение в Законе Герцогства Люксембург от 14.08.2000 № 96 «Об электронной коммерции», где однозначно установлено, что использование криптографических средств является свободным.

Но на самом деле не все так просто. Криптосистемы, используемые для защиты коммерческой, банковской и частной информации, а также криптосистемы, используемые для защиты государственно-значимой информации во многом схожи друг с другом, так как в основе их лежат одни и те же математи-

ческие принципы. Исходя из этого, в частности, в Российской Федерации, в отличие от Люксембурга, оборот криптографических систем не может быть полностью свободным. Второй момент, лежащий в основе собственно американской дискуссии, заключается в том, что спецслужбы государств в случае необходимости негласного ознакомления с зашифрованной информацией частных субъектов должны тратить слишком значительные усилия на аналитическое раскрытие этой информации без изначального знания ключей.

Именно поэтому в нашей стране до сего времени действует специализированный нормативный правовой акт – Указ Президента Российской Федерации от 03.04.1995 № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», нормами которого, в частности, запрещается использование «государственными организациями и предприятиями в информационно-телекоммуникационных системах шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись), и защищенных технических средств хранения, обработки и передачи информации, не имеющих сертификата ФАПСИ». К настоящему времени ФАПСИ как федеральный орган исполнительной власти упразднен, а его функции в данной части переданы ФСБ России [28].

Приведенные нормы свидетельствуют о том, что криптографические средства являются, говоря языком гражданского права, ограниченно оборотоспособными объектами (то есть объектами, оборот которых на территории Российской Федерации осуществляется на основании специальных норм). В силу указанного прямое отнесение цифровой подписи к видам криптографического преобразования в российском Законе об ЭП является обоснованным и носит ориентирующий характер для правоприменителя.

Данный подход, четко очерчивающий границы использования цифровой подписи и определяющий основные параметры используемого для ее выработки криптографического алгоритма – асимметричной криптосистемы, применя-

ется не во всех странах. Так, в частности, в английском Законе от 25.05.2000 № 1798 «Об электронных коммуникациях» устанавливается следующее:

«Электронная подпись является многим из чего-либо в электронной форме, что:

(a) инкорпорировано или иным образом логически ассоциировано с любым электронным сообщением или электронными данными;

(b) предполагает быть инкорпорированным или ассоциированным в целях использования для установления подлинности сообщения или данных, целостности сообщения или данных или того и другого вместе».

Такой подход дает чрезвычайно обширные возможности для использования тех или иных алгоритмов и средств в качестве электронной подписи. Можно сказать, что подходы российских и английских законодателей находятся на разных правовых полюсах: российский – жестко административный, английский – предельно широкий.

Посмотрим теперь, какие страны занимают промежуточное положение и насколько это обоснованная позиция. Но прежде всего, обратимся к ряду норм ТЗ ЭП, который проводит логику двухуровневой цифровой подписи. Часть 1 ст. 6 данного акта устанавливает, что «в тех случаях, когда законодательство требует наличия подписи лица, это требование считается выполненным в отношении сообщения данных, если использована электронная подпись, которая является настолько надежной, насколько это соответствует цели, для которой сообщение данных было подготовлено или передано, с учетом всех обстоятельств, включая любые соответствующие договоренности».

В данном случае разработчики Типового закона ставят уровень защиты, реализуемый цифровой подписью, в зависимость от цели, которую хотели бы достигнуть отправитель и адресат электронного сообщения. Такая трактовка допускает использование в качестве цифровой подписи любой системы подтверждения подлинности, о которых стороны заранее договорились. Это и есть «широкое понимание» электронной подписи.

Данную правовую логику в том или ином контексте восприняли отдельные национальные законы. Так, Федеральный закон Австрийской Республики от 19.08.1999 № 190 «Об электронной подписи» следующим образом разграничивает простую и безопасную цифровую подпись. Цифровая подпись определяется в данном акте как «электронные данные, присоединенные или логически связанные с другими электронными данными, служащие для аутентификации и установления идентичности подписывающего лица».

Как видно из данного определения, основным технологическим критерием цифровой подписи в данном случае является ее присоединение или логическая связь с основным электронным сообщением. В свою очередь, для безопасной цифровой подписи предусмотрен целый перечень дополнительных критериев, которым должен отвечать как сам алгоритм, так и организационная система. К ним относятся:

а) принадлежность цифровой подписи исключительно подписывающему лицу;

б) предоставление возможности идентификации подписывающего лица;

в) создание цифровой подписи с использованием средств, которые находятся под единоличным контролем подписывающего лица;

г) связанность с данными, к которым она относится, таким способом, что любое последующее изменение данных может быть установлено;

д) основанность цифровой подписи на квалифицированном сертификате и то, что она создается с использованием технических компонентов и процедур, соответствующих установленным требованиям.

Первые три условия определяют так называемую персонификацию подписи и ее компонентов. Вторые два условия определяют технические характеристики средства выработки и проверки цифровой подписи.

Говоря обобщенно, безопасная цифровая подпись должна быть юридически «привязана» к конкретному субъекту правоотношений, а средство выработки и проверки цифровой подписи должно отвечать нормативным определенным требованиям.

В Законе Республики Болгария от 07.04.2001 № 15 «Об электронном документе и электронной подписи» вообще предусмотрено три уровня цифровой подписи: простая, усовершенствованная и универсальная.

Применительно к простой подписи данным законодательным актом установлено, что ей является «любая информация, связанная с электронным сообщением способом, согласованным между автором и адресатом, достаточно надежным с учетом потребностей обращения, который: (а) раскрывает личность автора; (б) раскрывает согласие автора с электронным сообщением; (в) защищает содержание электронного сообщения от последующего изменения».

Если сравнивать данное определение с критериями австрийского закона относительно безопасной цифровой подписи, то они в общем и целом совпадают, за исключением требования нахождения средства выработки подписи под единоличным контролем подписывающего лица. Из этого следует, что болгарский закон изначально устанавливает для цифровой подписи более жесткие стартовые условия.

В ст. 14 болгарского закона содержится норма, устанавливающая, что «никто, кроме автора, не имеет права доступа к данным для создания электронной подписи». Но это скорее правомочие для лица, чем его обязанность не раскрывать соответствующую информацию третьим лицам, которая необходима для легитимации цифровой подписи.

Усовершенствованная цифровая подпись как юридическая категория определяется ст. 16 рассматриваемого закона на основании следующих критериев: (а) преобразование электронного сообщения, осуществляемое посредством цифровой подписи, либо включение или добавление данных цифровой подписи в основное сообщение должно быть осуществлено до преобразования; (б) указанные действия совершаются посредством алгоритмов, включающих использование частного ключа в асимметричной криптосистеме; (в) требования к алгоритмам определяются Правительством.

Говоря обобщенно, усовершенствованная цифровая подпись, исходя из требований болгарского закона, означает использование строго определенного алгоритма преобразования при выработке цифровой подписи. При этом формирование хэш-функции должно происходить до криптографического ее преобразования.

Помимо указанного, болгарский закон определяет дополнительные правовые условия, предъявляемые к усовершенствованной цифровой подписи, именуемые механизмом ее создания и проверки: (а) данные для создания цифровой подписи могут воспроизводиться только при ее создании и уверенности в их надежной защищенности; (б) данные для создания цифровой подписи недоступны, не могут быть извлечены и подпись защищена от подделки; (в) данные для создания цифровой подписи могут быть защищены автором от их использования другим лицом; (г) содержание сообщения доступно автору и остается неизменным до создания цифровой подписи.

В вышеприведенной норме содержится несколько полезных в принципе, а также пригодных для совершенствования аналогичного российского законодательства положений. Во-первых, данные для создания цифровой подписи, которые в системе отечественных терминов именуются закрытым ключом, не могут быть прочитаны или скопированы никем, даже их владельцем; их извлечение с носителя возможно только в момент создания цифровой подписи. Реализация этой обязывающей нормы повышает уровень защиты закрытого ключа и технологически реализуема. Во-вторых, алгоритм выработки цифровой подписи должен быть таким, что при любой обработке подписи сам закрытый ключ определен быть не может. Эта задача решается путем использования надежного криптографического преобразования, но здесь просматривается косвенно еще одно требование: закрытый ключ не должен оставаться нигде, кроме своего первичного носителя (например, не может копироваться и оставаться хранимым в средстве выработки цифровой подписи). Данное требование также существенно повышает уровень защищенности закрытого ключа и повышает степень достоверности цифровой подписи.

Касаясь проблемы безопасной цифровой подписи, необходимо отметить, что законодательство ряда стран достаточно однозначно определяет критерии, которым должны отвечать программно-технические средства для формирования цифровой подписи. Так, в частности, Закон Литовской Республики от 11.07.2000 № VIII-1822 «Об электронной подписи» для безопасного оборудования для формирования цифровой подписи устанавливает следующие критерии:

а) данные для формирования подписи, используемые для создания цифровой подписи, практически возможно получить только однажды, и их секретность обеспечивается;

б) данные для формирования подписи, используемые для создания цифровой подписи, практически невозможно воссоздать, и подпись защищена от подделки с использованием доступных в настоящее время технологий;

в) данные для формирования подписи, используемые для создания цифровой подписи, подписывающее лицо может достоверно оберегать от других лиц;

г) оборудование для формирования подписи при создании подписи не изменяет, подписываемые данные и не препятствует подписывающему лицу знакомиться с этими данными до подписания.

По сути, в приведенных нормах перечислены основные критерии, которым должны отвечать средства выработки цифровой подписи. Соответственно, все лица, осуществляющие разработку таких устройств, при декларировании того, что они качественные (в контексте рассматриваемого акта – безопасные), обязаны подтвердить, что они соответствуют указанным критериям.

Указание непосредственно в тексте закона таких критериев для Литвы является вполне обоснованным, так как в этом акте нигде далее не упоминается о сертификации средств цифровой подписи, имеется только норма о том, что уполномоченное правительством этой страны учреждение, осуществляющее надзор за цифровой подписью, разрабатывает требования к оборудованию цифровой подписи.

Анализ данной системы в нашей стране на сегодняшний момент времени показывает, что она является во многом запутанной и противоречивой. Так, основным законодательным актом, регулирующим отношения в области сертификации товаров и услуг, является Федеральный закон «О техническом регулировании», определяющий, что сертификат соответствия – это документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов, сводам правил или условиям договоров. Соответственно, технический регламент – это документ, который устанавливает обязательные требования к объектам технического регулирования и принимается федеральным законом или постановлением Правительства Российской Федерации. Соответственно, стандарт – это документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг [19].

Исходя из этого, государственные стандарты, регулирующие вопросы технических качественных характеристик средств цифровой подписи в Российской Федерации, не являются обязательными к соблюдению. Процедуры выработки и проверки электронной подписи на базы асимметричного криптографического алгоритма» показывает, что он не содержит каких-либо нормативно выраженных требований к качественным характеристикам средства ЭП.

Обратимся теперь к анализу ряда положений одного из первых в истории специализированных законодательных актов, регулирующих отношения в рассматриваемой сфере – Закона штата Юта (США) от 09.03.1995 «О цифровой подписи».

Как представляется автору, определение категории «цифровая подпись», приведенное в этом законе, четко и ясно раскрывает алгоритм формирования хэш-функции, а затем образования цифровой подписи: «цифровая подпись является последовательностью битов, которую лицо, имеющее намерение подпи-

сать, создает по отношению к явным образом выделенному сообщению путем проведения сообщения через однонаправленную функцию, шифруя затем полученный дайджест с использованием асимметричной криптосистемы и закрытого ключа лица».

Технология, скажем прямо, раскрыта немногословно и блестяще. Например, «технологическая» часть определения цифровой подписи, содержащаяся в российском Законе, менее информативна, так как здесь идет речь о реквизите электронного документа, полученного в результате криптографического преобразования информации с помощью закрытого ключа. И совсем не очевидно, что шифруется только «дайджест», а не все сообщение в целом.

Не проливает свет на процесс и определение закрытого ключа в российском Законе, где он определяется как уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной подписи с использованием средств электронной подписи.

Оба определения образуют замкнутый круг: одно определяется через другое, в результате чего возникает логическая ошибка, то есть нечто определяется через дополнительное понятие, предназначенное для реализации этого нечто.

На основании указанного необходимо предложить внести в дефиницию «электронная подпись», представленную в Федеральном законе «Об электронной подписи», ряд дополнений и изменений, и представить ее в следующем виде:

«Цифровая подпись – реквизит документа, предназначенный для подтверждения факта согласия подписавшего документ лица с его содержанием, а также защиты от подделки, полученный в результате криптографического преобразования информации, содержащейся в хэш-функции подписываемого электронного документа, с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца ключа подписи».

Обоснуем предложенные новеллы.

1. Главное в использовании цифровой подписи все же не защита документа от подделки (для этого существуют многие иные методы), а придание ей юридического значения, аналогичного с собственноручной подписью. А последнее заключается в том, что любая подпись проставляется для подтверждения согласия лица с текстом документа. Поэтому первое дополнение автор полагает принципиально важным.

2. Обязательное включение в алгоритм формирования цифровой подписи хэш-функции позволяет унифицировать его с аналогичными системами многих стран, чем облегчить признание отечественных сертификатов ключей подписи в других государствах, а также иностранных сертификатов в России.

4. Исключение из легального определения слова «электронная», а также установить отсутствие искажения информации в электронном документе связано с тем, что она по сути является речевым излишеством, так как такая функция цифровой подписи как защита электронного документа от подделки одновременно решает задачу установления факта иных искажений.

Обратимся теперь к анализу других дефиниций законов об электронных подписях.

В связи с тем, что практически общепризнанным для цифровых подписей является использование асимметричных систем криптографического преобразования информации, их основными компонентами являются закрытый и открытый ключи цифровой подписи.

В законах Республики Беларусь и Республики Таджикистан «Об электронном документе» используются понятия «личный ключ подписи» и «открытый ключ проверки подписи». Первая категория определяется как «набор символов, принадлежащий конкретному лицу и используемый при выработке электронной цифровой подписи», вторая – как «набор символов, доступный для всех заинтересованных лиц и используемый при проверке электронной цифровой подписи».

С точки зрения информативности и юридического значения эти дефиниции вряд ли представляют интерес, а вот их названия являются, по мнению автора, бо-

лее точными по сравнению с аналогичными российскими, так как первая прочно привязана к личности обладателя, а вторая – к своему предназначению.

В Законе Австрийской Республики «Об электронной подписи» в связи с более широкой трактовкой самой категории «электронная подпись», о чем автор говорил выше, применены категории «данные создания подписи» и «данные проверки подписи». Под первой понимаются «уникальные данные, такие как коды или частные ключи подписи», которые используются подписывающим лицом для создания подписи»; под второй – 2данные, такие как коды или открытые ключи подписи, которые используются для проверки подписи».

В Законе Индии «Об информационных технологиях» используются категории «закрытый ключ» и «открытый ключ», имеющие элементарно простые определения по цели использования. В нем также использовано понятие «ключевая пара», определяемое как «закрытый ключ и математически связанный с ним открытый ключ, которые связаны таким образом, что открытый ключ может проверять цифровую подпись, создаваемую закрытым ключом».

Следует отметить, что объективно существующая математическая связь между вышеуказанными ключами и их место в совместном использовании в виде определения кроме специализированного индийского закона используется в соответствующих законах Республики Корея, Сингапура, штата Юта (США). В большинстве случаев данной информации вполне достаточно, чтобы понять принцип. Например, в законе штата Юта «О цифровой подписи» дается следующее определение: «пара ключей означает закрытый ключ и соответствующий ему открытый ключ, которые являются ключами в асимметричной криптосистеме, имеющие свойство: один из пары расшифровывает то, что другой зашифровывает». Возможно, что во времена подготовки данного законодательного акта в штате Юта использовались именно такие криптографические алгоритмы, однако сейчас данные системы построены таким образом, что открытый ключ не расшифровывает, а проверяет данные, зашифрованные закрытым ключом, что повышает уро-

вень достоверности электронной подписи и ее «привязку» к конкретному субъекту.

В Законе ФРГ «О рамочных условиях для электронных подписей и изменении иных правовых актов» использованы категории «ключ подписи» и «ключ проверки подписи», где первая связана с понятием «личный криптографический ключ», а вторая – с понятием «публичный криптографический ключ». В общем и целом данные категории корреспондируются с юридическими свойствами и предназначением данных средств.

В качестве завершения к данному подвопросу исследования приведем еще одно определение категории «асимметричная криптосистема», содержащееся в Законе Республики Корея «О цифровой подписи»: «метод шифрования, при котором ключ, используемый для шифрования информации, отличен от ключа, используемого для извлечения зашифрованной информации».

Хотя данное определение является более близким по смыслу к категориальному аппарату закона штата, Юта, чем к аналогичному аппарату индийского закона, однако прямого противоречия в нем нет, так как под «извлечением» вполне можно понимать и проверку.

Подводя итог проведенному анализу, автор хотел бы отметить следующее:

1. Предназначение закрытых и открытых ключей цифровой подписи в модельном и национальном законодательстве трактуется примерно одинаково, что свидетельствует об объективном характере данных категорий.

2. В основном можно выделить широкий и узкий подходы к определению ключей цифровой подписи, которые зависят от трактовки самой подписи (узкий подход связан непосредственно с асимметричными криптосистемами).

3. Мы можем полагать, что в качестве наиболее точного названия данных объектов следующие: вместо категории «закрытый ключ» использовать категорию «личный ключ цифровой (электронной) подписи» как наиболее точно отражающую предназначение данного объекта; вместо категории «открытый

ключ» использовать категорию «ключ проверки цифровой (электронной) подписи» по тем же основаниям.

4. Целесообразно введения в число дефиниций российского закона об ЭП категории «ключевая пара» в которой можно описать связь между этими ключами, что является полезным для правоприменительной практики. Указанную дефиницию предлагаем в следующей редакции:

«Ключевая пара – личный ключ электронной цифровой подписи и ключ проверки электронной цифровой подписи, которые математически связаны между собой таким образом, что ключ проверки может проверять электронную цифровую подпись, создаваемую личным ключом, не выявляя при этом содержания личного ключа».

Обратимся теперь к анализу еще одной обязательной для законодательства о цифровых подписях совокупности норм, регулирующих отношения по установлению юридической силы цифровых подписей. Речь идет о нормативном определении условий признания юридической силы цифровой подписи.

Российский закон об ЭП в данном случае исходит из другой концепции. Изначально презюмируя незыблемость юридической силы собственноручной подписи в бумажном документе, данный законодательный акт определяет совокупность условий, выполнение либо обеспечение которых делают цифровую подпись равнозначной по юридическому значению с собственноручной. К этим условиям относятся:

1) сертификат ключа подписи, относящийся к этой цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

2) подтверждена подлинность цифровой подписи в документе;

3) цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Анализ данных положений подтверждает сделанный автором ранее вывод о «жесткости» отечественного Закона об ЭП: только электронный документ, а не электронное сообщение вообще, только «усовершенствованная» или «безопасная» цифровая подпись, основанная на подтверждаемом сертификате открытого ключа и т.п. И в данном случае два из трех условий связаны с сертификатом: он должен быть действующим, а правомочия подписавшего лица не должны выходить за совокупность тех, которые обозначены в сертификате (отметим попутно, что границы этих правомочий при использовании цифровой подписи в гражданско-правовых отношениях определяются владельцем сертификата самостоятельно, но не должны выходить за пределы общей правоспособности гражданина; при использовании цифровой подписи в административно-правовых отношениях – определяться императивно, исходя из должностного статуса субъекта; в отношении должностных лиц коммерческих организаций – не должны выходить за пределы определенных для них функциональных обязанностей).

Таким образом, можно констатировать, что юридическая сила цифровой подписи согласно концепции российского Закона об ЭП основывается на подтвержденной подписи, открытый ключ которой представлен в зарегистрированном в установленном порядке сертификате [38].

Примерно так же, но с некоторыми нюансами устанавливает равнозначность цифровой подписи и собственноручной подписи и Модельный закон государств-участнков СНГ «Об электронной цифровой подписи»:

– подпись прошла проверку на подлинность при помощи открытого ключа, имеющего регистрационное свидетельство аккредитованного центра регистрации или в порядке, предусмотренном соглашением сторон;

– цифровая подпись является действующей на момент подписания;

– подписавшее лицо правомерно владеет закрытым ключом, используемым для создания цифровой подписи.

Именно последняя норма является тем самым нюансом. Связано это с тем, что Модельный закон допускает возможность владения личным ключом подписи как физическим, так и юридическим лицом. Отсюда и отдельное требование о правомерности.

Федеральный закон Австрийской Республики «Об электронной подписи» подразделяет юридическую силу цифровых подписей на общую и специальную. При определении общей юридической силы устанавливается, что «в правовом и деловом обороте могут использоваться процедуры подписи с различными уровнями безопасности и классами сертификатов». При этом «юридическая сила электронной подписи и ее использование в качестве доказательства на могут исключаться только потому, что электронная подпись существует только в электронной форме, не основана на квалифицированном сертификате или на выданном аккредитованным поставщиком сертификационных услуг квалифицированном сертификате или не создана с применением технических компонентов и процедур.

Специальная юридическая сила присуща только безопасной цифровой подписи (о данной категории речь шла в этом параграфе выше). При этом конкретно оговаривается, в каких случаях безопасная цифровая подпись не обладает юридической силой письменной формы. Это:

1) юридические сделки по семейному и наследственному праву, которые связаны с письменной формой или более строгими формальными требованиями;

2) другие волеизъявления или юридические сделки, действительность которых связана с формой официального удостоверения, судебного или нотариального засвидетельствования или нотариального акта;

3) волеизъявления, юридические сделки или ходатайства, которые требуют для внесения в земельную книгу, фирменный или другой официальный реестр публичного удостоверения, судебного или нотариального засвидетельствования или нотариального акта;

4) гарантийные письма.

Из изложенного мы видим, что из сферы использования цифровой подписи исключены отношения, связанные с передачей имущества на долговременной основе (наследственные сделки и сделки с землей), подлежащие государственной регистрации, а также возникающие в связи с обеспечением обязательств (гарантия). По мнению автора, подход австрийских законодателей следует признать вполне обоснованным, так как вышеуказанные нормы четко предписывают правоприменителю исключения, не заставляя его сравнивать нормативные положения разных законов, что неизбежно порождает конкуренцию норм и преодоление противоречий.

Закон Республики Болгария «ОБ электронном документе и электронной подписи», исходя из контекста его положений, не содержит каких-либо ограничений по использованию усовершенствованной и универсальной цифровых подписей (об их отличиях говорилось выше), за исключением того, что усовершенствованная цифровая подпись не применяется при направлении документов между органами публичной власти. Универсальная цифровая подпись (аналог отечественной системы) применяется во всех отношениях без каких-либо ограничений.

Индийский Закон «Об информационных технологиях» содержит еще более простую формулировку: «В случае, когда любое законодательство предусматривает, что подлинность информации или любого другого документа должна подтверждаться путем скрепления подписью или любой документ должен подписываться либо содержать подпись любого лица, то независимо от чего-либо содержащегося в таком законодательстве, такое требование считается выполненным, если подлинность такой информации или документа подтверждается с использованием цифровой подписи, присоединенной таким способом, как это может быть предписано Центральным Правительством».

Более того, данный законодательный акт предоставляет возможность Правительству и его ведомствам весьма широкие полномочия по использова-

нию цифровых подписей в административно-правовых отношениях. Данное положение сформулировано в законе следующим образом:

«В случае, когда законодательство предусматривает:

(a) представление любой формы заявления или иного документа в любое учреждение, орган, организацию или ведомство, принадлежащее или контролируемое соответствующим Правительством по определенному вопросу;

(b) выдачу или предоставление любой лицензии; разрешение, утверждение или одобрение на какое-либо имя по определенному вопросу;

(c) получение или уплату денег по определенному вопросу,

то независимо от чего-либо содержащегося в любом другом действующем законодательстве, такое требование считается выполненным, если такое представление, выдача, получение или платеж, в зависимости от случая, осуществляются с использованием такой электронной формы, как это может быть предписано соответствующим Правительством».

Здесь необходимо некоторое пояснение. Индия является федеративным государством. И из анализа приведенных положений видно, что Центральное Правительство устанавливает алгоритм выработки цифровой подписи, а правительства штатов – формы электронных документов. Такое распределение полномочий автор полагает обоснованным. Помимо указанного, за этими нормами четко просматривается стремление к формированию электронного правительства, то есть облегчению получения и направления официальных документов гражданами и организациями.

Переход к представлению правоустанавливающих и других официальных документов в электронной форме отображения, по мнению автора, не должен быть бурным и спонтанным. Контролирующие органы и суды (во всяком случае, в нашей стране) не смогут одномоментно перестроить свои подходы к оценке легитимности таких документов из-за в том числе сохраняющегося среди государственных служащих низкого уровня знаний в области информационных технологий. Но и искусственно сдерживать этот процесс не следует. По-

этому, исходя из сложившейся в России системы административно-правового регулирования, Закон об ЭП должен содержать хотя бы отсылочную норму, обязывающую Правительство определять те официальные документы, которые возможно представлять в электронной форме отображения, с постепенным расширением данного перечня [68].

Закон Республики Корея «О цифровой подписи» также предоставляет практически неограниченные возможности по использованию безопасных (квалифицированных) цифровых подписей, то есть подтвержденных сертификатом открытого ключа, выданного лицензированным сертифицирующим органом. При этом цифровая подпись имеет юридическую силу как собственноручной подписи, так и подписи, скрепленной печатью.

В достаточной мере сложный подход к определению юридической силы цифровой подписи просматривается в Законе Литовской Республики «Об электронной подписи». С одной стороны, устанавливается, что «безопасная электронная подпись в электронных данных, созданная на безопасном оборудовании для формирования подписи и подтвержденная действительным квалифицированным сертификатом, имеет такую же юридическую силу, что и подпись в письменных документах, и допускается как средство доказывания в суде». С другой – «электронная подпись не может быть признана недействительной по любой из нижеперечисленных причин: (1) что она в электронной форме; (2) что она не поддерживается квалифицированным сертификатом; (3) что она не поддерживается квалифицированным сертификатом, выданным аккредитованным поставщиком сертификационных услуг; (4) что она не создана на безопасном оборудовании для формирования подписи».

На первый взгляд, между приведенными нормами существует прямое противоречие: в качестве средства доказывания в суде допускается только один вид цифровой подписи; однако, если подпись такими свойствами не обладает, то она также является действительной. С точки зрения юридической техники,

литовские законодатели могли бы найти более четкое изложение вкладываемого в процитированные положения смысла, однако вряд ли можно заподозрить их в некомпетентности. Тем более, что эти положения объединены в одну статью. По мнению автора, речь здесь идет о безусловной юридической силе цифровой подписи в первом случае и оспоримой юридической силе – во втором. Говоря иными словами, для подтверждения подлинности электронного документа, подписанного небезопасной цифровой подписью, могут потребоваться дополнительные доказательства.

Закон Сингапура «Об электронных сделках» предусматривает несколько иную схему: он устанавливает общие условия легитимности цифровой подписи, а затем подразделяет ее на безопасную и небезопасную.

Общие условия выглядят следующим образом:

«(1) В случае, когда норма закона требует подписи или предусматривает определенные последствия, если документ не подписан, данная норма удовлетворяется электронной подписью.

(2) Электронная подпись может доказываться любым образом, включая демонстрацию того, что существует процедура, посредством которой для стороны необходимо в целях дальнейшего совершения сделки применить символ или процедуру безопасности для того, что электронная запись принадлежит такой стороне».

В отношении ненадежных цифровых подписей сформулированы следующие условия:

«Если иное не предусмотрено законом или договором, лицо, полагающееся на подписанную цифровой подписью электронную запись принимает риск того, что цифровая подпись является недействительной в качестве подписи или средства подтверждения подлинности подписанной электронной записи, если доверие к цифровой подписи не является разумным с учетом обстоятельств, учитывая следующие факторы:

(a) факты, о которых лицо, полагающееся на подписанную цифровой подписью электронную запись, знает или уведомлено, включая все факты, указанные в сертификате или включенные в него путем отсылки;

(b) ценность или важность подписанной цифровой подписью электронной записи, если они известны;

(c) ход деловых отношений между лицом, полагающимся на подписанную цифровой подписью электронную запись, и абонентом, а также любые доступные показатели надежности или ненадежности, отличные от цифровой подписи; и

(d) любой торговый обычай, в частности, в сфере торговли, осуществляемой посредством надежных систем или других электронных средств».

Таким образом, получается, что лицо, использовавшее цифровую подпись для удостоверения своего волеизъявления или подтверждения факта, может представлять различные доказательства ее подлинности. С другой стороны, лицо, полагающееся на цифровую подпись (получатель документа) должен оценивать целый ряд факторов и принимать все риски ошибочной оценки на себя, если он соглашается использовать в своей деятельности электронные документы, подписанные небезопасной цифровой подписью, проверочный ключ которой не зафиксирован в сертификате, выданном уполномоченным субъектом.

Подход, как представляется автору, несколько усложненный, но тем не менее, вполне отвечающий правовой логике.

Все остальные законодательные акты, регулирующие рассматриваемые правоотношения, из числа доступных автору, либо используют один из описанных способов, либо в них вообще отсутствуют нормы, устанавливающие юридическую силу цифровых подписей.

Итак, для актов, регулирующих отношения по созданию аналогов собственноручной подписи в электронных документах центральным понятием и центральной дефиницией должно являться понятие «цифровая подпись». Добавление к нему дополнительного термина «электронная» является речевым излишеством. Анало-

гично, если используется категория «электронная подпись», то термин «цифровая» также является речевым излишеством. Автор обосновывает суждение о том, что наиболее адекватно отражает суть этой технологии категория «цифровая подпись», так как она может быть выражена и в виде файла, воспринимаемого компьютером, и в виде последовательности чисел, отображенных на бумажном носителе.

Самым существенным признаком цифровой подписи как юридической категории является (должно являться) указание на то, что она есть средство подтверждения факта свободного волеизъявления лица посредством ее проставления, дающего согласие с содержанием информации в документе.

Средства электронной подписи должны отвечать следующим основным требованиям:

закрытый и открытый ключи электронной подписи, вырабатываемые средством электронной цифровой подписи, должны быть гарантированно уникальными;

средства хранения закрытых ключей электронной подписи должны исключать возможность копирования записанной на них ключевой информации;

средства электронной подписи не изменяют содержание подписываемого электронного документа и не препятствуют владельцу сертификата ключа подписи знакомиться с содержанием электронного документа до его подписания».

Учитывая достаточно прочное вхождение в научный и нормативный оборот в Российской Федерации категории «электронная подпись», считаем целесообразным внести ряд дополнений и изменений в легальную дефиницию, определяющую эту категорию в Законе об ЭП, изложив ее в следующей редакции:

«Цифровая подпись – реквизит документа, предназначенный для подтверждения факта согласия подписавшего документ лица с его содержанием, а также защиты от подделки, полученный в результате криптографического преобразования информации, содержащейся в хэш-функции подписываемого электронного документа, с использованием закрытого ключа цифровой подписи и позволяющий идентифицировать владельца ключа подписи».

Учитывая, что определение категории «ключевая пара», в которой можно описать связь между закрытым ключом (личным ключом подписи) и открытым ключом (ключом проверки) цифровой подписи, автор полагает целесообразным дополнить Закон об ЭП дефиницией следующего содержания:

«Ключевая пара – личный ключ цифровой подписи и ключ проверки цифровой подписи, которые математически связаны между собой таким образом, что ключ проверки может проверять цифровую подпись, создаваемую личным ключом, не выявляя при этом содержания личного ключа».

ЗАКЛЮЧЕНИЕ

Возможно ли говорить о постиндустриальном обществе в России? Возможно так как все ярче проявляются черты информационного общества и отчасти общества потребления. С другой стороны, и российское информационное общество пока еще нельзя считать полноценным, в связи с тем, что непосредственно постиндустриальная или точнее индустриальная составляющая такого общества в нашей стране по своим характеристикам еще не достигла должного уровня. Что касается непосредственно информационного общества, то нужно признать, что для России с ее растянутостью транспортных коммуникаций, плохими дорогами или отсутствием таковых, и недостаточной телефонизацией сельских поселений использование мобильных телефонов и сети Интернет, все более активные позиции потребителей на рынке ИКТ (проявление черт информационного общества) имеют особое значение. Не менее важным представляется и тот факт, что достигнуто, не имевшее место ранее, товарное наполнение потребительского рынка. Эти обстоятельства должны способствовать значительному повышению качества жизни, в первую очередь, населения на периферии, обеспечивая ему возможности оперативной связи с родными и близкими, получение деловой, учебной, бытовой, развлекательной информации и открывая ему доступ к все более полному ассортименту современных товаров и услуг в целом. Информатизация и продвижение по пути к становлению общества потребления должны послужить локомотивом для прогресса всей информационной инфраструктуры, в том числе документооборота в электронной форме отображения, что для России с ее огромными территориями и сложной административной системой является решением многих проблем в государственном и корпоративном управлении.

Различные страны осуществляют работу с электронными документами, применяя специальные законы, регулирующие данные отношения, большинство из которых было ориентировано на сферу так называемой электронной торговли, открывавшей широкие перспективы для движения товаров, работ и услуг на новые рынки сбыта при снижении издержек.

Российский закон об ЭП презюмирует незыблемость юридической силы собственноручной подписи в бумажном документе, данный законодательный акт определяет совокупность условий, выполнение либо обеспечение которых делают электронную подпись равнозначной по юридическому значению с собственноручной. Анализ данных положений подтверждает «жесткость» отечественного Закона об ЭП.

Таким образом, можно констатировать, что юридическая сила электронной подписи согласно концепции российского Закона об ЭП основывается на подтвержденной подписи, открытый ключ которой представлен в зарегистрированном в установленном порядке сертификате.

Из изложенного мы видим, что из сферы использования электронной подписи исключены отношения, связанные с передачей имущества на долговременной основе (наследственные сделки и сделки с землей), подлежащие государственной регистрации, а также возникающие в связи с обеспечением обязательств (гарантия). На наш взгляд, подход австрийских законодателей следует признать вполне обоснованным, так как вышеуказанные нормы четко предписывают правоприменителю исключения, не заставляя его сравнивать нормативные положения разных законов, что неизбежно порождает конкуренцию норм и преодоление противоречий.

На основании положений изученных законодательных актов можно сделать вывод о том, что существуют два нормативно закрепленных подхода к сфере применения электронной подписи: неограниченное применение и законодательно ограниченное применение.

Хочется обозначить, что в нашей стране необходимо формулирование конкретных уголовно-правовых и административно-правовых норм, устанавливающих ответственность за правонарушения в сфере использования электронных подписей. Во-первых, из-за специфики данных отношений имеющиеся нормы общего характера довольно проблематично распространить на сферу электронной подписи. Во-вторых, это будет отвечать опыту развитых стран и поможет облегчить интеграцию отечественной системы защищенного элек-

тронного документооборота в складывающуюся в настоящее время общую систему. В качестве первостепенной видится необходимость в криминализации следующих деяний:

– противоправного использования закрытого (личного) ключа подписи другого лица для удостоверения электронных документов;

– противоправного распространения или передачи третьему лицу закрытого (личного) ключа подписи другого лица лицом, которое обязано сохранять его в тайне.

Процесс информатизации – это процесс организации социально-экономических и научно-технических оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов. Данное определение дает основание сделать вывод, что информатизация не является до конца изученной сферой правового регулирования. Информация, научно-технические разработки в этих областях всегда привлекали внимание ученых, которые смогут предложить дополнительные гарантии подтверждения подлинности электронного документа так же как и выделить отдельные его особенности.

Настоящее исследование не ставило, да и не могло ставить своей целью полное решение проблемных вопросов законодательного регулирования в сфере использования электронных подписей – слишком объемной и сложной представляется эта цель для одной монографии. Мы будем считать свои цели достигнутыми, если приведенный в данной работе систематизированный анализ международного законодательства в сфере применения электронных подписей и сделанные нами выводы смогут облегчить читателю вхождение в проблематику законодательного регулирования в сфере использования электронных подписей, а для тех специалистов, которые давно и плодотворно занимаются разработками этой и смежных тем, станут катализатором в дальнейшей научной дискуссии, новых суждениях и выводах по данному поводу.

СПИСОК ЛИТЕРАТУРЫ

Законодательные и иные нормативные правовые акты

1. Всеобщая декларация прав человека / ООН. Нью-Йорк. 10 апр. 1948 г. // РГ. – 1998. – 10 дек.

2. Конституция Российской Федерации от 12.12.1993 г. // РГ. – № 237. – 1993. – 25 дек.

3. Гражданский кодекс РФ, ч. 1 от 30.11.1994. № 51-ФЗ // СЗ РФ. - 1994. – № 32. – Ст. 3301, № 149-ФЗ (ред. от 23.05.2015).

4. Гражданский кодекс РФ, ч. 2 от 26.01.1996 № 14-ФЗ // СЗ РФ, 29.01.1996. – № 5. – Ст. 410, № 83-ФЗ (ред. от 07.04.2015 г.).

5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ, 17.06.1996. – № 25. – Ст. 2954, № 442-ФЗ (ред. от 23.05.15 г.).

6. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 г. № 195-ФЗ // СЗ РФ. – 2002. – № 1, ч. 1. – Ст. 1, № 442-ФЗ (ред. 23.05.15 г.).

7. Градостроительный кодекс Российской Федерации от 29.12.2004 г. – № 190-ФЗ, (ред. 31.12.2014 г.) № 314-ФЗ // СЗ РФ. – 2005. – № 1 (ч. 1). – Ст. 16.

8. Земельный кодекс Российской Федерации от 25.10.2001 г. № 136-ФЗ (ред. 08.03.2015 г.) № 365-ФЗ // СЗ РФ. – 2001. – № 44. – Ст. 4147.

9. О науке и государственной научно-технической политике: Федеральный закон от 23.08.1996 г. – № 127-ФЗ (ред. от 22.12.2014 г.) № 186-ФЗ // СЗ РФ, 26.08.1996. – № 35. – Ст. 4137.

10. О внесении изменений в Федеральный закон об обязательном экземпляре документа: Федеральный закон от 05.05.2014 г. № 100 // СЗ. – 2014. – № 19. – Ст. 2305.

11. Об информации, информационных технологиях и о защите информации : закон Российской Федерации от 27.07. 2006 г. № 149-ФЗ // Рос. газ. – 2006. – № 165 (ред. 24.11.2014 г.). – № 227-ФЗ.

12. О государственной регистрации прав на недвижимое имущество и сделок с ним : федер. закон от 21.07.1997 г. – № 122-ФЗ, Ст. 12 // СЗ РФ 28.07.1997 г. – № 30. – Ст. 3594, № 435-ФЗ (ред. 06.04.2015 г.).

13. О государственной регистрации юридических лиц и индивидуальных предпринимателей : федер. закон от 08.08.2001 г. № 129-ФЗ // СЗ РФ, 13.08.2001. – № 33 (ч. I). – Ст. 3431 (ред. 30.03.2015 г.).

14. Об электронной подписи : федер. закон от 06.04.2011 г. – № 63-ФЗ // Собрание законодательства, 11.04.2011. – № 15. – Ст. 2036 (ред. 28.06.2014 г.)

15. Об электронной подписи : комментарий к федер. закону от 06.04.2011 № 63-ФЗ // Р.В. Амелин, Е.А. Бевзюк, Ю.В. Волков, Ю.А. Марченко, Е.В. Холодная // Информационный банк «Постатейные комментарии и книги».

16. О персональных данных: комментарий к Федеральному закону от 27.07.2006 № 152-ФЗ / Р.В. Амелин, Н.В. Богатырева, Ю.В. Волков, Ю.А. Марченко, А.С. Федосин. – Режим доступа : СПС «ГАРАНТ».

17. Об общих принципах организации местного самоуправления в Российской Федерации : федер. закон от 06.10.2003. – № 131-ФЗ // СЗ РФ. – 2003. – № 40. – Ст. 3822 (ред. 30.03.2015 г.).

18. О государственной тайне : закон Российской Федерации от 21.07.1993 г. № 5485-1 // СЗ РФ. – 1997. – № 41. – С. 8220–8235 (ред. 21.12.2013 г.).

19. О техническом регулировании : федер. закон от 27.12.2002 г. – № 184-ФЗ // СЗ РФ. – 2002 г. – № 52 (ч. 1). – Ст. 5140 (ред. 23.06.2014 г., ФЗ № 243-ФЗ).

20. О связи: Федеральный закон от 07.07.2003 г. – № 126-ФЗ // СЗ РФ. 14.07.2003. – № 28. – Ст . 2895 (ред. 21.07.2014 г., ФЗ № 221-ФЗ).

21. Об обязательном экземпляре документов : федер. закон от 29.12.1994 г. – № 77-ФЗ // СЗ РФ. – 1995 – № 1. – Ст. 1 (ред. 05.05.2014 г., ФЗ № 100-ФЗ).

22. О федеральном бюджете на 2015 год : федер. закон от 01.12.2014 г. – № 384-ФЗ // СЗ РФ. – 2014 г. – № 49 (ч. 5). – Ст. 6893 (ред. 20.14.2015 г., ФЗ № 93-ФЗ).

23. Об утверждении Правил обмена документами в электронном виде при организации информационного взаимодействия: Постановление Правительства РФ от 25.12.2014. – № 1494 // СЗ РФ. – 05.01.2015. – № 1 (ч. II). – Ст. 284.

24. О проекте Федерального закона № 310163-4 Об электронной торговле: Постановление ГД ФС РФ от 15.06.2011. – № 5470-5 ГД // СЗ РФ. – 27.06.2011. – № 26. – Ст. 3718.

25. О концепции правовой информатизации России : указ Президента РФ. от 28.06.93 № 966 (ред. 22.03.2005 г.) // САПП РФ. – 1993. – № 27. – Ст. 2521.

26. О системе и структуре федеральных органов исполнительной власти : указ Президента Российской Федерации от 09.03.2004 г. № 314 // СЗ РФ. – 15.03.2004 г. – № 11. – Ст. 945 (ред. 22.06.2010 г., ФЗ № 773-ФЗ).

27. О мерах по обеспечению открытости и общедоступности нормативных актов : указ Президента РФ от 24.11.1995 № 1178 // СЗ РФ. – 1995. – № 48. – Ст. 4660.

28. О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации : указ Президента РФ от 3 апреля 1995 г. № 334 // СЗ РФ. – 1995. – № 15 – Ст. 1258. (ред. 25.07.2000 г., указ Президента РФ № 1358).

29. Об утверждении Положения о Федеральном агентстве по информационным технологиям : постановление Правительства РФ от 30.06.2004. – № 319 // СЗ РФ. – 2004. – № 27. – Ст. 2782.

30. Об утверждении Инструкции о действиях должностных лиц таможенных органов при совершении таможенных операций при таможенном декларировании в электронной форме товаров, находящихся в регионе деятельности

таможенного органа, отличного от места их декларирования : приказ ФТС России от 01.11.2013. – № 2081.

31. Об утверждении Инструкции по делопроизводству в государственных судебно-экспертных учреждениях Министерства юстиции Российской Федерации : приказ Минюста России от 05.06.2007. – № 115 (ред. от 10.11.2009).

32. Стратегия развития информационного общества в Российской Федерации, утверждена Президентом Российской Федерации 07.02.2008 г. № Пр-212 // Рос. газ. – № 34. – 2008.

33. ГОСТ 6.10.4-84 Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения. – М. : Изд-во стандартов, 1988.

34. ГОСТ Р 6.30-2003 Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов Пост. Госстандарта России от 03.03.2003 г. № 65. – М. : Госстандарт, 2003.

35. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М., 1989.

36. Окинавская хартия глобального информационного общества от 22.07.2000 г. // Энциклопедия российского права : электронная правовая база. – 2005. – № 194989.

Монографии, научные статьи, словари

37. Бачило И.Л. Причины и суть эволюции государственных и правовых институтов в условиях развитии информационного общества // Вопросы правоведения / И.Л. Бачило, 2011. – № 3. – С. 114–145.

38. Бачило И.Л. Правовые вопросы использования инфокоммуникационных ресурсов Российской Федерации / И.Л. Бачило // Информационные ресурсы России, 2013. – № 2. – С. 23–26.

39. Бачило И.Л. Проблемы развития информационного законодательства / И.Л. Бачило // Информатизация и связь. – 2010. – № 1. – С. 82–87.

40. Бачило И.Л. «Электронное правительство» и инновации в области государственных функции и государственных услуг / И.Л. Бачило // Информационные ресурсы России. – 2010. – № 1. – С. 13–17.

41. Бачило И.Л. Государство социальное или сервисное? (информационно-правовой аспект) / И.Л. Бачило // Право. Журнал Высшей школы экономики. 2010. – № 7. – С. 3–11.

42. Бачило И.Л. О методологии выявления связи феноменов «право» и «закон» и роли правосознания в этом процессе. подход к проблеме через призму теории информационного права / И.Л. Бачило // Вопросы правоведения. – 2013. – № 2. – С. 46–60.

43. Вилкас Э.Й. Решения: теория, информация, моделирование / Э.Й. Вилкас, Е.З. Майминас. – М. : Радио и связь, 1981. – 560 с.

44. Волков Ю.В. Защищенность субъекта при автоматизированной обработке его персональных данных / Ю.В. Волков // Вестник УрФО: Безопасность в информационной сфере. – 2012. – № 3–4. – С. 49–52.

45. Волков Ю. В. Информационные правонарушения: ответственность информационная / Ю.В. Волков // Актуальные вопросы административного и информационного права : материалы Междунар. науч.-практ. конф. / под ред.: М.А. Лапина, Г.Ф. Ручкина. – М. : Фин. ун-т, 2013. – С. 486–493.

46. Волков Ю. В. Информационные правоотношения / Ю.В. Волков // Актуальные проблемы права России и стран СНГ – 2013 : материалы XV Междунар. науч.-практ. конф. с элементами научной школы… Ч. 1. – Челябинск : Цицеро, 2013. – С. 145–149.

47. Герасименко В.А. Основы информационной грамоты / В.А. Герасименко. – М. : Энергоатомиздат, 1996. – 568 с.

48. Информационное общество : проблемы развития законодательства : сб. науч. работ // Ин-т государства и права РАН ; [сост. и отв. ред. И. Л. Бачило]. – М., 2012. – (Сер. Актуальные юридические исследования.)

49. Калужский М.Л. Электронная коммерция: маркетинговые сети и инфраструктура рынка / М.Л. Калужский. – ОмГТУ. – М. : Экономика, 2014. – 328 с.

50. Комиссия ООН по праву международной торговли. Ежегодник. 1996 год. Т. XXVII. – Нью-Йорк : Организация Объединенных Наций, 1998. – С. 319–323.

51. Копылов В.А. Информационное право / В.А. Копылов. – 2-е изд. – М. : Юристъ, М., 2002. – 512 с.

52. Морозов А.В. Информационное право как самостоятельная научная специальность / А.В. Морозов // Юридическое образование и наука. – 2013. – № 1. – С. 16–19.

53. Патрушев Н. П. Особенности современных вызовов и угроз национальной безопасности России / Н.П. Патрушев // Журнал российского права. – 2007. – № 7. – С. 3–12.

54. Румянцев О.Г. Юридический энциклопедический словарь / О.Г. Румянцев, В.Н. Додонов: – М. : Инфа-М, 1996. – 489 с.

55. Савельев Д.А. Информационное право и электронное государство Вводный курс : учеб. пособие / Д.А. Савельев. – СПб. : НИУ ИТМО, 2012. – 71 с.

56. Сатолина М.Н. Информационное общество: к вопросу об изменениях теоретико-правовых подходов к правовому регулированию общественных отношений / М.Н. Сатолина // Теоретические проблемы информационного права : сб. – М. : ИГиП РАН, 2006. – С. 39.

57. Талапина Э.В. О предмете информационного права // Государство и право / Э.В. Талапина. – 2013. – № 5. – С. 65–72.

58. Фария Х.А. Конвенция Организации Объединенных Наций об использо-

вании электронных сообщений в международных договорах. Вводный комментарий / Х.А. Фария // Международное публичное и частное право. – 2006. – № 6.

59. Фатьянов А.А. Проблемы формирования института служебной тайны в отечественном праве / А.А. Фатьянов // Государство и право. – 1999. – № 4. – 65 с.

60. Федотов М.А. К вопросу о концептуальных основах информационного права как права киберпространства / М.А. Федотов // Вопросы правоведения. – 2011. – № 3. – С. 71–98.

Учебники

61. Атаманчук Г.В. Теория государственного управления : учебник / Г.В. Атаманчук. – М. : Омега-Л, 2010. – 525 с.

62. Бачило И.Л. Информационное право : учебник для магистров / И.Л. Бачило ; Ин-т государства и права Рос. акад. наук, Акад. правовой ун-т (ин-т). – 3-е изд., перераб. и доп. – М. : Юрайт, 2012. – 564 с.

63. Городов, О. А. Информационное право : учебник / О. А. Городов. – М. : Проспект, 2014. – 242 с.

64. Информационные технологии в юридической деятельности : учебник для бакалавров / под общ. ред. проф. П.У. Кузнецова. – 2-е изд., перераб. и доп. – М. : Юрайт, 2013.– 441 с.

65. Кононов П.И. Административное право России : учебник / П.И. Кононов, В.Я. Кикоть, И.Ш. Килясханова. – М. : ЮНИТИ-ДАНА ; Закон и право. – 2012. – С. 687.

66. Костенников М.В. Актуальные проблемы административного права и процесса : учебник./ М.В. Костенников, А.В. Куракин, А.М. Кононов, П.И. Кононов, А.И. Стахов, Н.Д. Эриашвили. – М. : ЮНИТИ-ДАНА, 2015. – С. 495.

67. Кузнецов П.У. Основы информационного права : учебник для бакалавров / П.У. Кузнецов. – М. : Проспект, 2013. – 382 с .

68. Рассолов И.М. Информационное право : учебник для магистров / И.М. Рассолов. – 2-е изд., испр. и доп. – М. : Юристъ, 2012. – 444 с.

69. Теория государства и права : курс лекций / [Воротников А.А. и др.] ; под ред. Н.И. Матузова, А.В. Малько ; Рос. акад. наук, Сарат. фил. Ин-та гос. и права, ФГБОУ ВПО «Сарат. гос. юрид. акад.». – 3-е изд., перераб. и доп. – М. : Норма ; Инфра-М, 2012. – 639 с.

Учебные пособия

70. Гранкина А.Б. Документационное обеспечение управления в органах Следственного комитета Российской Федерации : учеб. пособие / под ред. А.М. Багмета. – М. : ЮНИТИ-ДАНА, 2015. – С. 167.

71. Правовое обеспечение информационной безопасности : учеб. пособие / под ред. С.Я. Казанцева. – М. : Академия, 2008. — 239 с.

72. Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации : учеб. пособие / А.А. Фатьянов. – М. : Юрист, 2001. – 412 с.

73. Фатьянов А.А. Правовое регулирование электронного документооборота : учеб.-практ пособие / А.А. Фатьянов. – М., 2005. – 273 с.

Авторефераты диссертаций

74. Титов Р.Н. Разработка системы электронного документооборота для автоматизации управления научно-техническими проектами : автореф. дис. … к-та техн. наук / Р.Н. Титов. – М., 2011. – 30 с.

75. Орлов И.А. Развитие механизма административно-правового регулирования электронного декларирования в таможенных органах : автореф. дис. ... канд. юрид. наук / И.А. Орлов. – Люберцы, 2013. – 31 с.

76. Ковалева Н.Н. Административно-правовое регулирование использования информационных технологий в государственном управлении : автореф. дис. ... д-ра юрид. наук / Н.Н. Ковалева. – Саратов, 2014. – 31 с.

77. Химченко А.И. Информационное общество: правовые проблемы в условиях глобализации : автореф. дис. … канд. юрид. наук / А.И. Химченко. – М., 2014. – 32с.

Иностранное законодательство

78. Закон штата Юта (США) от 09.03.1995 «О цифровой подписи».

79. Закон Федерации Малайзии от 26.03.1997 «О цифровой подписи».

80. Федеральный закон Австрийской Республики от 19.08.1999 № 190 «Об электронных подписях».

81. Закон Республики Болгария от 07.04.2001 № 15 «Об электронном документе и электронной подписи».

82. Ордонанс специального административного района Китая Гонконг № 553 от 2000 г. «Об электронных сделках».

83. Закон Королевства Дания от 31.05.2000. № 417 «Об электронных подписях».

84. Закон Канады от 13.04.2000 «О защите персональной информации и электронных документах».

85. Закон Республики Корея от 05.02.1999. № 5792 «О цифровой подписи».

86. Федеральный закон США от 30.06.2000 «Об электронных подписях в глобальной и национальной коммерции».

87. Закон Республики Филиппины от 14.06.2000. № 8792 «Об электронной коммерции».

88. Закон Федеративной Республики Германии от 16.05.2001 «О рамочных условиях для электронных подписей и изменении иных правовых актов».

89. Закон Королевства Швеция от 2000 г. № 832 «О квалифицированных электронных подписях».

90. Закон Эстонской Республики от 08.03.2000 «О цифровой подписи».

91. Закон Японии от 24.05.2000 «Об электронных подписях и сертификационных услугах».

92. Закон Великого герцогства Люксембург от 14.08.2000 № 96 «Об электронной коммерции».

Электронные ресурсы

93. Горовцова М. Переходим с обычной подписи на электронную: преимущества и нюансы [Электронный ресурс] / М. Горовцова. – Режим доступа : Информационно-правовой портал «Гарант» (дата обращения 09.07.2013 г.).

94. Туркин Р. Электронная подпись: опыт комплексного изучения [Электронный ресурс] / Р. Туркин. – Режим доступа : Первая социальная сеть для юристов. – (дата обращения 29.03.2013 г.).

95. Шадрина Т. Роскликом пера. Визировать документы теперь можно по Интернету [Электронный ресурс] / Т. Шадрина // Рос. газета. – 2011.

Научное издание

Щеголева Светлана Вячеславовна

ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

Монография

Подготовлено к печати
организационно-научным и редакционным отделом
Воронежского института ФСИН России
394072 г. Воронеж, ул. Иркутская, 1а

Подписано в печать 30.09.2015 г.
Формат 60 × 84 1/16. Усл. печ. л. 7,4.
Тираж 30. Заказ