Организация Объединенных Наций A/CN.9/630/Add.2

Генеральная Ассамблея

Distr.: General
26 April 2007

Russian
Original: English

Комиссия Организации Объединенных Наций по праву международной торговли
Сороковая сессия
Вена, 25 июня – 12 июля 2007 года

Возможная будущая работа в области электронной торговли

Комплексный справочный документ о необходимых элементах правовой базы, благоприятствующей развитию электронной торговли: выборочный раздел, касающийся международного использования электронных методов подписания и удостоверения подлинности

Записка Секретариата*

Добавление

В приложении к настоящей записке содержится часть (часть первая, глава II, разделы A и B) выборочного раздела комплексного справочного документа по правовым вопросам, связанным с международным использованием электронных методов подписания и удостоверения подлинности.

* Представление настоящего документа секретариатом Комиссии Организации Объединенных Наций по праву международной торговли было задержано по причине нехватки персонала.

V.07-82829 (R) 010607 040607

Приложение

Содержание

Часть первая
Электронные методы подписания и удостоверения подлинности

[…]

II. Правовой режим электронного удостоверения подлинности и электронных подписей

1. Для развития электронной торговли чрезвычайно важно обеспечить к ней доверие. Задача повышения определенности и безопасности при такой торговле может требовать установления специальных правил. Эти правила могут быть зафиксированы в самых разных законодательных текстах: международно-правовых документах (договорах и конвенциях); транснациональных типовых законах; национальном законодательстве (часто основанном на типовых законах); документах, разрабатываемых в порядке саморегулирования[1]; или договорных соглашениях[2].

2. Значительный объем электронных коммерческих сделок совершается в закрытых сетях, т.е. в рамках групп с ограниченным числом участников, доступ в которые открыт только лицам или компаниям, заблаговременно получившим соответствующий допуск. На основе закрытых сетей функционируют единые организации или сложившиеся закрытые группы пользователей, такие как межбанковские платежные системы с участием ряда финансовых учреждений, фондовые и товарные биржи или ассоциации авиакомпаний и туристических агентств. Круг участников таких сетей, как правило, ограничен организациями и компаниями, ранее допущенными в состав той или иной группы. Большинство этих сетей действуют уже несколько десятилетий, используют весьма совершенные технологии, а их участники досконально знакомы с функционированием системы. Быстрый рост электронной торговли в последние десять лет привел к появлению и других сетевых моделей, таких как цепи поставок и торговые платформы.

3. Хотя изначально эти новые объединения, как и большинство уже существовавших на тот момент закрытых сетей, строились на основе прямой связи между компьютерами, сейчас наблюдается растущая тенденция к

---

[1] См. например: Европейская экономическая комиссия, Центр Организации Объединенных Наций по упрощению процедур торговли и электронным деловым операциям, рекомендация № 32 – "Инструменты саморегулирования в области электронной торговли (кодексы поведения)" (ECE/TRADE/277), размещено по адресу http://www.unece.org/cefact/recommendations/rec_index.htm, дата посещения – 28 марта 2007 года.

[2] На разработку типовых договоров направлены многие инициативы национального и международного уровня. См., например: Европейская экономическая комиссия, Рабочая группа по упрощению процедур международной торговли, рекомендация № 26 – "Коммерческое использование соглашений об обмене для электронного обмена данными" (TRADE/WP.4/R.1133/Rev.1); и Центр Организации Объединенных Наций по упрощению процедур торговли и электронным деловым операциям, рекомендация № 31 – "Соглашение об электронной торговле" (ECE/TRADE/257), обе размещены по адресу http://www.unece.org/cefact/recommendations/rec_index.htm, дата посещения – 28 марта 2007 года.

использованию единой системы связи на основе таких общедоступных средств, как Интернет. При этом даже в рамках более современных моделей закрытая сеть сохраняет свой эксклюзивный характер. Обычно закрытые сети функционируют в соответствии с согласованными заранее договорными стандартами, соглашениями, процедурами и правилами, которые именуются по-разному: например, "правила системы", "порядок функционирования" или "соглашения о торговом партнерстве", и которые направлены на гарантированное обеспечение необходимых функциональных возможностей, надежности и безопасности для членов группы. Эти правила и соглашения часто касаются таких вопросов, как признание юридической значимости электронных сообщений, время и место отправки или получения сообщений данных, процедуры защиты доступа в сеть и методы удостоверения подлинности или подписания, которыми должны пользоваться стороны[3]. В пределах предусмотренной применимым правом свободы заключения договоров вопрос об обеспечении соблюдения таких правил и соглашений, как правило, решается в них самих.

4. Однако в отсутствие договорных норм или в условиях, когда исполнимость таких норм ограничена применимым правом, юридическая значимость используемых сторонами электронных методов удостоверения подлинности и подписания будет определяться применимыми правовыми нормами, носящими субсидиарный или императивный характер. В настоящем разделе рассматриваются различные варианты, используемые в разных правовых системах при определении правовых рамок применения электронных подписей и электронных методов удостоверения подлинности.

A. Подход к технологиям, применяемый в нормативных текстах

5. Законодательные нормы и подзаконные акты, касающиеся электронного удостоверения подлинности, существуют на международном и национальном уровнях в самых различных формах. Можно выделить три основных подхода к технологиям подписания и удостоверения подлинности: a) **минималистский подход**; b) **подход, ориентированный на конкретные технологии**; и c) **двухуровневый,** или **двойственный подход**[4].

1. Минималистский подход

6. В некоторых правовых системах проводится политика, нейтральная с точки зрения технологий, при которой признаются все технологии электронной подписи[5]. Этот подход также носит название минималистского, поскольку предполагает наделение всех видов электронной подписи неким минимальным юридическим статусом. В соответствии с минималистским подходом

---

[3] Анализ вопросов, обычно охватываемых соглашениями о торговом партнерстве, см. в Amelia H. Boss, “Electronic data interchange agreements: private contracting toward a global environment”, *Northwestern Journal of International Law and Business*, vol. 13, No. 1 (1992), p. 45.

[4] Susanna F. Fischer, “Saving Rosencrantz and Guildenstern in a virtual world? A comparative look at recent global electronic signature legislation,” *Journal of Science and Technology Law*, vol. 7, No. 2 (2001), pp. 234 ff.

[5] Например, в Австралии и Новой Зеландии.

электронные подписи считаются функциональным эквивалентом собственноручных подписей, при условии, что применяемая технология рассчитана на выполнение ряда определенных функций и при этом соответствует определенным требованиям в отношении надежности, нейтральным с технологической точки зрения.

7. В Типовом законе ЮНСИТРАЛ об электронной торговле[6] изложен наиболее широко применяемый набор законодательных критериев для установления общей функциональной эквивалентности между электронными и собственноручными подписями. Пункт 1 статьи 7 Типового закона гласит:

> "1) Если законодательство требует наличия подписи лица, это требование считается выполненным в отношении сообщения данных, если:
>
> a) использован какой-либо из способов для идентификации этого лица и указания на то, что это лицо согласно с информацией, содержащейся в сообщении данных; и
>
> b) этот способ является как надежным, так и соответствующим цели, для которой сообщение данных было подготовлено или передано, с учетом всех обстоятельств, включая любые соответствующие договоренности".

8. Данное положение охватывает две основные функции собственноручных подписей: идентификацию подписавшего и указание намерений подписавшего в отношении подписываемой информации. Согласно Типовому закону об электронной торговле, любая технология, способная обеспечить выполнение этих двух функций в электронной форме, должна считаться удовлетворяющей юридическому требованию в отношении подписи. Таким образом, Типовой закон нейтрален с точки зрения технологий, т.е. он не зависит от того, какие технологии используются, не предполагает использования тех или иных конкретных технологий и может применяться к передаче и хранению всех типов информации. Нейтральность с точки зрения технологий особенно важна в условиях быстрого развития техники и помогает обеспечить, чтобы законодательство могло применяться к будущим нововведениям и не слишком быстро устаревало. Поэтому было решено тщательно избегать в Типовом законе любых упоминаний о конкретных технических методах передачи или хранения информации.

9. Этот общий принцип воплощен в законах многих стран. Принцип нейтральности с точки зрения технологий позволяет учитывать будущие технические достижения. Кроме того, при данном подходе упор делается на праве сторон свободно выбирать отвечающую их потребностям технологию. Далее все зависит от способности сторон определить степень защиты, в которой нуждается передаваемая ими друг другу информация. Таким образом, можно обойтись без излишне сложных технических решений и избежать связанных с ними затрат[7].

---

[6] См. сноску […] [издание Организации Объединенных Наций, в продаже под No. R.99.V.4].

[7] S. Mason, “Electronic signatures in practice”, *Journal of High Technology Law,* vol. VI, No. 2 (2006), p. 153.

10. Если не считать Европы, где законодательство формируется главным образом под влиянием директив Европейского союза[8], то в большинстве стран, где приняты законодательные акты, касающиеся электронной торговли, в качестве образца для них был использован Типовой закон об электронной торговле[9]. Этот типовой закон также был положен в основу согласования законодательства об электронной торговле внутри стран, имеющих федеративное устройство, таких как Канада[10] и Соединенные Штаты Америки[11].

---

[8] В частности, Директива 1999/93/ЕС Европейского парламента и Совета об основах законодательства Сообщества в отношении электронных подписей (Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (см. сноску […])) [*Official Journal of the European Communities*, L 13]. За Директивой об электронных подписях последовала более общая Директива 2000/31/ЕС Европейского парламента и Совета от 8 июня 2000 года о некоторых юридических аспектах услуг информационного общества, и в частности электронной торговли, на внутреннем рынке (Директива об электронной торговле) (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)) (*Official Journal of the European Communities*, L 178, 17 July 2000), касающаяся различных аспектов оказания услуг с помощью информационных технологий, а также некоторых вопросов электронного заключения договоров.

[9] К январю 2007 года законодательство, вводящее в действие положения Типового закона ЮНСИТРАЛ об электронной торговле, было принято по меньшей мере в следующих странах: Австралия – Закон об электронных сделках от 1999 года; Венесуэла (Боливарианская Республика), *Ley sobre mensajes de datos y firmas electrónicas (2001*); Вьетнам – Закон об электронных сделках (2006 год); Доминиканская Республика – *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*; Индия – Закон об информационных технологиях от 2000 года; Иордания – Закон об электронных сделках от 2001 года; Ирландия – Закон об электронной торговле от 2000 года; Китай – Закон об электронных подписях, введен в действие в 2004 году; Колумбия – *Ley de comercio electrónico*; Маврикий – Закон об электронных сделках от 2000 года; Мексика – *Decreto por el que se reforman y adicionan diversas disposiciones del código civil para el distrito federal en materia federal, del Código federal de procedimientos civilies, del Código de comercio y de la Ley federal de protección al consumidor (2000);* Новая Зеландия – Закон об электронных сделках от 2002 года; Пакистан – Указ об электронных сделках от 2002 года; Панама – *Ley de firma digital (2001)*; Республика Корея – Рамочный закон об электронной торговле (2001 год); Сингапур – Закон об электронных сделках (1998 год); Словения – Закон об электронной торговле и электронной подписи (2000 год); Таиланд – Закон об электронных сделках (2001 год); Филиппины – Закон об электронной торговле (2000 год); Франция – *Loi 2000-230 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (2000*); Шри-Ланка – Закон об электронных сделках (2006 год); Эквадор – *Ley de comercio electrónico, firmas electrónicas y mensajes de datos (2002)*; и Южная Африка – Закон об электронных коммуникациях и сделках (2002 год). Типовой закон принят также на зависимых территориях Британской короны – в Бейливике Гернси (Закон Гернси об электронных сделках от 2000 года), Бейливике Джерси (Закон Джерси об электронных сделках от 2000 года) и на острове Мэн (Закон об электронных сделках от 2000 года); на заморских территориях Соединенного Королевства Великобритании и Северной Ирландии – Бермудских островах (Закон об электронных сделках от 1999 года), Каймановых островах (Закон об электронных сделках от 2000 года) и островах Тёркс и Кайкос (Указ об электронных сделках от 2000 года); а также в Особом административном районе (ОАР) Китая Гонконге (Указ об электронных сделках от 2000 года). Если не указано иное, последующие ссылки в настоящем документе на законодательные положения любой из этих стран относятся к положениям вышеперечисленных законов.

[10] В Канаде Типовой закон вводится в действие посредством Единообразного закона об электронной торговле, принятого в 1999 году Канадской конференцией по унификации

За очень немногими исключениями[12], в странах, которые ввели в действие Типовой закон, был сохранен используемый в нем подход, нейтральный с точки зрения технологий, при котором ни одна конкретная технология не считается обязательной к применению и не пользуется предпочтением. Такой же подход используется и в Типовом законе ЮНСИТРАЛ об электронных подписях[13], принятом в 2001 году, а также в более новой Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах[14] (принята Генеральной Ассамблеей 23 ноября 2005 года и открыта для подписания с 16 января 2006 года), хотя Типовой закон ЮНСИТРАЛ об электронных подписях содержит ряд дополнительных формулировок (см. ниже, пункты […]-[…]).

11. Если в законодательстве принят минималистский подход, то вопрос о том, считать ли доказанной эквивалентность электронной подписи, обычно решается судьей, арбитром или государственным органом – как правило, на основании так называемого "критерия соответствующей надежности". При этом все типы электронной подписи, удовлетворяющие данному критерию, считаются

законодательства (текст Закона с официальными комментариями к нему размещен по адресу http://www.chlc.ca/en/poam2/index.cfm?sec=1999&sub=1999ia, дата посещения – 12 апреля 2007 года). С тех пор этот закон вступил в силу в целом ряде провинций и территорий Канады, в число которых входят Альберта, Британская Колумбия, Манитоба, Нью-Брансуик, Ньюфаундленд и Лабрадор, Новая Шотландия, Онтарио, Остров Принца Эдуарда, Саскачеван и Юкон. В провинции Квебек принят особый законодательный акт (Закон о создании правовой основы развития информационных технологий от 2001 года), который, несмотря на более широкую сферу охвата и совершенно иные формулировки, обеспечивает достижение многих целей Единообразного закона об электронной торговле и в целом не противоречит Типовому закону ЮНСИТРАЛ об электронной торговле. Актуальную информацию о ходе принятия Единообразного закона об электронной торговле можно найти по адресу http://www.chlc.ca/en/cls/index.cfm?sec=4&sub=4b>, дата посещения – 7 февраля 2007 года.

[11] В Соединенных Штатах Америки Типовой закон ЮНСИТРАЛ об электронной торговле был использован Национальной конференцией членов комиссий по унификации законодательства штатов в качестве основы при разработке Единообразного закона об электронных сделках, принятого этой конференцией в 1999 году (текст Закона с официальными комментариями к нему размещен по адресу http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm, дата посещения – 7 февраля 2007 года). С тех пор Единообразный закон об электронных сделках был введен в действие в округе Колумбия и в следующих 46 штатах: Айдахо, Айова, Алабама, Аляска, Аризона, Арканзас, Вайоминг, Вермонт, Вирджиния, Висконсин, Гавайи, Делавэр, Западная Вирджиния, Индиана, Калифорния, Канзас, Кентукки, Колорадо, Коннектикут, Луизиана, Массачусетс, Миннесота, Миссисипи, Миссури, Мичиган, Монтана, Мэн, Мэриленд, Небраска, Невада, Нью-Хэмпшир, Нью-Джерси, Нью-Мексико, Огайо, Оклахома, Орегон, Пенсильвания, Род-Айленд, Северная Дакота, Северная Каролина, Теннеси, Техас, Флорида, Южная Дакота, Южная Каролина и Юта. В других штатах законодательство, обеспечивающее его осуществление, вероятно, будет принято в ближайшем будущем; это, в частности, касается штата Иллинойс, где Типовой закон ЮНСИТРАЛ уже введен в действие путем принятия Закона о безопасности электронной торговли (1998 год). Актуальную информацию о вводе в действие Единообразного закона об электронных сделках можно найти по адресу http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp, дата посещения – 7 февраля 2007 года.

[12] Доминиканская Республика, Индия, Колумбия, Маврикий, Панама, Эквадор и Южная Африка.

[13] См. сноску […] [издание Организации Объединенных Наций, в продаже под No. R.02.V.8].

[14] См. сноску […] [резолюция 60/21 Генеральной Ассамблеи, приложение].

действительными; таким образом, данный критерий воплощает в себе принцип нейтральности с точки зрения технологий.

12. При определении того, обеспечивает ли тот или иной способ удостоверения подлинности надлежащую степень надежности при данных обстоятельствах, может учитываться широкий круг правовых, технических и коммерческих факторов, включая следующие: a) сложность оборудования, используемого каждой из сторон; b) характер их коммерческой деятельности; c) частотность коммерческих сделок между сторонами; d) характер и объем сделки; e) функцию требований о подписи в конкретной нормативно-правовой среде; f) возможности систем связи; g) соблюдение процедур удостоверения подлинности, установленных посредниками; h) набор процедур удостоверения подлинности, предлагаемых каким-либо посредником; i) соблюдение торговых обычаев и практики; j) наличие механизмов страхового покрытия на случай передачи несанкционированных сообщений; k) важность и ценность информации, содержащейся в сообщении данных; l) наличие альтернативных способов идентификации и затраты на их использование; и m) степень принятия или непринятия данного способа идентификации в соответствующей отрасли или области как на момент достижения договоренности в отношении этого способа, так и на момент передачи электронного сообщения.

2. Подход, ориентированный на конкретные технологии

13. В связи со стремлением поощрять подход, нейтральный с точки зрения носителей информации, возникают и другие важные вопросы. Абсолютных гарантий от мошенничества и ошибок при передаче не может быть не только в сфере электронной торговли, но и при бумажном документообороте. Формулируя правила электронной торговли, законодатели зачастую склонны ставить своей целью наивысшую степень защиты, которую способна обеспечить существующая технология[15]. Практическая необходимость применения строгих мер безопасности для предотвращения несанкционированного доступа к данным, обеспечения неприкосновенности сообщений и защиты компьютерных и информационных систем сомнению не подлежит. Однако с точки зрения частного коммерческого права более целесообразным может быть установление градации требований в отношении безопасности по аналогии с различными

---

[15] Одним из первых примеров был Закон штата Юта о цифровой подписи, принятый в 1995 году, но отмененный с 1 мая 2006 года Постановлением № 20 законодательного собрания штата (размещен по адресу http://www.le.state.ut.us/~2006/htmdoc/sbillhtm/sb0020.htm, дата посещения – 28 марта 2007 года). Технологический уклон, присущий этому закону штата Юта, наблюдается в законодательстве целого ряда стран, где в качестве законных средств электронного удостоверения подлинности признаются лишь цифровые подписи, созданные в рамках инфраструктуры публичных ключей (ИПК); это относится, например, к законодательству Аргентины (*Ley de firma digital (2001)* и *Decreto No. 2628/2002 (Reglamentación de la Ley de firma digital*)); Германии (Закон о цифровой подписи, введен в действие в форме статьи 3 Закона об информационных и коммуникационных услугах от 13 июня 1997 года); Израиля (Закон об электронной подписи (2001 год)); Индии (Закон об информационных технологиях от 2000 года); Литвы (Закон об электронных подписях (2000 год)); Малайзии (Закон об электронных подписях от 1997 года); Польши (Закон об электронной подписи (2001 год)); Российской Федерации (Закон об электронной цифровой подписи (2002 год)); Эстонии (Закон о цифровых подписях (2000 год)); и Японии (Закон об электронных подписях и сертификационных услугах (2001 год)).

степенями юридической надежности, возможными при бумажном документообороте. Деловые люди, оперирующие бумажными документами, в большинстве случаев могут на свой выбор использовать широкий ассортимент методов обеспечения целостности и подлинности сообщений (например, собственноручные подписи разных степеней надежности под обычными договорами и нотариально заверенными актами). При подходе, ориентированном на конкретные технологии, действуют юридические правила, обусловливающие действительность электронной подписи использованием определенной технологии. Так обстоит дело, например, в случаях, когда закон, ставящий своей целью достижение более высокого уровня надежности, требует применения технологий на основе ИПК. Поскольку при этом предписывается использование конкретной технологии, такой подход называют также "предписательным".

14. Недостатки подхода, ориентированного на конкретные технологии, заключаются в том, что если предпочтение отдается отдельным видам электронной подписи, то возникает "риск того, что потенциально более эффективные конкурирующие технологии не будут допущены на рынок"[16]. Вместо того, чтобы поощрять рост электронной торговли и применение электронных методов удостоверения подлинности, такой подход может приводить к обратному результату. При этом требования к той или иной технологии могут оказаться зафиксированными в законодательстве еще до того, как эта технология достигнет зрелого этапа в своем развитии[17]. В результате законодательство может либо начать тормозить дальнейшее поступательное развитие технологии, либо быстро устареть в свете последующих достижений. Следует также отметить, что не для всех целей может требоваться уровень надежности, подобный тому, который обеспечивается теми или иными конкретно упоминаемыми технологиями, и в частности цифровыми подписями. Возможны также случаи, когда оперативность и удобство поддержания связи либо иные соображения могут быть более важными для сторон, чем обеспечение целостности электронной информации с помощью того или иного конкретного процесса. Требование использовать излишне надежные средства удостоверения подлинности может оборачиваться ненужными затратами денежных средств и усилий, что может стать препятствием распространению электронной торговли.

15. Законодательство, ориентированное на конкретные технологии, как правило, отдает предпочтение использованию цифровых подписей на основе ИПК. Структура ИПК, в свою очередь, является различной в разных странах в зависимости от степени государственного вмешательства. Здесь также можно выделить три основные модели:

a) **Саморегулирование**. В рамках этой модели услуги по удостоверению подлинности представляют собой широко открытое поле для деятельности. В то время как одна или несколько систем удостоверения подлинности могут быть

---

16 Stewart Baker and Matthew Yeo, in collaboration with the secretariat of the International Telecommunication Union, “Background and issues concerning authentication and the ITU”, briefing paper presented to the Experts Meeting on Electronic Signatures and Certification Authorities: Issues for Telecommunications, Geneva, 9 and 10 December 1999, Document No. 2, размещено по адресу www.itu.int/osg/spu/ni/esca/meetingdec9-101999/briefingpaper.html, дата посещения – 12 апреля 2007 года.

17 Вместе с тем, поскольку технология ИПК на сегодняшний день является вполне зрелой и устоявшейся, соображения такого рода отчасти утратили прежнюю актуальность.

учреждены правительством в рамках его собственных подразделений и связанных с ними организаций, частному сектору предоставлена свобода создания коммерческих или иных систем удостоверения подлинности по собственному усмотрению. Наличие удостоверяющего органа высокого уровня не является обязательным, а поставщики услуг по удостоверению подлинности самостоятельно несут ответственность за обеспечение взаимодействия с другими поставщиками внутри страны и на международном уровне, в зависимости от того, с какой целью создается система удостоверения подлинности. При этом такие поставщики не нуждаются в лицензиях или разрешениях на использование той или иной технологии (за возможным исключением правил, касающихся защиты потребителей)[18];

b) **Ограниченное государственное вмешательство**. Правительство может принять решение о создании удостоверяющего органа высокого уровня, подчинение которому может носить добровольный или обязательный характер. В этом случае поставщики услуг по удостоверению подлинности могут столкнуться с необходимостью взаимодействия с удостоверяющим органом высокого уровня для того, чтобы выдаваемые ими средства удостоверения (или иные подтверждения подлинности) признавались за пределами их собственных систем. При этом технические и административные спецификации поставщиков услуг по удостоверению подлинности должны как можно раньше быть опубликованы, чтобы правительственные подразделения и частный сектор могли учитывать их при составлении своих планов. От каждого поставщика услуг по удостоверению подлинности может требоваться получение лицензии и разрешений на использование соответствующих технологий[19];

c) **Процесс, осуществляемый под руководством правительства**. Правительство может принять решение об учреждении централизованного поставщика услуг по удостоверению подлинности, наделенного эксклюзивными правами. При этом с разрешения правительства могут учреждаться также специализированные поставщики услуг по удостоверению подлинности[20]. Еще один способ, посредством которого правительства могут косвенно направлять процесс использования цифровых подписей, связан с системами управления идентификационными записями (см. пункты [...]-[...] выше). Правительствами некоторых стран уже начаты программы выдачи своим гражданам идентификационных документов, пригодных для машинного считывания ("электронные удостоверения личности"), которые оснащены функциями создания цифровой подписи.

3. Двухуровневый, или двойственный подход

16. При этом подходе законом устанавливаются низкие пороговые требования, которым методы электронного удостоверения подлинности должны соответствовать для получения определенного минимального юридического статуса, тогда как некоторые способы электронного удостоверения подлинности (которые могут именоваться защищенными, усовершенствованными или особо

---

[18] Asia-Pacific Economic Cooperation, *Assessment Report on Paperless Trading of APEC Economies* (Beijing, APEC secretariat, 2005), pp. 63 and 64, где в качестве примера применения этой модели приводятся Соединенные Штаты Америки.

[19] Там же, в связи с примером Сингапура.

[20] Там же, в связи с примерами Китая и Малайзии.

надежными цифровыми подписями, либо отвечающими установленным требованиям сертификатами)[21] наделяются большей юридической силой. На базовом уровне законодательство, построенное по двухуровневой системе, обычно признает электронные подписи функционально эквивалентными собственноручным подписям исходя из критериев, нейтральных с точки зрения технологий. Подписи более высокого уровня надежности, в отношении которых действуют определенные опровержимые презумпции, должны отвечать особым требованиям, которые могут быть связаны с конкретной технологией. На сегодняшний день такие защищенные подписи обычно определяются в законах упомянутого типа со ссылкой на технологию ИПК.

17. Данный подход, как правило, применяется в правовых системах, где считается важным закрепить в законодательстве определенные требования в отношении технологий, оставив, однако, открытой возможность технического развития. Он позволяет обеспечить в вопросе об электронных подписях баланс между гибкостью и определенностью, предоставив сторонам возможность самостоятельно принимать, исходя из своих потребностей, коммерческое решение о том, готовы ли они идти на затраты и неудобства, связанные с использованием более надежных методов. В соответствующих текстах содержатся также указания относительно критериев признания электронных подписей в рамках модели, предусматривающей наличие сертификационного органа. Двухуровневый подход в принципе совместим с любыми моделями сертификации (будь то основанными на саморегулировании, добровольной аккредитации или руководящей роли правительства) и в этом смысле аналогичен подходу, ориентированному на конкретные технологии (см. выше, пункты [...]-[...]). Таким образом, хотя некоторые правила могут быть достаточно гибкими для того, чтобы применяться к различным моделям сертификации электронных подписей, в некоторых системах право выдачи "защищенных" или "отвечающих установленным требованиям" сертификатов может признаваться лишь за лицензированными поставщиками сертификационных услуг.

18. Законодательство, основанное на двухуровневом подходе, первыми приняли Сингапур[22] и Европейский союз[23]. За ними последовал ряд других

---

[21] Aalberts and van der Hof, *Digital Signature Blindness* ... (см. сноску […]), para. 3.2.2.

[22] В статье 8 Закона Сингапура об электронных сделках допускается использование любых видов электронной подписи, но при этом лишь в отношении защищенных электронных подписей, отвечающих требованиям статьи 17 данного закона (т.е. подписей, которые "a) принадлежат только использующему их лицу; b) обеспечивают возможность идентификации этого лица; c) созданы таким способом или с помощью таких средств, которые находятся под исключительным контролем использующего их лица; и d) связаны с электронной записью, к которой они относятся, таким образом, что в случае изменения этой записи электронная подпись становится недействительной"), действует презумпция, указанная в статье 18 (в частности, что подпись "является подписью лица, которому она соответствует" и что подпись "была поставлена этим лицом с намерением подписать или одобрить данную электронную запись"). Цифровые подписи, подкрепленные заслуживающим доверие сертификатом, соответствующим положениям статьи 20 данного закона, автоматически признаются "защищенными электронными подписями" для целей этого закона.

[23] Как и в Законе Сингапура об электронных сделках, в Директиве Европейского союза об электронных подписях (см. сноску […]) проводится различие между "электронной подписью" (определяемой в пункте 1 статьи 2 как "данные в электронной форме, присоединенные или логически привязанные к другим электронным данным и используемые

правовых систем[24]. Типовой закон ЮНСИТРАЛ об электронных подписях позволяет принимающему этот закон государству создать у себя двухуровневую систему на основе подзаконных актов, хотя специально не побуждает к этому[25].

19. В отношении второго уровня странам было предложено не требовать использования подписи второго уровня для выполнения требований в отношении формы международных коммерческих сделок, ограничив применение "защищенных" электронных подписей теми областями права, которые не оказывают существенного влияния на международную торговлю (такими, как доверительное распоряжение имуществом, семейное право, сделки с недвижимостью и т.д.)[26]. Более того, было предложено прямо подтверждать в двухуровневом законодательстве юридическую силу договорных соглашений об использовании и признании электронных подписей, чтобы основанные на договорах глобальные схемы удостоверения подлинности не приходили в противоречие с требованиями национального права.

в качестве средства удостоверения подлинности") и "усовершенствованной электронной подписью" (определяемой в пункте 2 статьи 2 как электронная подпись, отвечающая следующим требованиям: "a) она связана исключительно с подписавшим лицом; b) она обеспечивает возможность идентификации подписавшего лица; c) она создана с помощью средств, которые подписавшее лицо может удерживать под своим исключительным контролем; и d) она связана с данными, к которым она относится, таким образом, что любые последующие изменения этих данных поддаются обнаружению"). В пункте 2 статьи 5 данной директивы государствам – членам Европейского союза предписывается обеспечить, чтобы "юридическую силу электронной подписи и ее допустимость в качестве доказательства в процессе судопроизводства невозможно было отрицать лишь на том основании", что она "имеет электронную форму или не подкреплена отвечающим установленным требованиям сертификатом, или не подкреплена отвечающим установленным требованиям сертификатом, выданным аккредитованным поставщиком сертификационных услуг, или создана не с помощью защищенного устройства для создания подписей". В то же время лишь усовершенствованные электронные подписи, "подкрепляемые отвечающим установленным требованиям сертификатом и созданные с помощью защищенного устройства для создания подписей", признаются "a) удовлетворяющими юридическим требованиям в отношении подписи применительно к данным в электронной форме по аналогии с тем, как собственноручная подпись отвечает этим требованиям применительно к данным, зафиксированным на бумаге; и b) допустимыми в качестве доказательства в процессе судопроизводства" (см. пункт 1 статьи 5 Директивы).

[24] Например, Маврикий и Пакистан. Подробнее о соответствующих законах см. сноску [9] выше.

[25] В пункте 3 статьи 6 Типового закона ЮНСИТРАЛ об электронных подписях (см. сноску […]) говорится, что электронная подпись считается надежной, если: a) данные для создания электронной подписи в том контексте, в котором они используются, связаны с подписавшим и ни с каким другим лицом; b) данные для создания электронной подписи в момент подписания находились под контролем подписавшего и никакого другого лица; c) любое изменение, внесенное в электронную подпись после момента подписания, поддается обнаружению; и d) в тех случаях, когда одна из целей юридического требования в отношении наличия подписи заключается в гарантировании целостности информации, к которой она относится, любое изменение, внесенное в эту информацию после момента подписания, поддается обнаружению.

[26] Baker and Yeo, "Background and issues concerning authentication …" (см. сноску [16]).

B. Доказательственная ценность электронных методов подписания и удостоверения подлинности

20. Одной из главных целей Типового закона ЮНСИТРАЛ об электронной торговле и Типового закона ЮНСИТРАЛ об электронных подписях было предотвратить возникновение несоответствий и избежать чрезмерного регулирования, предложив общие критерии установления функциональной эквивалентности между электронными и предназначенными для бумажных документов методами подписания и удостоверения подлинности. Хотя Типовой закон ЮНСИТРАЛ об электронной торговле получил широкое признание и используется все большим числом государств в качестве основы национального законодательства об электронной торговле, пока еще нельзя исходить из того, что принципы этого типового закона применяются повсеместно. Отношение к электронным подписям и электронному удостоверению подлинности в разных правовых системах, как правило, отражает присущий той или иной правовой системе общий подход к требованиям в отношении письменной формы и к доказательственной ценности электронных записей.

1. "Удостоверение подлинности" и общая атрибуция электронных записей

21. Использование электронных методов удостоверения подлинности сопряжено с двумя аспектами, имеющими отношение к рассматриваемой теме. Первый аспект касается общего вопроса об атрибуции сообщения данных его предполагаемому составителю. Второй аспект касается приемлемости метода идентификации, который используется сторонами с целью соблюдения конкретных требований в отношении формы, и в частности юридических требований в отношении подписи. Кроме того, имеют значение правовые понятия, подразумевающие наличие собственноручной подписи, как, например, понятие "документ" в некоторых правовых системах. Хотя эти два аспекта часто могут объединяться или, в зависимости от обстоятельств, могут быть не вполне отличимыми друг от друга, попытка проанализировать их по отдельности может быть полезной, поскольку, как представляется, суды проявляют тенденцию к вынесению разных заключений в зависимости от функций, которыми наделяется тот или иной метод удостоверения подлинности.

22. Об атрибуции сообщений данных говорится в статье 13 Типового закона. Соответствующее положение имеет в своей основе статью 5 Типового закона ЮНСИТРАЛ о международных кредитовых переводах[27], в которой определяются обязанности отправителя платежного поручения. Предполагается, что статья 13 Типового закона об электронной торговле будет применяться в случае возникновения вопроса о том, действительно ли электронное сообщение было отправлено лицом, которое указано в качестве его составителя. При обмене сообщениями, составленными на бумаге, проблема такого рода возникает в случае, если подпись предполагаемого составителя объявляется поддельной. При электронном документообороте сообщение может быть направлено лицом, не имеющим на это полномочий, однако его подлинность будет точно удостоверена с помощью кода, шифра или иными подобными средствами. Цель

---

[27] Издание Организации Объединенных Наций, в продаже под No. R.99.V.11, размещено по адресу http://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf.

статьи 13 заключается не в атрибуции авторства сообщения данных и не в идентификации сторон. Вопрос об атрибуции сообщений данных решается в ней путем определения условий, при которых сторона может рассчитывать на то, что сообщение данных действительно исходит от предполагаемого составителя.

23. В пункте 1 статьи 13 Типового закона об электронной торговле делается ссылка на принцип, согласно которому составитель связан сообщением данных в том случае, если он действительно отправил это сообщение. Пункт 2 касается ситуации, когда сообщение было направлено иным лицом, чем составитель, которое правомочно действовать от имени составителя. В пункте 3 идет речь о двух типах ситуаций, в которых адресат может полагаться на сообщение данных как на сообщение составителя: это, во-первых, ситуации, когда адресат надлежащим образом применил процедуру удостоверения подлинности, предварительно согласованную с составителем; и, во-вторых, ситуации, когда сообщение данных явилось результатом действий лица, которое в силу своих взаимоотношений с составителем имело доступ к процедурам удостоверения подлинности, используемым данным составителем.

24. Норма, зафиксированная в статье 13 Типового закона об электронной торговле, включая презумпцию атрибуции, установленную в пункте 3 этой статьи, принята в целом ряде стран[28]. В некоторых странах использование кодов, паролей или других средств идентификации прямо отнесено к числу факторов, из которых возникает презумпция авторства[29]. Существуют также более общие версии статьи 13, в которых презумпция, возникающая в результате надлежащей проверки посредством заранее согласованной процедуры, переформулируется, приобретая форму указания элементов, которые могут использоваться для целей атрибуции[30].

25. В то же время в некоторых странах приняты лишь общие правила, изложенные в статье 13, а именно что сообщение данных является сообщением данных составителя, если оно было отправлено составителем лично либо лицом, действовавшим от имени составителя, либо системой, запрограммированной

---

[28] Венесуэла (Боливарианская Республика) (статья 9); Иордания (статья 15); Колумбия (статья 17); Маврикий (статья 12, пункт 2); Республика Корея (статья 7, пункт 2); Сингапур (статья 13, пункт 3); Таиланд (статья 16); Филиппины (статья 18, пункт 3); и Эквадор (статья 10). Такие же нормы содержатся и в законах зависимой территории Британской короны Джерси (статья 8) и британских заморских территорий Бермудские острова (статья 16, пункт 2) и Тёркс и Кайкос (статья 14). Подробнее о соответствующих законах см. в сноске [9] выше.

[29] Мексика (см. сноску [9] выше), статья 90, пункт I.

[30] Например, Единообразный закон Соединенных Штатов Америки об электронных сделках (UETA) в пункте (a) статьи 9 предусматривает, что электронная запись или электронная подпись "относимы к лицу, если они явились актом этого лица. Совершение такого акта этим лицом может быть доказано любым способом, включая доказывание эффективности любой контрольной процедуры, примененной для определения лица, к которому можно отнести электронную запись или электронную подпись". В пункте (b) статьи 9 предусматривается далее, что последствия электронной записи или электронной подписи, отнесенной к какому-либо лицу согласно пункту (a), "определяются с учетом контекста и сопутствующих обстоятельств во время ее создания, исполнения или принятия, включая соглашение сторон, если таковое было заключено, а также иным образом, как это предусмотрено законом".

составителем или от его имени функционировать в автоматическом режиме[31]. Кроме того, в нескольких странах, где введен в действие Типовой закон об электронной торговле, не предусмотрено никаких конкретных положений, которые основывались бы на статье 13[32]. В этих странах был сделан вывод, что в каких-либо специальных правилах нет необходимости и что вопрос об атрибуции лучше всего решать с использованием обычных методов доказывания, как это делается при атрибуции документов, составленных на бумаге: "лицо, полагающееся на любую подпись, принимает на себя риск того, что эта подпись окажется недействительной, и это правило остается неизменным также для электронной подписи"[33].

26. В других странах, однако, было сочтено более целесообразным рассматривать положения Типового закона об электронной торговле, касающиеся атрибуции, отдельно от положений об электронных подписях. Данный подход зиждется на понимании того, что применительно к документам атрибуция служит прежде всего для создания основы, позволяющей разумно полагаться на эти документы, и может включать более широкий набор средств, чем те, использование которых ограничивается идентификацией физических лиц. В некоторых законах, таких как Единообразный закон Соединенных Штатов Америки об электронных сделках, данный принцип подчеркивается, например, словами о том, что "электронная запись или электронная подпись относимы к лицу, если они явились актом этого лица"; последнее "может быть доказано любым способом, включая доказывание эффективности любой контрольной процедуры, примененной для определения лица, к которому можно отнести электронную запись или электронную подпись"[34]. Такое общее правило атрибуции не влияет на использование подписи как средства атрибуции записи тому или иному лицу, но основывается на признании того, что "подпись не является единственным способом атрибуции"[35]. Поэтому, как указывается в комментарии к закону Соединенных Штатов Америки,

---

[31] Австралия (статья 15, пункт 1); в принципе аналогичным образом – Индия (статья 11); Пакистан (статья 13, пункт 2); Словения (статья 5); зависимая территория Британской короны остров Мэн (статья 2); и ОАР Китая Гонконг (статья 18). Подробнее о соответствующих законах см. в сноске [9] выше.

[32] Например, в Ирландии, Канаде, Новой Зеландии, Франции и Южной Африке.

[33] Канада, Единообразный закон об электронной торговле (и официальный комментарий к нему) (см. сноску [10]), комментарий к статье 10.

[34] Соединенные Штаты Америки, Uniform Electronic Transactions Act (1999) (см. сноску [11]), section 9. В пункте 1 официального комментария к статье 9 приводятся следующие примеры случаев, когда возможна атрибуция как электронной записи, так и электронной подписи конкретному лицу: лицо "включает свое имя в закупочный заказ, направляемый по электронной почте"; "наемный работник лица на основании соответствующих полномочий включает имя лица в закупочный заказ, направляемый по электронной почте"; либо "компьютер лица, запрограммированный на отправку заказов на товары по получении информации об определенных параметрах инвентарных запасов, направляет закупочный заказ, составной частью которого является указание имени лица или другая идентифицирующая это лицо информация".

[35] Там же. В пункте 3 официального комментария к статье 9 говорится: "Использование факсимильных сообщений дает ряд примеров атрибуции с применением иной информации, чем подпись. Факсимильное сообщение может быть отнесено к лицу с учетом информации, напечатанной в начале страницы и указывающей на устройство, с которого она была отправлена. Аналогичным образом, сообщение может быть составлено на бланке, в котором

"4. В электронной среде может присутствовать определенная информация, которая, как представляется, не позволяет установить атрибуцию, но которая ясно связывает какое-либо лицо с какой-либо конкретной записью. Числовые коды, персональные идентификационные номера, комбинации публичного и частного ключей – все это служит делу выявления стороны, к которой следует отнести электронную запись. Несомненно, процедуры обеспечения неприкосновенности будут представлять собой еще одно доказательство для установления атрибуции.

Включение конкретной ссылки на процедуры обеспечения неприкосновенности как на средство установления атрибуции является полезным с учетом уникального значения процедур обеспечения неприкосновенности в электронной среде. В определенных процессах техническая и технологическая процедура обеспечения неприкосновенности может наилучшим способом убедить лицо, решающее вопрос факта, в том, что та или иная электронная запись или подпись является записью или подписью какого-либо конкретного лица. При определенных обстоятельствах использование процедуры обеспечения неприкосновенности для установления того, что запись или связанная с нею подпись исходит от коммерческого предприятия некоего лица, может быть необходимым для опровержения утверждений о вмешательстве хакера. Ссылка на процедуры обеспечения неприкосновенности не подразумевает, что другие формы доказательств атрибуции следует считать менее убедительными. Важно также помнить о том, что конкретная степень надежности какой-либо процедуры не затрагивает ее статус в качестве процедуры обеспечения неприкосновенности, но влияет лишь на то значение, которое следует придавать доказательствам, полученным с помощью данной процедуры обеспечения неприкосновенности и направленным на установление атрибуции"[36].

27. Кроме того, важно учитывать, что презумпция атрибуции как таковая не будет заменять собой применение норм права, касающихся подписей, в тех случаях, когда подпись является необходимой для действительности какого-либо акта или для доказательства его совершения. После установления того, что запись или подпись относится к какой-либо конкретной стороне, "последствия записи или подписи должны быть определены с учетом контекста и сопутствующих обстоятельств, в том числе соглашения сторон, если таковое было заключено", а также "других юридических требований, рассматриваемых с учетом контекста"[37].

указан отправитель. В ходе рассмотрения некоторых дел утверждалось, что бланк сообщения фактически представляет собой подпись, поскольку он является условным обозначением, используемым отправителем с намерением удостоверить подлинность факсимильного сообщения. Однако в том из этих дел, где было признано наличие подписи, это было сделано в результате установления необходимого намерения. По другим делам было установлено, что бланки факсимильных сообщений НЕ являлись подписями, поскольку отсутствовало необходимое для этого намерение. Решающий момент заключается в том, что с подписью или без таковой информация, содержащаяся в электронной записи, может быть вполне достаточной для установления фактов, приводящих к атрибуции электронной записи какой-либо конкретной стороне".

[36] Там же, официальный комментарий к статье 9.

[37] Там же, пункт 6 официального комментария к статье 9.

28. На фоне столь гибкого представления об атрибуции суды Соединенных Штатов Америки, как представляется, придерживаются либерального подхода к вопросу о допустимости электронных записей, включая электронную почту, в качестве доказательств в ходе гражданско-правового производства[38]. Суды Соединенных Штатов Америки отклоняли аргументы, согласно которым сообщения по электронной почте были недопустимыми в качестве доказательств на том основании, что их подлинность не была удостоверена и они являлись устными доказательствами[39]. Вместо этого суды приходили к выводу, что сообщения по электронной почте, полученные от истца в ходе процесса раскрытия, являются сообщениями с самоудостоверенной подлинностью, поскольку "предъявление в ходе раскрытия документов из архивов самих сторон является достаточным для обоснования вывода о самоудостоверении их подлинности"[40]. Эти суды склонны принимать во внимание все имеющиеся доказательства и не отклоняют электронные записи как недопустимые prima facie.

29. В странах, которые не приняли Типового закона об электронной торговле, как представляется, нет конкретных законодательных положений, где аналогичным образом решался бы вопрос об атрибуции. В таких странах атрибуция, как правило, представляет собой функцию правового признания электронных подписей и презумпций, относимых к записям, подлинность которых удостоверена электронной подписью конкретного типа. Озабоченность опасностью манипуляций электронными записями привела к принятию в некоторых странах судебных решений, отрицающих доказательственную ценность сообщений по электронной почте для целей судебного разбирательства на том основании, что целостность таких сообщений не может быть должным образом гарантирована[41]. Другие примеры более ограничительного подхода к доказательственной ценности электронных записей и вопросу об атрибуции можно найти в недавних делах, связанных с проведением аукционов в Интернете, в которых суды применяли высокий стандарт для атрибуции сообщений данных. Эти дела чаще всего были связаны с исками о неисполнении договоров, выразившемся в неоплате товаров, якобы приобретенных на Интернет-аукционах. Истцы утверждали, что ответчиками являются покупатели, поскольку подлинность заявки с предложением наиболее высокой цены за товары была удостоверена с помощью пароля ответчика, а сама заявка была направлена с адреса электронной почты ответчика. Суды приходили к заключению, что таких элементов недостаточно для однозначного вывода о том, что именно ответчик фактически участвовал в аукционе и представил

---

[38] *Commonwealth Aluminum Corporation v. Stanley Metal Associates*, United States District Court for the Western District of Kentucky, 9 August 2001, Federal Supplement, 2nd series, vol. 186, p. 770; и *Central Illinois Light Company (CILCO) v. Consolidation Coal Company (Consol)*, United States District Court for the Central District of Illinois, 30 December 2002, Federal Supplement, 2nd series, vol. 235, p. 916.

[39] *Sea-Land Service, Inc. v. Lozen International, Llc.*, United States Court of Appeals for the Ninth Circuit, 3 April 2002, Federal Reporter, 3rd series, vol. 285, p. 808.

[40] *Superhighway Consulting, Inc. v. Techwave, Inc.*, United States District Court for the Northern District of Illinois, Eastern Division, 16 November 1999, U.S. Dist. LEXIS 17910.

[41] Германия, Amtsgericht (окружной суд) Bonn, Case No. 3 C 193/01, 25 October 2001, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 332/2002, размещено по адресу http://www.jurpc.de/rechtspr/20020332.htm, дата посещения – 11 сентября 2003 года.

выигравшую заявку на приобретение товаров. Для обоснования такой позиции суды использовали различные аргументы. Например, пароль не является надежным средством, поскольку любое лицо, которое знало пароль ответчика, могло, находясь в любом месте, использовать его адрес электронной почты и участвовать в аукционе от имени ответчика[42], причем этот риск некоторые суды на основании показаний экспертов об угрозах безопасности коммуникационных сетей на базе Интернета – в частности в связи с использованием так называемых "троянских коней", способных "похитить" пароль пользователя, – оценили как "очень высокий"[43]. Риск несанкционированного использования идентификационного средства (пароля) какого-либо лица должна принимать на себя сторона, предлагающая товары или услуги через ту или иную конкретную сеть, поскольку не существует правовой презумпции, согласно которой сообщения, направленные через веб-страницу в Интернете с использованием пароля доступа какого-либо лица к такой веб-странице, могут быть отнесены к данному лицу[44]. Такую презумпцию можно представить себе в отношении "усовершенствованной электронной подписи", как она определена в законодательстве, но владелец обычного "пароля" не должен нести риска неправомерного использования этого пароля не уполномоченными на то лицами[45].

2. Возможность соответствия юридическим требованиям в отношении подписи

30. В ряде стран суды проявляли склонность к либеральному толкованию требований в отношений подписи. Как уже отмечалось (см. введение, пункты […]-[…]), в некоторых системах общего права это, как правило, имело место в связи с требованиями закона об обманных действиях, согласно которым сделки определенных видов считаются действительными лишь при условии, что они заключены в письменной форме и скреплены подписью. Суды Соединенных Штатов Америки также с готовностью принимали во внимание законодательные положения о признании электронных подписей, допуская их использование и в ситуациях, не предусмотренных прямо в санкционирующем законе, в частности

---

[42] Германия, Amtsgericht (окружной суд) Erfurt, Case No. 28 C 2354/01, 14 September 2001, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 71/2002, размещено по адресу http://www.jurpc.de/rechtspr/20020071.htm, дата посещения – 25 августа 2003 года; см. также Landgericht (земельный суд) Bonn, Case No. 2 O 472/03, 19 December 2003, *JurPC, Internet-Zeitschrift für Rechtsinformatik und Informationsrecht,* JurPC Web-Dok. No. 74/2004, размещено по адресу http://www.jurpc.de/rechtspr/20040074.htm, дата посещения – 2 февраля 2007 года.

[43] Германия, Landgericht (земельный суд) Konstanz, Case No. 2 O 141/01 A, 19 April 2002, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 291/2002, размещено по адресу http://www.jurpc.de/rechtspr/20020291.htm, дата посещения – 25 августа 2003 года.

[44] Германия, Landgericht (земельный суд) Bonn, Case No. 2 O 450/00, 7 August 2001, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 136/2002, размещено по адресу http://www.jurpc.de/rechtspr/20020136.htm, дата посещения – 25 августа 2003 года.

[45] Германия, Oberlandesgericht (апелляционный суд) Köln, Case No. 19 U 16/02, 6 September 2002, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 364/2002, размещено по адресу http://www.jurpc.de/rechtspr/20020364.htm, дата посещения – 25 августа 2003 года.

в связи с судебными предписаниями[46]. Для договорного контекста более важным является то, что суды оценивали адекватность удостоверения подлинности в свете отношений, существовавших между сторонами, а не на основе жесткого стандарта для всех ситуаций. Так, если стороны регулярно пользовались в ходе своих переговоров электронной почтой, то суды устанавливали, что указание имени составителя в сообщении по электронной почте отвечает статутным требованиям в отношении подписи[47]. "Сознательное указание каким-либо лицом своего имени в напечатанном виде в конце всех сообщений по электронной почте" было сочтено действительным удостоверением подлинности[48]. Готовность судов в Соединенных Штатах Америки признать, что сообщения по электронной почте и указанные в их тексте имена могут считаться удовлетворяющими требованиям в отношении письменной формы[49], соответствуют либеральному толкованию понятия "подпись" как включающего "любой символ, исполненный или принятый стороной с явным намерением удостоверить подлинность составленного в письменной форме документа", в связи с чем в некоторых случаях "набранное на клавиатуре имя или фирменный бланк, на котором составлен документ, являются достаточными для выполнения требования в отношении подписи"[50]. Если стороны не отрицают факт составления или получения ими сообщений по электронной почте, то требования закона в отношении подписи считаются выполненными, так как суды "уже в течение долгого времени признают, что подпись, влекущая за собой юридические обязательства, может принимать форму любой пометки или обозначения, которые сторона, принимающая обязательство, считает подходящими", при условии, что ее автор "намеревается связать себя обязательствами"[51].

31. Суды Соединенного Королевства Великобритании и Северной Ирландии придерживаются аналогичного подхода, обычно считая форму подписи менее важной, чем выполняемая ею функция. Так, судами принимается во внимание то, насколько те или иные средства пригодны как для атрибуции записи конкретному лицу, так и для указания на намерение данного лица по отношению к этой записи. Соответственно, сообщения, направляемые по электронной почте,

---

[46] *Department of Agriculture and Consumer Services v. Haire*, Fourth District Court of Appeal of Florida, Case Nos. 4D02-2584 and 4D02-3315, 15 January 2003.

[47] *Cloud Corporation v. Hasbro, Inc.*, United States Court of Appeals for the Seventh Circuit, 26 December 2002, Federal Reporter, 3rd series, vol. 314, p. 296.

[48] *Jonathan P. Shattuck v. David K. Klotzbach*, Superior Court of Massachusetts, 11 December 2001, 2001 Mass. Super. LEXIS 642.

[49] *Central Illinois Light Company v. Consolidation Coal Company*, United States District Court for the Central District of Illinois, Peoria Division, 30 December 2002, Federal Supplement, 2nd Series, vol. 235, p. 916.

[50] Там же, стр. 919: "Внутренние документы, фактуры и сообщения по электронной почте могут использоваться для выполнения требований закона об обманных действиях [Единообразный коммерческий кодекс] штата Иллинойс". По данному конкретному делу суд, однако, решил, что якобы существовавший договор не отвечал требованиям закона об обманных действиях – не потому, что сообщения по электронной почте как таковые не могли содержать действительные записи об условиях договора, а из-за отсутствия указаний на то, что авторы этих направлявшихся по электронной почте сообщений и упоминавшиеся в них лица являлись служащими ответчика.

[51] *Roger Edwards, LLC v. Fiddes & Son, Ltd.*, United States District Court for the District of Maine, 14 February 2003, Federal Supplement, 2nd Series, vol. 245, p. 251.

могут считаться "документами", а имена, набранные в тексте этих сообщений, – "подписями"[52]. По заявлениям некоторых судов, у них "нет сомнений в том, что если сторона создает и отсылает документ, созданный электронным способом, то последствия этого по закону будут для нее такими же, как если бы она подписала печатный экземпляр данного документа", причем "тот факт, что документ создан электронным способом, а не составлен на бумаге, ничего не меняет"[53]. Аргументы о том, что сообщения по электронной почте должны рассматриваться как подписанные договоры для целей закона об обманных действиях, время от времени отклонялись судами – главным образом ввиду отсутствия намерения принять на себя обязательства, вытекающие из подписи. Однако прецеденты, когда суды заведомо отрицали бы возможность соответствия направляемых по электронной почте сообщений и набранных в их тексте имен статутным требованиям в отношении письменной формы и подписи, по-видимому, отсутствуют. В ряде случаев требования закона об обманных действиях были сочтены невыполненными из-за того, что сообщения, направлявшиеся по электронной почте, отражали содержание ведущихся переговоров, а не окончательное соглашение – например постольку, поскольку одна из сторон на переговорах исходила из того, что имеющий обязательную силу договор не будет считаться заключенным до подписания "меморандума о сделке"[54]. В других случаях суды отмечали, что они, возможно, были бы готовы приравнять к подписи "фамилию или инициалы" составителя "в конце сообщения, направленного по электронной почте" или "в любой другой части такого сообщения", но что, по их мнению, "автоматическое указание адреса электронной почты того или иного лица [поставщиком Интернет-услуг] отправителя и/или получателя после передачи документа" не "предназначается в качестве подписи"[55]. Хотя британские суды, по-видимому, придерживаются более строгого подхода к толкованию требований закона об обманных действиях в отношении письменной формы, чем их коллеги в Соединенных Штатах Америки, они в целом склонны допускать использование любых методов электронного подписания или удостоверения подлинности, даже вне рамок какого-либо прямо разрешающего это закона, при условии, что соответствующий метод обеспечивает выполнение тех же функций, что и собственноручная подпись[56].

---

[52] *Hall v. Cognos Limited* (Hull Industrial Tribunal, Case No 1803325/97) (не опубликовано).

[53] *Mehta v. J. Pereira Fernandes S.A.* [2006] EWHC 813 (Ch), (United Kingdom, England and Wales High Court, Chancery Division), [2006] 2 Lloyd's Rep 244 (United Kingdom, England and Wales, Lloyd's List Law Rreports).

[54] *Pretty Pictures Sarl v. Quixote Films Ltd.*, 30 January 2003 ([2003] EWHC 311 (QB), (United Kingdom, England and Wales High Court, Law Reports Queen's Bench, [2003] All ER (D) 303 (January)) (United Kingdom, All England Direct Law Reports (Digests)).

[55] *Mehta v. J. Pereira Fernandes S.A.* (см. сноску [53]).

[56] *Mehta v. J. Pereira Fernandes S.A.* (см. сноску [53]), № 25: "Заслуживает внимания то мнение Юридической комиссии в отношении [Директивы Европейского союза об электронной торговле (2000/31/EC)], что законы, требующие наличия подписей, не нуждаются в существенных изменениях, поскольку выполнение таких требований может быть проверено с помощью функционального критерия, а именно вопроса о том, можно ли из поведения предполагаемого подписавшего сделать разумный вывод о наличии у него намерения удостоверить подлинность. … Таким образом, как мной уже отмечалось, если какая-либо сторона или агент этой стороны при направлении сообщения по электронной почте набирает в тексте этого сообщения – постольку, поскольку это требуется или разрешается

32. Суды в системах гражданского права, как правило, руководствуются более узким подходом – вероятно, в связи с тем, что во многих соответствующих странах понятие "документ" обычно предполагает ту или иную форму удостоверения подлинности и, таким образом, становится трудно отделимым от понятия "подпись". Во Франции, например, суды не были склонны рассматривать электронные средства идентификации в качестве эквивалента собственноручных подписей до принятия законодательства, прямо признающего юридическую силу электронных подписей[57]. Отражением несколько более либеральной позиции являются решения, допускающие подачу жалоб административного характера в электронной форме в целях соблюдения установленных законом сроков, при условии, что такие жалобы впоследствии подтверждаются обычными почтовыми отправлениями[58].

33. В отличие от своего ограничительного подхода к атрибуции сообщений данных при заключении договоров, суды Германии, по-видимому, проявляют либеральное отношение к признанию методов идентификации в качестве эквивалента собственноручных подписей в ходе судебного производства. Дискуссия в Германии развивалась вокруг вопроса о все более широком использовании отсканированных изображений подписи адвоката для удостоверения подлинности компьютерных факсимильных сообщений, содержащих ходатайства об обжаловании и препровождаемых непосредственно от компьютерной станции через модем на факсимильное устройство суда. В связи с предыдущими делами апелляционные суды[59] и Федеральный суд (Bundesgerichtshof)[60] полагали, что отсканированное изображение собственноручной подписи не удовлетворяет установленным требованиям в отношении подписи и не удостоверяет личность соответствующего лица. Идентификационная функция теоретически могла бы быть признана за "усовершенствованной электронной подписью", как она определена в германском законодательстве. Однако в целом считалось, что условия признания эквивалентности между сообщениями в письменной форме и нематериальными сообщениями, препровождаемыми путем передачи данных, должен установить

существующими положениями прецедентного права, – свое имя или имя своего принципала, то это, на мой взгляд, уже может считаться подписью для целей [закона об обманных действиях]".

57 Кассационный суд Франции отказал в принятии заявления об обжаловании, подписанного в электронной форме, из-за сомнений в отношении идентификации лица, поставившего подпись, и ввиду того, что заявление об обжаловании было подписано в электронной форме до вступления в силу закона от 13 марта 2000 года, в котором признается юридическая сила электронных подписей (Cour de cassation, Deuxième chambre civile, 30 avril 2003, *Sté Chalets Boisson c/ M. X.*, размещено по адресу www.juriscom.net/jpt/visu.php?ID=239, дата посещения – 12 сентября 2003 года).

58 Франция, Conseil d'État, 28 décembre 2001, N° 235784, *Élections municipales d'Entre-Deux-Monts*, размещено по адресу www.rajf.org/article.php3?id_article=467, дата посещения – 12 сентября 2003 года.

59 Например, Oberlandesgericht (апелляционный суд) Karlsruhe, Case No. 14 U 202/96, 14 November 1997, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 09/1998, размещено по адресу www.jurpc.de/rechtspr/19980009.htm, дата посещения – 12 сентября 2003 года.

60 Германия, Bundesgerichtshof (Федеральный суд), Case No. XI ZR 367/97, 29 September 1998, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 05/1999, размещено по адресу http://www.jurpc.de/rechtspr/19990005.htm, дата посещения – 12 сентября 2003 года.

именно законодатель, а не суды[61]. Такое понимание в конечном счете было отвергнуто с учетом единодушного мнения других высоких федеральных судов, которые признали возможность выдвижения определенных процессуальных аргументов посредством электронной передачи сообщения данных, сопровождаемого отсканированным изображением подписи[62].

34. Интересно отметить, что даже суды в некоторых системах гражданского права (таких, как Колумбия[63]), где принято законодательство, отдающее предпочтение использованию цифровых подписей на основе ИПК, применяют столь же либеральный подход и подтверждают, например, допустимость судопроизводства, осуществляемого целиком посредством электронных сообщений. Материалы, обмен которыми осуществляется в ходе такого судопроизводства, считаются действительными, даже если они не скреплены цифровой подписью, поскольку при передаче электронных сообщений используются методы, обеспечивающие возможность идентификации сторон[64].

35. Судебные прецеденты, касающиеся электронных подписей, до сих пор немногочисленны, и небольшое количество вынесенных на сегодняшний день судебных решений не дает достаточных оснований для однозначных выводов. Тем не менее краткий обзор имеющихся прецедентов позволяет выявить несколько тенденций. Представляется, что на позицию судов в этом вопросе влияет подход к электронным подписям и электронному удостоверению подлинности, применяемый в законодательстве. Можно говорить о том, что повышенное внимание законодателей к электронным "подписям" без сопутствующего этому общего правила, касающегося атрибуции, приводит к

---

[61] Там же.

[62] В решении по делу, переданному ей Федеральным судом (*Bundesgerichtshof*) (см. примечание 29 выше), федеральная Совместная палата высоких судов Германии *(Gemeinsamer Senat der obersten Gerichtshöfe des Bundes)* отметила, что требования в отношении формы в ходе судебного производства не являются самоцелью. Их цель заключается в обеспечении достаточно надежного (*"hinreichend zuverlässig"*) определения содержания письменного документа и личности того, от кого он исходит. Совместная палата отметила эволюцию практического применения требований в отношении формы с учетом предыдущих технических достижений, таких как телекс и телефакс. Совместная палата сочла, что принятие определенных процессуальных заявлений, представленных посредством электронной передачи сообщения данных с отсканированным изображением подписи, соответствовало бы духу существующего прецедентного права (Gemeinsamer Senat der obersten Gerichtshöfe des Bundes, GmS-OGB 1/98, 5 April 2000, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 160/2000, размещено по адресу http://www.jurpc.de/rechtspr/20000160.htm, дата посещения – 12 сентября 2003 года.

[63] Так, в Колумбии, принят Типовой закон ЮНСИТРАЛ об электронной торговле, включая общие положения его статьи 7, однако юридическая презумпция подлинности установлена лишь в отношении цифровых подписей (*Ley de comercio electrónico*, art. 28).

[64] Colombia, Juzgado Segundo Promiscuo Municipal Rovira Tolima, *Juan Carlos Samper v. Jaime Tapias*, 21 julio 2003, Rad. 73-624-40-89-002-2003-053-00. Суд пришел к заключению, что процесс, осуществлявшийся с помощью электронных средств, был действительным несмотря на то, что направлявшиеся по электронной почте сообщения не имели цифровой подписи, так как a) отправитель сообщений данных полностью поддавался идентификации; b) отправитель сообщений данных выразил согласие с содержанием направленных сообщений данных и подтвердил его; c) сообщения данных надежно хранились в трибунале; и d) сообщения были доступны для просмотра в любое время (размещено по адресу http://www.camara-e.net/_upload/80403--0-7-diaz082003.pdf, дата посещения – 2 февраля 2007 года).

чрезмерному сосредоточению на идентификационной функции методов удостоверения подлинности. В некоторых странах это порождает определенное недоверие к любым методам удостоверения подлинности, не подпадающим под предусмотренное законом определение электронной "подписи". Поэтому сомнительно, чтобы те же самые суды, которые занимают либеральную позицию в случаях судебного или административного обжалования, были столь же либеральны в отношении требований, касающихся подписания договоров как условия их действительности. Так, если в договорном контексте сторона может столкнуться с риском непризнания соглашения другой стороной, то в контексте гражданско-правового производства сторона, использующая электронные подписи или записи, как правило, сама заинтересована в подтверждении своего согласия с записью и ее содержанием.

3. Усилия по созданию электронных эквивалентов особых видов подписи

a) Апостили *

36. Как уже отмечалось, дух и буква подписанной в Гааге 5 октября 1961 года Международной конвенции, отменяющей требование легализации иностранных официальных документов, не создают препятствий использованию современных технологий[65]. Этот вывод был подтвержден в ходе Первого международного форума по электронной нотаризации и электронным апостилям, где было указано, что эффективность применения и действия Конвенции можно дополнительно повысить благодаря применению таких технологий[66]. Толкование данной конвенции в свете принципа функциональной эквивалентности позволило бы компетентным органам как вести электронные реестры, так и выдавать электронные апостили в целях дальнейшего совершенствования международной правовой помощи и услуг государственных учреждений.

37. В апреле 2006 года Гаагской конференцией по международному частному праву и Национальной ассоциацией нотариусов (НАН) Соединенных Штатов Америки была начата экспериментальная программа по электронным апостилям (э-АПП). В рамках э-АПП Гаагская конференция и НАН совместно с любыми заинтересованными государствами занимаются разработкой, распространением и содействием внедрению образцов программного обеспечения для a) выдачи и использования электронных апостилей (э-апостилей); и b) эксплуатации электронных реестров апостилей (э-реестров)[67].

---

* Данный раздел получит дальнейшее развитие в окончательном варианте комплексного справочного документа.

65 Hague Conference on Private International Law, "Conclusions and recommendations adopted by the Special Commission on the practical operation of The Hague Apostille, Evidence and Service Conventions: 28 October to 4 November 2003" (The Hague, 2003).

66 Conclusions adopted at the First International Forum on e-Notarization and e-Apostilles, held in Las Vegas, United States, on 30 and 31 May 2005, размещено по адресу http://www.hcch.net/upload/concl_forum.pdf, дата посещения – 7 февраля 2007 года.

67 э-АПП рассчитана на использование уже существующей и широко применяемой технологии. В ее основу положен формат электронных документов PDF со встроенным расширяемым языком гипертекстовой разметки (XML). Более подробную информацию можно найти по адресу http://hcch.e-vision.nl/index_en.php?act=text.display&tid=37, в разделе, посвященном второму Международному форуму по электронной нотаризации и электронным апостилям

b) Печати

38. В некоторых правовых системах требования, касающиеся печатей, уже отменены на том основании, что использование печатей утратило свою актуальность в современных условиях. Их место заняла засвидетельствованная (т.е. поставленная при свидетелях) подпись[68]. В других правовых системах имеется законодательство, согласно которому требование в отношении печати может считаться выполненным при наличии защищенной электронной подписи. Например, в Ирландии действуют конкретные положения, позволяющие использовать должным образом удостоверенные защищенные электронные подписи вместо печати, с согласия лица или публичного органа, которому должен или может быть представлен скрепленный печатью документ[69]. В Канаде установлено, что требования некоторых федеральных законов относительно личной печати считаются выполненными при наличии защищенной электронной подписи, в которой указано, что эта защищенная электронная подпись является личной печатью данного лица[70].

39. В целом ряде стран начаты также инициативы, предполагающие использование электронных документов и подписей при сделках с недвижимостью, требующих документального оформления. Схема, применяемая в Виктории (Австралия), включает использование технологии защищенных электронных подписей при передаче данных через Интернет с помощью цифровых карточек, выдаваемых сертификационным органом. В Соединенном Королевстве соответствующая схема предполагает оформление документов солиситорами по поручению своих клиентов через закрытую компьютерную сеть. В некоторых законодательных актах признается возможность использования "электронных печатей" в качестве альтернативы "ручным печатям"; при этом технические детали, касающиеся формы электронной печати, должны быть оговорены отдельно[71].

(Second International Forum on e-Notarization and e-Apostilles), состоявшемуся в Вашингтоне, О. К., с 27 по 29 мая 2006 года.

68 Например, Закон об имуществе (Прочие положения), принятый в Соединенном Королевстве в 1989 году во исполнение положений доклада Комиссии по правовой реформе на тему "Акты и депозитарные услуги" ("Deeds and escrows") (Law Com. No.143, 1987).

69 Ирландия, Закон об электронной торговле, статья 16. Однако в случаях, когда скрепленный печатью документ должен или может быть представлен публичному органу или лицу, действующему от имени публичного органа, публичный орган, дающий свое согласие на использование электронной подписи, может при этом потребовать ее соответствия конкретным положениям в отношении информационной технологии и процедуры.

70 Канада, Закон о защите персональной информации и электронных документах (2000 год), часть 2, статья 39. Ссылка на федеральные законы относится к Закону о федеральной собственности на недвижимость и федеральном недвижимом имуществе и к Положению о федеральной собственности на недвижимость.

71 Примеры можно найти в требованиях, касающихся подтверждения действительности документов лицензированными или зарегистрированными специалистами, например в Законе о специальностях, связанных с инженерно-техническими работами и науками о Земле (Манитоба, Канада), в котором "электронная печать" определяется как средство идентификации, выдаваемое ассоциацией любому своему члену для использования в целях электронного подтверждения действительности документов в форме, пригодной для компьютерной считки (см. http://apegm.mb.ca/keydocs/act/index.html, дата посещения – 4 апреля 2007 года).

40. В Единообразном законе Соединенных Штатов Америки об электронной регистрации прав на недвижимое имущество[72] прямо говорится, что электронная подпись не обязательно должна сопровождаться физическим или электронным изображением штемпеля, оттиска или печати. По существу необходимой является только информация, указанная на печати, но не сама печать. В этом законе также установлено, что требования любого закона, подзаконного акта или стандарта относительно личного или корпоративного штемпеля, оттиска или печати считаются выполненными при наличии электронной подписи. Такая физическая маркировка неприменима к документам, существующим только в электронной форме. Тем не менее данный закон требует, чтобы информация, которая в ином случае была бы указана на штемпеле, оттиске или печати, была присоединена или логически привязана к документу или подписи электронным способом[73]. Таким образом, нотариальный штемпель или оттиск, требуемый по законам некоторых штатов, не является необходимым при электронном нотариальном заверении согласно данному закону. Закон не требует также наличия корпоративного штемпеля или оттиска для заверения действий сотрудника компании, как это предусмотрено законами некоторых штатов.

c) Нотариальное заверение*

41. В Соединенных Штатах Америки существует три основополагающих закона, касающихся нотариального заверения: Единообразный закон об электронных сделках, Закон об электронных подписях в глобальной и национальной торговле (E-sign)[74] и Единообразный закон об электронной регистрации прав на недвижимое имущество[75]. Взятые в совокупности, они предусматривают, что юридические требования, согласно которым документ или связанная с документом подпись должны быть нотариально заверены, подтверждены, удостоверены, засвидетельствованы или исполнены под присягой, считаются выполненными, если к документу или подписи присоединена или логически привязана электронная подпись лица, уполномоченного на совершение этих действий, вместе со всей прочей информацией, включения которой требует другое применимое законодательство.

42. В Австрии архив электронной документации cyberDOC – независимая компания, учрежденная совместно Австрийской палатой гражданско-правовых нотариусов и компанией "Сименс АГ", – предоставляет в распоряжение

---

* Данный раздел получит дальнейшее развитие в окончательном варианте комплексного справочного документа.

72 Единообразный закон Соединенных Штатов Америки об электронной регистрации прав на недвижимое имущество (The Uniform Real Property Electronic Recording Act of the United States) был подготовлен Национальной конференцией членов комиссий по унификации законодательства штатов. Размещен по адресу http://www.law.upenn.edu/bll/ulc/urpera/URPERA_Final_Apr05-1.htm, дата посещения – 7 февраля 2007 года. Этот закон принят в Аризоне, Делавэре, округе Колумбия, Канзасе, Северной Каролине, Техасе, Вирджинии и Висконсине (см. http://www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-urpera.asp, дата посещения – 7 февраля 2007 года).

73 Т.е. предусматривает критерии, близкие к тем, которые установлены Единообразным законом Соединенных Штатов Америки об электронных сделках.

74 Кодифицировано в United States Code, title 15, chapter 96, sections 7001-7031.

75 См. сноску [72].

нотариусов электронный архив, снабженный функциями удостоверения подлинности[76]. Закон обязывает всех австрийских нотариусов регистрировать и хранить в этом архиве все документы, нотариально заверенные после 1 января 2000 года.

d) Засвидетельствование

43. Высказывались мнения, согласно которым традиционные процедуры с участием свидетелей, такие как засвидетельствование, не вполне поддаются адаптации к электронному подписанию документов, поскольку нет уверенности в том, что изображение на дисплее действительно представляет собой тот документ, который будет скреплен электронной подписью. На дисплее компьютера свидетель и подписывающий могут видеть лишь поддающееся восприятию человеком отображение того, что якобы содержится в компьютерной памяти. Видя, как подписывающий нажимает на клавиши, свидетель доподлинно не знает, что при этом происходит в действительности. Поэтому обеспечить уверенность в том, что изображение на дисплее соответствует содержанию памяти компьютера, а данные, вводимые подписывающим лицом с клавиатуры, соответствуют его намерениям, можно лишь в случае, если путем проверки на основе заслуживающих доверия критериев было установлено, что компьютер функционирует по заслуживающей доверия схеме[77].

44. Защищенная электронная подпись, однако, могла бы обеспечивать выполнение тех же функций, что и свидетель при подписании, т.е. идентифицировать лицо, предположительно подписавшее юридический документ. Использование защищенной электронной подписи могло бы позволять **без привлечения свидетелей** подтверждать подлинность подписи, личность того, кому принадлежит подпись, целостность документа и даже, вероятно, дату и время подписания. В этом отношении защищенная электронная подпись, возможно, даже превосходит обычную собственноручную подпись. Дополнительные преимущества, которые могут быть получены благодаря физическому присутствию свидетеля при проставлении цифровой подписи, скорее всего минимальны, если под сомнение не ставится добровольный характер подписания[78].

45. Эволюция существующего законодательства пока не дошла до полной замены засвидетельствования проставлением электронных подписей; законами предусматривается лишь возможность использования электронной подписи свидетелем. Согласно закону Новой Зеландии об электронных сделках,

---

[76] См. Österreichische Notariatskammer (Austrian Chamber of Civil Law Notaries), размещено по адресу http://www.notar.at/de/portal/einrichtungen/cyberdocgmbhcokg/, дата посещения – 7 февраля 2007 года.

[77] В литературе эта проблема выражается формулой "подписываю то, что вижу" ("What you see is what you sign" – WYSIWYS). См. V. Liu and others, "Visually sealed and digitally signed documents", Association of Computing Machinery, *ACM International Conference Proceedings Series*, vol. 56, *Proceedings of the Twenty-seventh Australasian Conference on Computer Science*, vol. 26, (Dunedin, New Zealand, 2004) p. 287 (см. там же о пользующихся доверием контроллерах изображения).

[78] См. об этом в Joint Infocomm Development Authority of Singapore and the Attorney-General's Chambers, *Joint IDA-AGC Review of Electronic Transactions Act Stage II: Exclusions under Section 4 of the ETA*, consultation paper LRRD No. 2/2004 (Singapore, 2004), parts 5 and 8, размещено по адресу www.agc.gov.sg, в разделе "Publications".

требование о том, чтобы подпись или печать были поставлены при свидетеле, считается выполненным при наличии электронной подписи свидетеля. Технология, с помощью которой должна быть создана цифровая подпись, конкретно не определяется, однако предусматривается, что она должна позволять "надлежащим образом идентифицировать свидетеля и надлежащим образом указывать на то, что подпись или печать засвидетельствованы", а также что она должна быть "настолько надежной, насколько это необходимо с учетом цели, для которой требуется подпись свидетеля, и обстоятельств, при которых она требуется"[79].

46. Согласно закону Канады о защите персональной информации и электронных документах, требования федерального законодательства относительно засвидетельствования подписи считаются выполненными применительно к электронному документу, если каждое подписывающее лицо и каждый свидетель поставят под ним свои защищенные электронные подписи[80]. Требуемое согласно некоторым федеральным законам заявление, в котором указывается или удостоверяется, что любая информация, сообщаемая лицом, от которого исходит это заявление, является достоверной, точной или полной, может быть сделано в электронной форме, если это лицо скрепит его своей защищенной электронной подписью[81]. Заявление, которое согласно федеральным законам должно быть сделано под присягой или в форме официального заверения, может быть сделано в электронной форме, если лицо, от которого оно исходит, скрепит его своей защищенной электронной подписью, а лицо, в присутствии которого это заявление было сделано и которое уполномочено принимать заявления под присягой или в форме официальных заверений, поставит под ним свою защищенную электронную подпись[82]. Альтернативный вариант, предложенный в целях дополнительного повышения уверенности, предполагает проставление электронной подписи только в присутствии пользующегося доверием специалиста, например адвоката или нотариуса[83].

---

[79] Новая Зеландия, Electronic Transactions Act (см. сноску [9]), section 23, размещено по адресу http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes, дата посещения – 4 апреля 2007 года.

[80] Канада, Personal Information Protection and Electronic Documents Act (см. сноску [70]), part 2, section 46.

[81] Там же, section 45.

[82] Там же, section 44.

[83] Нотариусам по операциям с недвижимостью необходимы электронные подписи и средства удостоверения подлинности, обеспечиваемые признанным сертификационным органом. Продавцы и покупатели, возможно, должны будут давать нотариусам по операциям с недвижимостью письменные доверенности на подписание документов. См. "E-conveyancing: the strategy for the implementation of e-conveyancing in England and Wales" (United Kingdom, Land Registry, 2005), размещено по адресу http://www.landregistry.gov.uk/assets/library/documents/e-conveyancing_strategy_v3.0.doc, дата посещения – 7 апреля 2007 года. Проект планируется осуществлять поэтапно с 2006 по 2009 год.