ЮНСИТРАЛ
КОМИССИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ПО ПРАВУ МЕЖДУНАРОДНОЙ ТОРГОВЛИ

Содействие укреплению доверия к электронной торговле: правовые вопросы международного использования электронных методов удостоверения подлинности и подписания

ОРГАНИЗАЦИЯ
ОБЪЕДИНЕННЫХ НАЦИЙ

КОМИССИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ
ПО ПРАВУ МЕЖДУНАРОДНОЙ ТОРГОВЛИ

Содействие укреплению доверия к электронной торговле: правовые вопросы международного использования электронных методов удостоверения подлинности и подписания

ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ
Вена, 2009 год

ИЗДАНИЕ ОРГАНИЗАЦИИ
ОБЪЕДИНЕННЫХ НАЦИЙ
В продаже под № R.09.V.4
ISBN 978-92-1-433058-5

Предисловие

Завершив в 2004 году свою работу над Конвенцией об использовании электронных сообщений в международных договорах, Рабочая группа IV (Электронная торговля) Комиссии Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ) просила Секретариат продолжать мониторинг различных вопросов, связанных с электронной торговлей, и в том числе аспектов, касающихся трансграничного признания электронных подписей, а также опубликовать результаты своих исследований в целях разработки рекомендаций для Комиссии относительно возможности проведения дальнейшей работы в этих областях (см. A/CN.9/571, пункт 12).

В 2005 году ЮНСИТРАЛ приняла к сведению работу, проделанную другими организациями в различных областях, связанных с электронной торговлей, и просила Секретариат подготовить более подробное исследование, в котором содержались бы предложения относительно формы и характера комплексного справочного документа о различных необходимых элементах правовой базы, благоприятствующей развитию электронной торговли, вопрос о подготовке которого ЮНСИТРАЛ могла бы рассмотреть в будущем в целях оказания помощи законодателям и лицам, ответственным за разработку политики, в различных странах мира[1].

В 2006 году ЮНСИТРАЛ рассмотрела записку, подготовленную ее секретариатом в ответ на эту просьбу (A/CN.9/604). В этой записке в качестве возможных компонентов комплексного справочного документа были определены следующие области: *a*) удостоверение подлинности и трансграничное признание электронных подписей; *b*) ответственность и стандарты поведения поставщиков информационных услуг; *c*) использование электронных счетов и юридические вопросы, связанные с системами поставок в электронной торговле; *d*) передача прав в материальных товарах и иных прав с помощью электронных сообщений; *e*) несправедливая конкуренция и мошенническая коммерческая практика в электронной торговле; и *f*) конфиденциальность и защита данных в электронной торговле. В записке были также определены другие вопросы, которые, хотя и более кратко, могут быть охвачены в таком документе: *a*) защита прав интеллектуальной собственности; *b*) незапрошенные электронные сообщения (спам); и *c*) киберпреступность. На этой сессии получило поддержку мнение о том, что задача законодателей и лиц, отвечающих за выработку политики, особенно в развивающихся странах, может быть в значительной степени облегчена, если ЮНСИТРАЛ подготовит комплексный справочный документ по темам, определенным Секретариатом. Было также отмечено, что такой документ может оказать ЮНСИТРАЛ помощь в выявлении областей, в которых она сама в будущем могла бы провести работу по согласованию. ЮНСИТРАЛ просила Секретариат подготовить выборочный раздел комплексного справочного документа, конкретно посвященный

[1] *Официальные отчеты Генеральной Ассамблеи, шестидесятая сессия, Дополнение № 17* (A/60/17), пункт 214.

вопросам, связанным с удостоверением подлинности и трансграничным признанием электронных подписей, для рассмотрения на ее сороковой сессии в 2007 году[2].

Выборочный раздел, подготовленный Секретариатом в соответствии с этой просьбой (A/CN.9/630 и Add.1-5), был представлен на рассмотрение ЮНСИТРАЛ на ее сороковой сессии. ЮНСИТРАЛ выразила Секретариату признательность за подготовку этого выборочного раздела и просила Секретариат опубликовать его в качестве отдельной публикации[3].

В настоящем издании анализируются основные юридические проблемы, возникающие в связи с использованием электронных подписей и методов удостоверения подлинности в международных сделках. В Части первой содержатся обзор методов, используемых для создания электронных подписей и электронного удостоверения подлинности, а также обзор их правового режима в различных странах. В Части второй рассматривается использование электронных методов подписания и удостоверения подлинности в международных сделках и указываются основные проблемы правового характера, связанные с трансграничным признанием этих методов. Как было отмечено, возникновение юридических трудностей в международном аспекте более вероятно в связи с трансграничным использованием таких электронных методов подписания и удостоверения подлинности, которые требуют участия в этом процессе третьих сторон. Это относится, в частности, к таким электронным методам подписания и удостоверения подлинности, которые основаны на использовании сертификатов, выдаваемых доверенной третьей стороной – поставщиком сертификационных услуг, например к цифровым подписям в рамках инфраструктуры публичных ключей (ИПК). По этой причине особое внимание в Части второй настоящего издания уделяется международному использованию цифровых подписей в рамках ИПК. Акцент на этом не должен восприниматься как выражение предпочтения или поддержки данного или любого иного конкретного метода или технологии удостоверения подлинности.

[2] Там же, *шестьдесят первая сессия, Дополнение № 17* (A/61/17), пункт 216.

[3] Там же, *шестьдесят вторая сессия, Дополнение № 17* (A/62/17), пункт 195.

Содержание

Введение

1. На основе информационных и компьютерных технологий разработаны различные средства, позволяющие увязывать информацию в электронной форме с конкретными физическими или юридическими лицами, обеспечивать целостность такой информации или предоставлять лицам возможность продемонстрировать наличие у них права или разрешения на доступ к тем или иным услугам или хранилищам информации. Иногда эти функции обобщенно именуют электронными методами "удостоверения подлинности" или "подписания". Вместе с тем между понятиями электронного удостоверения подлинности и электронной подписи порой проводятся различия. Используемая при этом терминология не только страдает непоследовательностью, но и в определенной мере способна ввести в заблуждение. Применительно к бумажным документам слова "удостоверение подлинности" и "подпись" и связанные с ними действия "удостоверяющего" и "подписывающего" несут в себе не вполне идентичные оттенки смысла в разных правовых системах и связаны с функциями, не всегда соответствующими цели и назначению так называемых электронных методов "удостоверения подлинности" и "подписания". Кроме того, термин "удостоверение подлинности" иногда используется в общем смысле для обозначения любого подтверждения как авторства информации, так и ее целостности, хотя в некоторых правовых системах между этими элементами может существовать разграничение. Поэтому для того, чтобы определить рамки настоящего документа, необходимо вкратце рассмотреть существующие различия в терминологии и ее юридическом толковании.

2. В соответствии с гражданскими нормами доказывания, принятыми в системах общего права, запись или документ считаются "подлинными" при наличии доказательств того, что такой документ или запись "соответствуют тому, что утверждает в отношении них представившая их сторона"[1]. Понятие "документ" как таковое является весьма широким и обычно охватывает "все, что содержит запись информации любого вида"[2]. Это включает, например, фотоснимки надгробий и зданий[3], бухгалтерские ведомости[4], чертежи и планы[5]. Приемлемость документа в качестве доказательства подтверждается путем установления связи между ним и тем или иным лицом, местом или предметом; в некоторых системах общего права этот процесс называется "удостоверением подлинности"[6]. Распространенным, хотя и не

[1] United States of America, Federal Rules of Evidence, rule 901, subdivision (*a*): "Требование относительно удостоверения подлинности или идентификации как необходимого условия приемлемости считается выполненным при наличии доказательств, достаточных для вывода о том, что представленное соответствует утверждениям представившей стороны".

[2] United Kingdom of Great Britain and Northern Ireland, Civil Evidence Act 1995, chapter 38, section 13.

[3] *Lyell v. Kennedy* (No. 3) (1884) 27 Ch.D. 1 (United Kingdom, Chancery Division).

[4] *Hayes v. Brown* [1920] 1 K.B. 250 (United Kingdom, Law Reports, King's Bench).

[5] *J. H. Tucker & Co., Ltd. v. Board of Trade* [1955] 2 All ER 522 (United Kingdom, All England Law Reports).

[6] *Farm Credit Bank of St. Paul v. William G. Huether*, 12 April 1990 (454 N.W.2d 710, 713) (United States, Supreme Court of North Dakota, North Western Reporter).

единственным способом "удостоверения подлинности" является подписание документа, и в определенных контекстах слова "подписывать" и "удостоверять подлинность" могут использоваться в качестве синонимов[7].

3. "Подпись", в свою очередь, означает "любое имя или символ, используемые стороной с намерением придать им статус своей подписи"[8]. Имеется в виду, что цель законодательных положений, требующих подписания того или иного документа тем или иным лицом, заключается в подтверждении подлинного происхождения этого документа[9]. В "классическом" варианте подпись представляет собой имя подписавшего, написанное его собственной рукой на бумажном документе ("собственноручная" или "рукописная" подпись)[10]. Однако собственноручная подпись не является единственным возможным видом подписи. Коль скоро суды рассматривают подпись как "не более чем знак", то, если по соответствующему закону подпись не обязательно должна быть собственноручной, "достаточным является набранное печатным способом имя лица, которое должно подписать документ", либо подпись "может быть нанесена на документ штемпелем, на котором выгравировано факсимиле обычной подписи подписывающего лица", при условии представления в этих случаях доказательств того, "что изображенная на штемпеле подпись была поставлена подписывающим лицом" или что такая подпись "была признана и доведена до его понимания как исполненная от его имени, с тем чтобы скрепить ею данный конкретный документ"[11].

4. Типичные примеры юридических требований относительно подписи как условия действительности тех или иных актов в системах общего права можно найти в британском Законе об обманных действиях[12] и его зарубежных аналогах[13]. Со временем суды стали склоняться к либеральному толкованию Закона об обманных действиях, исходя из того, что установленные им жесткие требования в отношении формы были задуманы применительно к конкретным условиям[14] и что строгое применение его

---

[7] Так, в контексте новой редакции статьи 9 Единообразного торгового кодекса Соединенных Штатов "удостоверение подлинности" определяется как "A) подписание или B) проставление или иное использование символа либо полное или частичное шифрование или аналогичная обработка записи, при наличии у удостоверяющего непосредственного намерения идентифицировать соответствующее лицо и принять или признать запись".

[8] *Alfred E. Weber v. Dante De Cecco*, 14 October 1948 (1 N.J. Super. 353, 358) (United States, New Jersey Superior Court Reports).

[9] *Lobb v. Stanley* (1844), 5 Q.B. 574, 114 E.R. 1366 (United Kingdom, Law Reports, Queen's Bench).

[10] Lord Denning in Goodman v Eban [1954] QBD 550 at 56: "В современном английском языке слова о том, что документ должен быть подписан кем-либо, означают, что данное лицо должно собственноручно написать на этом документе свое имя" (United Kingdom, Queen's Bench Division).

[11] *R. v. Moore: ex parte Myers* (1884) 10 V.L.R. 322 at 324 (United Kingdom, Victorian Law Reports).

[12] Закон об обманных действиях в его первоначальном варианте был принят в Великобритании в 1677 году "для предупреждения многих мошеннических деяний, обычно подкрепляемых попытками лжесвидетельства или подстрекательством к лжесвидетельству". В XX веке большинство положений этого закона в Соединенном Королевстве были отменены.

[13] Например, в подразделе 1 раздела 2-201 Единообразного торгового кодекса Соединенных Штатов смысл Закона об обманных действиях выражен следующим образом: "За исключением случаев, предусмотренных в настоящей статье, договор купли-продажи товаров на сумму в 500 долларов или более не подлежит исполнению в исковом порядке или в порядке защиты в отсутствие какой-либо записи, достаточной для указания на то, что между сторонами был заключен договор купли-продажи, и подписанной той стороной, в адрес которой обращено исковое требование, либо ее уполномоченным агентом или посредником".

[14] "Закон об обманных действиях был принят в период, когда законодательная власть была скорее склонна к установлению жестких правил вынесения решений по конкретным делам, нежели к тому, чтобы полагаться на суд в оценке весомости доказательств, представленных по каждому делу. Это, несомненно, отчасти объяснялось тем, что в период, о котором идет речь, истец и ответчик не рассматривались как правомочные свидетели" (J. Roxborough in *Leeman v. Stocks* [1951] 1 Ch 941 at 947-8) (United Kingdom, Law

положений может приводить к необоснованному лишению договоров юридической силы[15]. Таким образом, за последние 150 лет в системах общего права произошел перенос акцента с формальных на функциональные аспекты понятия подписи[16]. Судами Англии периодически рассматривались различные вариации на эту тему: от таких простых модификаций подписи, как крест[17] или инициалы[18], до псевдонимов[19] и кодовых фраз[20], имен, набранных печатным способом[21], подписей третьих сторон[22] и каучуковых штемпелей[23]. Во всех этих случаях судам удавалось решить вопрос о действительности подписи путем проведения аналогий с рукописной подписью. Таким образом, можно констатировать, что при наличии достаточно жестких общих требований в отношении формы суды стран общего права склонялись к расширительному толкованию смысла, вкладываемого в понятия "подписи" и "удостоверения подлинности", ставя во главу угла намерения сторон, а не форму их действий.

5. Подход к "удостоверению подлинности" и "подписи" в системах гражданского права не вполне идентичен подходу, характерному для общего права. В большинстве систем гражданского права прямо соблюдается[24] или подразумевается[25] принцип свободной формы договорных обязательств частноправового характера. При этом,

---

Reports, Chancery Division) citing approval for the views of J. Cave in *Evans v. Hoare* [1892] 1 QB 593 at 597) (United Kingdom, Law Reports, Queen's Bench).

[15] Как пояснял главный судья лорд Бингхэм, "быстро стало очевидным, что решение, использованное в XVII веке для пресечения одних правонарушений, одновременно создавало условия для других: что сторона, полагавшаяся в своих расчетах и действиях на устную договоренность, которую она считала юридически обязательной, оказывалась обманутой в своих коммерческих ожиданиях, когда дело доходило до принудительного исполнения, от которого противоположная сторона успешно уклонялась, ссылаясь на отсутствие письменного меморандума или записи об этой договоренности" (*Actionstrength Limited v. International Glass Engineering*, 3 April 2003, [2003] UKHL 17 (United Kingdom, House of Lords)).

[16] Chris Reed, "What is a signature?", *Journal of Information, Law and Technology*, vol. 3, 2000, и содержащиеся в данной работе ссылки на прецедентное право; размещено по адресу http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/ (дата посещения – 5 июня 2008 года).

[17] *Baker v. Dening* (1838) 8 A&E 94 (United Kingdom, Adolphus and Ellis' Queen's Bench Reports).

[18] *Hill v. Hill* [1947] Ch 231 (United Kingdom, Chancery Division).

[19] *Redding, in re* (1850) 14 Jur 1052, 2 Rob. Ecc. 339 (United Kingdom, Jurist Reports and Robertson's Ecclesiastical Reports).

[20] *Cook, In the Estate of (Deceased) Murison v. Cook and Another* [1960] 1 All ER 689 (United Kingdom, All England Law Reports).

[21] *Brydges v. Dicks* (1891) 7 TLR 215 (цитируется по Brennan v. Kinjella Pty Ltd., Supreme Court of New South Wales, 24 June 1993, 1993 NSW LEXIS 7543, 10). Вопрос о машинописных подписях также рассматривался в Newborne v. Sensolid (Great Britain), Ltd. [1954] 1 QB 45 (United Kingdom, Law Reports, Queen's Bench).

[22] *France v. Dutton*, Queen's Bench, 24 April 1891 [1891] 2 Q.B. 208 (United Kingdom, Law Reports, Queen's Bench).

[23] *Goodman v. J. Eban Ltd.*, [1954] 1 Q.B. 550, цитируется по *Lazarus Estates, Ltd. v. Beasley*, Court of Appeal, 24 January 1956 ([1956] 1 QB 702); *London County Council v. Vitamins, Ltd., London County Council v. Agricultural Food Products, Ltd.*, Court of Appeal, 31 March 1955 [1955] 2 QB 218 (United Kingdom, Law Reports, Queen's Bench).

[24] Это признается, например, в пункте 1 статьи 11 Кодекса обязательств Швейцарии. Аналогичным образом, согласно статье 215 Гражданского кодекса Германии, соглашения могут быть признаны недействительными лишь в случаях, когда они не соответствуют форме, предписанной законом или согласованной сторонами. За исключением конкретных случаев такого рода принято считать, что договоры, относящиеся к сфере частного права, не подпадают под какие-либо конкретные требования в отношении формы. Когда же та или иная форма прямо предписана законом, его положения подлежат строгому толкованию.

[25] Во Франции, например, свобода формы вытекает из основных положений Гражданского кодекса, регулирующих заключение договоров. Согласно статье 1108 Гражданского кодекса Франции, условиями действительности договора являются согласие лица, принимающего обязательства, его правоспособность, наличие конкретного предмета и законных мотивов; при выполнении этих условий договор приобретает "законную силу для сторон" согласно статье 1134. Аналогичная норма установлена статьями 1258 и 1278 Гражданского кодекса Испании. Такое же правило, хотя и не столь прямо, применяется в Италии (см. Гражданский кодекс Италии, статьи 1326 и 1350).

однако, различные правовые системы предусматривают более или менее обширный перечень исключений. Это означает, что составление договоров в "письменной форме" и наличие "подписи", как правило, в целом не обязательны для придания таким договорам юридической действительности и исковой силы. Вместе с тем в некоторых системах гражданского права для подтверждения содержания договоров, не относящихся к коммерческой сфере, в принципе требуется письменное свидетельство[26]. В отличие от систем общего права, в системах гражданского права правила доказывания обычно толкуются достаточно жестко. Гражданско-правовые нормы доказывания в большинстве случаев устанавливают иерархию доказательств, используемых для подтверждения содержания гражданских и торговых договоров. Наивысшее место в этой иерархии занимают документы, выданные публичными властями; за ними следуют подлинные документы частного характера. Нередко иерархия построена таким образом, что понятия "документ" и "подпись", будучи формально самостоятельными, становятся фактически неотделимыми друг от друга[27]. В то же время в других системах гражданского права между понятием "документ" и наличием "подписи" проводится позитивная связь[28]. Это не означает, что неподписанный документ вообще не может представлять какой-либо доказательственной ценности, однако в отношении такого документа не устанавливается никаких конкретных презумпций, и он, как правило, рассматривается в качестве "первой ступени доказывания"[29]. Понятие "удостоверение подлинности" в большинстве систем гражданского права трактуется в том довольно узком смысле, что подлинность документа проверена и подтверждена компетентным публичным органом или нотариусом. В гражданском процессе вместо этого обычно используется понятие "подлинника" документов.

6. Как и в странах общего права, в системах гражданского права "классическим" образцом подписи считается собственноручная подпись. Что касается подписи как таковой, то в некоторых правовых системах, невзирая на в целом формалистический подход к доказательствам, могут допускаться различные ее эквиваленты, включая механическое воспроизведение подписи[30]. В то же время в других правовых системах, допускающих использование механических подписей при коммерческих сделках[31],

---

[26] Согласно статье 1341 Гражданского кодекса Франции письменного подтверждения требуют договоры на сумму, превышающую определенный минимум, однако статья 109 Торгового кодекса при этом допускает различные виды доказательств, не устанавливая между ними какой-либо иерархии. В связи с этим французский Кассационный суд в 1892 году признал общий принцип свободы доказывания в коммерческих делах (Cass. civ. 17 mai 1892, DP 1892.1.604; цитируется по Luc Grynbaum, *Preuve, Répertoire de droit commercial Dalloz*, Juin 2002, sections 6 et 11).

[27] Например, по германским законам подпись не входит в число необходимых составляющих понятия "документа" (Urkunde) (Gerhard Lüke and Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozessordnung* (Munich, Beck, 1992), section 415, No. 6). Тем не менее иерархия документальных доказательств, предусмотренная в статьях 415, 416 и 419 Гражданско-процессуального кодекса Германии, устанавливает очевидную связь между документом и подписью. Так, статья 416, посвященная доказательственной силе частных документов (Privaturkunden), гласит, что частные документы являются "полноценным доказательством" содержащейся в них информации при условии, что они подписаны их автором или заверены нотариусом. Поскольку о документах без подписи при этом не упоминается, они, очевидно, подпадают под категорию неполноценных (т. е. искаженных или дефектных) документов, доказательственная сила которых "свободно определяется" судом (Гражданско-процессуальный кодекс Германии, статья 419).

[28] Так, во Франции подпись считается "обязательным элементом" частного документа (*actes sous sein privé*) (см. *Recueil Dalloz, Preuve*, No. 638).

[29] Таким образом обстоит дело, например, во Франции (см. *Recueil Dalloz, Preuve*, Nos. 657-658).

[30] Авторы комментариев к Гражданско-процессуальному кодексу Германии отмечают, что требование собственноручной подписи исключало бы любые виды механически проставляемых символов, что идет вразрез с повседневной практикой и техническим прогрессом (см. Gerhard Lüke and Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozessordnung* (Munich, Beck, 1992), section 416, No. 5).

[31] Например, во Франции (см. *Recueil Dalloz, Preuve*, No. 662).

договоры остальных видов до появления компьютерных технологий по-прежнему должны были скрепляться собственноручной подписью[32]. Поэтому можно сказать, что в рамках общего принципа свободы формы при заключении коммерческих договоров в странах гражданского права обычно применяются строгие нормы оценки доказательственной силы частных документов и могут не признаваться документы, подлинность которых невозможно непосредственно установить по подписи.

7. Из вышесказанного следует, что понятия подписи и удостоверения подлинности не только не имеют единого толкования в разных правовых системах, но и выполняют в них неодинаковые функции. И все же, невзирая на эти расхождения, можно выделить и ряд в целом совпадающих элементов. Юридический смысл понятий "подлинность" и "удостоверение подлинности" обычно связывают с подлинным происхождением документа или записи, т. е. с тем, является ли документ "подлинником" содержащейся в нем информации в той форме, в которой она была зафиксирована, без каких-либо изменений. Что касается подписей, то применительно к бумажным документам они выполняют три основные функции: позволяют идентифицировать подписавшее лицо (функция идентификации), со всей определенностью подтверждают его личное участие в процессе подписания (доказательственная функция) и устанавливают связь подписавшего лица с содержанием документа (атрибутивная функция). Можно говорить и о других функциях подписей, зависящих от характера подписанного документа. Например, подпись может подтверждать намерение стороны считать себя связанной положениями подписанного договора; намерение лица признать за собой авторство того или иного текста (являясь тем самым проявлением осведомленности о возможных юридических последствиях акта подписания); намерение лица связать себя с содержанием документа, написанного кем-то другим; а также тот факт, что в соответствующий момент данное лицо находилось в определенном месте[33,34].

8. Следует отметить, однако, что, хотя из наличия подписи часто делается вывод о подлинности документа, подпись сама по себе не "удостоверяет" его подлинность. При определенных обстоятельствах эти два элемента могут даже отделяться друг от друга. Так, подпись может оставаться "подлинной" несмотря на последующее изменение документа, под которым она была поставлена. Аналогичным образом, документ может быть "подлинным", даже если он содержит поддельную подпись. Кроме того, полномочия на участие в сделке и фактические данные о личности того или иного лица, хотя они и важны для установления подлинности документа или подписи, не могут быть вполне доказаны подписью как таковой, равно как и сами не являются достаточным подтверждением подлинного происхождения документа или подписи.

9. Это подводит к еще одному аспекту рассматриваемого вопроса. О какой бы правовой традиции ни шла речь, нигде – за очень редкими исключениями – подпись не является самодостаточной. Ее правовые последствия зависят от связи между

---

[32] Так, во Франции подпись не разрешалось заменять крестом или другими знаками, а также печатью или отпечатками пальцев (см. *Recueil Dalloz, Preuve*, No. 665).

[33] *Типовой закон ЮНСИТРАЛ об электронных подписях и Руководство по принятию, 2001 год* (издание Организации Объединенных Наций, в продаже под № R.02.V.8), часть вторая, пункт 29; размещено по адресу http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html (дата посещения – 6 июня 2008 года).

[34] Данный анализ уже был положен в основу критериев функциональной эквивалентности в статье 7 принятого ранее *Типового закона ЮНСИТРАЛ об электронной торговле и Руководства по принятию от 1996 года с дополнительной статьей 5 bis, принятой в 1998 году* (издание Организации Объединенных Наций, в продаже под № R.99.V.4; размещено по адресу http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html (дата посещения – 6 июня 2008 года).

подписью и лицом, которое может быть признано в качестве ее автора. На практике личность подписавшего можно проверить разными способами. Если все стороны одновременно присутствуют в одном и том же месте, они могут просто узнать друг друга в лицо; при телефонных переговорах собеседника можно узнать по голосу, и так далее. Многие подобные вещи происходят повседневно и не регулируются конкретными правовыми нормами. Однако в случаях, когда переговоры между сторонами ведутся посредством переписки или когда подписанные документы последовательно препровождаются одними участниками договорных отношений другим, могут практически отсутствовать способы доказательства того, что проставленные на некоем документе символы действительно исполнены рукой лица, с именем которого они якобы связаны, равно как и того, что подпись, которая должна налагать обязательства на конкретное лицо, могла быть создана только лицом, имеющим на это необходимые полномочия.

10. Таким образом, хотя собственноручная подпись и представляет собой хорошо известный способ "удостоверения подлинности", вполне подходящий для документации о сделках, передаваемой между знакомыми друг другу сторонами, во многих ситуациях коммерческого и административного характера подпись не обеспечивает максимальной надежности. Лицо, полагающееся на подписанный документ, часто не знает имен тех, кто обладает правом подписи, и не имеет в своем распоряжении образцов подписей для сравнения[35]. Это особенно относится ко многим документам, на которые полагаются зарубежные участники международных торговых сделок. Даже при наличии образца подписи уполномоченного лица выявить тщательную подделку может быть под силу лишь эксперту. При обработке больших количеств документов сверка подписей иногда не производится вообще, кроме как в случае особо важных сделок. Одной из первооснов международных деловых связей является доверие.

11. В большинстве правовых систем предусмотрены специальные процедуры или требования, направленные на повышение надежности собственноручных подписей. Соблюдение некоторых процедур является обязательным для придания юридической силы некоторым документам. Процедуры также могут носить факультативный характер и использоваться сторонами, желающими предотвратить возможные споры относительно подлинности тех или иных документов. Типичными примерами являются:

a) *Нотариальное заверение*. При определенных обстоятельствах акт подписания имеет особое формальное значение благодаря повышенной степени доверия, которая обеспечивается путем соблюдения специальной церемонии. Это относится, например, к нотариальному заверению, когда нотариус удостоверяет подлинность подписи под юридическим документом, для чего во многих случаях необходима физическая явка подписывающего документ лица к нотариусу;

b) *Засвидетельствование*. Засвидетельствованием называется наблюдение за подписанием юридического документа другим лицом и добавление к нему

[35] В некоторых областях права признается как изначальная ненадежность собственноручных подписей, так и практическая нецелесообразность жесткой увязки действительности юридических актов с соблюдением строгих требований в отношении формы; при этом в ряде случаев допускается даже возможность сохранения юридической силы документа, подпись под которым была подделана. Так, например, статья 7 Единообразного закона о переводном и простом векселях, содержащегося в приложении к Конвенции, устанавливающей Единообразный закон о переводном и простом векселях, подписанной в Женеве 7 июня 1930 года, гласит: "Если на переводном векселе имеются подписи лиц, не способных обязываться по переводному векселю, подписи подложные, подписи вымышленных лиц или подписи, которые по всякому иному основанию не могут обязывать тех лиц, которые их поставили или от имени которых он подписан, то подписи других лиц все же не теряют силы" (League of Nations, *Treaty Series*, vol. CXLIII, No. 3313).

своей подписи в качестве свидетеля. Цель засвидетельствования заключается в сохранении доказательств подписания. Ставя свою подпись, свидетель подтверждает факт подписания документа лицом, проделавшим это на его глазах. Засвидетельствование не означает поручительства за достоверность или правдивость документа. Свидетель может быть вызван для дачи показаний об обстоятельствах, сопутствовавших подписанию[36];

c) *Печати*. Практика использования печатей в дополнение к подписям или вместо них распространена достаточно широко, особенно в некоторых регионах мира[37]. Подпись или оттиск печати могут, например, служить подтверждением личности подписавшего, а также подтверждением того, что подписавший выразил согласие связать себя данным соглашением, причем сделал это добровольно; того, что данная версия документа является окончательной и полной; или того, что соответствующая информация не была изменена после подписания[38]. Они также могут оказывать предостерегающее воздействие на автора подписи, указывая на то, что совершаемым действиям имеется в виду придать юридическую силу.

12. Помимо этих особых ситуаций собственноручные подписи веками используются как во внутренних, так и в международных коммерческих сделках в отсутствие какого-либо специально предназначенного для них правового режима или свода практических правил. Надежность подписей в каждом конкретном случае оценивается адресатами или держателями подписанных документов исходя из степени доверия к подписавшему. На практике в подавляющем большинстве случаев заключение письменных международных контрактов – если они вообще заключаются в "письменной" форме – не обязательно сопровождается какими-либо особыми формальностями или процедурами удостоверения подлинности.

13. Трансграничное использование подписанных документов становится более сложным делом, когда в него вовлекаются публичные власти, поскольку иностранные органы при получении таких документов, как правило, требуют того или иного подтверждения личности и полномочий подписавшего. Эти требования традиционно выполняются посредством процедур так называемой "легализации", при которой подписи ставятся во внутренних документах, подлинность которых удостоверяется дипломатическими учреждениями для их использования за границей, и наоборот, консульские или дипломатические представители страны, где предполагается использовать документы, могут удостоверять подлинность подписей иностранных публичных органов, поставленных в стране их происхождения. Во многих случаях консульские или дипломатические представители удостоверяют лишь подписи отдельных высоких инстанций страны, где выдаются документы, – что влечет необходимость нескольких уровней признания подписей, если документ изначально выдан должностным лицом низового уровня, – или же требуют предварительного заверения подписей нотариусом в стране происхождения документов. Чаще всего легализация представляет собой громоздкую, длительную и дорогостоящую процедуру. В связи с этим была разработана Конвенция, отменяющая требование

[36] Adrian McCullagh, Peter Little and William Caelli, "Electronic signatures: understand the past to develop the future", *University of New South Wales Law Journal*, vol. 21, No. 2 (1998); см. раздел D главы III о концепции засвидетельствования.

[37] Печати используются в нескольких странах Восточной Азии, таких как Китай и Япония.

[38] Mark Sneddon, "Legislating to facilitate electronic signatures and records: exceptions, standards and the impact of the statute book", *University of New South Wales Law Journal*, vol. 21, No. 2 (1998); см. часть 2 главы II "Программные цели требований в отношении письменной формы и подписи".

легализации иностранных официальных документов[39], подписанная в Гааге 5 октября 1961 года, в соответствии с которой существовавшие до этого требования были заменены упрощенной стандартной формой ("апостилем"), используемой в государствах – участниках Конвенции для заверения некоторых официальных документов[40]. Правом приостановления апостиля обладает только компетентный орган, назначенный тем государством, где составлен данный официальный документ. Апостили удостоверяют подлинность подписи, качества, в котором выступало лицо, подписавшее документ, а также, в надлежащих случаях, подлинность скрепляющей документ печати или штемпеля, но не касаются содержания самого документа.

14. Как указывалось выше, во многих правовых системах коммерческие договоры не обязательно должны быть оформлены в виде документов или подтверждены письменно, чтобы считаться действительными. Даже при наличии письменного документа подпись не всегда необходима для того, чтобы договор имел обязательную силу для сторон. Безусловно, в случаях, когда согласно закону договоры должны составляться в письменной форме или подписываться, невыполнение этих требований лишает договор юридической силы. Более важными, чем требования в отношении формы для целей признания действительности договоров, вероятно, являются требования в отношении формы для целей доказывания. Трудность доказывания устных договоренностей представляет собой одну из главных причин, по которым коммерческие договоры фиксируются в письменных документах или в форме переписки – даже в случаях, когда устная договоренность считалась бы действительной и без этого. Стороны, чьи обязательства документированы в письменной форме за подписью, едва ли смогут с успехом отрицать содержание принятых ими обязательств. Строгие правила относительно документальных доказательств обычно рассчитаны на то, что их соблюдение будет повышать надежность соответствующих документов, что, как правило, рассматривается как способ увеличения правовой определенности. В то же время чем более усложняются требования к доказательствам, тем легче сторонам становится ссылаться на формальные отклонения от этих требований для отрицания действительности или исковой силы обязательств, которые они более не намерены исполнять, например, потому, что договор перестал отвечать их коммерческим интересам. Поэтому, стремясь к повышению надежности обмена электронными сообщениями, следует учитывать риск предоставления недобросовестным коммерсантам удобного способа уклоняться от добровольно принятых ими юридических обязательств. Нахождение сбалансированного подхода на основе норм и стандартов, признанных на международном уровне и пригодных для трансграничного применения, является одной из главных задач выработки политики в области электронной торговли. Цель настоящего документа – облегчить законодательным и директивным органам выявление основных правовых проблем, связанных с международным использованием электронных методов подписания и удостоверения подлинности, и анализ возможных путей их решения.

---

[39] United Nations, *Treaty Series*, vol. 527, No. 7625.

[40] К таким документам относятся: документы, исходящие от органа или должностного лица, связанного с судом или трибуналом данного государства (включая документы, выданные административным, конституционным или церковным судом или трибуналом, государственным прокурором, секретарем суда или судебным исполнителем); административные документы; нотариальные акты; а также официальные регистрационные пометки, которыми сопровождаются документы, подписанные частными лицами в личном качестве.

Часть первая

Электронные методы подписания и удостоверения подлинности

Содержание

I. Определение и методы электронного подписания и удостоверения подлинности

A. Общие замечания относительно терминологии

15. Термины “электронное удостоверение подлинности” и “электронная подпись” используются для обозначения различных методов, которые предлагаются на рынке в настоящее время или находятся в стадии разработки и целью которых является воспроизведение в электронной среде некоторых или всех функций, считающихся характерными для собственноручных подписей или иных традиционных методов идентификации.

16. За прошедшие годы разработан целый ряд различных способов создания электронных подписей. Все они предназначены для удовлетворения разных потребностей, рассчитаны на обеспечение разной степени надежности и связаны с разными техническими требованиями. Электронные методы подписания и удостоверения подлинности можно разделить на три категории: методы, основанные на информации, известной пользователю или получателю (например, пароли и персональные идентификационные номера (ПИНы)), методы, основанные на физических особенностях пользователя (например, биометрия), и методы, основанные на наличии у пользователя того или иного предмета (например, магнитной карты с записанными на ней кодами или иной информацией)[41]. К четвертой категории можно отнести различные типы методов подписания и удостоверения подлинности, которые, не подпадая ни под одну из вышеперечисленных категорий, также могут использоваться для указания на составителя электронного сообщения (такие, как факсимиле собственноручной подписи или имя, набранное в конце электронного сообщения). Среди используемых на сегодняшний день технологий – цифровые подписи в рамках инфраструктуры публичных ключей (ИПК), биометрические устройства, ПИНы, пароли, назначаемые пользователям или выбираемые ими самостоятельно, сканированные изображения собственноручных подписей, подписи, выполняемые цифровой ручкой, а также поля “ОК” или “Я согласен”, которые можно пометить курсором на дисплее[42]. Все большую популярность приобретают комбинированные решения, основанные на сочетании разных технологий, например такие, как использование паролей в комбинации с протоколами безопасности на транспортном уровне/протоколами защищенных соединений (TSL/SSL), обеспечивающими шифрование одновременно с помощью комбинации публичных и симметричных ключей. Особенности основных методов, используемых на сегодняшний день, описываются в тексте ниже (см. пункты 25–66).

---

[41] См. Доклад Рабочей группы по электронной торговле о работе ее тридцать второй сессии (Вена, 19–30 января 1998 года) (A/CN.9/446, пункты 91 и далее).

[42] *Типовой закон ЮНСИТРАЛ об электронных подписях*..., часть вторая, пункт 33.

17. Как часто происходит в подобных случаях, соответствующая технология была разработана задолго до того, как данная область попала в сферу правового регулирования. Образовавшийся в результате этого разрыв между правовыми нормами и технической реальностью становится причиной несоответствий не только в уровнях экспертных знаний, но и в использовании терминов. Выражения, традиционно имевшие конкретную коннотацию в рамках национальных законов, стали использоваться для описания электронных технологий, функции которых не всегда совпадают с функциями или характеристиками, присущими закрепленным за этими выражениями правовым понятиям. Как было показано выше (см. пункты 7–10), понятия "удостоверение подлинности", "подлинность", "подпись" и "идентификация", хотя они и являются в некоторых контекстах тесно взаимосвязанными, не тождественны друг другу и не взаимозаменяемы. Специалисты по информационным технологиям, для которых смысл соответствующих терминов определяется прежде всего задачами обеспечения безопасности сетей, не всегда оперируют теми же категориями, что и авторы правовой литературы.

18. В некоторых случаях слова "электронное удостоверение подлинности" употребляются применительно к методам, которые, в зависимости от обстоятельств их использования, могут включать такие различные элементы, как идентификация личности, подтверждение полномочий того или иного лица (как правило, на совершение действий от имени другого физического или юридического лица) или его прерогатив (например, членства в организации или подписки на услуги), либо удостоверение целостности информации. Если в одних случаях речь идет только об идентификации[43], то в других – также и о полномочиях[44] либо о сочетании всех или части этих элементов[45].

19. Термин "электронное удостоверение подлинности" не употребляется ни в Типовом законе ЮНСИТРАЛ об электронной торговле[46], ни в Типовом законе ЮНСИТРАЛ об электронных подписях[47] ввиду различных значений понятия

---

[43] Например, Технологическое управление Министерства торговли США определяет электронное удостоверение подлинности как "процесс обеспечения уверенности в отношении идентификационных данных пользователей, введенных электронным способом в информационную систему" (United States, Department of Commerce, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-63, version 1.0.2 (Gaithersburg, Maryland, April 2006), размещено по адресу http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf (дата посещения – 5 июня 2008 года)).

[44] Например, правительством Австралии разработана система электронного удостоверения подлинности, в рамках которой электронное удостоверение подлинности определяется как "процесс обеспечения определенной степени уверенности в отношении подлинности или действительности той или иной информации, представляемой при совершении сделок в режиме онлайн или по телефону. Это способствует повышению доверия к сделкам в режиме онлайн, позволяя участвующим в них сторонам так или иначе удостовериться в законности их операций. Речь может идти о такой информации, как личные данные, сведения о профессиональной квалификации или делегирование полномочий на совершение сделок" (Australia, Department of Finance and Administration, *Australian Government e-Authentication Framework: An Overview* (Commonwealth of Australia, 2005), размещено по адресу http://www.agimo.gov.au/infrastructure/authentication/agaf_b/overview/introduction#e-authentication (дата посещения – 5 июня 2008 года)).

[45] Так, в подготовленных правительством Канады Принципах электронного удостоверения подлинности удостоверение подлинности определяется как "процесс подтверждения сведений об участниках обмена электронными сообщениями или целостности сообщений". Сведения, в свою очередь, определяются как "информация о личности, привилегиях и правах участника или другого удостоверяемого субъекта" (Canada, Industry Canada, *Principles for Electronic Authentication: a Canadian Framework* (Ottawa, May 2004), размещено по адресу http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html (дата посещения – 5 июня 2008 года)).

[46] *Типовой закон ЮНСИТРАЛ об электронной торговле...*

[47] *Типовой закон ЮНСИТРАЛ об электронных подписях...*

"удостоверение подлинности" в разных правовых системах и во избежание путаницы с теми или иными конкретными процедурами или требованиями в отношении формы. Вместо этого в Типовом законе об электронной торговле используется понятие "подлинная форма", на основе которого определяются критерии функциональной эквивалентности "подлинной" электронной информации. Согласно статье 8 Типового закона, если законодательство требует, чтобы информация предоставлялась или сохранялась в ее подлинной форме, это требование считается выполненным с помощью сообщения данных, если:

a) имеются "надежные доказательства целостности информации с момента, когда она была впервые подготовлена в ее окончательной форме в виде сообщения данных или в каком-либо ином виде"; и

b) при необходимости предъявления информации эта информация "может быть продемонстрирована лицу, которому она должна быть предъявлена".

20. С учетом проводимого в большинстве правовых систем различия между подписью (или печатями, если они используются вместо подписи) как средством "удостоверения подлинности", с одной стороны, и "подлинностью" как качеством, присущим документу или записи, с другой, в обоих типовых законах понятие "подлинник" дополнено понятием "подпись". В подпункте *a*) статьи 2 Типового закона ЮНСИТРАЛ об электронных подписях электронная подпись определяется как данные в электронной форме, которые содержатся в сообщении данных, приложены к нему или логически ассоциируются с ним и которые могут быть использованы для "идентификации подписавшего" в связи с сообщением данных и "указания на то, что подписавший согласен с информацией, содержащейся в сообщении данных".

21. Определению "электронной подписи" в текстах ЮНСИТРАЛ намеренно придан широкий характер, с тем чтобы под него подпадали все существующие или будущие методы "электронного подписания". При условии, что используемые методы являются "настолько надежными, насколько это соответствует цели, для которой сообщение данных было подготовлено или передано, с учетом всех обстоятельств, включая любые соответствующие договоренности"[48], они должны рассматриваться как отвечающие юридическим требованиям в отношении подписи. Тексты ЮНСИТРАЛ, касающиеся электронной торговли, как и многие другие законодательные тексты, основаны на принципе нейтральности с точки зрения технологии и поэтому призваны охватить все формы электронных подписей. Таким образом, под сформулированное ЮНСИТРАЛ определение электронной подписи подпадает весь спектр методов "электронного подписания" – от наиболее надежных, таких как применение криптографических систем подтверждения подписей, увязанных со схемами ИПК (одна из распространенных форм "цифровой подписи" (см. пункты 25–53)), до методов, обеспечивающих меньшую степень надежности, таких как незашифрованные коды или пароли. Так, имя автора, просто набранное в конце текста сообщения, пересылаемого по электронной почте, т. е. самая распространенная форма электронной "подписи", выполняет функцию правильной идентификации автора письма во всех случаях, когда столь низкая степень надежности разумно приемлема.

22. Остальные положения типовых законов ЮНСИТРАЛ не касаются вопросов, связанных с контролем доступа и проверкой идентификационных данных. Это обусловлено также тем, что применительно к бумажным документам подписи могут рассматриваться как указание на ту или иную личность, при том что они в любом

[48] *Типовой закон ЮНСИТРАЛ об электронной торговле...*, статья 7, подпункт 1 *b*).

случае являются атрибутом конкретной личности. Что касается Типового закона ЮНСИТРАЛ об электронной торговле, то в нем говорится об условиях, при которых адресат сообщения данных вправе исходить из того, что сообщение действительно составлено лицом, указанным в качестве его составителя. Так, согласно статье 13 Типового закона, в отношениях между составителем и адресатом сообщение данных считается сообщением данных составителя, если оно было отправлено лицом, "которое имело полномочия действовать от имени составителя в отношении этого сообщения данных", или "информационной системой, запрограммированной составителем или от его имени функционировать в автоматическом режиме". В отношениях между составителем и адресатом адресат имеет право считать, что сообщение данных является сообщением данных составителя, и действовать исходя из этого предположения, если *a*) для того чтобы установить, что сообщение данных является сообщением данных составителя, "адресат надлежащим образом применил процедуру, предварительно согласованную с составителем для этой цели" или *b*) сообщение данных, полученное адресатом, явилось результатом действий лица, отношения которого с составителем или любым представителем составителя дали такому лицу возможность получить доступ к способу, используемому составителем для идентификации сообщений данных как своих собственных. В целом эти правила позволяют стороне делать вывод относительно личности какой-либо иной стороны, независимо от того, было ли сообщение "подписано" электронным способом, а также от того, может ли метод, использованный для атрибуции сообщения его составителю, действительным образом использоваться для целей "подписи". Это соответствует современной практике, связанной с использованием бумажных документов. Опознание того или иного лица по голосу, внешности или документам, удостоверяющим личность (например, национальному паспорту), может быть достаточным для вывода о том, что это лицо является тем, за кого оно себя выдает, для целей обмена сообщениями с данным лицом, но в большинстве правовых систем не может быть приравнено к "подписи" этого лица.

23. Наряду с возможностью недоразумений из-за несовпадения технических и правовых аспектов использования терминологии применительно к бумажным документам и электронным сообщениям, различные уже упоминавшиеся методы (см. пункт 16, выше, и, более подробно, пункты 24–66, ниже) могут применяться для разных целей и выполнять разные функции, в зависимости от контекста. Например, пароли или коды могут использоваться не только для "подписания" электронного документа, но и для получения доступа к сети, базе данных или другой электронной службе, во многом аналогично тому, как ключ используют для отпирания сейфа или дверного замка. Однако, если в первом случае пароль служит для установления личности, то во втором он выполняет функцию указания на полномочия, которые, хотя они обычно закреплены за конкретным лицом, могут быть переданы и кому-то другому, или подтверждения таких полномочий. В случае с цифровыми подписями неадекватность существующей терминологии еще более очевидна. Согласно широко распространенному представлению, цифровая подпись является одной из технологий "подписания" электронных документов. Однако с юридической точки зрения называть цифровой "подписью" применение асимметричной криптографии для удостоверения подлинности по меньшей мере сомнительно, поскольку речь в данном случае идет о функциях, выходящих за рамки традиционных функций собственноручной подписи. Цифровая подпись дает возможность как "проверять подлинность электронных сообщений", так и "гарантировать целостность их содержания". Кроме того, технология цифровой подписи позволяет не только устанавливать происхождение или целостность информации применительно к тем или иным лицам, как это

требуется при подписании, но и удостоверять подлинность, например, серверов, вебсайтов, программного обеспечения или любых других данных, распространяемых или хранящихся в цифровом формате, благодаря чему электронные подписи могут применяться намного шире, чем просто в качестве электронного аналога собственноручных подписей[49].

B. Основные методы электронного подписания и удостоверения подлинности

24. Для целей данного изложения будут рассмотрены четыре основных метода подписания и удостоверения подлинности: цифровые подписи, биометрические методы, использование паролей и комбинированных методов, а также сканированные подписи или подписи, введенные с клавиатуры.

1. Цифровые подписи, проставляемые при помощи криптографии с использованием публичных ключей

25. "Цифровой подписью" называются технологические решения на основе асимметричной криптографии, именуемые также системами шифрования с публичным ключом, позволяющие обеспечить подлинность электронных сообщений и гарантировать неприкосновенность содержания этих сообщений. Существует множество различных видов цифровых подписей, включая подписи, ошибка в проставлении которых останавливает совершение операций, "слепые" подписи и неоспоримые цифровые подписи.

a) Технические понятия и терминология

i) *Криптография*

26. Цифровые подписи создаются и проверяются с помощью криптографии – отрасли прикладной математики, позволяющей преобразовывать сообщения в кажущуюся непонятной форму и обратно в первоначальную форму. При проставлении цифровых подписей применяется метод, который известен как криптография с использованием публичных ключей и который часто основывается на применении алгоритмических функций для создания двух разных, но математически соотносящихся "ключей" (т. е. больших чисел, выведенных путем применения ряда математических формул к простым числам)[50]. Один ключ используется для создания цифровой подписи или преобразования данных в кажущуюся непонятной форму, а другой – для проверки подлинности цифровой подписи или для восстановления

[49] Babette Aalberts and Simone van der Hof, Digital Signature Blindness: *Analysis of Legislative Approaches toward Electronic Authentication* (November 1999), p. 8; размещено по адресу http://rechten.uvt.nl/simone/Digsigbl.pdf (дата посещения – 5 июня 2008 года).

[50] Вместе с тем следует отметить, что рассматриваемое здесь понятие криптографии с использованием публичных ключей не обязательно подразумевает применение алгоритмов, основывающихся на простых числах. В настоящее время используются или разрабатываются и другие математические методы, такие как криптосистемы на основе эллиптических кривых, которые часто считаются обеспечивающими высокую степень защиты данных при значительно меньшей длине используемых ключей.

сообщения в его первоначальном виде[51]. Компьютерное оборудование и программное обеспечение, использующие два таких ключа, часто совокупно именуются "криптосистемами" или, более конкретно, "асимметрическими криптосистемами", если в них применяются асимметричные алгоритмы.

ii) *Публичные и частные ключи*

27. Взаимодополняющие ключи для цифровой подписи называются "частным ключом", используемым только подписывающим лицом, которое создает с его помощью цифровую подпись и должно держать этот ключ в секрете, и "публичным ключом", который обычно известен более широко и используется полагающейся стороной для проверки подлинности цифровой подписи. Частный ключ может быть записан на интеллектуальной карточке либо доступен через персональный идентификационный номер (ПИН) или биометрическое идентификационное устройство, например определитель отпечатков пальцев. Если подлинность цифровых подписей конкретного лица должна проверяться многими людьми, то публичный ключ должен быть доступен всем этим людям или распространен среди них, например, путем приложения к подписям соответствующих сертификатов или иным способом, обеспечивающим, чтобы эти сертификаты могли быть получены только полагающимися сторонами и теми, кто должен проверять подлинность подписей. Если асимметрическая криптосистема разработана и реализована надежно, то даже несмотря на то, что ключи одной пары математически соотносятся друг с другом, определить частный ключ на основании публичного ключа практически невозможно. Наиболее распространенные алгоритмы кодирования с помощью публичных и частных ключей основаны на важной особенности больших простых чисел: если путем перемножения двух таких чисел получено некое новое число, то определить по нему эти два исходных числа – очень трудная задача, требующая больших затрат времени[52]. Таким образом, хотя знать публичный ключ того или иного подписавшего лица и использовать этот ключ для проверки подлинности подписей могут многие, это не дает им возможности определить соответствующий частный ключ и подделывать с его помощью цифровые подписи.

---

[51] Хотя применение криптографии является одной из основных особенностей цифровых подписей, сам факт использования цифровой подписи для удостоверения подлинности сообщения, содержащего информацию в цифровой форме, не следует путать с более общим применением криптографии в целях обеспечения конфиденциальности. Криптографические методы обеспечения конфиденциальности заключаются в кодировании электронного сообщения, с тем чтобы только его составитель и адресат были в состоянии его прочесть. В ряде стран применение криптографии для обеспечения конфиденциальности ограничивается законом по соображениям публичного порядка, которые могут включать соображения национальной обороны. Однако применение криптографии в целях удостоверения подлинности путем создания цифровой подписи не обязательно предполагает кодирование какой-либо информации для обеспечения ее конфиденциальности при передаче сообщений, поскольку криптографическая цифровая подпись может быть всего лишь добавлена к незакодированному сообщению.

[52] В некоторых существующих стандартах используется понятие "невычисляемости", под которым имеется в виду предполагаемая необратимость этого процесса, т. е. надежда на то, что секретный частный ключ пользователя невозможно определить на основании его публичного ключа. «"Невычисляемость" является относительным понятием и определяется исходя из ценности защищаемых данных, дополнительных компьютерных ресурсов, необходимых для их защиты, срока, в течение которого их необходимо защищать, а также материальных затрат и времени, необходимых для взлома защиты данных, – причем эти факторы оцениваются как на текущий момент, так и с учетом будущего технического прогресса» (American Bar Association, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (Chicago, American Bar Association, 1 August 1996), p. 9, note 23; размещено по адресу http://www.abanet.org/scitech/ec/isc/dsgfree.html (дата посещения – 4 июня 2008 года)).

iii) *Функция хеширования*

28. Помимо генерирования пар ключей при создании цифровых подписей и проверке их подлинности используется еще один основополагающий процесс, обычно именуемый "функцией хеширования". Функция хеширования представляет собой математическую процедуру, основанную на использовании алгоритма, который создает цифровое отображение или сжатую форму сообщения (часто называемую "резюме", или "отпечатком" сообщения) в виде "величины хеширования" или "результата хеширования" стандартной длины; обычно она намного короче самого сообщения, но по содержанию может быть отнесена только к нему. Любое изменение в сообщении неизбежно дает иной результат хеширования, если применяемая функция хеширования не изменилась. При использовании надежной функции хеширования, иногда именуемой "функцией одностороннего хеширования", восстановить оригинал сообщения по его величине хеширования практически невозможно. Еще одна важнейшая особенность функций хеширования заключается в том, что практически невозможно также найти другой бинарный объект (кроме объекта, использованного для получения данного резюме), резюме которого было бы идентичным. Соответственно, функции хеширования позволяют программному обеспечению для создания цифровых подписей оперировать меньшим и более предсказуемым количеством данных, сохраняя при этом надежно доказуемую связь подписи с исходным содержанием сообщения и тем самым обеспечивая эффективную гарантию того, что в сообщение не вносились изменения после его подписания в цифровой форме.

iv) *Создание цифровой подписи*

29. Чтобы подписать какой-либо документ или любой другой элемент информации, подписывающее лицо сначала определяет точные границы того, что предстоит подписать. Затем с помощью программного обеспечения, использующего функцию хеширования, подписывающее лицо исчисляет результат хеширования, относящийся (для всех практических целей) только к подписываемой информации. Далее подписывающее лицо при помощи программного обеспечения преобразует результат хеширования в цифровую подпись, используя свой частный ключ. Созданная таким образом цифровая подпись относится только к подписываемой информации и только к частному ключу, использованному для создания этой подписи. Как правило, цифровая подпись (результат хеширования сообщения, зашифрованный частным ключом подписавшего) прилагается к сообщению и хранится или передается вместе с этим сообщением. Однако она также может передаваться или храниться в качестве отдельного элемента данных до тех пор, пока она сохраняет надежную связь со своим сообщением. Поскольку цифровая подпись относится только к данному конкретному сообщению, она становится бесполезной, если окончательно утрачивает связь с ним.

v) *Проверка подлинности цифровой подписи*

30. Проверка подлинности цифровой подписи представляет собой процесс сверки такой подписи с подлинным сообщением и определенным публичным ключом в целях установления того, была ли эта цифровая подпись создана для данного конкретного сообщения с использованием частного ключа, соответствующего указанному публичному ключу. Подлинность цифровой подписи проверяется путем исчисления нового результата хеширования подлинного сообщения с помощью той же функции хеширования, которая была применена для создания цифровой подписи. Затем, используя публичный ключ и новый результат хеширования, проверяющий

устанавливает, была ли цифровая подпись создана с использованием соответствующего частного ключа и совпадает ли вновь исчисленный результат хеширования с первоначальным результатом хеширования, который был преобразован в цифровую подпись в процессе подписания.

31. Используемое для такой проверки программное обеспечение подтверждает цифровую подпись как криптографически "проверенную", если *a*) для подписания сообщения в цифровой форме использовался частный ключ подписавшего лица, что считается доказанным, если подпись прошла проверку публичным ключом подписавшего лица, так как публичный ключ подписавшего лица сходится лишь с цифровой подписью, созданной при помощи его частного ключа; и *b*) в сообщение не были внесены изменения, что считается доказанным, если результат хеширования, исчисленный проверяющим, идентичен результату хеширования, полученному из цифровой подписи в процессе проверки.

vi) *Другие виды применения технологии цифровой подписи*

32. Технология цифровой подписи применяется значительно более широко, чем просто для "подписания" электронных сообщений по аналогии с собственноручным подписанием документов. Так, подписанные цифровым способом сертификаты часто используются в качестве "удостоверений" для серверов или веб-сайтов – например, чтобы гарантировать пользователям, что данный сервер или веб-сайт является именно тем, в качестве которого он им себя представляет, или действительно связан с компанией, утверждающей, что он находится под ее управлением. Технология цифровой подписи может использоваться также для "удостоверения" компьютерных программ – например, чтобы гарантировать, что загружаемое через веб-сайт программное обеспечение является подлинным или что на данном сервере используется технология, которая, по общему признанию, обеспечивает определенный уровень защиты соединений, – или для подтверждения подлинности любых других данных, распространяемых или хранящихся в цифровой форме.

b) Инфраструктура публичных ключей и поставщики сертификационных услуг

33. Чтобы проверить подлинность цифровой подписи, проверяющий должен иметь доступ к публичному ключу подписавшего лица и быть уверенным в том, что он соответствует частному ключу подписавшего лица. Однако пара публичного и частного ключей не имеет внутренне присущей ей связи с каким-либо лицом: это всего лишь пара чисел. Необходим дополнительный механизм для того, чтобы надежно установить наличие связи какого-либо конкретного физического или юридического лица с данной парой ключей. Это особенно важно, так как между подписавшим и получателями сообщения, имеющего цифровую подпись, ранее могло не существовать доверительных отношений. Поэтому участвующие стороны должны испытывать определенное доверие к выдаваемым публичным и частным ключам.

34. Требуемая степень доверия может наличествовать между сторонами, которые верят друг другу, имели дело друг с другом в течение определенного периода времени, общаются через закрытые системы, действуют в пределах замкнутой группы или способны регулировать свои сделки договорным путем, например на основе соглашения о торговом партнерстве. В случае сделки, затрагивающей только две стороны, каждая сторона может просто сообщить (по относительно надежному каналу,

такому как курьерская связь или телефон) публичный ключ из той пары ключей, которую будет использовать каждая сторона. Однако такая степень доверия может отсутствовать, если стороны редко ведут дела друг с другом, общаются через открытые системы (например, по всемирной сети через Интернет), не входят в замкнутую группу или не заключили соглашений о торговом партнерстве и не располагают другими нормами права, регулирующими их взаимоотношения. Кроме того, следует иметь в виду, что в случае необходимости урегулирования споров через суд или арбитраж тот факт, что некий публичный ключ действительно был – или не был – передан получателю его законным владельцем, может быть труднодоказуемым.

35. Лицо, намеревающееся использовать цифровую подпись, может сделать публичное заявление о том, что подписи, прошедшие проверку тем или иным конкретным публичным ключом, следует рассматривать как исходящие от этого лица. Форма и юридические последствия такого заявления будут регулироваться законодательством принимающего соответствующую норму государства. Например, презумпция атрибуции электронной подписи конкретному подписывающему лицу может быть установлена путем опубликования соответствующего заявления в официальном вестнике или в документе, признаваемом государственными органами в качестве "подлинного". Однако другие стороны могут и не пожелать признать это заявление, особенно при отсутствии заранее заключенного договора, устанавливающего юридическую силу такого опубликованного заявления со всей определенностью. Сторона, полагающаяся на такое неподтвержденное заявление, опубликованное в открытой системе, весьма рискует по неосторожности довериться мошеннику или столкнуться с необходимостью уличать другую сторону в недобросовестном отказе от своей цифровой подписи (вопрос, часто упоминаемый в контексте "неотказа" от цифровых подписей), если сделка окажется невыгодной для подразумеваемого подписавшего лица.

36. Один вариант решения некоторых из этих проблем заключается в том, чтобы использовать третью сторону или стороны для установления связи между идентифицированным подписавшим лицом или его именем и конкретным публичным ключом. В большинстве технических стандартов и руководящих принципов такую третью сторону обычно называют "сертификационным органом" или "поставщиком сертификационных услуг" (в Типовом законе ЮНСИТРАЛ об электронных подписях было решено использовать термин "поставщик сертификационных услуг"). В ряде стран такие сертификационные органы образуют иерархию, часто называемую "инфраструктурой публичных ключей" (ИПК). В рамках иерархической структуры ИПК может быть установлен порядок, согласно которому некоторые сертификационные органы занимаются только сертификацией других сертификационных органов, а те, в свою очередь, предоставляют услуги непосредственно пользователям. В такой структуре одни сертификационные органы подчинены другим сертификационным органам. Возможны и другие структуры, где все сертификационные органы действуют на равноправной основе. В любой крупной ИПК скорее всего будут и подчиненные, и вышестоящие сертификационные органы. К прочим возможным решениям относится, например, выдача сертификатов полагающимися сторонами.

i) *Инфраструктура публичных ключей*

37. Создание ИПК позволяет обеспечить уверенность в том, что *a*) публичный ключ пользователя не был изменен и действительно соответствует частному ключу этого пользователя; и *b*) используемые криптографические методы являются надежными. Для обеспечения такой уверенности ИПК может предлагать ряд услуг, включая

следующие: *a*) управление криптографическими ключами, используемыми для цифровых подписей; *b*) сертификация того, что публичный ключ соответствует частному ключу; *c*) предоставление ключей конечным пользователям; *d*) опубликование информации об аннулировании публичных ключей или сертификатов; *e*) управление личными опознавательными средствами (например, интеллектуальными карточками), которые могут идентифицировать пользователя с помощью уникальной личной идентификационной информации или могут генерировать и хранить частные ключи соответствующего лица; *f*) проверка правильности идентификации конечных пользователей и предоставление им услуг; *g*) предоставление услуг по регистрации времени; и *h*) управление криптографическими ключами, используемыми для кодирования в целях обеспечения конфиденциальности, если такое их применение санкционировано.

38. ИПК может состоять из различных иерархических уровней. Например, в моделях, рассматриваемых в некоторых странах в связи с возможным созданием ИПК, фигурируют следующие уровни: *a*) единый "базовый орган", который сертифицирует технологию и практику всех сторон, уполномоченных выдавать пары криптографических ключей или сертификаты в связи с использованием таких пар ключей, и осуществляет регистрацию подчиненных сертификационных органов[53]; *b*) различные сертификационные органы, занимающие более низкую ступень по сравнению с базовым органом, которые удостоверяют, что публичный ключ пользователя действительно соответствует частному ключу этого пользователя (т. е. не был изменен); и *c*) различные регистрационные органы местного уровня, которые занимают более низкую ступень по сравнению с сертификационными органами и которые принимают заявки пользователей на предоставление пар криптографических ключей или сертификатов в связи с использованием таких пар ключей, запрашивают подтверждение идентификационных данных и проверяют личность потенциальных пользователей. В некоторых странах предусматривается, что выступать в роли местных регистрационных органов или оказывать им поддержку могут государственные нотариусы.

39. ИПК, организованные по иерархическому принципу, можно наращивать, то есть присоединять к ним целые новые "ИПК-сообщества" просто путем установления их базовым органом доверительных отношений с базовыми органами таких сообществ[54]. Базовый орган нового сообщества может непосредственно подчиняться базовому органу принимающей ИПК, приобретая тем самым статус нижестоящего поставщика сертификационных услуг в рамках этой ИПК. Базовый орган нового сообщества может как поставщик сертификационных услуг также занимать подчиненное положение по отношению к одному из поставщиков сертификационных услуг в рамках существующей ИПК. Еще одной привлекательной особенностью иерархических ИПК является простота построения сертификационных цепочек, которые пролегают в одном и том же направлении – от пользовательского сертификата обратно к "центру доверия". Кроме того, сертификационные цепочки в иерархической ИПК являются сравнительно короткими, причем по положению, занимаемому в иерархии тем или иным поставщиком сертификационных услуг, пользователи способны определить, для каких целей можно использовать полученный от него сертификат. Однако у иерархических ИПК есть и недостатки, главным образом связанные с наличием

[53] Вопрос о том, должно ли правительство располагать техническими возможностями для хранения или воссоздания частных ключей, используемых в целях обеспечения конфиденциальности, может быть решен на уровне базового органа.

[54] William T. Polk and Nelson E. Hastings, *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures*, National Institute of Standards and Technology (September 2000); размещено по адресу http://csrc.nist.gov/pki/documents/B2B-article.pdf (дата посещения – 5 июня 2008 года).

единого "центра доверия". Если базовый орган скомпрометирован, то вместе с ним становится скомпрометированной вся ИПК. Некоторые страны столкнулись также с трудностями при попытках избрать в качестве базового органа ту или иную конкретную организацию и заставить всех других поставщиков сертификационных услуг принять такую иерархию[55].

40. Альтернативой иерархическому построению ИПК является так называемая "сотовая" ИПК. В рамках этой модели поставщики сертификационных услуг занимают равноправное положение по отношению друг к другу. При этом все они могут быть центрами доверия. Как правило, пользователи доверяют тому поставщику сертификационных услуг, который выдал им сертификат. Поставщики сертификационных услуг выдают сертификаты друг другу; эти пары сертификатов отражают их взаимные отношения доверия. Отсутствие иерархии в такой системе означает, что поставщики сертификационных услуг не могут устанавливать условия, регулирующие типы сертификатов, выдаваемых другими поставщиками сертификационных услуг. Если поставщик сертификационных услуг желает ограничить степень доверия, оказываемого другим поставщикам сертификационных услуг, то он должен указать соответствующие ограничения в сертификатах, выдаваемых им своим коллегам[56]. Однако согласование условий и пределов взаимного признания может быть исключительно сложным делом.

41. Третий вариант структуры опирается на так называемого "связующего" поставщика сертификационных услуг. Такая структура может быть особенно полезной в том смысле, что она позволяет различным существующим ИПК-сообществам полагаться на сертификаты друг друга. В отличие от поставщика сертификационных услуг в рамках сотовой ИПК, связующий поставщик сертификационных услуг непосредственно пользователям сертификатов не выдает. Он также не должен, подобно базовому поставщику сертификационных услуг, служить центром доверия для пользователей ИПК. Вместо этого связующий поставщик сертификационных услуг вступает в равноправные отношения доверия с различными пользовательскими сообществами, позволяя пользователям сохранять отношения с естественными для них центрами доверия в рамках соответствующих ИПК. Если пользовательское сообщество строит свой домен доверительных отношений в форме иерархической ИПК, то связующий поставщик сертификационных услуг устанавливает отношения с базовым органом этой ИПК. Если же пользовательское сообщество строит домен доверительных отношений по принципу сотовой ИПК, то связующему поставщику сертификационных услуг достаточно установить отношения с одним из поставщиков сертификационных услуг такой ИПК, который при этом становится в ней "основным" поставщиком сертификационных услуг для целей создания "связующего звена доверия" с другой ИПК. Это "звено доверия", объединяющее две или более ИПК через их взаимные отношения со связующим поставщиком сертификационных услуг, дает пользователям, входящим в разные пользовательские сообщества, возможность взаимодействовать друг с другом через связующего поставщика сертификационных услуг при конкретно определенном уровне доверия[57].

---

[55] Как отмечают Polk and Hastings (*Bridge Certification Authorities*...), в США оказалось очень нелегко выделить конкретное учреждение правительства, которое приняло бы на себя управление всей федеральной ИПК.

[56] *Polk and Hastings, Bridge Certification Authorities ...* .

[57] Структура с использованием связующего поставщика сертификационных услуг была в итоге избрана для создания системы ИПК правительства США (Polk and Hastings, *Bridge Certification Authorities* ...). По той же схеме разрабатывалась система ИПК для правительства Японии.

ii) *Поставщик сертификационных услуг*

42. Чтобы установить связь между парой ключей и будущим подписывающим лицом, поставщик сертификационных услуг (или сертификационный орган) выдает сертификат, представляющий собой электронную запись, в которой в качестве "предмета" сертификата указываются публичный ключ и имя абонента сертификата и в которой также может подтверждаться, что будущее подписывающее лицо, указанное в сертификате, является держателем соответствующего частного ключа. Основная функция сертификата заключается в увязывании публичного ключа с конкретным подписывающим лицом. "Получатель" сертификата, желающий положиться на цифровую подпись, созданную подписывающим лицом, которое поименовано в сертификате, может использовать указанный в сертификате публичный ключ для проверки того, что та или иная конкретная цифровая подпись была создана с помощью соответствующего частного ключа. Если такая проверка дает положительный результат, то это служит определенной технической гарантией того, что цифровая подпись была создана соответствующим подписывающим лицом и что часть сообщения, к которой была применена функция хеширования (и, следовательно, соответствующее сообщение данных), не подверглась изменениям после ее подписания в цифровой форме.

43. Чтобы удостоверить подлинность сертификата с точки зрения как его содержания, так и его источника, поставщик сертификационных услуг скрепляет его цифровой подписью. Подлинность цифровой подписи поставщика сертификационных услуг на выданном им сертификате может быть проверена с помощью публичного ключа этого поставщика сертификационных услуг, указанного в другом сертификате другим поставщиком сертификационных услуг (который может, но не обязательно должен находиться на более высоком уровне в иерархии), а подлинность этого другого сертификата может быть, в свою очередь, удостоверена публичным ключом, указанным в еще одном сертификате, и т. д., до тех пор пока лицо, полагающееся на цифровую подпись, не получит должной гарантии ее истинности. Еще одним возможным способом подтверждения подлинности цифровой подписи является ее включение в сертификат, выданный поставщиком сертификационных услуг (который иногда именуется "базовым сертификатом")[58].

44. В каждом случае выдающий сертификат поставщик сертификационных услуг имеет возможность подписать в цифровой форме свой собственный сертификат в течение срока действия другого сертификата, используемого для проверки подлинности цифровой подписи данного поставщика сертификационных услуг. Согласно законам некоторых государств, одним из способов повышения доверия к цифровой подписи поставщика сертификационных услуг может быть опубликование публичного ключа этого поставщика сертификационных услуг или некоторых данных, относящихся к базовому сертификату (таких, как "цифровой отпечаток"), в официальном вестнике.

45. Соответствующая сообщению цифровая подпись, независимо от того, была ли она создана подписавшим лицом для удостоверения подлинности сообщения или же поставщиком сертификационных услуг для удостоверения подлинности своего сертификата, должна быть, как правило, надежно датирована, чтобы проверяющий мог точно установить, была ли цифровая подпись создана в течение срока действия,

[58] *Типовой закон ЮНСИТРАЛ об электронных подписях*..., часть вторая, пункт 54.

указанного в сертификате, и был ли сертификат действительным (т. е. не числился ли он в списке аннулированных сертификатов) на соответствующий момент, что является условием подтверждения подлинности цифровой подписи.

46. Чтобы публичный ключ и данные о его соответствии конкретному подписавшему лицу были легкодоступными для использования при проверке подлинности, сертификат может быть опубликован в соответствующем реестре или предоставляться для ознакомления каким-либо иным образом. Реестры обычно представляют собой функционирующие в режиме онлайн базы данных о сертификатах и другой информации, которая может быть получена и использована для проверки подлинности цифровых подписей.

47. Уже выданный сертификат может оказаться ненадежным, например в ситуациях, когда подписавший представил поставщику сертификационных услуг неверные идентификационные данные о себе. В других случаях сертификат может быть надежным при выдаче, но стать ненадежным впоследствии. Если частный ключ "скомпрометирован", например в результате потери подписывающим лицом контроля над ним, то сертификат может перестать заслуживать доверия или утратить надежность и поставщик сертификационных услуг (по просьбе подписывающего лица или, в зависимости от обстоятельств, даже без его согласия) может приостановить действие (временно прервать срок действительности) такого сертификата или аннулировать его (навсегда признать недействительность). После приостановления действия или аннулирования сертификата от поставщика сертификационных услуг может ожидаться своевременное опубликование уведомления об аннулировании или приостановлении действия сертификата либо направление извещений об этом лицам, запрашивающим такую информацию или получившим, согласно имеющимся данным, цифровую подпись, для проверки которой предназначен утративший надежность сертификат. Аналогичным образом, проверке на предмет возможного аннулирования должны, если это применимо, подлежать сертификат самого поставщика сертификационных услуг, равно как и тот сертификат, которым подтверждается подпись, проставляемая органом по регистрации времени на временных метках, и сертификат поставщика сертификационных услуг, выдавшего сертификат органу по регистрации времени.

48. Функционирование сертификационных органов может обеспечиваться частными поставщиками услуг или правительственными учреждениями. В ряде стран по соображениям публичного порядка предусматривается, что только правительственные учреждения могут быть уполномочены действовать в качестве сертификационных органов. В большинстве стран, однако, оказание сертификационных услуг либо целиком возложено на частный сектор, либо осуществляется параллельно государственными и частными поставщиками. Существуют также закрытые системы сертификации, в рамках которых небольшие группы учреждают собственного поставщика сертификационных услуг. В некоторых странах государственные поставщики сертификационных услуг выдают сертификаты только для подтверждения цифровых подписей, используемых органами государственного управления. Независимо от того, обеспечивается ли функционирование сертификационных органов государственными учреждениями или частными поставщиками услуг и требуется ли, чтобы сертификационные органы получали лицензию на свою деятельность, обычно в рамках ИПК действуют не один, а несколько поставщиков сертификационных услуг. Особого внимания требуют взаимоотношения между различными сертификационными органами (см. пункты 38–41, выше).

49. На поставщика сертификационных услуг или базовый орган может быть возложена обязанность обеспечивать, чтобы его требования в отношении надлежащих действий выполнялись на постоянной основе. Хотя выбор сертификационных органов может основываться на ряде факторов, включая надежность используемого публичного ключа и идентификационные данные пользователя, доверие к любому поставщику сертификационных услуг может также зависеть от его способности обеспечить соблюдение стандартов, касающихся выдачи сертификатов, и от надежности проводимой им оценки данных, получаемых от пользователей, которые обращаются за сертификатами. Особое значение имеет режим ответственности, применяемый к любому поставщику сертификационных услуг в связи с необходимостью постоянного выполнения им установленных базовым органом или вышестоящим поставщиком сертификационных услуг требований в отношении надлежащих действий и обеспечения неприкосновенности данных или же любых других соответствующих требований. Не меньшее значение имеет и обязанность поставщика сертификационных услуг действовать в соответствии с заверениями, которые он дает в отношении принципов и практики своей деятельности, предусмотренная в пункте 1 *a*) статьи 9 Типового закона об электронных подписях.

c) Практические проблемы внедрения инфраструктур публичных ключей

50. Несмотря на немалый объем знаний о технологиях цифровой подписи и о том, как они функционируют, практическое внедрение инфраструктур публичных ключей и систем цифровой подписи сдерживается рядом проблем, из-за которых масштабы применения цифровых подписей до сих пор не соответствуют ожиданиям.

51. Цифровые технологии подписания хорошо обеспечивают проверку подлинности подписей, созданных в течение срока действия сертификата. Однако по истечении этого срока или в случае аннулирования сертификата соответствующий публичный ключ становится недействительным, даже если соответствующая пара ключей не была скомпрометирована. Соответственно, в рамках ИПК должна быть предусмотрена система обслуживания цифровых подписей, обеспечивающая возможность их использования в течение длительного времени. Главная трудность здесь связана с тем, что "исходные" электронные записи (т. е. единицы бинарного кода, или биты, из которых состоит компьютерный файл с записью соответствующей информации), включая цифровую подпись, могут со временем стать недоступными для прочтения или утратить надежность – прежде всего в связи с устареванием программного обеспечения, оборудования или того и другого. Кроме того, защита цифровой подписи может стать ненадежной из-за новых научных достижений в области криптографического анализа, программное обеспечение для проверки подписей может по прошествии длительного времени стать труднодоступным либо может быть нарушена целостность самого документа[59]. В силу этого долгосрочное сохранение электронных подписей в целом представляется проблематичным. Хотя одно время бытовало мнение о незаменимости электронных подписей для архивных нужд, опыт показал, что и они подвержены воздействию долгосрочных факторов риска. Поскольку любое изменение записанных данных после создания подписи приводит к тому, что подпись

[59] Jean-François Blanchette, "Defining electronic authenticity: an interdisciplinary journey"; размещено по адресу http://polaris.gseis.ucla.edu/blanchette/papers/dsn.pdf (дата посещения –5 июня 2008 года) (статья, опубликованная в подборке дополнительных материалов 2004 International Conference on Dependable Systems and Networks (DSN 2004), Florence, Italy, 28 June – 1 July 2004), pp. 228-232.

при проверке перестает опознаваться как подлинная, операции по переформатированию (такие, как перенос или преобразование данных), призванные обеспечить возможность считки записи в будущем, могут отразиться на долговечности подписи[60]. Собственно говоря, цифровые подписи были задуманы скорее как средство защиты информации при ее передаче, чем как средство ее сохранения в течение длительного времени[61]. Инициативы по преодолению этой проблемы до сих пор не привели к ее надежному решению[62].

---

[60] "В конечном счете, сохранение информации в электронной форме сводится к сохранению битов. Однако давно стало очевидным, что сохранение набора битов на неопределенный срок представляет собой очень нелегкую задачу. С течением времени набор битов перестает поддаваться расшифровке (компьютером, а значит и человеком) из-за технического устаревания прикладных программ и/или аппаратуры (например, считывающего устройства). Проблема долговечности цифровых подписей на основе ИПК до сих пор мало изучена по причине ее сложности. …Хотя средства удостоверения, применявшиеся в прошлом, – такие, как собственноручные подписи, печати, штемпели, отпечатки пальцев и т. д. – также нуждаются в переформатировании (например, переносе на микропленку) в связи с устареванием бумажного носителя, после такого переформатирования они никогда не становятся полностью непригодными для использования по назначению. Всегда остается хотя бы копия, которую можно сравнить с подлинниками других средств удостоверения". (Jos Dumortier and Sofie Van den Eynde, *Electronic Signatures and Trusted Archival Services*, p. 5 (размещено по адресу http://www.law.kuleuven.ac.be/icri/publications/ 172DLM2002.pdf?where (дата посещения – 5 июня 2008 года)).

[61] В 1999 году архивными работниками ряда стран был начат Международный исследовательский проект по бессрочному сохранению подлинных записей в электронных системах (ИнтерПАРЕС), направленный на "получение теоретических и методологических знаний, необходимых для долгосрочного сохранения подлинных записей, созданных и/или существующих в цифровой форме" (см. http://www.interpares.org/; дата посещения – 5 июня 2008 года). В проекте доклада Целевой группы по вопросам подлинности (размещено по адресу http://www.interpares.org/documents/atf_draft_final_report.pdf; дата посещения – 5 июня 2008 года), действовавшей в рамках первого этапа проекта (ИнтерПАРЕС-1, завершен в 2001 году), отмечается, что "цифровые подписи и инфраструктуры публичных ключей (ИПК) являются примерами технологий, разработанных и внедренных для целей удостоверения подлинности электронных записей при передаче в пространстве. Хотя хранители документации и специалисты по информатике полагаются на технологии удостоверения подлинности как на средство подтверждения подлинного происхождения записей, эти технологии никогда не предназначались и на сегодняшний день не могут служить в качестве средства, гарантирующего подлинность электронных записей по прошествии времени" (выделение добавлено). Итоговый доклад ИнтерПАРЕС-1 доступен по адресу http://www.interpares.org/book/index.htm (дата посещения – 5 июня 2008 года). Следующий этап этого проекта (ИнтерПАРЕС-2) нацелен на разработку и формулирование концепций, принципов, критериев и методов, позволяющих обеспечить создание и хранение точных и надежных записей, а также долгосрочную сохранность подлинных записей, связанных с художественной, научной и правительственной деятельностью, за период с 1999 по 2001 год.

[62] Например, в 1999 году Совет по стандартам в области информационных и коммуникационных технологий – группа сотрудничающих между собой организаций, занимающихся стандартизацией и связанной с этим деятельностью в области информационных и коммуникационных технологий, призванная координировать усилия по стандартизации во исполнение Директивы Европейского союза об электронных подписях, – положил начало Европейской инициативе по стандартам для электронных подписей (ЕИСЭП) (см. *Official Journal of the European Communities*, L 13/12, 19 January 2000). Консорциум ЕИСЭП (предпринимавший усилия по стандартизации с целью воплощения положений директивы Европейского союза об электронных подписях в конкретные нормы для европейских стран) стремился обеспечить удовлетворение потребности в долгосрочном хранении документов, подписанных криптографическим способом, на основе своего стандартного "формата электронной подписи" (Electronic Signature Formats ES 201 733, ETSI, 2000). Согласно этому формату в процессе подтверждения подлинности подписей выделяются такие моменты, как исходное подтверждение и последующее подтверждение. Формат для последующего подтверждения заключает в себе всю информацию, которая может быть рано или поздно использована в процессе подтверждения: данные об аннулировании, маркеры времени, сведения о процедурах создания подписей и т. д. Эта информация собирается на этапе исходного подтверждения подлинности. Разработчики упомянутых форматов электронной подписи были озабочены тем, что из-за постепенного снижения надежности криптографической защиты действительность подписи может со временем оказаться под угрозой. Чтобы застраховаться от такого снижения надежности, подписи, основанные на стандарте ЕИСЭП, регулярно маркируются свежими временными метками, в которых используются алгоритмы подписания и длина ключей, соответствующие наиболее современным методам криптографического анализа. Проблема долговечности программного обеспечения рассматривалась в докладе ЕИСЭП за 2000 год, где впервые говорилось об "услугах по доверительному архивному хранению" – новой разновидности коммерческих услуг, которые предлагались бы не названными конкретно компетентными организациями и специалистами в целях гарантированного длительного сохранения документов, подписанных криптографическим способом.

52. Еще одна область, где в связи с цифровыми подписями и ИПК могут возникать проблемы практического характера, связана с защитой данных и неприкосновенностью частной жизни. Поставщики сертификационных услуг должны надежно хранить ключи, используемые для подписания сертификатов, которые они выдают своим клиентам, в условиях, когда посторонние лица могут пытаться получить несанкционированный доступ к этим ключам (см. также Часть вторую, пункты 223–226, ниже). Кроме того, поставщики сертификационных услуг должны получать от лиц, обращающихся за сертификатами, персональные данные и коммерческую информацию по ряду вопросов. Эта информация должна храниться у поставщика сертификационных услуг для последующей сверки. Поставщики сертификационных услуг должны принимать необходимые меры для обеспечения того, чтобы доступ к такой информации осуществлялся в соответствии с действующими законами о защите данных[63]. Тем не менее угроза несанкционированного доступа остается реальной.

2. Биометрические данные

53. Биометрическими данными называются данные измерений, используемые для идентификации конкретного лица по его физическим или поведенческим особенностям. К особенностям, которые могут служить для биометрического опознания, относятся ДНК, отпечатки пальцев, радужная оболочка глаза, сетчатка глаза, геометрия ладони или лица, термальный образ лица, форма ушной раковины, голос, естественный запах, конфигурация кровеносных сосудов, почерк, походка и динамика ввода данных с клавиатуры.

54. Использование биометрических устройств, как правило, предполагает фиксацию в цифровой форме биометрического образца той или иной биологической особенности человека. Затем из этого образца извлекаются биометрические данные, с помощью которых составляется проверочный эталон. Впоследствии для установления личности человека, которому соответствует биометрический образец, или для подтверждения подлинности сообщений, якобы исходящих от данного лица, его биометрические данные сопоставляются с данными, заключенными в проверочном эталоне[64].

В докладе перечислен ряд технических требований, которым должны отвечать такие архивные услуги: в их число входит "совместимость с предыдущими версиями" компьютерной аппаратуры и программного обеспечения, достигаемая путем сохранения такой аппаратуры или ее имитации (см. Blanchette, "Defining electronic authenticity …"). Дальнейшее исследование на эту тему под названием *European Electronic Signature Standardization Initiative: Trusted Archival Services* (Phase 3, final report, 28 August 2000), проведенное Междисциплинарным центром права и информационных технологий при Лювенском католическом университете, Бельгия, и посвященное рекомендации ЕИСЭП об услугах по доверительному архивному хранению, размещено по адресу http://www.law.kuleuven.ac.be/icri/publications/91TAS-Report.pdf?where= (дата посещения – 5 июня 2008 года). ЕИСЭП была завершена в октябре 2004 года. Системы, позволяющие реализовать рекомендации ЕИСЭП, судя по всему, до сих пор не внедрены (см. Dumortier and Van den Eynde, Electronic Signatures and Trusted Archival Services...).

[63] См. The Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris, 1980), размещено по адресу http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (дата посещения – 5 июня 2008 года); Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, European Treaty Series, No. 108), размещено по адресу http://conventions.coe.int/Treaty//Treaties/Html/108.htm (дата посещения – июнь 2008 года); Руководящие принципы регламентации компьютерных картотек, содержащих данные личного характера (резолюция 45/95 Генеральной Ассамблеи); и Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (*Official Journal of the European Communities*, L 281, 23 November 1995, размещено по адресу http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett (дата посещения – июнь 2008 года)).

[64] International Association for Biometrics and International Computer Security Association, *1999 Glossary of Biometric Terms* (экземпляр имеется в Секретариате).

55. Хранение биометрических данных связано с целым рядом факторов риска, так как биометрические особенности человека, как правило, носят имманентный характер. Если биометрические системы оказываются скомпрометированными, то законные пользователи не имеют иного выбора, кроме как отозвать свои идентификационные данные и заменить их другим набором таких данных, который не был скомпрометирован. Поэтому для предотвращения неправомерного использования банков биометрических данных необходимы специальные правила.

56. Биометрические методы не могут быть абсолютно точными, так как биологическим параметрам изначально свойственна изменчивость, и при любых измерениях возможны погрешности. В свете этого биометрические данные рассматриваются не как уникальные, а лишь как "полууникальные" отличительные признаки. Для учета возможных вариаций точность биометрического контроля можно регулировать, устанавливая пороговые уровни соответствия извлеченного образца проверочному эталону. При этом, однако, низкий пороговый уровень может чрезмерно повышать вероятность ложных совпадений, а высокий – вероятность ложных несовпадений. И все же точность удостоверения, обеспечиваемая биометрическими устройствами, может быть достаточной для большинства видов их коммерческого применения.

57. Кроме того, в связи с хранением и раскрытием биометрических данных возникают вопросы, касающиеся защиты данных и прав человека. Законы о защите данных[65], хотя они могут и не содержать прямых упоминаний о биометрической информации, направлены на защиту индивидуальных данных, относящихся к физическим лицам, а обработка таких данных как в сыром виде, так и в виде эталонов составляет основу биометрической технологии[66]. При этом могут требоваться меры для защиты потребителей от опасностей, связанных с частным использованием биометрической информации, а также с возможным хищением идентификационных данных. Затронутыми могут оказаться и другие области законодательства, такие как законы о труде и охране здоровья[67].

58. Для ряда проблем могут быть предложены технические решения. Например, хранение биометрических данных на интеллектуальных карточках или аппаратных ключах может предохранить их от несанкционированного доступа, возможного в случае, если эти данные содержатся в централизованной компьютерной системе. Разработаны также оптимальные способы снижения риска в отношении таких различных аспектов, как сфера применения и возможности устройств, защита данных, контроль над персональными данными со стороны пользователя, а также раскрытие данных, аудит, подотчетность и надзор[68].

59. Как правило, биометрические устройства считаются обеспечивающими высокую степень надежности. Хотя они подходят для разнообразного применения, в настоящее время их используют в основном в государственных учреждениях и, в

---

[65] См. сноску 63.

[66] Paul de Hert, Biometrics: *Legal Issues and Implications*, background paper for the Institute for Prospective Technological Studies of the European Commission (European Communities, Directorate General Joint Research Centre, 2005), p. 13; размещено по адресу http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de Hert.pdf (дата посещения – 5 июня 2008 года).

[67] Например, в Канаде использование биометрических данных обсуждалось в связи с применением на рабочих местах Закона о защите персональной информации и электронных документах (2000, с. 5) (см. Turner v. TELUS Communications Inc., 2005 FC 1601, 29 November 2005 (Federal Court of Canada)).

[68] В качестве примера оптимальной практики см. the International Biometric Group BioPrivacy Initiative, "Best practices for privacy-sympathetic biometric deployment"; размещено по адресу http://www.bioprivacy.org (дата посещения – 5 июня 2008 года).

частности, в правоохранительных органах – например, для иммиграционного контроля и в системах режимного доступа.

60. Разработаны также коммерческие технологии использования биометрических данных; многие из них предусматривают процедуру удостоверения по сочетанию двух параметров, один из которых должен физически наличествовать у удостоверяемого лица (биометрические данные), а другой должен быть ему известен (как правило, пароль или ПИН). Созданы также прикладные системы, позволяющие фиксировать и сопоставлять характеристики собственноручных подписей. Для этого используются цифровые планшеты, регистрирующие нажим ручки и время, затрачиваемое на проставление подписи. Соответствующие данные затем сохраняются в виде алгоритма для сверки с будущими подписями. Однако ввиду имманентных особенностей биометрической информации в этой связи высказываются также предостережения о рисках, связанных с постепенным бесконтрольным распространением таких систем в повседневной коммерческой практике.

61. Если биометрические подписи станут использоваться вместо собственноручных, это может привести к возникновению проблемы доказывания. Уже отмечалось, что степень надежности биометрических данных как доказательства может быть различной в зависимости от используемой технологии и выбранного допустимого процента ложных совпадений. Кроме того, хранящиеся в цифровой форме биометрические данные могут быть умышленно искажены или фальсифицированы.

62. К использованию биометрических подписей могут применяться общие критерии надежности, предусмотренные Типовым законом ЮНСИТРАЛ об электронных подписях и Типовым законом ЮНСИТРАЛ об электронной торговле, а также принятой позднее Конвенцией Организации Объединенных Наций об использовании электронных сообщений в международных договорах[69]. Для обеспечения единообразия может также быть полезной разработка международных руководящих принципов использования и регулирования биометрических методов[70]. Вопрос о том, не будет ли установление таких стандартов преждевременным при нынешнем уровне развития биометрических технологий и не станет ли это препятствием их дальнейшему совершенствованию, необходимо тщательно продумать.

3. Пароли и комбинированные методы

63. Пароли и коды используются как для регулирования доступа к информации или услугам, так и для “подписания” электронных сообщений. Последнее практикуется реже, чем первое, из-за опасности компрометации кода в случае его передачи в незашифрованных сообщениях. Вместе с тем пароли и коды являются наиболее широко применяемым средством “удостоверения” для целей регулирования доступа и проверки личности при совершении самых различных операций: так, они чаще всего используются при управлении банковскими счетами через Интернет, при пользовании автоматами для выдачи наличных и при расчетах по потребительским кредитным картам.

---

[69] Проект конвенции об использовании электронных сообщений в международных договорах был одобрен ЮНСИТРАЛ на ее тридцать восьмой сессии (Вена, 4–15 июля 2005 года). Конвенция была официально принята Генеральной Ассамблеей в резолюции 60/21 от 23 ноября 2005 года.

[70] Их можно сопоставить с критериями надежности, изложенными в Руководстве по принятию Типового закона ЮНСИТРАЛ об электронных подписях (Типовой закон ЮНСИТРАЛ об электронных подписях.., часть вторая, пункт 75).

64. Следует иметь в виду, что для целей "удостоверения" при электронных сделках могут использоваться различные технологии. При этом в связи с одной и той же сделкой возможно применение нескольких технологий либо несколько видов применения одной технологии. Например, анализ динамики проставления собственноручной подписи для подтверждения подлинности может сочетаться с криптографией для защиты целостности сообщения. В другом варианте пароли могут передаваться через Интернет с применением криптографической защиты (например, SSL-протокола в интернет-обозревателях), в то время как биометрические данные могут использоваться для создания цифровой подписи (асимметричная криптография), которая после ее доставки получателю генерирует пользовательский мандат согласно протоколу "Керберос" (симметричная криптография). При разработке юридических рамок и общих правил использования этих технологий следует уделить внимание роли их возможных сочетаний. Юридические рамки и общие правила электронного удостоверения подлинности должны быть достаточно гибкими для того, чтобы ими можно было охватить комбинированные технологические решения, так как их привязка к конкретным технологиям может помешать совместному использованию этих технологий[71]. Положения, нейтральные с точки зрения технологий, способствовали бы внедрению таких комбинированных технологических решений.

4. Отсканированные подписи и имена, введенные с клавиатуры

65. Интерес законодателей к вопросам электронной торговли с точки зрения частного права объясняется прежде всего озабоченностью тем, как появление новых технологий может отразиться на применении правовых норм, задуманных в расчете на иные носители информации. Такое повышенное внимание к техническим аспектам нередко приводит к умышленному или неумышленному сосредоточению на сложных технологиях, обеспечивающих наиболее высокую надежность электронного удостоверения подлинности и электронных подписей. При этом часто забывают, что очень большое количество, если не большинство, сообщений, связанных с деловыми операциями повсюду в мире, пересылаются вообще без применения каких бы то ни было технологий подписания или удостоверения подлинности.

66. В своей повседневной практике компании разных стран нередко довольствуются, например, перепиской по электронной почте без применения каких-либо способов удостоверения подлинности или подписания помимо указания имен, должностей и адресов участников, вводимых с помощью клавиатуры в конце сообщения. Иногда сообщениям придают более официальный вид, используя факсимильные или отсканированные изображения собственноручных подписей, которые, разумеется, представляют собой не более чем оцифрованную копию рукописного оригинала. Ни подписи, введенные с клавиатуры, ни передаваемые по электронной почте незашифрованные письма, ни отсканированные изображения подписей не обеспечивают высокой степени надежности и не могут служить однозначным подтверждением личности составителя электронного сообщения, частью которого они являются. Тем не менее коммерческие структуры сознательно отдают предпочтение таким формам "удостоверения подлинности" в интересах простоты, оперативности и удешевления

---

[71] См. Foundation for Information Policy Research, *Signature Directive Consultation Compilation*, 28 October 1998 – подготовленная по просьбе Европейской комиссии подборка замечаний, высказанных в ходе консультаций по проекту директивы Европейского союза об электронных подписях; размещено по адресу www.fipr.org/publications/sigdirecon.html (дата посещения – 5 июня 2008 года).

связи. Важно, чтобы законодатели и лица, ответственные за принятие директивных решений, рассматривая вопрос о регулировании электронных методов подписания и удостоверения подлинности, имели в виду эту широко распространенную в деловых отношениях практику. Строгие требования в отношении электронного удостоверения подлинности и использования электронных подписей, и особенно навязывание того или иного метода или технологии, могут непреднамеренно поставить под сомнение действительность и исковую силу значительного числа сделок, заключаемых ежедневно без применения каких-либо специальных методов удостоверения подлинности и подписания. Это, в свою очередь, может подтолкнуть недобросовестные стороны к уклонению от последствий добровольно принятых ими обязательств путем оспаривания подлинности своих собственных электронных сообщений. Нереалистично ожидать, что директивное установление высоких требований к удостоверению подлинности и подписанию в итоге приведет к тому, что все стороны будут фактически применять их на повседневной основе. Недавний опыт использования наиболее современных методов, таких как цифровое подписание, показывает, что сомнения, обусловленные дороговизной и сложностью технологий подписания и удостоверения подлинности, зачастую ограничивают масштабы их практического применения.

C. Управление электронными идентификационными записями

67. В электронной среде физические и юридические лица имеют возможность прибегать к услугам целого ряда поставщиков. Всякий раз, когда лицо регистрируется у того или иного провайдера услуг с целью получения доступа к этим услугам, для него создается электронная идентификационная запись. При этом одна такая запись может быть связана с целым рядом учетных записей для каждой прикладной программы или платформы. Умножение числа идентификационных записей и соответствующих им учетных записей может затруднять работу с ними как для пользователя, так и для поставщика услуг. Этих трудностей можно избежать, предусмотрев для каждого лица единую электронную идентификационную запись.

68. Регистрация у поставщика услуг и создание идентификационной записи ведут к установлению отношений взаимного доверия между соответствующим лицом и конкретным поставщиком. Для создания единой электронной идентификационной записи эти двусторонние отношения должны быть сведены в более общую систему, обеспечивающую возможность для совместного управления; это называется управлением идентификационными записями. С точки зрения поставщиков преимущества управления идентификационными записями могут включать более надежную защиту, упрощение соблюдения норм регулирования и повышение маневренности при осуществлении коммерческих операций, а с точки зрения пользователей – облегчение доступа к информации.

69. Управление идентификационными записями можно представить себе в рамках следующих двух подходов:

a) *традиционный принцип пользовательского доступа*. Данный принцип предполагает подключение пользователя к системе, обычно с использованием данных, хранимых при помощи того или иного устройства, например интеллектуальной карточки, или имеющихся у клиента в иной форме, при вводе которых клиент

получает доступ к услуге. Подход к управлению, основанный на пользовательском доступе, ставит во главу угла административную поддержку процедур удостоверения личности пользователей, а также вопросы прав доступа, ограничений доступа, учетных записей, паролей и других атрибутов одной или нескольких прикладных программ или систем. Он призван облегчать и регулировать доступ к прикладным программам и ресурсам, одновременно обеспечивая защиту конфиденциальной личной и коммерческой информации от несанкционированных пользователей;

b) *более новаторский принцип обслуживания на базе системы*, предоставляющей пользователям и их устройствам персонализованные услуги. При применении этого принципа рамки управления идентификационными записями расширяются и охватывают все ресурсы компании, используемые для оказания услуг в режиме онлайн: сетевое оборудование, серверы, порталы, информационное наполнение, прикладные программы и продукты, а также данные, подтверждающие статус пользователей, принадлежащие пользователям адресные книги, сведения об их предпочтениях и правах. На практике речь может идти, например, о настройках ограничений для доступа детей или об участии в программах для постоянных клиентов.

70. Усилия по расширению практики управления идентификационными записями предпринимаются как на уровне коммерческих предприятий, так и на уровне правительств. Следует отметить, однако, что политика, проводимая в этом отношении этими группами участников, может существенно различаться. Подход правительств может быть в большей степени направлен на оптимальное удовлетворение нужд граждан и, следовательно, более ориентирован на взаимодействие с физическими лицами. Напротив, подходы, применяемые коммерческими структурами, должны учитывать расширяющееся применение автоматической аппаратуры при проведении деловых операций и поэтому могут содержать элементы, рассчитанные на специфические потребности использования такой аппаратуры.

71. Трудности, отмечаемые в связи с использованием систем управления идентификационными записями, включают проблемы защиты конфиденциальных личных данных от риска, связанного с неправомерным использованием уникальных опознавательных признаков. Проблемы могут возникать также из-за различий в действующих юридических нормах, особенно касающихся возможности делегирования полномочий на совершение действий от имени другого лица. В этой связи предлагаются решения, основанные на добровольном деловом сотрудничестве по принципу так называемого кругового доверия, когда участники должны полагаться на достоверность и точность информации, предоставляемой им другими членами круга. Однако такой подход сам по себе может быть не вполне достаточным для урегулирования всех связанных с этим вопросов, и наряду с ним может все же потребоваться принятие юридических норм. Разработаны также руководящие принципы, призванные заложить правовую основу для сообществ пользующихся взаимным доверием инфраструктур[72].

[72] Проект "Альянс за свободу" (см. www.projectliberty.org) представляет собой консорциум с участием более 150 компаний, некоммерческих и государственных организаций разных стран мира. Он ставит перед собой задачу выработки открытого стандарта "федеративной" сетевой идентификационной записи, совместимой со всеми существующими и разрабатываемыми видами сетевого оборудования. "Федеративная" идентификационная запись позволяет коммерческим предприятиям, правительствам, служащим и потребителям проще и надежнее контролировать идентификационную информацию в условиях современной компьютеризованной экономики и является ключевым фактором, способствующим более активному использованию электронной торговли и персонализованных информационных услуг, а также услуг, предоставляемых через Интернет. Возможность присоединения к консорциуму открыта для всех коммерческих и некоммерческих организаций.

72. В связи с проблемой технического взаимодействия систем Международный союз электросвязи учредил целевую группу по вопросам управления идентификационными записями для облегчения и ускорения разработки единой схемы, а также средств обнаружения рассредоточенных автономных идентификационных записей, их федераций и разновидностей[73].

73. Способы управления идентификационными записями разрабатываются также в контексте электронного правления. Например, в рамках инициативы Европейского союза "i2010: Европейское информационное общество как фактор экономического роста и обеспечения занятости"[74] начато исследование, посвященное управлению идентификационными записями в процессе электронного правления и призванное ускорить выработку согласованного подхода к данному вопросу в Европейском союзе на основе экспертных знаний и инициатив, имеющихся в государствах – членах Европейского союза[75].

74. Распространение устройств для создания электронных подписей, нередко выполненных в форме интеллектуальных карточек, все шире практикуется в рамках инициатив по переходу к электронному правлению. Например, общенациональные мероприятия по выдаче таких карточек населению начали проводиться в Бельгии, где эти карточки сначала были введены в ряде провинций в 2003 году[76], а затем, после успешного завершения испытательного срока, стали использоваться на всей территории страны[77]. Суть бельгийской системы сводится к физической выдаче удостоверений личности в виде карточек с микропроцессором, в котором хранятся данные, необходимые гражданину для создания цифровой подписи[78].

75. В Австрии создана система управления идентификационными записями, в рамках которой соответствующие опознавательные признаки закрепляются за каждым гражданином страны, но не указываются в официальных документах, удостоверяющих личность. Вместо этого в Австрии было решено установить стандарты, нейтральные с точки зрения технологий и позволившие разработать и ввести в потребительскую практику целый ряд различных технических решений. В основу австрийской системы положена так называемая "связь лица с идентификационной записью", т. е. механизм, скрепленный подписью государственного органа, выдающего сертификаты, посредством которого неповторимый опознавательный признак

---

[73] См. http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html (дата посещения – 20 марта 2008 года).

[74] Communication from the Commission of the European Communities to the European Council, the European Parliament, the European Economic and Social Committee and the Committee of the regions: "i2010 – A European Information Society for growth and employment", COM(2005) 229 final, (Brussels, 1 June 2005); размещено по адресу http://eur-lex.europa.eu (дата посещения – 20 марта 2008 года).

[75] См. *Modinis Study on Identity Management in eGovernment: Identity Management Issue Report* (European Commission, Directorate General Information Society and Media, 18 September 2006), pp. 9-12; размещено по адресу https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi (дата посещения – 6 июня 2008 года).

[76] Электронные удостоверения личности были введены в Бельгии в 2003 году в соответствии с Законом от 25 марта 2003 года о внесении изменений в Закон от 8 августа 1983 года о создании Национальной системы регистрации физических лиц и в Закон от 19 июля 1991 года о регистрации населения и удостоверениях личности и о внесении изменений в Закон от 8 августа 1983 года о создании Национальной системы регистрации физических лиц (Moniteur belge, Ed. 4, 28 Mars 2003, p. 15921).

[77] См. Arrêté royal du 1er septembre 2004 portant la décision de procéder à l'introduction généralisée de la carte d'identité électronique (Moniteur belge, Ed. 2, 15 Septembre 2004, p. 56527). Общую информацию см. по адресу http://eid.belgium.be (дата посещения – 6 июня 2008 года).

[78] Общую информацию см. по адресу http://eid.belgium.be (дата посещения – 6 июня 2008 года).

лица (например, его регистрационный номер) закрепляется за одним или несколькими сертификатами, принадлежащими этому лицу. Эта связь лица с идентификационной записью может использоваться для автоматической однозначной идентификации данного лица при его контактах с государственными органами в рамках той или иной процедуры[79]. Данные о таком "неповторимом опознавательном признаке" могут храниться на любой карточке с микропроцессором, по усмотрению гражданина (включая карточки для снятия наличных через банкоматы, карточки системы социального страхования, членские карточки профессиональных союзов и ассоциаций, а также в стационарных и портативных персональных компьютерах). Наряду с этим данные для создания цифровых подписей могут передаваться по мобильным телефонам в виде одноразовых кодов, специально генерируемых оператором сети сотовой связи, который также выступает в роли хранителя информации о неповторимых опознавательных признаках граждан.

76. Вышеупомянутая система обеспечивает возможность разделения присваиваемых пользователям опознавательных признаков по секторам. При этом все они привязаны к централизованному банку идентификационных данных, но строго отделены друг от друга по секторальному признаку. Такая архитектура позволяет избежать проблем совместного доступа к данным и обеспечить защиту информации частного характера. Карточкам, называемым "карточками гражданина", имеется в виду придать статус официальных удостоверений личности для целей электронных административных процедур, таких как подача заявлений через Интернет. С введением карточек гражданина создается общедоступная инфраструктура защиты данных, открытая также для коммерческих пользователей. У компаний появляется возможность использовать основанную на этих карточках инфраструктуру для безопасного обеспечения своих клиентов услугами в режиме онлайн.

77. В результате подобных инициатив очень многие граждане получают в свое распоряжение недорогостоящие устройства, способные, среди прочего, служить для создания электронных подписей. Хотя основные цели таких инициатив не обязательно связаны с торговлей, устройства подобного рода могут с тем же успехом использоваться и в коммерческой сфере. Сближение этих двух областей их применения признается все чаще[80].

---

[79] Zentrum für sichere Informationstechnologie Austria (A-Sit), *XML Definition of the Person Identity Link*; размещено по адресу http://www.buergerkarte.at/konzept/personenbindung/spezifikation/aktuell/ (дата посещения – 6 июня 2008 года).

[80] См., например, *2006 Korea Internet White Paper* (Seoul, National Internet Development Agency of Korea, 2006), p. 81, где упоминается о двойном применении положений Закона Республики Корея об электронной подписи для целей электронного правления и электронной торговли; размещено по адресу http://www.ecommerce.or.kr/activities/documents_view.asp?bNo= 642&Page=1 (дата посещения – 6 июня 2008 года).

II. Правовой режим электронного удостоверения подлинности и электронных подписей

78. Для развития электронной торговли чрезвычайно важно обеспечить доверие к ней. 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[81]; или договорных соглашениях[82].

79. 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.

80. 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 использованию единой системы связи на основе таких общедоступных средств, как Интернет. При этом даже в рамках таких 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, "системные правила", "оперативные правила" или "соглашения о торговом партнерстве") и которые направлены

[81] 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 – 5 июня 2008 года).

[82] 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 рекомендации размещены по адресу http://www.unece.org/cefact/recommendations/rec_index.htm (дата посещения – 5 июня 2008 года)).

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[83]. В пределах предусмотренной применимым правом свободы договоров вопрос об обеспечении соблюдения таких правил и соглашений, как правило, решается в них самих.

81. Однако в отсутствие договорных норм или в условиях, когда возможности для обеспечения принудительного исполнения таких норм ограничены 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

82. 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 двусоставный подход[84].

1. Минималистский подход

83. В некоторых правовых системах проводится нейтральная с точки зрения технологий политика, при которой признаются все технологии электронной подписи[85]. Этот подход носит название минималистского, поскольку предполагает наделение всех видов электронной подписи неким минимальным юридическим статусом. В соответствии с минималистским подходом 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.

84. В Типовом законе ЮНСИТРАЛ об электронной торговле изложен наиболее широко применяемый набор законодательных критериев для установления общей

---

[83] 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.

[84] 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.

[85] Например, в Австралии и Новой Зеландии.

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".

85. 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 видов 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.

86. 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[86].

87. Если не считать Европы, где законодательство формируется главным образом под влиянием директив Европейского союза[87], то в большинстве стран, где приняты законодательные акты, касающиеся электронной торговли, в качестве образца для них был использован Типовой закон об электронной торговле[88]. Этот Типовой закон

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

[87] 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, *Official Journal of the European Communities*, L 13, 19 January 2000). 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 (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, *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.

[88] По состоянию на январь 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 (1999 год); Венесуэла (Боливарианская Республика) – Закон

также был положен в основу согласования законодательства об электронной торговле внутри стран, имеющих федеративное устройство, таких как Канада[89] и Соединенные Штаты Америки[90]. За очень немногими исключениями[91], в странах, которые ввели в действие Типовой закон, был сохранен используемый в нем технологический нейтральный подход, 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 (принят в 2001 году), а также в более новой Конвенции Организации Объединенных Наций

о сообщениях данных и электронных подписях (2001 год); Вьетнам – Закон об электронных сделках (2006 год); Доминиканская Республика – Закон об электронной торговле, цифровых документах и подписях (2002 год); Индия – Закон об информационных технологиях (2000 год); Иордания – Закон об электронных сделках (2001 год); Ирландия – Закон об электронной торговле (2000 год); Китай – Закон об электронных подписях, введен в действие в 2004 году; Колумбия – Закон об электронной торговле; Маврикий – Закон об электронных сделках (2000 год); Мексика – Декрет о пересмотре и дополнительном включении различных положений в гражданские кодексы субъектов федерации по вопросам, отнесенным к ведению федерации, а также в Федеральный гражданско-процессуальный кодекс, Торговый кодекс и Федеральный закон о защите потребителей (2000 год); Новая Зеландия – Закон об электронных сделках (2002 год); Пакистан – Указ об электронных сделках (2002 год); Панама – Закон о цифровой подписи (2001 год); 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 – Закон 2000-230 о приспособлении правил доказывания для учета информационных технологий и электронных подписей (2000 год); Шри-Ланка – Закон об электронных сделках (2006 год); Эквадор – Закон об электронной торговле, электронных подписях и сообщениях данных (2002 год); и Южная Африка – Закон об электронных коммуникациях и сделках (2002 год). Типовой закон принят также в зависимых территориях Британской короны – в Бейливике Гернси (Закон Гернси об электронных сделках (2000 год)), Бейливике Джерси (Закон Джерси об электронных сделках (2000 год)) и на острове Мэн (Закон об электронных сделках (2000 год)); в заморских территориях Соединенного Королевства Великобритании и Северной Ирландии – Бермудских островах (Закон об электронных сделках (1999 год)), Каймановых островах (Закон об электронных сделках (2000 год)) и островах Тёркс и Кайкос (Указ об электронных сделках (2000 год)); а также в Специальном административном районе (САР) Китая Гонконге (Указ об электронных сделках (2000 год)). Если не указано иное, последующие ссылки в настоящем документе на законодательные положения любой из этих стран относятся к положениям вышеперечисленных законов.

[89] В Канаде Типовой закон вводится в действие посредством Единообразного закона об электронной торговле, принятого в 1999 году Канадской конференцией по унификации 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 – 6 июня 2008 года). С тех пор этот Закон вступил в силу в 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 (2001 год)), 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. Обновленную информацию о ходе принятия Единообразного закона об электронной торговле можно найти по адресу http://www.ulcc.ca (дата посещения – 5 июня 2008 года).

[90] В Соединенных Штатах Типовой закон ЮНСИТРАЛ об электронной торговле был использован Национальной конференцией уполномоченных по унификации законодательства штатов в качестве основы при разработке Единообразного закона об электронных сделках, принятого 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 – 6 июня 2008 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, Виргиния, Висконсин, Гавайи, Делавэр, Западная Виргиния, Индиана, Калифорния, Канзас, Кентукки, Колорадо, Коннектикут, Луизиана, Массачусетс, Миннесота, Миссисипи, Миссури, Мичиган, Монтана, Мэн, Мэриленд, Небраска, Невада, Нью-Гэмпшир, 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 введение в действие этого Закона, 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). Обновленную 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 – 6 июня 2008 года).

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

об использовании электронных сообщений в международных договорах (принята Генеральной Ассамблеей в ее резолюции 60/21 от 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, пункт 95).

88. Если в законодательстве принят минималистский подход, то вопрос о том, считать ли доказанной эквивалентность электронной подписи, обычно решается судьей, арбитром или публичным органом – как правило, на основании так называемого "надлежащего критерия надежности". При этом все типы электронной подписи, удовлетворяющие предъявляемым требованиям, считаются действительными; таким образом, данный критерий воплощает в себе принцип нейтральности с точки зрения технологий.

89. При определении того, обеспечивает ли тот или иной способ удостоверения подлинности надлежащую степень надежности в соответствующих 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*) функции 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 любым 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 внедрение; 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

90. 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 часто склонны считать своей целью наивысшую степень защиты, которую способна обеспечить существующая технология[92]. Практическая

[92] 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 (размещено по адресу http://www.le.state.ut.us/~2006/htmdoc/ sbillhtm/sb0020.htm; дата посещения – 6 июня 2008 года). Технологическая предвзятость, присущая этому закону штата Юта, также прослеживается 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 (Закон о цифровой подписи (2001 год) и Декрет № 2628/2002 (постановление о порядке применения Закона о цифровой подписи)); 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 (2000 год)); Литвы (Закон об электронных подписях (2000 год)); Малайзии (Закон об электронной подписи (1997 год)); 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)).

необходимость применения строгих мер безопасности для предотвращения несанкционированного доступа к данным, а также 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 степенями юридической надежности, возможными при бумажном документообороте. Деловые люди, оперирующие бумажными документами, в большинстве случаев могут по своему выбору 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 правила, обусловливающие действительность электронной подписи использованием определенной технологии. Так обстоит дело, например, в случаях, когда закон, преследующий цель достижения более высокого уровня надежности, требует применения технологий на основе ИПК. Поскольку при этом предписывается использование конкретной технологии, такой подход называют также "предписательным".

91. 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"[93]. 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[94]. 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 способно стать препятствием распространению электронной торговли.

92. 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 правительственного 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

---

[93] Stewart Baker and Matthew Yeo, в сотрудничестве с секретариатом Международного союза электросвязи, "Background and issues concerning authentication and the ITU", информационная записка, представленная на Совещании экспертов по вопросам электронных подписей и сертификационных органов, Женева, 9–10 декабря 1999 года, document No. 2; размещено по адресу www.itu.int/osg/spu/ni/esca/meetingdec9-101999/briefingpaper.html (дата посещения – 6 июня 2008 года).

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

как одна или несколько систем удостоверения подлинности могут быть 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 на выполнение своих функций или в разрешениях на использование той или иной технологии (за возможным исключением правил, касающихся защиты потребителей)[95];

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[96];

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[97]. Еще один способ, посредством которого правительства могут косвенно направлять процесс использования цифровых подписей, связан с системами управления идентификационными записями (см. пункты 66–77, выше). Правительствами некоторых стран уже начаты программы выдачи своим гражданам удостоверений личности, пригодных для машинного считывания (“электронные удостоверения личности”), которые оснащены функциями создания цифровой подписи.

3. Двухуровневый или двусоставный подход

93. 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 надежными цифровыми

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

[96] См. Asia-Pacific Economic Cooperation, *Assessment Report* ... о примере Сингапура.

[97] См. Asia-Pacific Economic Cooperation, *Assessment Report* ... о примерах Китая и Малайзии.

подписями либо отвечающими установленным требованиям сертификатами)[98] 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 действует ряд опровержимых презумпций, необходимы для выполнения особых требований, которые могут быть связаны с конкретной технологией. На сегодняшний день такие защищенные подписи обычно определяются в законах упомянутого типа со ссылкой на технологию ИПК.

94. Данный подход, как правило, применяется в правовых системах, где считается важным закрепить в законодательстве определенные требования в отношении технологий, оставив, однако, открытой возможности для технического прогресса. Он позволяет обеспечить в вопросе об электронных подписях баланс между гибкостью и определенностью, предоставив сторонам возможность самостоятельно принимать, исходя из своих потребностей, коммерческие решения 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 90–92). 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.

95. Законодательство, основанное на двухуровневом подходе, первыми приняли Сингапур[99] и Европейский союз[100]. За ними последовал ряд других правовых

---

[98] Aalberts and van der Hof, *Digital Signature Blindness* …, para. 3.2.2.

[99] 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 этого Закона (т. е. подписей, которые "*a*) являются уникальными и 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"), действуют презумпции, указанные в статье 18 (в частности, что подпись "является подписью лица, с которым она связана" и что подпись "была поставлена этим лицом с намерением подписать или одобрить соответствующую электронную запись"). Цифровые подписи, подкрепленные заслуживающим доверие сертификатом, соответствующим положениям статьи 20 этого Закона, автоматически признаются "защищенными электронными подписями" для целей Закона.

[100] Как и в Законе Сингапура об электронных сделках, в Директиве Европейского союза об электронных подписях (*Official Journal of the European Communities*, L 13/12, 19 January 2000) 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 в качестве средства удостоверения подлинности") и "усовершенствованной электронной подписью" (определяемой в пункте 2 статьи 2 как электронная подпись, отвечающая следующим требованиям: "*a*) наличие уникальной связи с подписавшим лицом; *b*) подпись 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 этой Директивы государствам – членам Европейского союза предписывается обеспечить, чтобы "электронная подпись не могла

систем[101]. Типовой закон ЮНСИТРАЛ об электронных подписях позволяет принимающему его государству создать у себя двухуровневую систему на основе подзаконных актов, хотя специально не побуждает к этому[102].

96. В отношении второго уровня странам было предложено не требовать использования подписей второго уровня для выполнения требований в отношении формы применительно к международным коммерческим сделкам, 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.)[103]. Более того, было предложено прямо подтверждать в двухуровневом законодательстве юридическую силу договорных соглашений об использовании и признании электронных подписей, с тем чтобы основанные на договорах глобальные схемы удостоверения подлинности не входили в противоречие с требованиями национального права.

B. Доказательственная ценность электронных методов подписания и удостоверения подлинности

97. Одна из основных целей Типового закона ЮНСИТРАЛ об электронной торговле и Типового закона ЮНСИТРАЛ об электронных подписях заключается в предотвращении возникновения несоответствий, а также возможного чрезмерного регулирования за счет предложения общих критериев 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.

быть лишена юридической силы или не признана в качестве доказательства в процессе судопроизводства 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).

[101] Например, Маврикий и Пакистан. Подробнее о соответствующих законах см. сноску 88 выше.

[102] В пункте 3 статьи 6 Типового закона ЮНСИТРАЛ об электронных подписях 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.

[103] Baker and Yeo, "Background and issues concerning authentication …".

1. “Удостоверение подлинности” и общая атрибуция электронных записей

98. 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, так как суды, по-видимому, проявляют тенденцию к вынесению разных заключений в зависимости от функций, которыми наделяется тот или иной метод удостоверения подлинности.

99. Об атрибуции сообщений данных говорится в статье 13 Типового закона об электронной торговле. Это положение основывается на статье 5 Типового закона ЮНСИТРАЛ о международных кредитовых переводах[104], 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 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.

100. 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 случая, когда сообщение было направлено иным, чем составитель, лицом, которое правомочно действовать от имени составителя. В пункте 3 идет речь о двух типах ситуаций, когда адресат может полагаться на сообщение данных как на сообщение составителя: это, во-первых, случаи, 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 отношений с составителем имело доступ к процедурам удостоверения подлинности, используемым составителем.

101. Норма, зафиксированная в статье 13 Типового закона об электронной торговле, включая презумпцию атрибуции, установленную в пункте 3 этой статьи, принята в

[104] Издание Организации Объединенных Наций, в продаже под № R.99.V.11; размещено по адресу http://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf (дата посещения – 6 июня 2008 года).

целом ряде стран[105]. В некоторых странах использование кодов, паролей или других средств идентификации прямо отнесено к числу факторов, из которых возникает презумпция авторства[106]. 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[107].

102. В то же время в некоторых странах приняты лишь общие правила, изложенные в статье 13 и состоящие в том, что сообщение данных является сообщением данных составителя, если оно было отправлено составителем лично либо лицом, действовавшим от имени составителя, либо системой, запрограммированной составителем или от его имени функционировать в автоматическом режиме[108]. 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[109]. 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"[110].

103. 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 исходит из понимания 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 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

---

[105] 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. сноску 88, выше.

[106] Мексика (см. сноску 88, выше), статья 90, пункт I.

[107] Например, Единообразный закон Соединенных Штатов об электронных сделках (см. сноску 90) 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".

[108] Австралия (статья 15, пункт 1); в принципе аналогичным образом – Индия (статья 11); Пакистан (статья 13, пункт 2) и Словения (статья 5). См. также: зависимая территория Британской короны остров Мэн (статья 2) и САР Китая Гонконг (статья 18). Подробнее о соответствующих законах см. сноску 88, выше.

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

[110] Канада, Единообразный закон об электронной торговле (и официальный комментарий к нему) (см. сноску 89), комментарий к статье 10.

быть доказано любым способом, включая доказывание эффективности любой контрольной процедуры, примененной для определения лица, к которому можно отнести электронную запись или электронную подпись"[111]. 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"[112]. Поэтому, как указывается в комментарии к закону Соединенных Штатов,

> "4. В электронной среде может присутствовать определенная информация, которая, как представляется, не позволяет произвести 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 для выявления стороны, к которой следует отнести электронную запись. Еще одно доказательство для целей атрибуции, связано, несомненно, с процедурами контроля.
>
> Включение конкретной ссылки на процедуры контроля как на средство доказывания атрибуции является полезным ввиду уникального значения процедур контроля в электронной среде. В рамках некоторых процессов техническая и технологическая процедура контроля может лучше всего 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 контроля 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 контроля не подразумевает, что другие формы доказывания атрибуции следует считать менее убедительными. Важно также помнить о том, что конкретная степень надежности какой-либо процедуры не затрагивает ее статус в качестве процедуры контроля, но влияет лишь на то значение, которое следует придавать доказательствам, полученным с помощью данной процедуры контроля и направленным на произведение атрибуции"[113].

---

[111] Соединенные Штаты, Единообразный закон об электронных сделках (1999 год) (см. сноску 90), статья 9. В пункте 1 официального комментария к статье 9 приводятся следующие примеры случаев, когда уместна 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 определенной информации о параметрах инвентарных запасов, направляет закупочный заказ, составной частью которого является указание имени лица или другая идентифицирующая это лицо информация".

[112] 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 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. Самое важное 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".

[113] Официальный комментарий к статье 9.

104. 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"[114].

105. На фоне столь гибкого представления об атрибуции суды Соединенных Штатов, как представляется, придерживаются либерального подхода к вопросу о допустимости электронных записей, включая электронную почту, в качестве доказательств в ходе гражданско-правового производства[115]. Суды Соединенных Штатов 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[116]. Вместо этого суды приходили к выводу, что сообщения по электронной почте, предоставленные истцом в процессе предъявления доказательств, являются сообщениями с самоудостоверенной подлинностью, поскольку "предъявление сторонами в качестве доказательств документов из их собственных архивов является достаточным для обоснования вывода о самоудостоверении их подлинности"[117]. Суды склонны принимать во внимание все имеющиеся доказательства и не отклоняют электронные записи как недопустимые prima facie.

106. В странах, которые не приняли Типового закона об электронной торговле, как представляется, конкретных законодательных положений, где аналогичным образом решался бы вопрос об атрибуции, не имеется. В таких странах атрибуция, как правило, представляет собой следствие правового признания электронных подписей и презумпций, относимых к записям, подлинность которых удостоверена электронной подписью конкретного типа. Так, 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[118]. Другие примеры более ограничительного подхода к доказательственной ценности электронных записей и вопросу об атрибуции можно найти в недавних связанных с проведением аукционов в Интернете делах, при рассмотрении 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

---

[114] Пункт 6 официального комментария к статье 9.

[115] *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.

[116] *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.

[117] *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.

[118] 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 – 6 июня 2008 года).

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 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[119], 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"[120]. 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[121]. Такую презумпцию можно представить себе в отношении "усовершенствованной электронной подписи", как она определена в законодательстве, но владелец обычного пароля не должен нести риск неправомерного использования этого пароля не уполномоченными на то лицами[122].

2. Возможность соответствия юридическим требованиям в отношении подписи

107. В ряде стран суды проявляли склонность к либеральному толкованию требований в отношений подписи. Как уже отмечалось (см. "Введение", пункты 2–4), 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 также с готовностью принимали во внимание законодательные положения о признании электронных подписей, допуская их использование и в ситуациях, не предусмотренных прямо в

---

[119] 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/20020291.htm (дата посещения – 6 июня 2008 года); см. также Landgericht (Суд земли) 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 – 6 июня 2008 года).

[120] Германия, Landgericht (суд земли) 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 – 6 июня 2008 года).

[121] Германия, Landgericht (суд земли) 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 – 6 июня 2008 года).

[122] 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 – 6 июня 2008 года).

санкционирующем законе, в частности в связи с судебными предписаниями[123]. 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[124]. Сознательное указание каким-либо лицом своего имени в напечатанном виде в конце всех сообщений по электронной почте было сочтено действительным удостоверением подлинности[125]. Готовность судов Соединенных Штатов признать, что сообщения по электронной почте и указанные в их тексте имена могут считаться удовлетворяющими требованиям в отношении письменной формы[126], соответствуют либеральному толкованию понятия "подпись" как включающего "любой символ, исполненный или принятый стороной с присутствующим у нее 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"[127]. Если стороны не отрицают факта 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, связывающая поставившее ее лицо, может принимать форму любой пометки или обозначения, которые сторона, принимающая на себя обязательство, считает подходящими", при условии что ее автор "намеревается связать себя обязательствами"[128].

108. 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 носители 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, могут быть признаны "документами", а имена, набранные в тексте этих сообщений, – "подписями"[129]. 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

---

[123] *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.

[124] *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.

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

[126] *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.

[127] Ibid, p. 919: "Внутренние документы, счета-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.

[128] *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.

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

данного документа", причем "тот факт, что документ создан электронным способом, а не составлен на бумаге, ничего не меняет"[130]. 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 не выполненными из-за того, что сообщения, направлявшиеся по электронной почте, отражали содержание ведущихся переговоров, а не окончательное соглашение – например, по той причине, что одна из сторон на переговорах исходила из того, что имеющий обязательную силу договор не будет считаться заключенным до подписания "меморандума о сделке"[131]. 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"[132]. 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, 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[133].

109. 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[134].

---

[130] *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).

[131] *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)).

[132] *Mehta v. J. Pereira Fernandes S.A. ...* .

[133] *Mehta v. J. Pereira Fernandes S.A. ...* , No. 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 путем ответа на вопрос 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 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]".

[134] Кассационный суд Франции отказал в принятии заявления об обжаловании, подписанного в электронной форме, из-за сомнений в отношении идентификации лица, поставившего подпись, и ввиду

Отражением несколько более либеральной позиции являются решения, допускающие подачу жалоб административного характера в электронной форме в целях соблюдения установленных законом сроков, пусть даже при условии, чтобы такие жалобы впоследствии были подтверждены обычными почтовыми отправлениями[135].

110. 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 передаваемых непосредственно с компьютера через модем на факсимильную аппаратуру суда. В связи с предыдущими делами апелляционные суды[136] и Федеральный суд[137] 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 именно законодатель, а не суды[138]. Такое понимание в конечном счете было отвергнуто с учетом единодушного мнения других высоких федеральных судов, которые признали возможность подачи определенных процессуальных документов посредством электронной передачи сообщения данных, сопровождаемого отсканированным изображением подписи[139].

111. Интересно отметить, что даже суды в некоторых системах гражданского права, где принято законодательство, отдающее предпочтение использованию циф-

---

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 http://www.juriscom.net/jpt/visu.php?ID=239 (дата посещения – 6 июня 2008 года)).

[135] Франция, Conseil d'État, 28 décembre 2001, N° 235784, *Élections municipales d'Entre-Deux-Monts* (текст имеется в Секретариате).

[136] 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 http://www.jurpc.de/rechtspr/19980009.htm (дата посещения – 6 июня 2008 года).

[137] 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 – 6 июня 2008 года).

[138] Ibid.

[139] В решении по делу, переданному ей германским Федеральным судом, Совместная палата высоких федеральных судов Германии отметила, что требования в отношении формы в ходе судебного производства не являются самоцелью. Они призваны обеспечить возможность достаточно надежного определении 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 подача определенных процессуальных документов, представленных посредством электронной передачи сообщения данных с отсканированным изображением подписи, соответствовала бы духу имеющегося 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 – 6 июня 2008 года)).

ровых подписей на основе ИПК, например в Колумбии[140], применяют столь же либеральный подход и подтверждают, например, допустимость судопроизводства, осуществляемого целиком посредством электронных сообщений. Материалы, обмен которыми имеет место в ходе такого судопроизводства, считаются действительными, даже если они не скреплены цифровой подписью, поскольку при передаче электронных сообщений используются методы, обеспечивающие возможность идентификации сторон[141].

112. 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 отношении электронных подписей и электронного удостоверения подлинности влияет подход к этим вопросам, применяемый в законодательстве. Можно говорить о том, что повышенное внимание законодателей к электронным "подписям" без сопутствующего этому общего правила, касающегося атрибуции, приводит к 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 контексте 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) Применение на международном уровне: электронные апостили

113. С 28 октября по 4 ноября 2003 года в Гааге проходили заседания Специальной комиссии по рассмотрению практического действия Конвенции, отменяющей требование легализации иностранных официальных документов (Гаагская конвенция об апостиле), Конвенции о вручении за границей судебных и внесудебных документов

[140] 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 (Закон об электронной торговле, статья 28).

[141] 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 суде; 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 – 6 июня 2008 года)).

по гражданским и торговым делам[142] (Гаагская конвенция о вручении) и Конвенции о получении за границей доказательств по гражданским или торговым делам (Гаагская конвенция о доказательствах)[143]. На сессии Специальной комиссии по рассмотрению практического действия гаагских конвенций об апостиле, доказательствах и вручении присутствовали 116 делегатов от 57 государств-членов, являвшихся участниками одной или более рассматриваемых конвенций, а также наблюдателей. Специальная комиссия отметила, что в условиях применения этих трех конвенций происходят важные изменения, связанные с развитием техники. Специальная комиссия подчеркнула, что, хотя такую эволюцию было невозможно предвидеть в то время, когда принимались упомянутые конвенции, сегодня передовые технологии прочно вошли в жизнь общества, а их применение стало реальностью[144]. В этой связи Специальная комиссия указала, что дух и буква конвенций не создают препятствий использованию современных технологий и что эффективность применения и действия конвенций можно дополнительно повысить с помощью таких технологий[145]. Специальная комиссия рекомендовала государствам-участникам и Постоянному бюро Гаагской конференции по международному частному праву предпринять усилия по разработке способов выдачи электронных апостилей, "принимая во внимание, в частности, типовые законы ЮНСИТРАЛ об электронной торговле и электронных подписях, каждый из которых основан на принципах недискриминации и функциональной эквивалентности"[146]. В апреле 2006 года Постоянным бюро Гаагской конференции по международному частному праву и Национальной ассоциацией нотариусов (НАН) Соединенных Штатов была начата экспериментальная программа по электронным апостилям (э-АПП). В рамках этой программы 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)[147]. Программой предусмотрены два отдельных, но в конечном счете идентичных друг другу формата э-апостилей. Оба соответствующих метода обеспечивают защиту от несанкционированных изменений исходного документа и сертификата э-апостиля, но различаются по форме их представления получателю.

114. В соответствии с первым методом компетентный орган добавляет сертификат апостиля в виде заключительной страницы к удостоверяемому им публичному документу в соответствующем формате (программа э-АПП предполагает обмен документами в формате PDF (Portable Document Format)). При этом получатель, открыв документ и дойдя до его последней страницы, видит на ней сертификат э-апостиля. Выбор данного метода означает, что и удостоверяемый публичный документ, и сертификат

---

[142] United Nations, *Treaty Series*, vol. 658, No. 9432.

[143] Ibid., vol. 847, No. 12140.

[144] 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", para.4 (размещено по адресу http://hcch.e-vision.nl/upload/wop/lse_concl_e.pdf (дата посещения – 6 июня 2008 года)).

[145] Hague conference on Private International Law "Conclusions and recommendations adopted by the Special Commission ...".

[146] Hague conference on Private International Law "Conclusions and recommendations adopted by the Special Commission ...", para. 24.

[147] Christophe Bernasconi and Rich Hansberger, "Electronic Apostille Pilot Program (e-APP): memorandum on some of the technical aspects underlying the suggested model for the issuance of electronic apostilles (e-apostilles)"; размещено по адресу http://www.hcch.net/upload/wop/ genaff_pd18e2007.pdf (дата посещения – 26 мая 2008 года).

э-апостиля становятся частью единого документа или, иными словами, одного и того же электронного файла. Это, впрочем, не мешает при желании распечатывать из такого файла отдельные страницы и, следовательно, сертификат э-апостиля также может быть напечатан отдельно[148].

115. При использовании второго метода удостоверяемый публичный документ присоединяется к сертификату э-апостиля в качестве отдельного файла. Получателю, как и в первом случае, предоставляется единый PDF-файл, открыв который он, однако, сначала просматривает сертификат э-апостиля, а затем может отдельно открыть в формате PDF приложение с удостоверяемым публичным документом. Существует мнение, что такой метод интуитивно более удобен для получателя снабженного апостилем документа (так, именно он был избран Государственным департаментом Соединенных Штатов для оформления электронных патентных заявок и в качестве образца для э-апостилей). Когда файл с удостоверяемым публичным документом прилагается к сертификату э-апостиля, имеется в виду дать получателю при первом же открытии документа со всей очевидностью понять, что перед ним – апостиль. После этого получатель может открыть сам публичный документ для ознакомления с его содержанием[149].

116. В рамках как одной, так и другой модели использование э-апостилей предполагает выдачу сертификатов в электронной форме за цифровой подписью органа, обладающего необходимой компетенцией для целей Гаагской конвенции об апостиле. При этом каждый компетентный орган должен вести электронный реестр, обеспечивающий возможность проверки выданных сертификатов э-апостиля[150].

117. В странах, где требования легализации и апостили были упразднены, можно представить себе создание систем, при которых записи, заверенные иностранным нотариусом, получали бы юридическое признание на основании проверки электронной подписи этого нотариуса или использованного им электронного средства удостоверения подлинности. Электронная подпись нотариуса, заверившего документ, должна поддаваться простой и быстрой проверке пользователем документа (в роли которого обычно выступает другой нотариус). Такая проверка может производиться с помощью Интернета, через сайт поставщика сертификационных услуг, которыми пользуется первый нотариус; как правило, по крайней мере в странах Европы, таким поставщиком является национальная нотариальная палата, в которой состоит этот нотариус. В данной связи возникает также вопрос о проверке полномочий заверившего документ нотариуса выполнять функции заверения документов в той правовой системе, в которой он осуществляет свою деятельность. Для упрощения этой процедуры и во избежание необходимости обращаться в иностранный надзорный орган по лицензированию нотариусов, если таковой имеется в соответствующей стране, было предложено, чтобы поставщики сертификационных услуг при нотариальных палатах выдавали сертификаты только тем нотариусам, которые на данный момент допущены к выполнению нотариальных функций; таким образом, при любом приостановлении или аннулировании полномочий нотариуса его подпись автоматически переставала бы опознаваться как действительная[151].

---

[148] “Electronic Apostille Pilot Programme …”, para. 18.

[149] “Electronic Apostille Pilot Programme …”, para. 19.

[150] Дополнительную информацию об использовании э-апостилей см. на веб-сайте э-АПП по адресу http://www.e-app.info/ (дата посещения – 6 июня 2008 года).

[151] Ugo Bechini et Bernard Reynis, “La signature électronique transfrontalière des notaires: une réalité européenne”, *La semaine juridique (L'édition notariale et immobilière)*, No. 39, 24 September 2004, p. 1447.

b) Внутригосударственное применение: печати, нотариальное заверение и засвидетельствование

118. 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[152]. В других правовых системах действует законодательство, согласно которому требование в отношении печати может считаться выполненным при наличии защищенной электронной подписи. Например, в Ирландии приняты конкретные положения, позволяющие использовать вместо печати, с согласия лица или публичного органа, которому должен или может быть представлен скрепленный печатью документ, должным образом удостоверенные защищенные электронные подписи[153]. 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[154].

119. В целом ряде стран начаты также инициативы, предполагающие использование электронных документов и подписей при сделках с недвижимостью, требующих составления актов за печатью. Схема, применяемая в штате Виктория (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 соответствующих документов солиситорами по поручению своих клиентов через закрытую компьютерную сеть. В некоторых законодательных актах официально признается возможность использования "электронных печатей" в качестве альтернативы "ручным печатям"; при этом технические детали, касающиеся формы электронной печати, должны быть оговорены отдельно[155].

120. В Единообразном законе Соединенных Штатов об электронной регистрации прав на недвижимое имущество[156] прямо говорится, что электронная подпись не

---

[152] 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 депонированные документы за печатью" (Law Com. No.143, 1987).

[153] 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.

[154] Канада, Закон о защите личной информации и электронных документах (2000 год), часть 2, статья 39. Ссылка на федеральные законы относится к Закону о федеральной земельной собственности и федеральном недвижимом имуществе и к Постановлению о федеральной земельной собственности.

[155] 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 для целей Профессиональной ассоциации инженеров и специалистов провинции Манитоба, занимающихся науками о Земле, "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 – 6 июня 2008 года)).

[156] Единообразный закон Соединенных Штатов об электронной регистрации прав на недвижимое имущество был подготовлен Национальной конференцией уполномоченных по унификации законодательства штатов; размещен по адресу http://www.law.upenn.edu/bll/ulc/urpera/URPERA_Final_Apr05-1.htm (дата посещения – 6 июня 2008 года). Этот закон принят в Айдахо, Аризоне, Арканзасе, Вашингтоне, Виргинии,

обязательно должна сопровождаться физическим или электронным изображением штемпеля, оттиска или печати. По существу, необходимой является только информация, указанная на печати, но не сама печать. Предусмотрено также, 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[157]. 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.

121. В системах гражданского права печати редко применяются при оформлении документов частного характера, но в большинстве таких систем для подтверждения личности сторон и подлинности документов широко используется нотариальное заверение. В ряде стран гражданского права нотариусы уже внедрили достижения информационных и коммуникационных технологий в свою повседневную работу. При нотариальных палатах многих стран организовано оказание сертификационных услуг и выдаются сертификаты, обеспечивающие возможность использования электронных подписей (как правило, цифровых) нотариусами – членами палаты, а иногда и другими гражданами.

122. В Италии Управление по информационно-технологическому обеспечению государственных учреждений 12 сентября 2002 года постановило разрешить Нотариальному совету оказывать сертификационные услуги итальянским нотариусам, цифровые подписи которых можно проверить в режиме онлайн[158]. Кроме того, нотариусы в Италии сейчас полностью переходят на электронные способы передачи записей в публичные регистры. Так, передача уставных актов и документов компаний, а также поправок к ним, в регистры коммерческой документации уже осуществляется целиком на безбумажной основе. Значительный прогресс достигнут также в области электронной передачи записей о сделках с недвижимостью, хотя для этого до сих пор используются и бумажные документы, что объясняют задержками с внедрением технологий электронного обмена сообщениями в судебной системе. Услуги такого рода оказываются при поддержке корпорации, специально созданной Советом и Национальным фондом нотариата в 1997 году для содействия итальянским нотариусам в использовании информационных и коммуникационных технологий[159]. Аналогичная система действует в Испании, где Всеобщим нотариальным советом учрежден собственный сертификационный орган, а нотариусами создан механизм электронной регистрации записей в коммерческих регистрах[160].

Висконсине, Делавэре, Иллинойсе, Канзасе, округе Колумбия, Коннектикуте, Миннесоте, Неваде, Нью-Мексико, Северной Каролине, Теннесси, Техасе, Флориде и Южной Каролине (см. http://www.nccusl.org (дата посещения – 20 марта 2008 года)).

[157] Т. е. предусматриваются критерии, близкие к тем, которые установлены Единообразным законом Соединенных Штатов об электронных сделках.

[158] См. http://ca.notariato.it (дата посещения – 6 июня 2008 года).

[159] См. www.notariato.it, раздел “Servizi Notartel” (дата посещения – 6 июня 2008 года).

[160] См. http://www.notariado.org/n_tecno (дата посещения – 6 июня 2008 года).

123. Во Франции пересмотренный вариант статьи 1317 Гражданского кодекса разрешает, например, делать "подлинные записи актов" электронным способом при соблюдении условий, которые должны быть определены Государственным советом. Высший нотариальный совет Франции установил систему сертификации электронных подписей, используемых французскими нотариусами[161]. Система, которой пользуются французские нотариусы, сертифицируется корпорацией по оказанию сертификационных услуг, учрежденной несколькими ведомствами правительства страны. Хотя во Франции нотариусы используют электронную передачу записей еще не так широко, как в Италии и Испании, разработанная в мае 2006 года прикладная программа "Télé@actes" должна позволить им полностью перейти на электронный обмен документацией с ипотечными регистрами для целей передачи и получения свидетельств о праве собственности. Ведется работа по переносу на цифровые носители бумажных документов о правах на недвижимость.

124. В Германии Федеральный закон 1993 года об ускорении регистрационных процедур[162] открыл возможность регистрации недвижимости, а также ведения коммерческих и других предусмотренных законодательством реестров в электронной форме. Судебные органы земель используют эту возможность в неодинаковой степени, применяя отличные друг от друга технические решения[163]. Введение системы электронной регистрации позволило германским нотариусам обмениваться информацией с регистрами напрямую, посредством электронных сообщений. Для придания нотариально заверенным электронным записям той же степени надежности, какой обладают нотариально заверенные бумажные документы, германскими нотариусами был в соответствии с требованиями Закона Германии об электронных подписях учрежден орган по оказанию сертификационных услуг. 15 декабря 2000 года учреждение, занимающееся в Германии регулированием деятельности в сфере телекоммуникаций, выдало этому поставщику сертификационных услуг соответствующую лицензию. Созданная германскими нотариусами сертификационная система, как и ее аналоги, возникшие ранее в других странах, основана на использовании ИПК и технологии цифровых подписей. Сертификаты, выдаваемые поставщиком сертификационных услуг при Федеральной нотариальной палате, удостоверяют не только публичный ключ, используемый нотариусом для подписания документов, но и полномочия подписавшего лица как присяжного нотариуса. В германской системе цифровые подписи используются для удостоверения подлинности записей как при их создании, так и при любом последующем воспроизведении. В руководящих принципах, изданных Федеральной нотариальной палатой Германии, нотариусам напоминается о необходимости обеспечивать безопасность электронных документов при их передаче, например, используя для этого только каналы, защищенные протоколом SSL[164]. В целях упрощения обработки электронных записей регистрами и их использования клиентами германские нотариусы обязаны составлять документы в стандартном формате (с использованием расширяемого языка гипертекстовой разметки,

---

[161] "La signature électronique notariale certifiée," *La Revue Fiscale Notariale*, No. 10, Octobre 2007, Alerte 53.

[162] Германия, Bundesgesetztblatt, часть I, 20 декабря 1993 года, p. 2182.

[163] См. информацию Федеральной нотариальной палаты о масштабах внедрения электронных реестров в Германии по адресу http://www.bnotk.de/Service/Elektronischer_Rechtsverkehr/Registerelektronisierung.html (дата посещения – 6 июня 2008 года).

[164] См. "*Empfehlungen zur sicheren Nutzung des Internet*", Rundschreiben 13/2004 der Bundesnotarkammer vom 12.03.2004 (размещено по адресу http://www.bnotk.de/Service/Rundschreiben/RS.2004.13.sichere.Internetnutzung.html (дата посещения – 6 июня 2008 года)).

или XML)[165]. Действующие в Германии правила электронного оформления подлинных записей предусматривают два уровня нотариального заверения. Все электронные записи вместе с приложениями и файлами, содержащими цифровую подпись нотариуса, объединяются в единый архивный файл формата ZIP, после чего сам этот ZIP-файл вновь скрепляется цифровой подписью нотариуса.

125. Электронные эквиваленты нотариальных актов все шире используются в Австрии. По своим основным элементам австрийская система электронной нотаризации в целом близка к немецкой. Одной из ее особенностей, однако, является наличие централизованного электронного регистра ("cyberDOC") для хранения документов в электронной форме. Независимая компания, учрежденная совместно Австрийской нотариальной палатой и компанией "Сименс АГ", предоставляет в распоряжение нотариусов электронный архив, снабженный функциями удостоверения подлинности[166]. Закон обязывает австрийских нотариусов регистрировать и хранить в этом архиве все документы, заверенные ими после 1 января 2000 года.

126. Если функция нотариуса по заверению подписей может быть в основном воспроизведена в электронной среде с помощью электронных методов подписания и удостоверения подлинности, то для воспроизведения других функций могут потребоваться более широкие подходы. Как правило, в нотариальных актах проставляется, в зависимости от случая, дата их составления, дата регистрации, дата подписания или снятия копий. Нотариальное удостоверение даты предположительно можно заменить простым применением автоматизированных методов[167].

127. Более важное значение, однако, имеют процедуры ведения электронных реестров нотариально заверенных актов. В соответствии с законом нотариусы, как правило, обязаны вести регистрацию представленных им или оформленных ими документов. Создание электронного аналога такого общего реестра требует решения целого ряда трудных задач. Другая, еще более важная, проблема связана с потенциальной технической несовместимостью разных видов программного обеспечения и оборудования, которые могут использоваться нотариусами для этой цели. Быстрое развитие информационных и коммуникационных технологий порождает все большую потребность в переформатировании данных и их переносе с одних носителей на другие. Однако гарантия того, что данные, перезаписанные на новых носителях в измененном формате, будут по-прежнему поддаваться считке, существует не всегда. В связи с этим потребуется выработать процедуры контроля, позволяющие проверять целостность содержания записи до и после переноса. Как уже отмечалось, технология шифрования на основе ИПК не гарантирует даже возможности считки самих цифровых подписей по прошествии определенного времени (см. выше, пункт 51). Поэтому процесс перехода на новые форматы и носители должен осуществляться продуманно, а изначальное удостоверение подлинности, возможно, будет требовать подтверждения. Опыт показал, что в интересах согласованности и совместимости эту функцию более целесообразно поручать пользующейся доверием третьей стороне, а не каждому нотариусу по отдельности[168].

---

[165] См. "*Hinweise und Anwendungsempfehlungen für den elektronischen Handels-, Genossenschafts- und Partnerschaftsregisterverkehr*" Rundschreiben 25/2006 der Bundesnotarkammer vom 07.12.2006 (размещено по адресу http://www.bnotk.de/Service/Empfehlungen+Hinweise/RS25-06_El-Handelsregisterverkehr.html (дата посещения – 6 июня 2008 года)).

[166] См. Österreichische Notariatskammer (Австрийская нотариальная палата); размещено по адресу http://www.notar.at, раздел "Cyberdoc" (дата посещения – 6 июня 2008 года).

[167] Didier Froger, "Les contraintes du formalisme et de l'archivage de l'acte notarié établi sur support dématérialisé", La semaine juridique (édition notariale et immobilière), No. 11, 12 Mars 2004, p. 1130.

[168] Didier Froger, "Les Contraintes du formalisme ...".

128. В частности, именно на такой модели остановили свой выбор французские законодатели. В ходе недавнего пересмотра правил, регулирующих нотариально заверенные записи, были определены общие условия функциональной эквивалентности между нотариально заверенными актами, оформленными на бумаге, и электронными записями[169]. Наряду с другими положениями, касающимися в основном защиты информации, новые правила предусматривают создание централизованного архива нотариально заверенных актов в электронной форме, обеспечивающего хранение электронных записей без нарушения их целостности; их доступность лишь для тех нотариусов, которыми они были созданы; их перевод по мере технической необходимости в новые форматы без изменения их содержания; а также возможность добавления нотариусом новой информации к существующим записям без изменения их первоначального содержания.

129. Невзирая на достижения последних лет, по-прежнему существуют определенные сомнения в отношении того, как можно будет совместить новые правила, узаконивающие электронный эквивалент нотариально заверенных актов, составляемых на бумаге, с основными признаками подлинности таких актов, и в частности с требованием физического присутствия сторон перед нотариусом[170]. Если исходить из того, что для юридического оформления подлинной записи физическое присутствие необходимо, то задача состоит в нахождении возможных способов адаптации существующих форм к технологиям будущего[171]. В этой связи отмечалось, что криптография не может заменить собой наглядные символы публичной власти и согласия сторон[172]. Поэтому некоторые из правил требуют, чтобы стороны и свидетели имели возможность воочию увидеть отображение своих подписей на экране; аналогичным образом, все акты должны включать изображение печати нотариуса[173].

130. В Соединенных Штатах существуют три основополагающих закона, касающихся нотариального заверения: Единообразный закон об электронных сделках[174], Закон об электронных подписях в глобальной и национальной торговле (E-sign)[175] и Единообразный закон об электронной регистрации прав на недвижимое имущество[176]. 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 иной информацией, включения которой требуют другие применимые нормы права. После принятия этих законов во многих штатах были созданы системы нотаризации с использованием электронных

---

[169] Франция "Décret n° 2005-973, 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires", Journal Officiel, 11 Août 2005, p. 96.

[170] Pierre-Yves Gautier et Xavier Linant de Bellefonds, "De l'écrit électronique et des signatures qui s'y attachent", *La semaine juridique (édition générale)*, No. 24, 14 Juin 2000, I 236, sects. 8-10.

[171] Pierre Catala, "Le formalisme et les nouvelles technologies", *Répertoire du notariat Defrénois*, № 20, 2000, pp. 897-910.

[172] Luc Grynbaum, "Un acte authentique électronique pour les notaires," Communication Commerce électronique № 10, Octobre 2005, com. 156.

[173] Декрет № 71-941, с поправками, внесенными в него Декретом № 2005-973, ст. 17, пункт 3 (см. сноску 169).

[174] См. сноску 90.

[175] Кодифицировано в United States Code, title 15, chapter 96, sections 7001-7031.

[176] См. сноску 156.

средств. Так, Департаментом штата Пенсильвания совместно со специальной группой окружных регистраторов была разработана Программа электронного нотариального реестра и электронных нотариальных печатей, позволяющая в режиме реального времени осуществлять подтверждение полномочий нотариусов и использовать защищенные сетевые каналы для скрепления документов прошедшей проверку электронной печатью. Цель этой системы электронной нотаризации – упростить оформление коммерческих сделок между государственными должностными лицами и коммерческими предприятиями, а также усилить защиту граждан от подлога и мошенничества, сохранив при этом основные элементы нотариальных действий. В системе используются услуги по цифровой сертификации, предоставляемые коммерческим поставщиком[177].

131. Нотариусы, заинтересованные в участии в этой инициативе по электронной нотаризации, должны обратиться в Бюро по должностным патентам, выборам и законодательству штата с просьбой присвоить им квалификацию электронного нотариуса (э-нотариуса). Государственный нотариус должен за соответствующую плату получить цифровой сертификат в форме электронной нотариальной печати от сертифицированного на федеральном уровне сертификационного органа, выбранного участвующими в этой инициативе регистраторами заверяемых актов с одобрения Административной канцелярии и Государственного секретаря штата Пенсильвания. Перед получением цифрового сертификата лицо, которому присвоена квалификация э-нотариуса, должно лично явиться к любому из регистраторов заверяемых актов, участвующих в инициативе по электронной нотаризации, и предъявить ему письмо Департамента штата о присвоении вышеупомянутой квалификации, а также документы, достаточные для удостоверения личности. Сертифицированный э-нотариус должен обеспечивать, чтобы при каждой электронной нотаризации к заверяемой, подтверждаемой или проверяемой электронной подписи или электронной записи прилагалась или логически привязывалась следующая информация: полное имя э-нотариуса с добавлением слов “государственный нотариус”, названия населенного пункта и округа, где расположена контора э-нотариуса, а также дата окончания срока действия его патента. Э-нотариус должен требовать персональной явки к нему лица, которому он оказывает услуги по электронной нотаризации документов, при каждой такой нотаризации. Позиция Департамента штата Пенсильвания состоит в том, что основополагающие элементы нотаризации, включая личное присутствие подписывающих документ сторон перед нотариусом, при этом по-прежнему необходимы. В то же время вместо чернильного оттиска нотариальной печати на бумажном документе нотариус цифровым способом присоединяет свою идентификационную информацию к документу, существующему в виде электронных данных, предназначенных для компьютерной считки[178].

132. Как и в странах гражданского права, в странах общего права имели место некоторые дискуссии относительно того, могут ли функции, выполнявшиеся посредством традиционных методов удостоверения подлинности и нотариального заверения, быть воспроизведены с помощью электронных средств. До тех пор пока нотариальное заверение по существу ограничивается подтверждением целостности документов и личности тех, кем они подписаны, использование электронных

[177] Anthony Garritano, “National e-notary standards in progress”, *Mortgage Servicing News* (New York), vol. 10, No. 2, 1 March 2006, p. 11.

[178] См. http://www.dos.state.pa.us/dos/site/default.asp, разделы “Notaries”, “Electronic Notarization”(дата посещения – 5 июня 2008 года).

сообщений вместо бумажной документации, по-видимому, не должно представлять непреодолимых трудностей. Однако ситуация выглядит не столь ясной в случаях, когда для удостоверения подлинности документа или записи нотариус должен подтвердить присутствие того или иного лица при оформлении этого документа или записи[179].

133. Утверждается, что традиционные процедуры с участием свидетелей, такие как засвидетельствование, которые могут использоваться как в связи с составлением подлежащего заверению документа государственным нотариусом, так и независимо от этого, не вполне поддаются адаптации к электронному подписанию документов, поскольку нет уверенности в том, что изображение на экране действительно представляет собой тот документ, который будет скреплен электронной подписью. На экране компьютера свидетель и подписывающий могут видеть лишь поддающееся восприятию человеком отображение того, что якобы содержится в информационной системе. Видя, как подписывающий нажимает на клавиши, свидетель доподлинно не знает, что при этом происходит в действительности. Поэтому обеспечить уверенность в том, что изображение на экране соответствует введенному в информационную систему содержанию, 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 информационная система функционирует по заслуживающей доверия схеме[180].

134. 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

---

[179] «В условиях, когда техника позволяет проводить "телеконференции" с участием сторон, находящихся в разных городах и даже в разных странах, следует ожидать появления в будущем более широких законодательных определений "личного присутствия", в соответствии с которыми нотариус в Лос-Анджелесе сможет при помощи видеотрансляции засвидетельствовать акт подписания документа лицом, находящимся в Лондоне. Важными условиями такой дистанционной электронной нотаризации представляются наличие аудиоконтакта между нотариусом и отсутствующим лицом, которое ставит свою подпись, а также передача видеоизображения подписывающего лица в режиме реального времени. При этом, если совершение электронных нотариальных актов в условиях, когда нотариус находится в одном пункте, а лицо, принимающее обязательство или подписывающее документ, – в другом, можно хотя бы теоретически представить себе и при отсутствии аудиоконтакта – что подтверждается широким применением электронной почты, – без визуального контакта обойтись, по-видимому, невозможно. Как еще может нотариус убедиться в том, что лицо, совершающее акт подписания в другом месте, делает это не по явному принуждению, и записать видеоизображение, доказывающее, что документ исходит не от мошенника, воспользовавшегося похищенным частным ключом? По тем же причинам, по которым Верховный суд штата Небраска в 1984 году (*Christensen v. Arant*) постановил, что одного лишь аудиоконтакта с лицом, находящимся за дверью, недостаточно для того, чтобы констатировать физическое присутствие этого лица в традиционном юридическом смысле, один лишь электронный контакт по каналам, не обеспечивающим передачи визуальных изображений, едва ли будет считаться достаточным подтверждением физического присутствия в том юридическом смысле, который этот термин получит в будущем» (Charles N. Faerber, "Being there: the importance of physical presence to the notary," The John Marshall Law Review, vol. 31, spring 1998, pp. 749-776).

[180] В литературе эта проблема выражается формулой "подписываю то, что вижу" ("What you see is what you sign" – WYSIWYS) (см. также обсуждение вопроса о пользующихся доверием контроллерах изображения) (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).

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[181].

135. Эволюция законодательства пока не дошла до полной замены засвидетельствования электронными подписями: законы предусматривают лишь возможность использования электронной подписи свидетелем. Согласно Закону Новой Зеландии об электронных сделках, 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 оговаривается, 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[182].

136. Согласно закону Канады о защите личной 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[183]. 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[184]. 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 и лицо, в присутствии которого это заявление было сделано и которое уполномочено принимать заявления под присягой или в форме официальных заверений, также поставит под ним свою защищенную электронную подпись[185]. Альтернативный вариант, предложенный в целях дополнительного повышения уверенности, предполагает, что электронная подпись должна ставиться только пользующимся доверием специалистом, например адвокатом или нотариусом, либо в присутствии такого специалиста[186].

---

[181] См. обсуждение этого вопроса 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 и 8; размещено по адресу www.agc.gov.sg, раздел "Publications" (дата посещения – 6 июня 2008 года).

[182] Новая Зеландия, Закон об электронных сделках (см. сноску 88), статья 23.

[183] Канада, Закон о защите личной информации и электронных документах (2000 год), часть 2, статья 46.

[184] Канада, Закон о защите..., статья 45.

[185] Канада, Закон о защите..., статья 44.

[186] 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.cofrestrfatir.gov.uk/assets/library/documents/e-conveyancing_strategy_v3.0.doc (дата посещения – 5 июня 2008 года). Проект планируется осуществлять поэтапно с 2006 по 2009 год.

Часть вторая

Трансграничное использование электронных методов подписания и удостоверения подлинности

Содержание

I. Юридическое признание иностранных электронных методов подписания и удостоверения подлинности

137. Двумя основными факторами, затрудняющими трансграничное использование электронных методов подписания и удостоверения подлинности, особенно в случаях, когда они должны выполнять функции юридически действительной подписи, являются юридическая и техническая несовместимость. Техническая несовместимость препятствует взаимодействию систем удостоверения подлинности. Юридическая несовместимость может иметь место в случаях, когда законы, действующие в разных правовых системах, предусматривают различные требования в отношении использования электронных методов подписания и удостоверения подлинности и признания их действительности.

A. Международные последствия внутреннего законодательства

138. Там, где внутреннее законодательство допускает использование электронных эквивалентов вместо тех методов удостоверения подлинности, которые основаны на бумажной документации, критерии действительности таких электронных эквивалентов не всегда согласуются между собой. Например, если законом признаются лишь цифровые подписи, то другие формы электронных подписей не будут считаться приемлемыми. Другие противоречия между критериями признания электронных методов подписания и удостоверения подлинности могут в принципе не исключать их трансграничного использования, однако затраты и неудобства, связанные с выполнением требований различных правовых систем, могут частично сводить на нет такие преимущества использования электронных сообщений, как быстрота и эффективность.

139. В нижеследующих разделах говорится о последствиях различных юридических подходов к соответствующим технологиям с точки зрения более широкого трансграничного признания этих технологий. В них также кратко изложен намечающийся международный консенсус в отношении мер, которые потенциально могли бы облегчить использование электронных методов подписания и удостоверения подлинности на международном уровне.

1. Препятствия на международном уровне, возникающие из-за противоречий между национальными подходами

140. Подходы, нейтральные с точки зрения технологии, – особенно те из них, которые включают “критерий надежности”, – обычно позволяют преодолеть

юридическую несовместимость. К числу международно-правовых документов, использующих такой подход, относятся Типовой закон ЮНСИТРАЛ об электронной торговле (пункт 1 *b*) статьи 7) и Конвенция Организации Объединенных Наций об использовании электронных сообщений в международных договорах (пункт 3 статьи 9). Согласно этому подходу электронные методы подписания или удостоверения подлинности, предоставляющие возможность как идентифицировать подписавшую сторону, так и указать намерение этой стороны в отношении информации, содержащейся в электронном сообщении, отвечают требованиям, предъявляемым к подписи, при условии соблюдения нескольких критериев. С учетом всех обстоятельств, включая возможную договоренность между составителем и адресатом сообщения данных, должно быть продемонстрировано, что подпись или метод удостоверения подлинности являются настолько надежными, насколько это соответствует цели, для которой сообщение данных было подготовлено или передано. В качестве альтернативы должно быть доказано, что они сами по себе или в сочетании с другими подтверждениями обеспечили достижение этих целей.

141. Имеются основания считать, что "минималистский" подход облегчает трансграничное использование электронных методов удостоверения подлинности и электронных подписей, так как согласно этому подходу любой метод электронного подписания или удостоверения подлинности может быть действительным образом использован для подписания или заверения договора или сообщения, если он соответствует изложенным выше общим условиям. Однако этот подход ведет к тому, что такие условия, как правило, подтверждаются лишь a posteriori, и нельзя быть уверенным в том, что суд признает правомерным применение того или иного конкретного метода.

142. Трансграничное использование электронных методов удостоверения подлинности и электронных подписей становится реальной проблемой в системах, предписывающих или поощряющих применение той или иной конкретной технологии. Сложность этой проблемы возрастает прямо пропорционально степени государственного регулирования вопросов использования электронных подписей и электронных методов удостоверения подлинности, а также того уровня юридической определенности, которую с точки зрения закона обеспечивает тот или иной метод или технология. Причины этого просты: там, где закон не признает какой-либо особой юридической силы за использованием конкретных видов электронных подписей или методов удостоверения подлинности и не устанавливает в связи с этим каких-либо презумпций, но просто признает их общую эквивалентность собственноручным подписям или бумажным средствам удостоверения подлинности, доверие к электронной подписи чревато таким же риском, как и доверие к собственноручной подписи в рамках действующего законодательства. Там же, где закон устанавливает больше юридических презумпций в связи с определенными видами электронных подписей (обычно теми, которые считаются "защищенными" или "современными"), дополнительный риск перекладывается с одной из сторон на другую. Одна из главных исходных посылок законодательства, привязанного к конкретным технологиям, заключается в том, что степень надежности, обеспечиваемая ими при соблюдении определенных стандартов и процедур, оправдывает такой общий априорный перенос юридического риска. Недостатком этого подхода является то, что, если надежность изначально предполагает (наряду с другими условиями) использование той или иной конкретной технологии, все другие технологии – и даже эта конкретная технология, применяемая при несколько иных условиях, – становятся априорно ненадежными или, во всяком случае, подпадают под изначальное подозрение в ненадежности.

143. Таким образом, коллизии национальных законов, привязанных к конкретным технологиям, могут препятствовать, а не способствовать использованию электронных подписей в международной торговле. Это может происходить двумя различными, но тесно взаимосвязанными путями.

144. Во-первых, если в отношении электронных подписей и удостоверяющих их подлинность поставщиков сертификационных услуг в разных правовых системах действуют идущие вразрез друг с другом юридические и технические требования, это может затруднять или исключать использование электронных подписей во многих трансграничных сделках, поскольку эти электронные подписи не способны одновременно удовлетворять требованиям разных правовых систем.

145. Во-вторых, привязанное к конкретным технологиям законодательство, особенно отдающее предпочтение цифровым подписям – что относится и к двухуровневому подходу, – имеет тенденцию приводить к появлению множества противоречащих друг другу технических стандартов и лицензионных требований, крайне осложняющих трансграничное использование электронных подписей. Система, при которой каждая страна устанавливает собственные стандарты, может также препятствовать заключению сторонами соглашений о взаимном признании и перекрестной сертификации[187]. Так, одной из главных нерешенных проблем, касающихся, в частности, цифровых подписей, является проблема трансграничного признания. Как отмечает Рабочая группа по безопасности и конфиденциальности информации (РГБКИ) Организации экономического сотрудничества и развития (ОЭСР) (далее именуется "РГБКИ ОЭСР"), хотя подход, принятый в большинстве правовых систем, производит впечатление недискриминационного, расхождения в местных требованиях будут и впредь создавать проблемы, затрудняющие взаимодействие[188]. Применительно к данному исследованию заслуживают внимания следующие из недостатков, на которые указывает РГБКИ ОЭСР:

a) *Возможность взаимодействия*. Трудности и препятствия в этом отношении отмечаются повсеместно. На техническом уровне, несмотря на обилие различных стандартов, проблема усматривается в отсутствии единых "базовых" стандартов для некоторых технологий. К факторам, препятствующим прогрессу на юридическом/директивном уровне, относят отсутствие у принципалов достаточной ясности по поводу их отношений с доверенными лицами, включая вопросы компенсации и передачи ответственности. По мнению РГБКИ ОЭСР, эти вопросы "очевидно, требуют более пристального изучения и анализа на предмет возможной разработки общего инструментария, облегчающего достижение между различными правовыми системами того уровня взаимодействия, который желателен для решения той или иной конкретной задачи или функционирования той или иной системы".

b) *Признание иностранных услуг по удостоверению подлинности*. По данным РГБКИ ОЭСР, основные усилия до сих пор направлялись на создание внутренних служб. Соответственно, механизмы признания иностранных услуг по удостоверению подлинности "в целом не столь хорошо развиты". Исходя из этого, РГБКИ ОЭСР отмечает, что в данной области "представляется полезной дальнейшая работа.

---

[187] Baker and Yeo, "Background and issues concerning authentication ...". Document No. 2.

[188] Organization for Economic Cooperation and Development, Working Party on Information Security and Privacy, *The Use of Authentication across Borders in OECD Countries* (DSTI/ICCP/REG(2005)4/FINAL); размещено по адресу http://www.oecd.org/dataoecd/1/10/35809749.pdf (дата посещения – 6 июня 2008 года).

Учитывая, что любая такая работа будет тесно связана с более общей темой способности к взаимодействию, эти темы можно было бы объединить".

c) *Признание свидетельств*[189]. В некоторых случаях в качестве препятствия для взаимодействия упоминалось непризнание свидетельств, выданных другими юридическими лицами. В связи с этим РГБКИ ОЭСР предлагает рассмотреть возможность разработки комплекса практических рекомендаций или руководящих принципов, касающихся выдачи свидетельств для целей удостоверения подлинности. В нескольких правовых системах, возможно, уже ведется работа в данном направлении, которая может стать полезным вкладом в любые потенциальные инициативы РГБКИ ОЭСР по этим вопросам.

d) *Использование целого ряда методов удостоверения подлинности*. РГБКИ ОЭСР констатировала, что практически во всех государствах – членах ОЭСР применяется целый ряд технических решений для удостоверения подлинности. Они предусматривают различные методы: от использования паролей, с одной стороны, до применения аппаратных ключей, цифровых подписей и биометрических данных – с другой. В зависимости от конкретной задачи и связанных с ней требований эти методы могут применяться по отдельности или в комбинации друг с другом. Многие могли бы счесть это позитивным моментом, однако информация, собранная РГБКИ ОЭСР в ходе проведенного обследования, свидетельствует о том, что операторы и пользователи соответствующих систем, столкнувшись со столь широким спектром возможностей, рискуют оказаться полностью дезориентированными относительно того, какой из методов наиболее отвечает их потребностям. По мнению РГБКИ ОЭСР, это указывает на целесообразность подготовки справочного пособия, позволяющего оценивать различные методы удостоверения подлинности и определять, насколько их свойства отвечают потребностям операторов или пользователей систем.

146. Повышению доверия к электронным методам подписания и удостоверения подлинности при международных сделках могли бы способствовать широкое принятие Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах и применение предусмотренного ею подхода к электронным подписям и удостоверению подлинности, нейтрального с точки зрения технологии. Однако было бы нереалистичным ожидать, что это полностью устранит необходимость согласованного решения проблемы несовместимости юридических и технических стандартов. Во многих странах по-прежнему предписывается использование конкретных методов удостоверения подлинности при сделках определенных видов. Кроме того, некоторые страны могут ощущать потребность в более конкретных рекомендациях по оценке надежности методов подписания и удостоверения подлинности, особенно применяемых в других странах, и степени их эквивалентности методам, используемым или хотя бы известным в данной стране.

[189] Под свидетельством понимается выданное опознавательное средство, подтверждающее, что соответствующее лицо или устройство прошло процедуру удостоверения. Свидетельства, привязанные к их держателю, необходимы для целей идентификации. Для получения некоторых видов полномочий может быть достаточно свидетельства, оформленного на предъявителя. Примерами могут служить действительное водительское удостоверение, индивидуальный номер физического лица в системе социального страхования или иной идентификационный номер, а также пластиковые карты с микропроцессорами (Centre for Democracy and Technology, "Privacy principles for authentication systems"; размещено по адресу http://www.cdt.org/privacy/authentication/030513interim.shtml (дата посещения – 5 июня 2008 года)).

2. Формирующийся консенсус

147. Наблюдаемые на международном уровне расхождения в принципиальных подходах, по всей вероятности, обусловлены различными комбинациями ряда факторов. Как это уже показано ранее (см. пункты 2–6, выше), некоторые страны придерживаются более строгих и детализированных требований в отношении формы подписей и документов, тогда как другие уделяют основное внимание намерениям подписавшей стороны и допускают подтверждение действительности подписи множеством различных способов. Эти общие расхождения обычно находят свое отражение в конкретных законодательных актах, касающихся электронных методов подписания и удостоверения подлинности (см. пункты 83–112, выше). Еще одной причиной расхождений являются различия в степени государственного вмешательства в технические аспекты электронного подписания и удостоверения подлинности. Правительства некоторых стран склонны непосредственно участвовать в определении стандартов для новых технологий, возможно, полагая, что это обеспечивает конкурентные преимущества отечественным компаниям[190].

148. Различия в принципиальных подходах также могут быть следствием несовпадения взглядов на то, как будут развиваться технологии удостоверения подлинности в будущем. Согласно одному из сценариев, получившему название "универсальная парадигма удостоверения подлинности"[191], главной целью технологии удостоверения подлинности будет проверка личности и других характеристик, присущих лицам, не состоявшим ранее в каких-либо отношениях друг с другом, для которых совместное использование технических средств не является предметом договорного соглашения. Соответственно, технология подписания или удостоверения подлинности должна позволять удостоверять личность или иные характеристики, присущие тому или иному лицу, для потенциально неограниченного круга сторон и для потенциально неограниченного числа целей. Данная модель ставит во главу угла технические стандарты и функциональные требования поставщиков сертификационных услуг, когда речь идет об участии доверенных третьих сторон. Другой сценарий – так называемая "ограниченная парадигма удостоверения подлинности" – исходит из того, что основным назначением технологий подписания и удостоверения подлинности будет проверка личности и других характеристик, присущих лицам, совместно использующим технические средства в рамках договорных соглашений[192]. Соответственно, технология удостоверения подлинности должна позволять удостоверять личность или другие характеристики, присущие держателям сертификата, лишь для ряда конкретных целей и для ограниченного круга потенциально доверяющих данной технологии сторон, связанных общими условиями ее использования. В этой модели основное значение придается юридическому признанию договорных соглашений.

149. Несмотря на эти расхождения, часть из которых сохраняется по сей день, выводы РГБКИ ОЭСР[193] указывают на расширяющийся международный консенсус в отношении основных принципов, которыми должна регулироваться электронная торговля, и в частности, использование электронных подписей. Для целей настоящего исследования наибольший интерес представляют следующие выводы:

---

[190] Baker and Yeo, "Background and issues concerning authentication ...". Document No. 2.

[191] Baker and Yeo, "Background and issues concerning authentication ...". Document No. 2.

[192] Baker and Yeo, "Background and issues concerning authentication ...". Document No. 2.

[193] Organization for Economic Cooperation and Development, *The Use of Authentication across Borders in OECD Countries ...* .

a) *Недискриминационный подход к "иностранным" подписям и услугам*. Законодательные положения не отрицают юридической силы подписей, созданных с помощью служб, базирующихся в других странах, если эти подписи были созданы при таких же условиях, как те, которые имеют юридическую силу в данной стране. С этой точки зрения подобный подход представляется недискриминационным при условии выполнения местных или эквивалентных им требований. Это соответствует выводам предыдущих обследований по вопросам удостоверения подлинности, проводившихся РГБКИ ОЭСР.

b) *Нейтральность с точки зрения технологий*. Хотя практически все респонденты указывали, что принятые у них нормативно-правовые рамки деятельности служб удостоверения подлинности и создания электронных подписей нейтральны с точки зрения технологии, большинство отмечало, что при использовании электронных средств для правительственных нужд и в случаях, когда в отношении электронной подписи требуется максимальная юридическая определенность, предписывается использование ИПК. Таким образом, даже при технологической нейтральности законодательных норм, на директивном уровне, по-видимому, требуется применение конкретных технологий.

c) *Преобладание ИПК*. Согласно данным РГБКИ ОЭСР, в случаях, когда требуется надежное удостоверение личности и высокая юридическая определенность электронной подписи, предпочтение при выборе метода удостоверения отдается ИПК. Она используется в конкретных "сообществах по интересам", где все пользователи, по-видимому, уже состоят друг с другом в тех или иных деловых отношениях. Внедрение поддерживающих ИПК интеллектуальных карт и оснащение прикладных программ встроенными функциями выдачи и проверки цифровых сертификатов упростили для пользователей применение этого метода. Вместе с тем обычно признается, что ИПК необходима не во всех случаях и что выбор метода удостоверения подлинности должен определяться его соответствием тем задачам, для которых он будет использоваться.

150. Кроме того, РГБКИ ОЭСР констатировала, что во всех охваченных обследованием странах имеется тот или иной комплекс законодательных или нормативных положений, обеспечивающих юридическую силу электронных подписей на национальном уровне. РГБКИ ОЭСР пришла к выводу о том, что, хотя законы разных правовых систем могут различаться в деталях, в них просматривается и общий подход, заключающийся в том, что большинство этих законов опираются на существующие международные или транснациональные правовые режимы (в частности, Типовой закон ЮНСИТРАЛ об электронных подписях и Директиву 1999/93/ЕС Европейского парламента и Совета об основах законодательства Сообщества в отношении электронных подписей)[194].

151. Основные моменты этого формирующего консенсуса были вновь отмечены в принятой 12 июня 2007 года Советом ОЭСР рекомендации по электронному удостоверению подлинности, в которой, в частности, государствам предлагается:

a) работать над созданием технологически нейтральных подходов для эффективного внутреннего и трансграничного электронного удостоверения личности физических и юридических лиц;

[194] *Official Journal of the European Communities*, L 13/12, 19 January 2000.

b) содействовать разработке, созданию и использованию продуктов и услуг электронного удостоверения подлинности, воплощающих в себе передовые методы деловой практики, включая технические и нетехнические гарантии, отвечающие потребностям участников, в частности в отношении безопасности и конфиденциальности их информации и личных данных;

c) поощрять как в частном, так и публичном секторах достижение коммерческой, юридической и технической совместимости систем удостоверения подлинности с целью облегчения межсекторального и межюрисдикционного взаимодействия и заключения сделок в режиме онлайн и создания условий для внедрения как на национальном, так и на международном уровнях продуктов и услуг удостоверения подлинности;

d) принимать меры по расширению осведомленности всех участников, в том числе в странах, не являющихся государствами-членами, о преимуществах использования электронного удостоверения подлинности на национальном и международном уровнях[195].

152. Данные рекомендации во многом согласуются с общим подходом, принятым ЮНСИТРАЛ в области электронной торговли (например, упрощение, а не регулирование процедур, технологическая нейтральность, уважение свободы договора, недискриминация). Существует, однако, ряд правовых вопросов, которые необходимо рассмотреть для облегчения использования электронных методов подписания и удостоверения подлинности в международном или трансграничном контексте.

B. Критерии признания иностранных электронных методов удостоверения подлинности и подписания

153. Как уже отмечалось, одним из основных препятствий для трансграничного использования электронных подписей и методов удостоверения подлинности является отсутствие возможности взаимодействия, обусловленное противоречиями и расхождениями в стандартах либо их непоследовательным применением. Для содействия применению ИПК, опирающейся на соответствующие стандарты, обеспечивающей такое взаимодействие и способной лечь в основу обеспечения надежности электронных коммерческих сделок, учрежден целый ряд форумов. В их число входят

[195] *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication* (Paris, June 2007); размещено по адресу http://www.oecd.org/dataoecd/32/45/38921342.pdf (дата посещения – 6 июня 2008 года).

как межправительственные[196], так и смешанные публично-частные организации[197] глобального[198] или регионального уровня.

154. Часть этой работы направлена на подготовку технических стандартов представления информации, необходимой для выполнения определенных юридических требований[199]. Однако в значительной мере эта важная работа посвящена именно техническим, а не юридическим аспектам и выходит за рамки настоящего исследования. Поэтому в последующих разделах основное внимание уделяется формальным и материально-правовым требованиям, касающимся трансграничного признания электронных подписей.

---

[196] В Азиатско-тихоокеанском регионе имеются разработанные Азиатско-тихоокеанским форумом по экономическому сотрудничеству (АТЭС) "Руководящие принципы для систем выдачи сертификатов, пригодных к использованию в электронной торговле между субъектами, относящимися к различным правовым системам" (eSecurity Task Group, APEC Telecommunications and Information Working Group, December 2004); размещено по адресу http://www.apectelwg.org/contents/documents/eSTG/PKIGuidelines-Final_2_web.pdf (оригинал имеется в Секретариате)). Эти руководящие принципы предназначены в помощь при разработке потенциально способных к взаимодействию систем и оценке возможности взаимодействия систем, которые уже существуют. Руководящие принципы охватывают категории или типы сертификатов, используемые только в транснациональной электронной торговле. Они не рассчитаны на сертификаты других типов и не претендуют на то, чтобы ограничить круг выдаваемых сертификатов лишь теми, которые подпадают под эти Руководящие принципы.

[197] В Европейском союзе в 1999 году Совет по стандартам в области информационных и коммуникационных технологий (ИКТ) учредил Европейскую инициативу по стандартам для электронных подписей (ЕИСЭП) с целью координации деятельности по стандартизации во исполнение Директивы Европейского союза 1999/93/ЕС об электронных подписях. Совет по стандартам в области ИКТ сам представляет собой инициативу Европейского комитета по стандартизации (ЕКС), созданного национальными организациями по стандартизации при участии двух некоммерческих организаций – Европейского комитета по электротехническим стандартам (СЕНЕЛЕК) и Европейского института по стандартизации в области электросвязи (ЕТСИ). В рамках ЕИСЭП разработан ряд стандартов, рассчитанных на облегчение взаимодействия, которые, однако, внедряются медленными темпами по причине, как утверждается, их сложности (Paolo Balboni, "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication," *Information and Communications Technology Law*, vol. 13, No. 3 (2004), pp. 211-242).

[198] Например, Организация по развитию стандартов структурированной информации (ОРССИ) – некоммерческий международный консорциум, основанный в 1993 году в целях содействия разработке, сближению и принятию стандартов для электронных сделок. ОРССИ учредила Технический комитет по ИПК, в состав которого входят пользователи ИПК, ее поставщики и эксперты в этой области и в котором рассматриваются вопросы внедрения технологии цифровых сертификатов. Техническим комитетом по ИПК составлен план действий, который предусматривает, в частности, выработку конкретных моделей или руководящих принципов для практического применения стандартов, обеспечивающих возможность взаимодействия систем ИПК; установление новых стандартов, по мере необходимости; а также разработку тестов на способность к взаимодействию и проведение мероприятий по тестированию (OASIS, PKI Technical Committee, "PKI action plan" (February 2004); размещено по адресу http://www.oasis-open.org/committees/pki/ pkiactionplan.pdf (дата посещения – 6 июня 2008 года)).

[199] Например, ЕТСИ разработал стандарт (TS 102 231) для создания неиерархической структуры, обеспечивающей, среди прочего, возможность взаимного признания между доменами ИПК и, соответственно, подтверждения действительности сертификатов. Смысл технического стандарта ЕТСИ TS 102 231 сводится к определению параметров представления информации о статусе поставщика сертификационных услуг ("доверенного поставщика услуг"). Он имеет форму скрепленного подписью списка, именуемого "Trust-service Status List", на основе которого представляется соответствующая информация. Такой "статусный список", составляемый согласно спецификациям ЕТСИ, отвечает требованию относительно подтверждения того, была ли деятельность доверенного поставщика сертификационных услуг санкционирована той или иной признанной системой – будь то на момент оказания услуг или на момент совершения сделки сторонами, полагающимися на эти услуги. Чтобы соответствовать этому требованию, "статусный список" должен содержать информацию, позволяющую установить, был ли оператор упомянутой системы на момент сделки осведомлен о сертификационных услугах, оказываемых данным поставщиком, и если да, то каким был статус выданного этому поставщику разрешения (т. е. было ли оно действительно, приостановлено, аннулировано или отозвано). Таким образом, "статусный список", предусмотренный техническим стандартом ЕТСИ TS 102 231, должен содержать информацию не только о текущем, но и о прошлом статусе поставщика услуг. Иными словами, он сочетает в себе перечень поставщиков, имеющих действительные разрешения ("белый" список), и поставщиков, чьи разрешения аннулированы или отозваны ("черный" список) (см. http://portal.etsi.org/stfs/STF_HomePages/STF290/draft_ts_102231v010201p&RGW.doc, дата посещения – 6 июня 2008 года).

1. Место происхождения, взаимность и подтверждение в другой стране

155. Место происхождения является одним из традиционных факторов, определяющих юридическое признание иностранных документов или актов. Как правило, такое признание имеет место на основе взаимности, т. е. подписи и сертификаты из другой страны наделяются на внутреннем уровне такой же юридической силой, какая признается за национальными подписями и сертификатами. Еще одним возможным подходом является требование о том, чтобы иностранные подписи и сертификаты так или иначе заверялись или подтверждались отечественным поставщиком сертификационных услуг, сертификационным или регулирующим органом. Иногда имеет место сочетание всех этих подходов[200].

156. Национальные законы обычно не содержат положений, прямо исключающих юридическое признание подписей или сертификатов иностранного происхождения, что может восприниматься как свидетельство их недискриминационного характера. На практике, однако, положения о признании, предусмотренные во многих правовых режимах, часто ведут, пусть и непреднамеренно, к тем или иным дискриминационным последствиям. Так, Директива Европейского союза об электронных подписях в целом запрещает дискриминацию иностранных сертификатов, соответствующих установленным требованиям (т. е. цифровых подписей на основе ИПК). Однако на практике это касается главным образом сертификатов, выданных поставщиками сертификационных услуг, учрежденными на территории государств – членов Европейского союза. Поставщик сертификационных услуг, базирующийся в стране, которая не входит в Европейский союз, может обеспечить признание своих сертификатов в Европейском союзе тремя способами: выполнить требования Директивы Европейского союза об электронных подписях и получить аккредитацию в системе, учрежденной в одном из государств-членов; заключить соглашение о перекрестной сертификации с поставщиком сертификационных услуг, учрежденным в одном из государств – членов Европейского союза; либо действовать в рамках общих положений о признании, предусмотренных на уровне международного соглашения[201]. То, как в Директиве Европейского союза регулируются соответствующие международные аспекты, позволяет предположить, что одной из ее целей было создание условий для доступа поставщиков сертификационных услуг из стран Европейского союза на внешние рынки[202]. Добавляя к требованию относительно эквивалентности существу

---

[200] В Аргентине, например, иностранные сертификаты и электронные подписи признаются при наличии соглашения о взаимности между Аргентиной и страной происхождения иностранного сертификационного органа либо в случае их признания сертификационным органом, лицензированным в Аргентине и имеющим удостоверение, выданное правоприменительной инстанцией (см. Закон о цифровой подписи (2001 год), статья 16).

[201] Так, в соответствии со статьей 7 упомянутой Директивы, государства – члены Европейского союза обязаны обеспечить признание сертификатов, выданных поставщиком сертификационных услуг в третьей стране, в качестве юридически эквивалентных сертификатам, выданным поставщиком сертификационных услуг, учрежденным на территории Сообщества, если: *a*) данный поставщик сертификационных услуг "отвечает требованиям, изложенным в Директиве, и аккредитован в системе добровольной аккредитации, учрежденной в одном из государств-членов"; или *b*) сертификат "гарантирован" поставщиком сертификационных услуг, учрежденным на территории Сообщества и отвечающим требованиям, изложенным в Директиве; или c) сертификат или поставщик сертификационных услуг "признан в рамках двустороннего или многостороннего соглашения между Сообществом и третьими странами или международными организациями".

[202] О стремлении обеспечить европейским поставщикам сертификационных услуг доступ на иностранные рынки наглядно свидетельствует формулировка пункта 3 статьи 7 Директивы, согласно которому "если Комиссии становится известно о каких-либо трудностях, испытываемых предприятиями Сообщества

норм Европейского союза еще одно требование аккредитации в системе, учрежденной в одном из государств-членов, Директива Европейского союза об электронных подписях фактически требует от иностранных поставщиков сертификационных услуг соблюдения как своего национального режима, так и режима Европейского союза, т. е. устанавливает для них более высокий стандарт, чем тот, который применяется к поставщикам сертификационных услуг, аккредитованных в государствах – членах Европейского союза[203].

157. В части практического выполнения статьи 7 Директивы Европейского союза об электронных подписях имеют место определенные расхождения[204]. Например, в Ирландии и на Мальте иностранные цифровые подписи (или, согласно терминологии Европейского союза, отвечающие установленным требованиям сертификаты) признаются эквивалентными национальным подписям при условии соблюдения других юридических требований. В других случаях такое признание обусловлено подтверждением в принимающей стране (Австрия, Люксембург) или решением внутренней инстанции (Польша, Чешская Республика, Эстония). Такая тенденция к обязательному сохранению национального контроля в той или иной форме, что, как правило, обосновывается законной обеспокоенностью относительно уровня надежности иностранных сертификатов, на практике приводит к возникновению системы дискриминации иностранных сертификатов по признаку их географического происхождения.

2. Эквивалентность по существу

158. Следуя давней традиции, ЮНСИТРАЛ не дала согласия на включение географических соображений в число факторов, определяющих признание иностранных сертификатов и электронных подписей. Так, в пункте 1 статьи 12 Типового закона ЮНСИТРАЛ об электронных подписях прямо говорится, что при определении того, обладает ли – или в какой мере обладает – сертификат или электронная подпись юридической силой, не учитываются ни место выдачи сертификата или создания или использования электронной подписи, ни местонахождение коммерческого предприятия эмитента или подписавшего.

159. В пункте 1 статьи 12 Типового закона ЮНСИТРАЛ об электронных подписях имелось в виду отразить тот основополагающий принцип, что место происхождения само по себе ни в коей мере не следует считать фактором, определяющим то, должны ли сертификаты или электронные подписи иностранного происхождения признаваться способными обладать юридической силой, и если должны, то в какой степени. Вопрос о том, может ли электронная подпись обладать юридической силой, и если да, то в какой степени, должен решаться в зависимости от ее технической надежности, а не от места, где был выдан сертификат или создана электронная подпись. Положения о недискриминации, аналогичные статье 12 Типового закона об электронных подписях, можно найти и в некоторых национальных режимах, таких

при получении доступа на рынки третьих стран, она может, в случае необходимости, представить Совету предложения относительно соответствующего мандата на проведение переговоров о предоставлении предприятиям Сообщества сопоставимых прав в таких третьих странах".

[203] Jos Dumortier and others, "The legal and market aspects of electronic signatures", study for the European Commission Directorate General Information Society, Katholieke Universiteiet Leuven, 2003, p. 58.

[204] Jos Dumortier and others, "The legal and market aspects of electronic signatures" ..., pp. 92-94.

как Закон Соединенных Штатов от 2000 года об электронных подписях в глобальной и национальной торговле[205]. Согласно этим положениям, место происхождения само по себе не следует считать фактором, определяющим то, должны ли сертификаты или электронные подписи иностранного происхождения признаваться в принимающем государстве способными обладать юридической силой, и если должны, то в какой степени. В них устанавливается, что юридическая сила сертификата или электронной подписи должна зависеть от их технической надежности[206].

160. Вместо географических факторов Типовой закон предусматривает критерий эквивалентной надежности, по существу обеспечиваемой соответствующими сертификатами и подписями. Так, если сертификат иностранного происхождения обеспечивает уровень надежности, по существу эквивалентный уровню надежности сертификата, выданного в принимающем Типовой закон государстве, то он обладает такой же юридической силой. Аналогичным образом, электронная подпись, созданная или использованная за пределами страны, обладает такой же юридической силой, как и электронная подпись, созданная или использованная в данной стране, если она обеспечивает по существу эквивалентный уровень надежности. Эквивалентность уровней надежности, обеспечиваемых сертификатами и подписями иностранного и внутреннего происхождения, должна определяться исходя из признанных международных стандартов и любых других соответствующих факторов, включая наличие между сторонами договоренности об использовании определенных видов электронных подписей или сертификатов, за исключением случаев, когда такая договоренность не будет действительной или не будет иметь юридической силы согласно применимому праву.

161. Типовой закон не содержит требований о взаимности и не побуждает к заключению таких соглашений. В нем не предусмотрено никаких конкретных предложений относительно правовых методов, с помощью которых принимающее Типовой закон государство может обеспечить заблаговременное признание надежности сертификатов и подписей, отвечающих требованиям законодательства зарубежной страны (например, посредством односторонней декларации или заключения международного договора)[207]. К возможным методам достижения этого результата, упоминавшимся в ходе подготовки Типового закона, относится, например, автоматическое признание подписи, соответствующей законам другого государства, если законы иностранного государства предусматривают уровень надежности, по меньшей мере эквивалентный тому, который требуется от эквивалентных подписей внутреннего происхождения. В число других правовых методов, с помощью которых принимающее Типовой закон государство может обеспечить заблаговременное признание надежности иностранных сертификатов и подписей, могут входить односторонние декларации или международные договоры[208].

---

[205] United States Code, title 15, chapter 96, section 7031 (Principles governing the use of electronic signatures in international transactions).

[206] См. *Типовой закон ЮНСИТРАЛ об электронных подписях* ..., часть вторая, пункт 83.

[207] Там же, пункт 157.

[208] См. Доклад Рабочей группы по электронной торговле о работе ее тридцать седьмой сессии (A/CN.9/483, пункты 39 и 42).

II. Методы и критерии установления правовой эквивалентности

162. Как это уже отмечалось выше, обследование, проведенное РГБКИ ОЭСР, показало, что законодательство большинства стран по крайней мере в принципе не является дискриминационным по отношению к иностранным электронным подписям и средствам удостоверения подлинности, при условии соблюдения местных или эквивалентных им требований – в том смысле, что оно не отрицает юридической силы подписей, происхождение которых связано с услугами, оказываемыми в других странах, если эти подписи созданы при тех же условиях, что и подписи, признаваемые согласно внутреннем праву[209]. Вместе с тем РГБКИ ОЭСР отметила, что механизмы признания иностранных услуг по удостоверению подлинности, как правило, недостаточно развиты, и указала, что в этой области было бы полезно провести дальнейшую работу. Поскольку любая такая работа будет тесно связана с более общим вопросом о возможности взаимодействия, РГБКИ ОЭСР предложила объединить эти две темы. РГБКИ ОЭСР выдвинула идею разработки комплекса оптимальных методов или руководящих принципов. Позднее ОЭСР отметила, что механизмы признания иностранных услуг по удостоверению подлинности получили достаточное развитие, но отсутствует необходимый опыт их применения в различных правовых системах. Кроме того, правовые системы нуждаются в определенных средствах оценки доверительных систем, созданных в странах-партнерах. Хотя ОЭСР выразила надежду, что в этом отношении полезными могут оказаться предлагаемые ею собственные рекомендации и создаваемая на их основе система, она тем не менее отметила, что решение этой проблемы требует более глубокой проработки[210]. В нижеследующих разделах рассматриваются юридические положения и механизмы, обеспечивающие возможность международного взаимодействия, а также факторы, определяющие взаимную эквивалентность режимов ответственности. Они посвящены прежде всего вопросам, возникающим в связи с международным использованием электронных методов подписания и удостоверения подлинности на основе сертификатов, выдаваемых доверенной третьей стороной – поставщиком сертификационных услуг, и в частности цифровых подписей в рамках ИПК, поскольку возникновение юридических трудностей более вероятно в связи с трансграничным использованием таких электронных методов подписания и удостоверения подлинности, которые требуют участия в этих действиях третьих сторон.

A. Типы и механизмы перекрестного признания

163. Дополнительное бремя, налагаемое на иностранных поставщиков сертификационных услуг национальными требованиями, установленными применительно

[209] Organization for Economic Cooperation and Development, *The Use of Authentication across Borders in OECD Countries ...* .

[210] *OECD Recommendation on Electronic Authentication* …, p. 27.

к конкретным технологиям, является потенциальным препятствием для международной торговли[211]. Например, законы, касающиеся способов признания национальными органами иностранных электронных подписей и сертификатов, могут носить дискриминационный характер по отношению к иностранным коммерческим предприятиям. До сих пор каждый законодательный орган, рассматривавший данный вопрос, включал в свои законодательные акты те или иные требования относительно стандартов, соблюдаемых иностранным поставщиком сертификационных услуг; таким образом, данный вопрос неразрывно связан с более общей проблемой коллизии национальных стандартов. В то же время закон может устанавливать и другие географические или процедурные ограничения, препятствующие трансграничному признанию электронных подписей.

164. В отсутствие международной ИПК может возникать целый ряд проблем, связанных с признанием сертификатов сертификационными органами зарубежных стран. Признание иностранных сертификатов часто обеспечивается методом, известным как "перекрестная сертификация". Для нее необходимо, чтобы в основном эквивалентные друг другу сертификационные органы (или сертификационные органы, готовые пойти на определенный риск в том, что касается сертификатов, выданных другими сертификационными органами) признавали услуги, оказываемые каждым из них, благодаря чему пользователи этих услуг могли бы поддерживать между собой более эффективные контакты и больше доверять выдаваемым сертификатам. При перекрестной или многоступенчатой сертификации, когда в процесс вовлечено несколько участников, имеющих собственную политику обеспечения надежности, могут возникать юридические проблемы, связанные, например, с определением того, кто допустил нарушения, приведшие к убыткам, и на чьи именно заверения полагался пользователь.

1. Перекрестное признание

165. Перекрестным признанием называется механизм взаимодействия, при котором полагающаяся сторона, находящаяся в зоне действия ИПК, может использовать удостоверяющую подлинность информацию в зоне действия другой ИПК для удостоверения личности какого-либо субъекта в зоне этой другой ИПК[212]. Как правило, это становится возможным в результате официальной процедуры лицензирования или аккредитации в зоне другой ИПК или же официальной процедуры аудита типичного поставщика сертификационных услуг в данной зоне ИПК[213]. Вопрос о доверии к иностранной зоне ИПК должен решаться полагающейся стороной или владельцем соответствующего прикладного программного обеспечения или службы, а не тем поставщиком сертификационных услуг, которому непосредственно доверяет полагающаяся сторона.

---

[211] См. Alliance for Global Business, "A discussion paper on trade-related aspects of electronic commerce in response to the WTO's e-commerce work programme", April 1999, p. 29 (размещено по адресу http://www.biac.org/statements/iccp/AGBtoWTOApril1999.pdf, дата посещения – 6 июня 2008 года).

[212] Концепция перекрестного признания была разработана в 2000 году действовавшей в то время Целевой группой по электронным методам удостоверения подлинности Рабочей группы по телекоммуникациям и информации Азиатско-тихоокеанского форума по экономическому сотрудничеству (см. E*lectronic Authentication: Issues Relating to Its Selection and Use*, APEC publication No. 202-TC-01.2 (APEC, 2002); размещено по адресу http://www.apec.org/apec/publications/all_publications/telecommunications.html (дата посещения – 6 июня 2008 года)).

[213] Определение, основанное на материалах Целевой группы по электронным методам удостоверения подлинности Рабочей группы АТЭС по телекоммуникациям и информации.

166. Перекрестное признание, как правило, имеет место на уровне ИПК, а не на уровне отдельно взятых поставщиков сертификационных услуг. Так, когда одна ИПК признает другую ИПК, она при этом автоматически признает и любых аккредитованных в данной ИПК поставщиков таких услуг. Признание основывается на оценке применяемых в рамках другой ИПК процедур аккредитации, а не на оценке каждого конкретного поставщика сертификационных услуг, аккредитованного в этой ИПК. Если в соответствующих зонах ИПК выдаются сертификаты нескольких категорий, то процесс перекрестного признания включает определение категории сертификатов, пригодной для использования в обеих этих зонах, причем данная категория сертификатов и принимается за основу при оценке.

167. При перекрестном признании вопросы способности к техническому взаимодействию возникают только на уровне прикладного программного обеспечения, т. е. программное обеспечение должно быть способно произвести обработку иностранного сертификата и получить доступ в систему директорий иностранной зоны ИПК для подтверждения статуса этого иностранного сертификата. Следует отметить, что на практике поставщики сертификационных услуг выдают сертификаты разной степени надежности, исходя из того, для чего пользователи намерены применять их. В зависимости от уровня своей надежности сертификаты и электронные подписи могут иметь различную юридическую силу как внутри страны, так и за рубежом. Например, в отдельных странах даже сертификаты, называемые иногда "сертификатами низкого уровня" или "недорогостоящими сертификатами", могут при определенных обстоятельствах (например, если стороны в договорном порядке решили использовать такие инструменты) иметь юридическую силу (см. ниже, пункты 202–210). Поэтому эквивалентность должна устанавливаться между функционально сопоставимыми сертификатами.

168. Как отмечалось выше, при перекрестном признании решение о том, заслуживает ли доверия иностранный сертификат, принимается полагающейся стороной, а не ее поставщиком сертификационных услуг. Это не обязательно предполагает наличие договора или соглашения между двумя доменами ИПК. При этом не требуется также подробного анализа и сопоставления правил применения сертификатов[214] и положений о сертификационной практике[215], поскольку полагающаяся сторона определяет для себя приемлемость иностранного сертификата исходя из того, заслуживает ли доверия выдавший его иностранный поставщик сертификационных услуг. Поставщик сертификационных услуг считается заслуживающим доверия, если он лицензирован или аккредитован официальным лицензирующим или аккредитационным органом или прошел аудиторскую проверку, которую проводила пользующаяся доверием независимая третья сторона. Полагающаяся сторона в одностороннем порядке принимает осознанное решение, исходя из анализа правил применения сертификатов или положения о сертификационной практике, принятых в иностранном домене ИПК.

---

[214] Правила применения сертификатов представляют собой именованный набор правил, определяющих пригодность сертификата для того или иного сообщества и/или категории применения с общими требованиями в отношении надежности.

[215] Положением о сертификационной практике называется заявление о практике, которой следует поставщик сертификационных услуг при выдаче сертификатов.

2. Перекрестная сертификация инфраструктур публичных ключей

169. Перекрестной сертификацией называется практика признания публичного ключа другого поставщика сертификационных услуг с присвоением ему согласованного уровня доверия, обычно на основании договора. Это приводит к фактическому слиянию (полному или частичному) двух доменов ИПК в один более крупный домен. Для пользователей сертификационных услуг одного поставщика пользователи сертификационных услуг другого поставщика становятся обычными подписавшими лицами в рамках расширенного домена ИПК.

170. Перекрестная сертификация предполагает возможность технического взаимодействия и согласование правил применения сертификатов и положений о сертификационной практике. Выработка согласованных правил путем согласования правил применения сертификатов и положений о сертификационной практике необходима для обеспечения совместимости доменов ИПК как с точки зрения их операций с сертификатами (т. е. выдачи, приостановления действия и аннулирования сертификатов), так и в плане соблюдения ими аналогичных операционных требований и требований по обеспечению надежности. Важным аспектом в этой связи является также объем покрытия ответственности. Данный этап весьма сложен, так как речь обычно идет об объемных документах, охватывающих широкий круг вопросов.

171. Перекрестная сертификация лучше всего подходит для сравнительно закрытых коммерческих моделей, например для случаев, когда в обоих доменах ИПК предлагается один и тот же набор прикладных программ и услуг, таких как электронная почта или программы для выполнения финансовых операций. Наличие технически совместимых и функциональных систем, согласованных правил поведения и одинаковых правовых структур весьма облегчает перекрестную сертификацию.

172. Односторонняя перекрестная сертификация (когда один домен ИПК пользуется доверием другого, но не наоборот) встречается редко. Домен ИПК, оказывающий доверие другому, должен в одностороннем порядке обеспечить совместимость своих правил с правилами пользующегося доверием домена ИПК. Применение такой схемы, по-видимому, ограничивается прикладными программами и услугами, рассчитанными на сделки, которые требуют доверия лишь с одной стороны, например, когда для получения конфиденциальной информации от клиента торговая фирма должна доказать ему достоверность представленных ею о себе данных.

B. Эквивалентность стандартов поведения и режимов ответственности

173. Независимо от того, основывается ли международное использование электронных методов подписания и удостоверения подлинности на системе перекрестного признания или перекрестной сертификации, решение о признании той или иной ИПК целиком либо одного или нескольких конкретных иностранных поставщиков сертификационных услуг либо решение о приравнивании друг к другу соответствующих категорий сертификатов, выдаваемых в разных ИПК, предполагает оценку степени эквивалентности между внутренней и иностранной сертификационной практикой и

сертификатами, выдаваемыми в стране и за рубежом[216]. С юридической точки зрения оценка эквивалентности должна производиться по трем основным параметрам: эквивалентность юридического значения, эквивалентность юридических обязанностей и эквивалентность ответственности.

174. Эквивалентность юридического значения означает придание иностранному сертификату и иностранной подписи той же юридической силы, какой обладают их внутренние эквиваленты. При этом юридическая сила внутри страны определяется преимущественно в зависимости от того значения, которое, согласно внутреннему законодательству, придается электронным методам подписания и удостоверения подлинности, о чем уже говорилось ранее (см. выше, пункты 107–112). Признание эквивалентности юридических обязанностей и режимов ответственности подразумевает вывод о том, что обязанности сторон, действующих в рамках режима ИПК, по существу соответствуют тем, которые предусмотрены соответствующим режимом внутри страны, а за невыполнение этих обязанностей стороны несут по существу одинаковую ответственность.

175. В связи с ответственностью в контексте электронных подписей могут возникать различные вопросы, в зависимости от используемой технологии и инфраструктуры сертификации. Возникновение сложных проблем особенно вероятно в тех случаях, когда услуги по сертификации оказываются специализирующейся на этом третьей стороной – поставщиком сертификационных услуг. В этот процесс фактически вовлечены три участника: поставщик сертификационных услуг, подписавшее лицо и полагающаяся на подпись третья сторона. В той мере, в которой действия или бездействие одной из сторон причиняют ущерб какой-либо другой стороне или противоречат ее прямым или подразумеваемым обязанностям, каждая из этих сторон может нести ответственность за возмещение такого ущерба или утрачивать право на получение возмещения от другой стороны. В законодательстве к вопросу об ответственности при использовании цифровых подписей применяются разные подходы:

a) *Отсутствие конкретных положений о стандартах поведения или ответственности*. В качестве одного из возможных вариантов закон может обойти этот вопрос молчанием. Закон Соединенных Штатов от 2000 года об электронных подписях в глобальной и национальной торговле[217] не предусматривает ответственности ни одной из сторон, участвующих в процессе оказания сертификационных услуг. Такой порядок, говоря в целом, предусмотрен и в большинстве других правовых систем, придерживающихся минималистского подхода к электронным подписям, например в Австралии[218].

---

[216] Например, Рабочей группой по правилам применения сертификатов при Федеральном управлении США по определению политики в области инфраструктур публичных ключей разработана методика вынесения заключений относительно эквивалентности соответствующих правил (на основе схемы, определенной в "запросе замечаний" RFC 2527). Эта методика может использоваться при оценке и сопоставлении различных ИПК или при сопоставлении конкретной ИПК с упомянутыми руководящими принципами (см. http://www.cio.gov/fpkipa, дата посещения – 6 июня 2008 года).

[217] United States Code, title 15, chapter 96, section 7031.

[218] Так, было сочтено, что допускаемые австралийским законодательством частноправовые механизмы, такие как договорные положения об исключениях, отказе и освобождении от ответственности, а также установленные общим правом ограничения действия этих механизмов, лучше подходят для регулирования ответственности, чем положения законов (см. Mark Sneddon, *Legal liability and e-Transactions: a Scoping Study for the National Electronic Authentication Council* (National Office for the Information Economy, Canberra, 2000, pp. 43-47; размещено по адресу http://unpan1.un.org/intradoc/groups/public/documents/APCITY/ UNPAN014676.pdf, дата посещения – 6 июня 2008 года).

b) *Установление стандартов поведения и норм ответственности только для поставщиков сертификационных услуг*. Еще один подход заключается в том, чтобы предусмотреть ответственность по закону только для поставщиков сертификационных услуг. Он применен в Директиве Европейского союза 1999/93/ЕС об основах законодательства Сообщества в отношении электронных подписей[219], в пункте 22 которой говорится, что "в отношении поставщиков сертификационных услуг, оказывающих сертификационные услуги населению, действуют национальные нормы, касающиеся ответственности", как об этом говорится в статье 6 Директивы. Уместно отметить, что статья 6 распространяется лишь на "подписи, отвечающие установленным требованиям", что на сегодняшний день означает только цифровые подписи на основе ИПК[220].

c) *Установление стандартов поведения и норм ответственности для подписавших лиц и поставщиков сертификационных услуг*. В некоторых правовых системах закон предусматривает ответственность подписавшего лица и поставщика сертификационных услуг, но при этом не устанавливает какого-либо стандарта осмотрительности для полагающейся стороны. Так обстоит дело в Китае в соответствии с Законом об электронных подписях от 2005 года. Аналогичная ситуация существует в Сингапуре согласно Закону об электронных сделках от 1998 года.

d) *Установление стандартов поведения и норм ответственности для всех сторон*. Наконец, законодательство может предусматривать стандарты поведения и основания ответственности для всех участвующих сторон. Такой подход воплощен в Типовом законе ЮНСИТРАЛ об электронных подписях, в котором указаны обязанности, связанные с поведением подписавшего лица (статья 8), поставщика сертификационных услуг (статья 9) и полагающейся стороны (статья 11). Можно сказать, что в Типовом законе установлены критерии для оценки поведения упомянутых сторон. Однако последствия неспособности выполнить различные обязанности, а также основания потенциальной ответственности различных сторон, участвующих в использовании электронных систем подписи, должны, согласно этому закону, определяться внутренним правом.

176. Различия между национальными режимами ответственности могут создавать препятствия для трансграничного признания электронных подписей. Это объясняется двумя основными причинами. Во-первых, поставщики сертификационных услуг могут неохотно признавать иностранные сертификаты или ключи, выданные иностранными поставщиками сертификационных услуг, ответственность или стандарты осмотрительности которых могут быть ниже их собственных. Во-вторых, лица, использующие электронные методы подписания и удостоверения подлинности, также могут опасаться того, что более низкие пределы ответственности или стандарты осмотрительности, действующие для иностранного поставщика сертификационных услуг, ограничивают доступные им средства правовой защиты, например, в случае подделки или ошибочного доверия. По этим же причинам там, где использование электронных методов подписания и удостоверения подлинности или деятельность поставщиков сертификационных услуг имеют под собой законодательную основу, закон, как правило, так или иначе обусловливает признание иностранных

[219] *Official Journal of the European Communities*, L 13/12, 19 January 2000.

[220] Данному подходу следует законодательство, принятое в странах Европейского союза, например германский Закон об электронной подписи (SignaturGesetz - SigG) и связанное с ним постановление (SigV) от 2001 года, австрийский Федеральный закон об электронной подписи (SigG) и Положение об электронных подписях (раздел 4), принятое в 2002 году в Соединенном Королевстве.

сертификатов или поставщиков сертификационных услуг оценкой того, насколько обеспечиваемая ими надежность по существу эквивалентна надежности отечественных сертификатов и поставщиков сертификационных услуг. Главным юридическим критерием, по которому определяется такое соответствие, служат стандарты осмотрительности и уровни ответственности, установленные для различных сторон. Кроме того, имеющиеся у поставщика сертификационных услуг возможности для ограничения своей ответственности или отказа от нее также влияют на уровень соответствия, признаваемый за его сертификатами.

1. Основания ответственности в рамках инфраструктуры публичных ключей

177. Распределение ответственности в рамках ИПК обеспечивается в основном двумя путями: на договорной основе или на основе законодательства (прецедентного права, закона или того и другого). Отношения между поставщиком сертификационных услуг и подписавшим лицом, как правило, носят договорный характер, вследствие чего ответственность обычно возникает из нарушения той или другой стороной своих договорных обязательств. Отношения подписавшего лица с третьей стороной зависят от характера операций, осуществляемых между ними в каждом конкретном случае. Они могут быть или не быть основанными на договоре. Наконец, отношения между поставщиком сертификационных услуг и полагающейся на его услуги третьей стороной чаще всего не имеют под собой договорной основы[221]. В большинстве правовых систем основание ответственности (будь то договорное или деликтное) имеет далеко идущие и немаловажные последствия для режима ответственности, в частности, применительно к следующим элементам: *a*) степень вины, необходимая для наступления ответственности той или иной стороны (иными словами, "стандарт осмотрительности", диктуемый обязательствами одной стороны перед другой); *b*) стороны, имеющие право требовать возмещения ущерба, и объем возмещения, на которое они могут претендовать; и *c*) может ли виновная сторона ограничить свою ответственность или отказаться от нее, и если да, то в каких пределах.

178. Из вышесказанного вытекает не только то, что в разных странах предусмотрены различные стандарты ответственности, но и то, что они различаются также в пределах отдельно взятой страны в зависимости от характера отношений между стороной, привлекаемой к ответственности, и стороной, которой причинен ущерб. Кроме того, на те или иные аспекты ответственности в рамках как договорного режима ответственности, так и режима, основанного на общем праве или статутных нормах, могут оказывать свое влияние различные юридические положения и правовые теории, иногда сглаживающие различия между этими двумя режимами. Настоящее исследование не может претендовать на всеобъемлющий подробный анализ вышеупомянутых общих вопросов. Вместо этого внимание в нем будет сосредоточено на аспектах, конкретно возникающих в контексте ИПК, и на кратком обзоре подхода к ним во внутреннем законодательстве.

---

[221] Штеффен Хинделанг подробно рассматривает вопрос о возможности договорных отношений между поставщиком сертификационных услуг и третьей стороной согласно английскому праву и приходит к отрицательному выводу (Steffen Hindelang, "No remedy for disappointed trust: the liability regime for certification authorities towards third parties outwith the EC Directive in England and Germany compared", *Journal of Information, Law and Technology*, No. 1, 2002, размещено по адресу http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/hindelang (дата посещения – 6 июня 2008 года)). Однако существуют правовые системы, где такие договорные отношения возможны.

a) Стандарт осмотрительности

179. Хотя в разных правовых системах используются различные градации и теории, для целей настоящего исследования предполагается, что ответственность сторон в рамках ИПК основывается, главным образом, на трех возможных стандартах: простая небрежность или вина; презумпция небрежности (или вина с перенесенным бременем доказывания); а также абсолютная ответственность[222].

i) *Простая небрежность*

180. В соответствии с этим общим стандартом юридической обязанностью лица является предоставление другим лицам компенсации за негативные последствия своих действий, при условии что согласно закону характер отношений с этими другими лицами обязывает проявлять осмотрительность. При этом необходимым стандартом осмотрительности, как правило, является "разумная осмотрительность", определяемая просто как та степень заботливости, которую при таких же или аналогичных обстоятельствах проявляло бы лицо, наделенное обычным уровнем осторожности, осведомленности и дальновидности. В системах общего права данный стандарт часто называют стандартом "разумного лица", тогда как в ряде систем гражданского права в этой связи часто используется выражение "добрый отец семейства" (*bonus pater familias*). С узко коммерческой точки зрения разумная осмотрительность означает ту степень заботливости, которую при аналогичных обстоятельствах проявляло бы лицо, наделенное обычным уровнем осторожности и компетентности и занимающееся тем же видом коммерческой или иной деятельности. Там, где основанием для наступления ответственности обычно считается простая небрежность, на потерпевшую сторону возлагается доказывание того, что причиной ущерба стало неисполнение обязательств другой стороны, имевшее место по ее вине.

181. Общим стандартом осмотрительности, из которого исходит Типовой закон ЮНСИТРАЛ об электронных подписях, является разумная осмотрительность (или простая небрежность). Этот стандарт осмотрительности применяется к поставщикам сертификационных услуг в связи с выдачей и аннулированием сертификатов, а также разглашением информации[223]. Для оценки соблюдения поставщиком сертификационных услуг установленного для него общего стандарта осмотрительности может использоваться ряд факторов[224]. Такой же стандарт применяется и к подпи-

---

[222] О системе ответственности в данном контексте см. Balboni, "Liability of certification service providers …", pp. 232 и далее.

[223] Пункт 1 статьи 9 Типового закона гласит: "В тех случаях, когда поставщик сертификационных услуг предоставляет услуги для подкрепления электронной подписи, которая может быть использована в качестве подписи, имеющей юридическую силу, такой поставщик сертификационных услуг: […] *b*) проявляет разумную осмотрительность для обеспечения точности и полноты всех исходящих от него существенных заверений, которые относятся к сертификату в течение всего его жизненного цикла или которые включены в сертификат; *c*) обеспечивает разумно доступные средства, которые позволяют полагающейся стороне установить по сертификату: […]; *d*) обеспечивает разумно доступные средства, которые позволяют полагающейся стороне установить, соответственно, по сертификату или иным образом: […]".

[224] *Типовой закон об электронных подписях...* . В пункте 146 Руководства по принятию говорится: "При оценке ответственности поставщика сертификационных услуг во внимание принимаются, в частности, следующие факторы: *a*) затраты на получение сертификата; *b*) характер сертифицируемой информации; *c*) наличие и степень любого ограничения цели, для которой может использоваться сертификат; *d*) наличие любого заявления, ограничивающего масштаб или объем ответственности поставщика сертификационных услуг; и *e*) любое действие полагающейся стороны, способствовавшее причинению ущерба. В ходе подготовки Типового закона было достигнуто общее мнение о том, что при определении возместимого ущерба в принимающем государстве следует учитывать нормы, регулирующие вопросы ограничения ответственности в государстве, в котором учрежден соответствующий поставщик сертификационных услуг, или в любом другом государстве, право которого будет применимым согласно соответствующей коллизионной норме".

савшим лицам для целей предупреждения несанкционированного использования и обеспечения надежного хранения устройств для создания подписей[225]. Тот же общий стандарт разумной осмотрительности распространяется в Типовом законе на полагающуюся сторону, от которой требуются разумные шаги по проверке как надежности электронной подписи, так и того, является ли сертификат действительным или же его действие приостановлено или прекращено, а также по соблюдению любых ограничений, касающихся этого сертификата[226].

182. В нескольких странах, в основном из числа государств, принявших Типовой закон ЮНСИТРАЛ об электронной торговле, общий стандарт "разумной осмотрительности" установлен применительно к действиям поставщика сертификационных услуг[227]. В ряде стран к поставщикам сертификационных услуг, как представляется, "вероятнее всего будет применяться общий стандарт разумной осмотрительности", хотя тот факт, что поставщики сертификационных услуг по своей сути являются сторонами, обладающими специальной квалификацией, которым неспециалисты оказывают большее доверие, чем обычным участникам рынка, "может в итоге приводить к наделению их статусом специалистов или иному установлению для них более строгой обязанности проявлять осмотрительность, принимая разумные меры с использованием своей специальной квалификации"[228]. Именно так, по-видимому, и обстоит дело в большинстве стран, о чем говорится ниже (см. пункт 189).

183. Применительно к подписавшему лицу в некоторых правовых системах, где принят Типовой закон ЮНСИТРАЛ об электронных подписях, действует общий стандарт разумной осмотрительности[229]. В ряде стран соответствующий закон содержит более или менее обширный перечень позитивных обязательств, но при этом не оговаривает применимый стандарт осмотрительности, а также последствия неисполнения этих обязательств[230]. В некоторых странах, однако, закон прямо дополняет перечень обязательств общим положением об ответственности подписавшего за их

---

[225] Статья 8 Типового закона гласит: "В тех случаях, когда данные для создания подписи могут быть использованы для создания подписи, имеющей юридическую силу, каждый подписавший: *a*) проявляет разумную осмотрительность для недопущения несанкционированного использования его данных для создания подписи; и *b*) без неоправданных задержек использует средства, предоставленные в его распоряжение поставщиком сертификационных услуг […], или иным образом предпринимает разумные усилия для уведомления любого лица, которое, как подписавший может разумно предполагать, полагается на электронную подпись или предоставляет услуги в связи с ней, если: i) подписавшему известно, что данные для создания подписи были скомпрометированы; или ii) обстоятельства, известные подписавшему, обусловливают существенный риск того, что данные для создания подписи могли быть скомпрометированы". Подписавший должен также "проявлять разумную осмотрительность для обеспечения точности и полноты всех исходящих от подписавшего существенных заверений, которые относятся к сертификату в течение всего его жизненного цикла или которые должны быть включены в сертификат".

[226] Статья 11, подпункты *a*), *b*) i) и *b*) ii).

[227] См., например: Каймановы Острова, Закон об электронных сделках (2000 год), статья 28, а также Таиланд, Закон об электронных сделках (2001 год), статья 28.

[228] "Certification authority: liability issues", prepared for the American Bankers Association by Thomas J. Smedinghoff, February 1998, section 1.1; размещено по адресу http://www.bakernet.com/ecommerce/CA-Liability-Analysis.doc (дата посещения – 6 июня 2008 года).

[229] Например, согласно статье 27 Закона Таиланда об электронных сделках (2001 год).

[230] См., например: Аргентина, Закон о цифровой подписи (2001 год), статья 25; Венесуэла (Боливарианская Республика), Закон о сообщениях данных и цифровых подписях, статья 19; Индия, Закон об информационных технологиях (2000 год), статьи 40–42; Каймановы Острова, Закон об электронных сделках (2000 год), статья 31; Маврикий, Закон об электронных сделках (2000 год), статьи 33–36; Перу, Закон о цифровых подписях и сертификатах, статья 17; Тунис, Закон об электронном обмене данными и электронной торговле, статья 21; Турция, Указ о процедурах и принципах, связанных с применением Закона об электронной подписи (2005 год), статья 15; Чили, Закон об электронных документах, электронной подписи и услугах по сертификации такой подписи (2002 год), статья 24; а также Эквадор, Закон об электронной торговле, электронных подписях и сообщениях данных, статья 17.

нарушение[231], за которое в одном из случаев предусмотрена даже уголовная ответственность[232]. Можно говорить не о существовании единого стандарта осмотрительности, а о ступенчатой системе, при которой субсидиарной нормой применительно к обязательствам подписавшего является общий стандарт разумной осмотрительности, повышаемый, однако, до уровня гарантии в случае ряда конкретных обязательств, как правило связанных с точностью и правдивостью предоставляемых заверений[233].

184. Полагающаяся сторона находится в особом положении, так как ее действия или бездействие едва ли могут причинить ущерб подписавшему или поставщику сертификационных услуг. Если полагающаяся сторона действует без должной осмотрительности, то в большинстве ситуаций это будет иметь соответствующие последствия для нее самой, но не повлечет какой-либо ответственности перед поставщиком сертификационных услуг. Поэтому неудивительно, что положения национальных законов об электронных подписях, касающиеся роли полагающихся сторон, редко идут дальше общего перечня основных обязанностей полагающейся стороны. Так, как правило, обстоит дело в правовых системах, где принят Типовой закон ЮНСИТРАЛ об электронных подписях, рекомендующий применять к действиям полагающейся стороны стандарт разумной осмотрительности[234]. В некоторых случаях, однако, данное требование прямо не сформулировано[235]. Следует отметить, что прямые или подразумеваемые обязанности полагающейся стороны нельзя считать несущественными для поставщика сертификационных услуг. Так, ссылка на неисполнение полагающейся стороной своей обязанности проявлять осмотрительность может стать аргументом для защиты поставщика сертификационных услуг от требований полагающейся стороны о возмещении ущерба, например, если поставщик сертификационных услуг способен доказать, что ущерб полагающейся стороне можно было предотвратить или смягчить, если бы полагающаяся сторона приняла разумные меры для проверки действительности сертификата или того, для каких целей он мог использоваться.

---

[231] Венесуэла (Боливарианская Республика), Закон о сообщениях данных и электронных подписях, статья 19; Вьетнам, Закон об электронных сделках, статья 25; Доминиканская Республика, Закон об электронной торговле и цифровых документах и подписях (2002 год), статьи 53 и 55; Китай, Закон об электронных подписях (введен в действие в 2004 году), статья 27; Колумбия, Закон № 527 об электронной торговле, статья 40; Мексика, Торговый кодекс, Декрет об электронной подписи (2003 год), статья 99; Панама, Закон о цифровой подписи (2001 год), статьи 37 и 39; а также Российская Федерация, Федеральный закон об электронной цифровой подписи (2002 год), статья 12.

[232] Пакистан, Указ об электронных сделках (2002 год), статья 34.

[233] Например, пункт 2 статьи 37 Закона Сингапура об электронных сделках (глава 88) предусматривает, что, соглашаясь использовать сертификат, подписавший удостоверяет для всех, кто разумно полагается на содержащуюся в сертификате информацию, что: *a*) абонент на законных основаниях владеет частным ключом, соответствующим публичному ключу, указанному в сертификате; *b*) все заявления, предоставленные абонентом сертификационному органу по существу указанной в сертификате информации, соответствуют действительности; и *c*) вся содержащаяся в сертификате информация в пределах того, что известно абоненту, соответствует действительности. В свою очередь, пункт 1 статьи 39 предусматривает лишь обязанность проявлять разумную осмотрительность для сохранения контроля над частным ключом, соответствующим публичному ключу, указанному в таком сертификате, и для недопущения разглашения его лицу, не уполномоченному на создание цифровой подписи абонента. То же самое, по-видимому, предусмотрено и в Боливарианской Республике Венесуэла, где в статье 19 Закона о сообщениях данных и электронных подписях прямо оговорено, что обязательство не допускать несанкционированного использования устройства для создания подписей предполагает "должную предусмотрительность", тогда как другие обязательства выражены в категорической форме.

[234] Каймановы острова, Закон об электронных сделках (2000 год), статья 21; Мексика, Торговый кодекс, Декрет об электронной подписи (2003 год), статья 107; а также Таиланд, Закон об электронных сделках (2001 год), статья 30.

[235] Вьетнам, Закон об электронных сделках, статья 26, а также Турция, Указ о процедурах и принципах, связанных с применением Закона об электронной подписи (2005 год), статья 16.

ii) *Презумпция небрежности*

185. Вторым возможным вариантом является основывающаяся на вине система с переносом бремени доказывания. Согласно этой системе во всех случаях, когда та или иная сторона может быть признана совершившей действия, в результате которых был причинен ущерб, действует презумпция ее вины. Обоснованием такой системы обычно служит тезис о том, что при обычном развитии событий причинение ущерба в некоторых ситуациях возможно только в случае неисполнения стороной своих обязательств или несоблюдения установленного для нее стандарта поведения.

186. В гражданском праве презумпция вины возможна применительно к ответственности за нарушение договора[236], а также в ряде ситуаций, связанных с ответственностью из деликта. Примерами являются субститутивная ответственность за действия наемных работников, агентов, малолетних детей или животных и ответственность, возникающая в процессе некоторых видов коммерческой или промышленной деятельности (ущерб окружающей среде, ущерб прилегающим владениям, дорожно-транспортные происшествия). Теоретические обоснования переноса бремени доказывания и конкретные случаи, когда он допускается, являются различными в разных странах.

187. Практический результат применения такой системы близок к повышенному стандарту осмотрительности, предусматриваемому для специалистов в системе общего права. Специалисты должны обладать определенным минимумом специальных знаний и навыков, необходимым для выполнения их профессиональных функций, и обязаны действовать так, как в данных обстоятельствах действовал бы разумный представитель соответствующей профессии[237]. Это не обязательно означает перенос бремени доказывания, однако практический смысл предусмотренного для специалистов повышенного стандарта осмотрительности заключается в том, что соблюдение этого стандарта, как принято считать, позволяет специалистам не допускать ущерба лицам, которые прибегают к их платным услугам или иным образом доверяют им свое благополучие. При определенных обстоятельствах, однако, так называемая доктрина res ipsa loquitur позволяет судам, в отсутствие доказательств противного, исходить из того, что ущерб "при обычном развитии событий" был возможен лишь в случае отсутствия разумной осмотрительности со стороны того или иного лица[238].

---

[236] Например, согласно пункту 1 статьи 280 Гражданского кодекса Германии должник обязан возместить ущерб, причиненный в результате неисполнения договорного обязательства, за исключением случаев, когда он не несет ответственности за такое неисполнение. В пункте 1 статьи 97 швейцарского Кодекса обязательств этот принцип сформулирован еще четче: в случае неспособности кредитора добиться исполнения обязательств должник обязан компенсировать причиненный этим ущерб, если он не сможет доказать, что неисполнение имело место не по его вине. Аналогичное правило закреплено в статье 1218 Гражданского кодекса Италии. Согласно французскому праву, презумпция небрежности существует во всех случаях, когда договор предполагал определенный результат, однако в случаях, когда в договоре предусматривался некий стандарт исполнения, а не достижение конкретного результата, факт небрежности должен быть доказан (см. Gérard Légier, "Responsabilité contractuelle", *Répertoire de droit civil Dalloz*, № 58-68, August 1989).

[237] W. Page Keeton and others, *Prosser and Keeton on the Law of Torts*, 5th ed. (Saint Paul, Minnesota, West Publishing, 1984), section 32, p. 187.

[238] "Небрежность должна быть разумно доказана. Однако если было показано, что соответствующий объект находился под управлением ответчика или его служащих, а происшествие таково, что при обычном развитии событий оно не могло бы иметь места, если бы управляющие проявили должную осмотрительность, то отсутствие объяснений со стороны ответчиков служит разумным доказательством того, что происшествие допущено по неосмотрительности" (C. J. Erle in Scott v. *The London and St. Katherine's Docks Co*., Ex. Ch., 3 H & C 596, 601, 159 Eng. Rep. 665, 667 (1865)).

188. Применительно к деятельности поставщиков сертификационных услуг данное правило означало бы, что во всех случаях, когда полагающаяся сторона или подписавшее лицо несут ущерб в результате использования электронной подписи или сертификата и этот ущерб может быть признан следствием неисполнения поставщиком сертификационных услуг своих договорных или предусмотренных законом обязательств, в отношении такого поставщика сертификационных услуг возникает презумпция небрежности.

189. Презумпция небрежности, по-видимому, является преобладающим стандартом во внутреннем законодательстве. Например, согласно Директиве Европейского союза об электронных подписях, поставщик сертификационных услуг несет ответственность за возмещение ущерба любому субъекту, разумно полагающемуся на отвечающий установленным требованиям сертификат, за исключением случаев, когда поставщик сертификационных услуг может доказать отсутствие небрежности в своих действиях[239]. Иными словами, основанием ответственности поставщика сертификационных услуг является небрежность с переносом бремени доказывания: доказать, что небрежность с его стороны отсутствовала, должен сам поставщик сертификационных услуг, поскольку он располагает для этого наилучшими возможностями, такими как техническая квалификация и доступ к соответствующей информации (в то время как подписавшие лица и полагающиеся третьи стороны могут не иметь ни того, ни другого).

190. Таким же образом решаются эти вопросы и в национальных законах различных стран, не входящих в Европейский союз, где предусматривается обширный перечень обязанностей поставщиков сертификационных услуг, как правило, возлагающий на них ответственность за любые убытки, вызванные неисполнением ими своих обязательств по закону[240]. Не вполне ясно, во всех ли этих законах действительно имеет место перенос бремени доказывания, но в некоторых из них такой перенос – либо в целом[241], либо применительно к конкретным обязательствам[242] – предусмотрен прямо.

---

[239] *Official Journal of the European Communities*, L 13/12, 19 January 2001. Статья 6 Директивы устанавливает минимальный стандарт ответственности. Принимающие Директиву государства имеют возможность усилить ответственность поставщика сертификационных услуг, например, путем введения режима абсолютной ответственности или путем распространения ответственности также на сертификаты, не отвечающие установленным требованиям. Это, однако, до сих пор не произошло и едва ли произойдет, так как в подобном случае поставщики сертификационных услуг одной из стран оказались бы в невыгодном положении по сравнению с другими поставщиками сертификационных услуг в Европейском союзе (Balboni "Liability of certification service providers …", p. 222).

[240] Аргентина, Закон о цифровой подписи (2001 год), статья 38; Панама, Закон о цифровой подписи (2001 год), статья 51; Тунис, Закон об электронном обмене данными и электронной торговле, статья 22; Чили, Закон об электронных документах, электронной подписи и услугах по сертификации такой подписи (2002 год), статья 14; а также Эквадор, Закон об электронной торговле, электронных подписях и сообщениях данных, статья 31.

[241] Китай, Закон об электронных подписях (введен в действие в 2004 году), статья 28: "Если лицу, поставившему электронную подпись или полагающемуся на электронную подпись, причинен ущерб вследствие его решения положиться на услуги по сертификации электронных подписей, оказываемые поставщиком электронных сертификационных услуг в процессе гражданской деятельности, и если поставщиком электронных сертификационных услуг не представлено доказательств того, что это произошло не по вине данного поставщика, то поставщик электронных сертификационных услуг несет ответственность за ущерб"; см. также статью 13 Закона Турции об электронной подписи (2004 год): "Поставщики услуг по электронной сертификации обязаны возмещать ущерб, причиненный третьим сторонам в результате нарушения положений настоящего Закона или указов, опубликованных в соответствии с настоящим Законом. Ответственность за возмещение ущерба не наступает в случае, если поставщик услуг по электронной сертификации докажет отсутствие небрежности".

[242] "Уполномоченный поставщик сертификационных услуг не несет ответственности за ошибки в информации, содержащейся в аккредитованном сертификате, если: *a*) эта информация была представлена лицом, указанным в аккредитованном сертификате, или от его имени; и *b*) поставщик сертификационных

191. Такое предпочтение в пользу системы, основанной на презумпции вины, можно объяснить опасениями по поводу того, что режим ответственности, использующий в качестве основы простую небрежность, был бы несправедливым по отношению к полагающейся стороне, которая может не обладать техническими знаниями и доступом к соответствующей информации, необходимыми для того, чтобы взять на себя бремя доказывания небрежности поставщика сертификационных услуг.

iii) *Абсолютная ответственность*

192. Правило абсолютной, или "объективной", ответственности используется в различных правовых системах для возложения ответственности на определенных лиц (как правило, производителей или операторов потенциально опасной или вредной продукции или оборудования) без установления их вины или неисполнения ими обязанности соблюдать осмотрительность. Для наступления ответственности при этом достаточно поставки на рынок дефектной продукции или выхода оборудования из строя. Поскольку ответственность вытекает из самого факта причинения убытка или ущерба, отсутствует необходимость установления конкретных юридических элементов, требуемых для доказывания таких актов, как проявление небрежности, неисполнение гарантийных обязательств или умышленные действия.

193. В большинстве правовых систем правило абсолютной ответственности носит исключительный характер и обычно не подразумевается, если на этот счет отсутствуют четкие законодательные положения. В контексте электронных методов подписания и удостоверения подлинности режим абсолютной ответственности может быть излишне обременительным для поставщиков сертификационных услуг и тем самым вести к подрыву коммерческой жизнеспособности данной отрасли на ранней стадии ее развития. На сегодняшний день абсолютная ответственность, по-видимому, не установлена для поставщиков сертификационных услуг или для каких-либо иных сторон, участвующих в процессе использования электронных подписей, ни в одной стране. Правда, в странах, где для поставщиков сертификационных услуг предусмотрен комплекс позитивных обязательств, действующий в отношении таких поставщиков, стандарт осмотрительности обычно очень высок и в некоторых случаях приближается к режиму абсолютной ответственности, но и в этих случаях поставщик сертификационных услуг может быть освобожден от ответственности, если он докажет, что действовал с необходимой предусмотрительностью[243].

b) Стороны, имеющие право требовать возмещения ущерба, и объем возместимого ущерба

194. Один из вопросов, играющих важную роль при определении объема ответственности поставщиков сертификационных услуг и подписавших лиц, касается того, какая группа лиц может иметь право требовать возмещения ущерба, причиненного вследствие нарушения любой из сторон своих договорных или предусмотренных законом обязательств. С этим связан также вопрос об объеме обязательства возмещать ущерб и о подлежащих возмещению типах ущерба.

услуг может доказать, что им были приняты все разумные практические меры для проверки этой информации" (Барбадос, глава 308B, Закон об электронных сделках (1998 год), статья 20); см. также Бермудские Острова, Закон об электронных сделках (1999 год), статья 23, пункт 2 *b*).

[243] Например, в Панаме, Чили и Эквадоре.

195. Ответственность по договору наступает, как правило, при нарушении договорного обязательства. В контексте ИПК договор существует обычно между подписавшим лицом и поставщиком сертификационных услуг. Последствия нарушения одной из сторон своих договорных обязательств по отношению к другой стороне определяются в тексте договора, регулируемого применимыми нормами договорного права. В том, что касается электронных подписей и сертификатов, ответственность вне четко определенных договорных рамок наступает, как правило, в ситуациях, когда то или иное лицо понесло ущерб вследствие своего разумного решения положиться на информацию, которая была представлена поставщиком сертификационных услуг либо подписавшим лицом и которая оказалась ложной или неточной. Полагающаяся третья сторона обычно не заключает договора с поставщиком сертификационных услуг и, скорее всего, вообще никак не взаимодействует с ним, если не считать того, что она полагается на услуги по сертификации. В связи с этим могут возникать трудноразрешимые вопросы, на которые в некоторых правовых системах отсутствует исчерпывающий ответ.

196. В большинстве систем гражданского права даже в отсутствие конкретных положений на этот счет в специализированных законодательных актах об электронных подписях можно исходить из того, что поставщик сертификационных услуг несет ответственность за убытки, понесенные полагающейся стороной по той причине, что она полагалась на неточную или ложную информацию. В ряде правовых систем такая ответственность может вытекать из общего положения о деликтной ответственности, которое включено в большинство гражданских кодексов[244], за редкими исключениями[245]. В некоторых правовых системах можно провести аналогию между деятельностью поставщиков сертификационных услуг и публичных нотариусов, которые обычно несут ответственность за ущерб, причиненный вследствие небрежности при исполнении ими своих обязанностей.

197. В системах общего права, однако, ситуация порой не столь ясна. В случае деликта при исполнении действий, регулируемых договором, в системах общего права традиционно требуется наличие у лица, совершившего деликт, и потерпевшей стороны некоего общего договорного интереса. Поскольку полагающаяся сторона не заключает договора с поставщиком сертификационных услуг и, скорее всего, вообще не взаимодействует с ним, кроме как полагаясь на дефектную сертификацию, в некоторых системах общего права (в отсутствие прямых законодательных положений на этот счет) полагающейся стороне может быть трудно найти основания для предъявления иска поставщику сертификационных услуг[246]. В отсутствие

---

[244] Согласно статье 1382 Гражданского кодекса Франции, любое действие лица, причинившее ущерб другому лицу, обязывает того, по чьей вине оно имело место, возместить этот ущерб. Это общее правило ответственности дало импульс к принятию в ряде других стран аналогичных положений, таких как статья 2043 Гражданского кодекса Италии и статья 483 Гражданского кодекса Португалии.

[245] Гражданский кодекс Германии содержит три общих положения (статьи 823 I, 823 II и 826) и несколько конкретных норм, касающихся ряда довольно узко определяемых деликтов. Основное положение на этот счет зафиксировано в статье 823 I, отличающейся от положений Гражданского кодекса Франции тем, что в ней прямо говорится о причинении ущерба жизни, здоровью, свободе, имуществу или иному праву другого лица.

[246] Например, в отношении английского общего права один из авторов приходит к выводу о том, что "в отсутствие соответствующего законодательства ответственность [поставщика сертификационных услуг] перед [третьей стороной] далеко не очевидна, хотя [третья сторона] несет предсказуемые убытки в результате его небрежности. Более того, трудно найти средства, с помощью которых [третья сторона] могла бы защитить свои интересы. Отсутствие ответственности, по крайней мере, позволяет говорить о существовании пробела в правовых нормах, каковой пробел, в частности, несомненно обнаруживается в случае небрежности со стороны [поставщика сертификационных услуг]. Пробелы в общем праве могут

общего договорного интереса для обоснования иска из деликта в рамках общего права необходимо доказать нарушение соответствующим лицом обязательства проявлять осмотрительность, которым он связан по отношению к потерпевшей стороне. Вопрос о том, существует ли для поставщика сертификационных услуг подобное обязательство в отношении всех потенциальных полагающихся сторон, не вполне ясен. Вообще говоря, в системах общего права считается нежелательным возлагать "ответственность в неопределенном объеме, на неопределенный срок и по отношению к неопределенному кругу сторон"[247] на лиц, представивших неверную информацию по небрежности, за исключением случаев, когда сказанное по небрежности "произнесено прямо, исходит от лица, осведомленного или проинформированного о том, что его слова будут положены в основу действий, и обращено к лицу, с которым говорящий в силу публичного долга, договора или по иной причине связан отношениями, так или иначе обязывающими его действовать осмотрительно, если он будет действовать вообще"[248].

198. В данном случае речь идет об определении круга лиц, по отношению к которым поставщик сертификационных услуг (или же подписавшее лицо) несет обязательство действовать осмотрительно. Для определения круга лиц, имеющих в подобной ситуации законные основания для предъявления исков поставщику сертификационных услуг, могут использоваться три основных стандарта[249]:

a) *стандарт предсказуемости*. Это наиболее широкий из всех стандартов ответственности. Согласно этому стандарту подписавшее лицо или поставщик сертификационных услуг несут ответственность перед любым лицом, в отношении которого можно было разумно предвидеть, что оно будет полагаться на ложные заверения;

b) *стандарт, основанный на намерении и осведомленности*. Это более узкий стандарт, ограничивающий ответственность возмещением убытков, причиненных члену группы лиц, в интересах и для ориентации которых сторона намеревается предоставить информацию или, как известно этой стороне, информацию намерен предоставить получатель;

c) *стандарт общих договорных интересов*. Это самый узкий стандарт, создающий обязательства лишь по отношению к клиенту или лицу, с которым у поставщика информации имелся непосредственный контакт.

199. В Типовом законе ЮНСИТРАЛ об электронных подписях не делается попыток ограничить круг лиц, потенциально подпадающих под категорию "полагающихся сторон", в который могут входить "любые лица, состоящие или не состоящие в договорных отношениях с подписавшим или с поставщиком сертификационных услуг"[250]. Аналогичным образом, в соответствии с Директивой Европейского союза об электронных подписях поставщик сертификационных услуг обязан возместить ущерб "любому субъекту, юридическому или физическому лицу, разумно полагающемуся"

заполняться, однако этот процесс малопредсказуем и ненадежен" (Paul Todd, E-Commerce Law (Abingdon, Oxon, Cavendish Publishing Limited, 2005), pp. 149-150). Аналогичные выводы были сделаны и в отношении австралийского права: см. Sneddon, *Legal liability and e-transactions* …, p. 15.

[247] Судья Кардосо в деле *Ultramares Corporation v. George A. Touche et al*, Court of Appeals of New York, 6 January 1931, 174 N.E. 441, p. 445.

[248] Судья Кардосо в деле *Ultramares Corporation v. George A. Touche et al*..., p. 447.

[249] Smedinghoff, "Certification authority: liability issues" ..., sect. 4.3.1.

[250] *Типовой закон ЮНСИТРАЛ об электронных подписях* ..., пункт 150.

на отвечающий установленным требованиям сертификат. Директива Европейского союза, несомненно, составлена в расчете на систему ИПК, поскольку она применяется лишь в отношении электронных подписей (отвечающих установленным требованиям сертификатов). Понятие субъекта обычно толкуется как относящееся к третьим полагающимся сторонам, и при выполнении Директивы все государства – члены Европейского союза, кроме двух, руководствуются именно этим[251].

200. Как и Типовой закон ЮНСИТРАЛ об электронных подписях, Директива Европейского союза об электронных подписях не сужает категории лиц, которые могут подпадать под определение полагающихся сторон. Поэтому уже отмечалось, что даже в рамках общего права "при оказании сертификационных услуг вполне очевидно, что поставщик сертификационных услуг принимает перед всеми, кто может полагаться на его сертификат, признавая ту или иную электронную подпись для целей той или иной сделки, обязательство действовать осмотрительно, поскольку такой сертификат выдан именно с тем, чтобы побудить других полагаться на него"[252].

201. Еще один заслуживающий внимания вопрос касается характера убытков, возмещение которых может быть получено от подписавшего лица или от поставщика сертификационных услуг. Например, в некоторых системах общего права иск о возмещении чисто экономических убытков, причиненных дефектной продукцией, не может быть предъявлен из деликта. Однако случаи сознательного мошенничества – а в некоторых правовых системах даже неумышленного введения в заблуждение – рассматриваются как исключение из упомянутого правила об экономических убытках[253]. В этой связи интересно отметить, что в Положении об электронных подписях, принятом в Соединенном Королевстве в 2002 году, не воспроизводятся положения Директивы Европейского союза об электронных подписях, касающиеся ответственности. Это означает применение стандартных норм ответственности, которые в данном случае увязаны с критерием непосредственного характера ущерба[254]. Сумма убытков, подлежащих возмещению, как правило, определяется в соответствии с общими нормами договорного или деликтного права. Некоторые законы прямо обязывают поставщиков сертификационных услуг оформлять страхование своей ответственности или иным образом доводить до общего сведения всех, кто может выступать в роли подписавших лиц, наряду с прочей информацией, информацию о финансовых гарантиях, которыми обеспечена их потенциальная ответственность[255].

c) Возможность ограничения ответственности или отказа от ответственности по договору

202. Следует ожидать, что поставщики сертификационных услуг будут постоянно стремиться к максимальному ограничению своей договорной и деликтной ответственности по отношению к подписавшему лицу и полагающимся сторонам. Применительно к подписавшему лицу ограничительные положения, как правило, будут

---

[251] Исключениями являются Венгрия и Дания, Balboni, "Liability of certification service providers …", p. 220.

[252] Lorna Brazell, *Electronic Signatures: Law and Regulation* (London, Sweet and Maxwell, 2004), p. 187.

[253] Smedinghoff, "Certification authority: liability issues" ..., section 4.5.

[254] Dumortier and others, "The legal and market aspects of electronic signatures" ..., p. 215.

[255] Турция, Закон об электронной подписи (2004 год), статья 13, а также Аргентина, Закон о цифровой подписи (2001 год), статья 21 *a*) 1); см. также: Мексика, Торговый кодекс, Декрет об электронной подписи (2003 год), статья 104 III).

содержаться в тех или иных элементах договорной документации, таких как положения о сертификационной практике. Этими положениями может устанавливаться предельный объем ответственности по каждому случаю, по каждой серии случаев и за определенный период времени, а также может исключаться ответственность за некоторые виды ущерба. Еще одним приемом является указание в сертификатах максимальной суммы сделок, для которых эти сертификаты могут использоваться, или установление ограничений на использование сертификата, допускающих его применение лишь для определенных целей[256].

203. Хотя в большинстве правовых систем в целом признается право договаривающихся сторон ограничивать или снимать с себя ответственность на основании положений договора, это право обычно сопровождается различными ограничениями и условиями. Так, в большинстве систем гражданского права возможность полного освобождения лица от ответственности за ущерб, причиненный по его вине, не допускается[257] или недвусмысленно ограничивается[258]. Кроме того, если положения договора не согласованы путем свободных переговоров, а навязаны или предопределены одной из сторон ("договоры присоединения"), то некоторые виды положений об ограничении ответственности могут быть признаны "неправомерными" и, соответственно, недействительными.

204. В системах общего права аналогичный результат может вытекать из нескольких теорий. В Соединенных Штатах, например, суды обычно отказывают в приведении в исполнение договорных положений, признанных "безответственными". Хотя смысл этого понятия обычно зависит от оценки конкретных обстоятельств дела, в целом речь идет о договорных положениях, "которые, с одной стороны, не могли быть предложены ни одним лицом, находящимся в здравом рассудке или даже пребывающим в заблуждении, а с другой – не могли быть приняты ни одним лицом, действующим честно и добросовестно"[259], и которые характеризуются "отсутствием реального выбора у одной из сторон при том, что условия договора выгодны другой стороне сверх разумных пределов"[260]. Подобно гражданско-правовой концепции "договора присоединения", эта доктрина применяется для недопущения "неблаговидной коммерческой практики" сторон, выступающих с более сильных позиций при заключении сделок[261]. Не все условия договоров, заключенных подобным

---

[256] См. Smedinghoff, "Certification authority: liability issues" ..., section 5.2.5.4; и Hindelang, "No remedy for disappointed trust …", section 4.1.1.

[257] Во Франции освобождение от ответственности за нарушение договора в принципе возможно, однако на практике суды склонны объявлять положения об этом недействительными во всех случаях, когда устанавливается, что эти положения позволяли бы стороне избежать последствий нарушения "основополагающего" договорного обязательства (см. Légier, "Responsabilité contractuelle" …, Nos. 262 et 263).

[258] В большинстве стран гражданского права закон запрещает отказ от ответственности за грубую небрежность или неисполнение обязанности, установленной в силу норм публичного порядка. В некоторых странах действуют специальные правила на этот счет, такие, как положения статьи 100 II швейцарского Кодекса обязательств и статьи 1229 Гражданского кодекса Италии. В других странах, например в Португалии, законодательство не содержит аналогичной нормы, но на практике обеспечивается по существу тот же результат, что и в Италии (см. António Pinto Monteiro, *Cláusulas Limitativas e de Exclusão de Responsabilidade Civil* (Coimbra, Faculdade de Direito de Coimbra, 1985, p. 217)).

[259] *First Financial Ins. Co. v. Purolator Security, Inc*., 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979), со ссылкой на *Hume v. U.S.*, 132 U.S. 406, 410 (1975); цитируется по Smedinghoff, "Certification authority: liability issues" ..., section 5.2.5.4.

[260] *First Financial Ins. Co. v. Purolator Security, Inc* ..., со ссылкой на *Williams v. Walker-Thomas Furniture Co*., 350 F.2d 315, 320 (D.C. 1965); цитируется по Smedinghoff, "Certification authority: liability issues" ..., section 5.2.5.4.

[261] *First Financial Ins. Co. v. Purolator Security, Inc*., 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979); цитируется по Smedinghoff, "Certification authority: liability issues" ..., section 5.2.5.4.

образом, являются недействительными. В то же время, хотя суды обычно обеспечивают исполнение стандартных договоров или договоров присоединения (даже потребительских), условия которых не подлежат изменению путем переговоров между сторонами, иногда суд может отказать в приведении в исполнение того или иного положения стандартного договора, если включение этого положения было для другой стороны неоправданной неожиданностью[262].

205. Наконец, и в гражданско-правовых системах, и в системах общего права нормы о защите потребителей могут значительно сокращать для поставщиков сертификационных услуг возможность ограничения их ответственности перед подписавшим лицом в случаях, когда такое ограничение ответственности фактически лишило бы подписавшее лицо какого-либо права или средства правовой защиты, признанного согласно применимому законодательству.

206. Еще более жесткие пределы в большинстве случаев установлены в отношении права поставщика сертификационных услуг ограничивать свою потенциальную ответственность перед полагающейся стороной. Не считая коммерческих моделей закрытого типа, в рамках которых от полагающейся стороны требуется присоединение к условиям договора[263], полагающаяся сторона часто не связана договорными отношениями ни с поставщиком сертификационных услуг, ни даже с подписавшим лицом. Таким образом, при предъявлении полагающейся стороной поставщику сертификационных услуг или подписавшему лицу иска из деликта эти стороны могут быть лишены возможности ограничить свою ответственность, поскольку в большинстве правовых систем для этого необходимо должным образом уведомить о таком ограничении полагающуюся сторону. Отсутствие информации, идентифицирующей полагающуюся сторону, до причинения ей ущерба может не позволить поставщику сертификационных услуг выстроить эффективную систему ограничения своей ответственности (еще в большей степени это, по-видимому, относится к подписавшему лицу). Данная проблема, типичная для открытых систем, в рамках которых не знакомые друг с другом стороны взаимодействуют без каких-либо предварительных контактов, порой чревата самыми пагубными последствиями для подписавшего лица[264]. По мнению многих, и прежде всего представителей сектора сертификационных услуг, это является серьезным препятствием для более широкого использования электронных методов подписания и удостоверения подлинности, так как затрудняет поставщикам сертификационных услуг оценку потенциальных рисков применительно к ответственности.

207. Стремление внести ясность в данный аспект законодательства побудило целый ряд стран прямо признать за поставщиками сертификационных услуг право на ограничение своей ответственности. Так, Директива Европейского союза об электронных подписях обязывает государства – члены Европейского союза предоставить поставщикам сертификационных услуг право указывать в отвечающем установленным требованиям сертификате “ограничения на использование этого сертификата”,

---

[262] Raymond T. Nimmer, *Information Law*, section 11.12[4][a], at 11-37; цитируется по Smedinghoff, “Certification authority: liability issues” ..., section 5.2.5.4.

[263] Как это, например, предусмотрено в Федерации электронного удостоверения подлинности, действующей под управлением Администрации по общему обслуживанию при правительстве Соединенных Штатов (см. E-Authentication Federation, Interim Legal Document Suite, version 4.0.7; размещено по адресу http://www.cio.gov/eauthentication/documents/LegalSuite.pdf (дата посещения – 6 июня 2008 года)).

[264] Sneddon, “*Legal liability and e-transactions* …”, p. 18.

при условии что эти ограничения "понятны третьим сторонам"[265]. Как правило, речь может идти о двух категориях ограничений: ограничениях видов сделок, для которых могут использоваться конкретные сертификаты или категории сертификатов, а также ограничениях предельных сумм сделок, в связи с которыми разрешается использовать сертификаты или категории сертификатов. И при том, и при другом варианте поставщик сертификационных услуг прямо освобождается от ответственности "за ущерб, понесенный вследствие использования отвечающего установленным требованиям сертификата с нарушением предусмотренных для него ограничений"[266]. Кроме того, Директива Европейского союза об электронных подписях предписывает государствам – членам Европейского союза предоставить поставщикам сертификационных услуг "право указывать в отвечающем установленным требованиям сертификате ограничение суммы сделок, для которых может использоваться данный сертификат, при условии что это ограничение понятно третьим сторонам"[267]. В этом случае поставщик сертификационных услуг не несет ответственности за ущерб, вызванный превышением таких ограничений[268].

208. Директива Европейского союза об электронных подписях не устанавливает пределов ответственности поставщика сертификационных услуг. Однако эта Директива позволяет поставщику сертификационных услуг ограничивать максимальную сумму каждой сделки, для которой могут использоваться сертификаты, что освобождает поставщика сертификационных услуг от ответственности сверх этой максимальной суммы[269]. В деловой практике поставщиков сертификационных услуг также нередко используются положения об ограничении общего объема их ответственности на договорной основе.

209. Такая договорная практика находит поддержку в законах еще нескольких стран, где признается возможность ограничения ответственности поставщика сертификационных услуг по отношению к любой потенциально затронутой стороне. Как правило, эти законы разрешают установление ограничений согласно положению о сертификационной практике поставщика сертификационных услуг, а некоторые из них прямо освобождают поставщика сертификационных услуг от ответственности в случае использования сертификата для иной цели, чем та, для которой он был выдан[270]. Кроме того, в некоторых законах за поставщиками сертификационных услуг признается право выдавать сертификаты различных категорий и устанавливать в связи с ними разные рекомендуемые уровни доверия[271], как правило, предпо-

---

[265] European Union Directive on Electronic Signatures , article 6, paragraph 3.

[266] European Union Directive on Electronic Signatures ... .

[267] European Union Directive on Electronic Signatures ..., article 6, paragraph 4.

[268] European Union Directive on Electronic Signatures ... .

[269] Dumortier and others, "The legal and market aspects of electronic signatures" …, p. 55; см. также Hindelang, "No remedy for disappointed trust …", section 4.1.1; Balboni ("Liability of certification service providers …", p. 230) идет еще дальше, утверждая, что "статья 6 4) позволяет лишь ограничивать сумму сделки […], что не имеет никакого отношения к ограничению потенциального объема ущерба, который может быть причинен такой сделкой".

[270] Аргентина, Закон о цифровой подписи (2001 год), статья 39; Барбадос, глава 308B, Закон об электронных сделках (1988 год), статья 20, пункты 3 и 4; Бермудские Острова, Закон об электронных сделках (1999 год), статья 23, пункты 3 и 4; Вьетнам, Закон об электронных сделках, статья 29, пункты 7 и 8 (в последнем случае, впрочем, отсутствует прямое освобождение от ответственности); а также Чили, Закон об электронных документах, электронной подписи и услугах по сертификации такой подписи (2002 год), статья 14.

[271] Маврикий, Закон об электронных сделках (2000 год), статьи 38 и 39; а также Сингапур, Закон об электронных сделках (глава 88) (1998 год), статьи 44 и 45.

лагающие различные степени ограничения (и надежности) в зависимости от размера взимаемой платы. В то же время некоторые законы прямо запрещают любые ограничения ответственности, кроме тех, которые вытекают из ограничений на использование сертификатов или из соответствующих предельных сумм сделок[272].

210. В свою очередь, страны, избравшие минималистский подход, считают законодательное вмешательство в данную сферу в целом нежелательным и предпочитают, чтобы эти вопросы регулировались сторонами на договорной основе[273].

2. *Конкретные случаи ответственности в рамках инфраструктуры публичных ключей*

211. Главной темой дискуссий об ответственности в связи с использованием электронных методов подписания и удостоверения подлинности являются основания и параметры ответственности поставщиков сертификационных услуг. Общепризнано, что основополагающая обязанность поставщика сертификационных услуг заключается в том, чтобы использовать надежные системы, процедуры и людские ресурсы и действовать в соответствии с заверениями, которые поставщик сертификационных услуг дает в отношении принципов и практики своей деятельности[274]. Кроме того, поставщик сертификационных услуг должен проявлять разумную осмотрительность для обеспечения точности и полноты всех исходящих от него существенных заверений, которые относятся к сертификату. Вся эта деятельность потенциально влечет за собой различные степени ответственности поставщика сертификационных услуг, в зависимости от применимого права. В нижеследующих пунктах указываются случаи, связанные для поставщика сертификационных услуг с наибольшим риском наступления ответственности, и вкратце говорится о том, как эта ответственность регулируется внутренним законодательством.

a) Невыдача или задержка выдачи сертификата

212. Как правило, поставщик сертификационных услуг выдает сертификаты по заявкам лиц, желающих использовать электронную подпись. Если заявка отвечает критериям, которые установлены поставщиком сертификационных услуг, то он может выдать сертификат. Возможны ситуации, когда отвечающая этим критериям заявка тем не менее отклоняется или удовлетворяется с запозданием – либо просто из-за ошибки поставщика сертификационных услуг, либо из-за структурной или непредвиденной неготовности используемого поставщиком сертификационных услуг механизма приема заявок, либо из-за того, что поставщик сертификационных услуг по тем или иным скрытым мотивам задерживает выдачу сертификата или не желает выдавать сертификат по данной заявке. У подателей заявок, которые были при подобных обстоятельствах отклонены или удовлетворены с запозданием, могут возникнуть претензии к поставщику сертификационных услуг[275].

---

[272] Турция, Закон об электронной подписи (2004 год), статья 13.

[273] Об Австралии см. Sneddon, *Legal liability and e-transactions* ..., pp. 44-47; о Соединенных Штатах см. Smedinghoff, “Certification authority: liability issues”..., section 5.2.51.

[274] Типовой закон ЮНСИТРАЛ об электронных подписях ... , статья 9, подпункты 1 *a*) и *b*).

[275] Smedinghoff, “Certification authority: liability issues” ... , section 3.2.1.

213. При наличии конкурентного рынка сертификационных услуг умышленный или неумышленный отказ поставщика сертификационных услуг в выдаче сертификата может не причинить подателю заявки ощутимого ущерба. Однако в отсутствие реальной конкуренции отказ поставщика сертификационных услуг выдать сертификат или выдача сертификата с запозданием может повлечь за собой серьезный ущерб подателю неудовлетворенной заявки, если без сертификата он будет не в состоянии заключить какую-либо сделку. Даже при наличии конкурирующих альтернативных поставщиков можно представить себе ситуацию, когда лицо, запросившее сертификат для той или иной сделки, понесет в связи с данной конкретной сделкой убытки, если из-за отклонения или позднего удовлетворения заявки сертификат не будет получен им своевременно и подателю заявки придется отказаться от важной сделки[276].

214. В международном контексте такой сценарий маловероятен, так как большинство желающих использовать электронную подпись, скорее всего, будут обращаться к поставщикам сертификационных услуг, базирующимся в их собственных странах.

b) Небрежность при выдаче сертификата

215. Основная функция сертификата заключается в увязывании идентификационных данных подписавшего лица с тем или иным публичным ключом. Соответственно, главная задача поставщика сертификационных услуг состоит в том, чтобы, следуя заявленной им практике, проверить, действительно ли податель заявки является подписавшим лицом и имеет в своем распоряжении частный ключ, соответствующий указанному в сертификате публичному ключу. Невыполнение этой задачи может повлечь за собой ответственность поставщика сертификационных услуг по отношению к подписавшему или к третьей стороне, полагающейся на сертификат.

216. Ущерб подписавшему может быть причинен, например, в случае ошибочной выдачи сертификата постороннему лицу, присвоившему себе чужие идентификационные данные. При этом возможен сговор с участием служащих или подрядчиков самого поставщика сертификационных услуг с целью использования ключа подписи этого поставщика сертификационных услуг для удовлетворения мошеннических заявок постороннего лица. Эти сотрудники или подрядчики также могут выдать неверный сертификат по небрежности, не выполнив должным образом при рассмотрении мошеннической заявки объявленные поставщиком сертификационных услуг процедуры проверки либо использовав ключ подписи поставщика сертификационных услуг для несанкционированного создания сертификата. Наконец, злоумышленник может выдать себя за подписавшее лицо, предъявив поддельные, но схожие с подлинными идентификационные документы, и добиться выдачи сертификата по мошеннической заявке даже при отсутствии небрежности со стороны поставщика сертификационных услуг и несмотря на тщательное соблюдение им своих опубликованных правил[277].

217. Ошибочная выдача сертификата мошеннику может иметь самые серьезные последствия. Полагающиеся стороны, заключающие с мошенником сделки в режиме онлайн, могут, положившись на недостоверные данные в неверно выданном сертификате, отгрузить товары, перечислить средства, предоставить кредит или совершить другие операции, считая, что они ведут дело с тем, за кого выдает себя

[276] Smedinghoff, “Certification authority: liability issues” ... , section 3.2.1.

[277] Smedinghoff, “Certification authority: liability issues” ... , section 3.2.1.

мошенник. К моменту обнаружения мошенничества полагающимся сторонам может быть причинен значительный ущерб. При подобных обстоятельствах в положении потерпевших оказываются две стороны: полагающаяся сторона, введенная в заблуждение неверно выданным сертификатом, и сторона, на имя которой мошеннику был ошибочно выдан сертификат. И у той, и у другой будут претензии к поставщику сертификационных услуг. Еще одним возможным сценарием является выдача сертификата по небрежности на имя несуществующего лица, что чревато причинением ущерба только полагающейся стороне[278].

218. В статье 9 Типового закона ЮНСИТРАЛ об электронных подписях предусматривается, в частности, что поставщик сертификационных услуг должен проявлять разумную осмотрительность для обеспечения точности и полноты всех исходящих от него существенных заверений, которые относятся к сертификату в течение всего его жизненного цикла или которые включены в сертификат. Положение о такой общей обязанности буквально воспроизведено во внутреннем законодательстве ряда стран, где был принят Типовой закон[279], хотя в некоторых странах соответствующий стандарт, по-видимому, был повышен от уровня разумной осмотрительности до более высокого уровня гарантии[280].

219. Режим, установленный Директивой Европейского союза об электронных подписях, обязывает государства – члены Европейского союза "как минимум" обеспечить, чтобы поставщик сертификационных услуг, выдающий сертификаты, представляемые населению как отвечающие установленным требованиям, или гарантирующий населению такие сертификаты, нес ответственность за возмещение ущерба, причиненного любому субъекту или юридическому или физическому лицу, разумно полагающемуся на такой сертификат: *a*) в отношении точности всей информации, содержащейся в отвечающем установленным требованиям сертификате на момент его выдачи, а также того, что сертификат содержит все сведения, которые предписано включать в отвечающий установленным требованиям сертификат; *b*) в отношении заверения в том, что на момент выдачи сертификата у подписавшего лица, указанного в отвечающем установленным требованиям сертификате, имелись данные для создания подписи, соответствующие данным для проверки подписи, приведенным или указанным в сертификате; *c*) в отношении заверения в том, что эти данные для создания подписи и данные для проверки подписи могут использоваться взаимодополняющим образом в случаях, когда и те, и другие данные составляются поставщиком сертификационных услуг – за исключением случаев, когда поставщик сертификационных услуг может доказать отсутствие небрежности в своих действиях[281].

220. Законы других стран в целом не отличаются друг от друга в том смысле, что все они обязывают поставщиков сертификационных услуг проверять точность

---

[278] Smedinghoff, "Certification authority: liability issues" ... , section 3.2.1.

[279] См., например, Таиланд, Закон об электронных сделках (2001 год), статья 28, пункт 2; а также Каймановы Острова (заморская территория Соединенного Королевства), Закон об электронных сделках (2000 год), статья 28 *b*).

[280] См., например, Китай, Закон об электронных подписях, статья 22: "Поставщики электронных сертификационных услуг **обеспечивают** полноту и точность содержания сертификатов электронных подписей в течение срока их действия, а также обеспечивают сторонам, полагающимся на электронные подписи, возможность проверки или понимания всего, что зафиксировано в сертификатах электронных подписей, а также информации по другим связанным с этим вопросам", выделение добавлено.

[281] European Union directive on electronic signatures …, article 6, paragraph 1.

информации, на основании которой выдается сертификат. В ряде стран поставщик сертификационных услуг вообще несет ответственность перед любым лицом, разумно полагавшимся на сертификат, за точность всей информации, содержащейся в аккредитованном сертификате на момент его выдачи[282], или гарантирует ее точность[283], хотя в некоторых таких странах поставщик сертификационных услуг может ограничить это гарантийное обязательство, включив в сертификат соответствующее заявление[284]. Вместе с тем некоторые законы прямо освобождают поставщика сертификационных услуг от ответственности за неточность информации, представленной подписавшим, при условии ее проверки в соответствии с положением о сертификационной практике, если поставщик сертификационных услуг может доказать, что им были приняты все разумные меры для проверки этой информации[285].

221. В других странах достижение такого же результата обеспечивается не с помощью требуемой по закону гарантии, а путем возложения на поставщиков сертификационных услуг общей обязанности перед выдачей сертификата проверять информацию, представленную подписавшим[286], или создать системы для проверки такой информации[287]. В ряде случаев предусмотрена обязанность немедленно аннулировать сертификат, если станет известно, что информация, на основании которой сертификат был выдан, является неточной или ложной[288]. В некоторых случаях, однако, закон обходит выдачу сертификатов молчанием, требуя лишь соблюдения поставщиком сертификационных услуг его положения о сертификационной практике[289] или выдачи сертификата согласно договоренности с подписавшим[290]. Это не означает, что в законе не предусмотрено никакой ответственности поставщиков сертификационных услуг. Напротив, некоторые законы прямо предусматривают такую ответственность, требуя, чтобы поставщики сертификационных услуг обеспечивали надлежащее страховое покрытие своей гражданской ответственности, распространяющееся на любой охваченный и не охваченный договором ущерб подписавшим лицам и третьим сторонам[291].

222. Обязанность поставщика сертификационных услуг проверять точность представляемой информации дополняется обязанностью подписавшего “проявлять

---

[282] Барбадос, глава 308B, Закон об электронных сделках (1998 год), статья 20, пункт 1 *a*); Бермудские Острова, Закон об электронных сделках (1999 год), статья 23; Индия, Закон об информационных технологиях (2000 год), статья 36 *e*); Маврикий, Закон об электронных сделках (2000 год), статья 27, пункт 2 *d*); Сингапур, Закон об электронных сделках, статьи 29, подпункты 2 *a*) и *c*), и 30 1); а также Специальный административный район (САР) Китая Гонконг, Указ об электронных сделках, статья 39.

[283] Вьетнам, Закон об электронных сделках, статья 31 *d*); а также Тунис, Закон об электронном обмене данными и электронной торговле, статья 18.

[284] Например, в Барбадосе, Бермудских Островах, Маврикии, САР Китая Гонконге и Сингапуре.

[285] Аргентина, Закон о цифровой подписи (2001 год), статья 39 *c*).

[286] Аргентина, Закон о цифровой подписи (2001 год), статья 21 *o*); Венесуэла (Боливарианская Республика), Закон о сообщениях данных и электронных подписях, статья 35; Мексика, Торговый кодекс, Декрет об электронной подписи (2003 год), статья 104 I); а также Чили, Закон об электронных документах, электронной подписи и услугах по сертификации такой подписи, статья 12 *e*).

[287] Эквадор, Закон об электронной торговле, электронных подписях и сообщениях данных, статья 30 *d*).

[288] Аргентина, Закон о цифровой подписи (2001 год), статья 19 *e*) 2).

[289] Перу, Декрет о порядке введения в действие закона о цифровых подписях и сертификатах, статья 29 *a*).

[290] Доминиканская Республика, Закон об электронной торговле и цифровых документах и подписях (2002 год), статья 40 *a*); Колумбия, Закон № 527 об электронной торговле, статья 32 *a*); а также Панама, Закон о цифровой подписи (2001 год), статья 49, пункт 7.

[291] Венесуэла (Боливарианская Республика), Закон о сообщениях данных и электронных подписях, статья 32.

разумную осмотрительность для обеспечения точности и полноты всех исходящих от подписавшего существенных заверений, которые относятся к сертификату в течение всего его жизненного цикла или которые должны быть включены в сертификат"[292]. Таким образом, подписавший может нести ответственность перед поставщиком сертификационных услуг или перед полагающейся стороной за представление поставщику сертификационных услуг ложной или неточной информации при подаче заявки на получение сертификата. Иногда это выражено в форме общего обязательства представлять поставщику сертификационных услуг точную информацию[293] или проявлять разумную осмотрительность для обеспечения достоверности этой информации[294]; в других случаях на подписавшего прямо возлагается ответственность за ущерб, причиненный в результате невыполнения им данного конкретного требования[295].

c) Несанкционированное использование подписи или нарушение положения о сертификационной практике

223. Проблема несанкционированного использования устройств для создания подписи и сертификатов имеет два аспекта. С одной стороны, возможны нарушения режима эксплуатации устройств для создания подписи или другие случаи, когда они могут быть скомпрометированы, например их незаконное присвоение агентом подписавшего. С другой стороны, может быть скомпрометирована сама иерархия создания подписи, используемая поставщиком сертификационных услуг, например в случае утраты собственного ключа подписи поставщика сертификационных услуг или же корневого ключа, а также в случае, если эти ключи стали известны посторонним, были использованы ими или иным образом скомпрометированы.

224. Иерархия создания подписей может быть скомпрометирована различными путями. Поставщик сертификационных услуг либо кто-то из его служащих или подрядчиков может случайно уничтожить ключ или выпустить его из под своего контроля; центр данных, где хранится частный ключ, может быть поврежден в результате аварии; или же ключ, принадлежащий поставщику сертификационных услуг, может быть умышленно уничтожен или скомпрометирован кем-то (например, хакером) в противозаконных целях. Последствия компрометации иерархии создания подписей могут быть весьма серьезными. Например, если частный ключ подписи или корневые ключи попадут в руки злоумышленника, он получит возможность создавать подложные сертификаты и использовать их якобы от имени реальных или фиктивных подписавших лиц, нанося этим ущерб полагающимся сторонам. Кроме того, в случае обнаружения подобного ущерба все сертификаты, выданные данным поставщиком сертификационных услуг, будет необходимо аннулировать, что может стать причиной огромных исков со стороны всего сообщества подписавших лиц о возмещении убытков, причиненных невозможностью использования этих сертификатов.

---

[292] Типовой закон ЮНСИТРАЛ об электронных подписях ... , статья 8, подпункт 1 *c*).

[293] Аргентина, Закон о цифровой подписи (2001 год), статья 25; Мексика, Торговый кодекс, Декрет об электронной подписи (2003 год), статья 99 III); а также Чили, Закон об электронных документах, электронной подписи и услугах по сертификации такой подписи (2002 год), статья 24.

[294] Каймановы Острова, Закон об электронных сделках (2000 год), статья 31 *c*).

[295] Доминиканская Республика, Закон об электронной торговле и цифровых документах и подписях (2002 год), статья 55; Колумбия, Закон № 527 об электронной торговле, статья 40; Мексика, Торговый кодекс, Декрет об электронной подписи (2003 год), статья 99 III); а также Панама, Закон о цифровой подписи (2001 год), статья 39.

225. В Типовом законе ЮНСИТРАЛ об электронных подписях данный вопрос подробно не рассматривается. Можно исходить из того, что предусмотренное Типовым законом общее обязательство поставщика сертификационных услуг "использовать надежные системы, процедуры и людские ресурсы"[296] означает, что поставщик сертификационных услуг должен принимать все необходимые меры для недопущения компрометации своего собственного ключа (а вместе с ним и всей своей иерархии создания подписей). В законах нескольких стран такое обязательство предусмотрено прямо, нередко в сочетании с обязанностью поставщика сертификационных услуг использовать надежные системы[297]. В некоторых случаях особо оговорена обязанность принимать меры во избежание подделки сертификатов[298]. Поставщик сертификационных услуг обязан воздерживаться от создания подписей подписавших лиц и от получения доступа к данным, используемым для создания их подписей, и может нести ответственность за подобные действия, умышленно совершенные его служащими[299]. Если данные, предназначенные для создания подписи, были скомпрометированы, то это обязывает поставщика сертификационных услуг просить об аннулировании соответствующего сертификата, выданного им самим[300].

226. Соблюдение всей надлежащей осмотрительности требуется и от подписавшего. Например, согласно Типовому закону ЮНСИТРАЛ об электронных подписях подписавший должен "проявлять разумную осмотрительность для недопущения несанкционированного использования его данных для создания подписи"[301]. Аналогичная обязанность, хотя и с некоторыми вариациями, предусмотрена в большинстве национальных законов. В некоторых случаях закон налагает на подписавшего строгое обязательство сохранять за собой исключительный контроль над устройством для создания подписи и не допускать его несанкционированного использования[302] или объявляет подписавшего единолично ответственным за сохранность устройства для создания подписи[303]. Нередко, однако, это обязательство сопровождается оговоркой, ограничивающей его обязанностью сохранять надлежащий контроль над устройством для создания подписи или принимать надлежащие меры для сохранения над ним контроля[304], либо проявлять должную заботливость для предотвращения его несанкционированного использования[305], либо проявлять разумную осмотри-

---

[296] Статья 9, подпункт 1 *f*).

[297] Аргентина, Закон о цифровой подписи (2001 год), статья 21 *c*) и *d*); Колумбия, Закон № 527 об электронной торговле, статья 32 *b*); Маврикий, Закон об электронных сделках (2000 год), статья 24; Панама, Закон о цифровой подписи (2001 год), статья 49, пункт 5; Таиланд, Закон об электронных сделках (2001 год), статья 28, пункт 6; а также Тунис, Закон об электронном обмене данными и электронной торговле, статья 13.

[298] Венесуэла (Боливарианская Республика), Закон о сообщениях данных и электронных подписях, статья 35.

[299] Аргентина, Закон о цифровой подписи (2001 год), статья 21 *b*).

[300] Аргентина, Закон о цифровой подписи (2001 год), статья 21 *p*).

[301] Статья 8, подпункт 1 *a*).

[302] Аргентина, Закон о цифровой подписи (2001 год), статья 25 *a*); Доминиканская Республика, Закон об электронной торговле и цифровых документах и подписях (2002 год), статья 53 *d*); Колумбия, Закон № 527 об электронной торговле, статья 39, пункт 3; Панама, Закон о цифровой подписи (2001 год), статья 37, пункт 4; Российская Федерация, Федеральный закон об электронной цифровой подписи (2002 год), статья 12, пункт 1; а также Турция, Указ о процедурах и принципах, связанных с применением Закона об электронной подписи (2005 год), статья 15 *e*).

[303] Тунис, Закон об электронном обмене данными и электронной торговле, статья 21.

[304] Вьетнам, Закон об электронных сделках, статья 25, пункт 2 *a*), а также Чили, Закон об электронных документах, электронной подписи и услугах по сертификации такой подписи (2002 год), статья 24.

[305] Венесуэла (Боливарианская Республика), Закон о сообщениях данных и электронных подписях, статья 19.

тельность во избежание несанкционированного использования своего устройства для создания подписи[306].

d) Непринятие мер по приостановлению действия или аннулированию сертификата

227. Поставщик сертификационных услуг может также нести ответственность за непринятие мер по приостановлению действия или аннулированию скомпрометированного сертификата. Для того чтобы инфраструктура цифровых подписей функционировала должным образом и пользовалась доверием, совершенно необходим механизм, позволяющий в режиме реального времени определять, является ли тот или иной сертификат действительным или же его действие приостановлено либо он аннулирован. Например, в случае любой компрометации частного ключа аннулирование сертификата представляет собой главный механизм, с помощью которого подписавший может оградить себя от попыток совершения мошеннических сделок посторонними лицами, которые могли завладеть копией его частного ключа.

228. Следовательно, оперативность, с которой поставщик сертификационных услуг по просьбе подписавшего аннулирует выданный ему сертификат или приостанавливает его действие, имеет решающее значение. Промежуток времени между подачей подписавшим лицом просьбы об аннулировании сертификата, его фактическим аннулированием и публикацией уведомления об аннулировании может быть использован посторонним лицом для заключения мошеннических сделок. Поэтому, если поставщик сертификационных услуг допускает необоснованные задержки с внесением соответствующих данных в список аннулированных сертификатов или не делает этого вовсе, это может повлечь за собой значительный ущерб как для подписавшего, так и для введенной в заблуждение третьей стороны, полагающейся на якобы действительный сертификат. Кроме того, в ассортимент сертификационных услуг, предлагаемых их поставщиками, могут входить услуги по ведению хранилищ данных и списков аннулированных сертификатов, доступных полагающимся сторонам в режиме онлайн. Наличие такой базы данных связано с двумя основными факторами риска: возможными неточностями в данных хранилища или в списках аннулированных сертификатов, на которые получатели такой информации будут полагаться в ущерб себе, а также возможностью того, что хранилище данных или список аннулированных сертификатов окажутся недоступными (например, из-за отказа системы), что помешает завершению сделок между подписавшими и полагающимися сторонами.

229. Как это уже отмечалось, в Типовом законе ЮНСИТРАЛ об электронных подписях предполагается возможность выдачи поставщиком сертификационных услуг сертификатов различных уровней с разной степенью надежности и защищенности. Соответственно, Типовой закон не предписывает поставщику сертификационных услуг обеспечивать наличие системы аннулирования сертификатов при любых обстоятельствах, так как применительно к некоторым видам сертификатов, рассчитанным

[306] Индия, Закон об информационных технологиях (2000 год), статья 42, пункт 1; Каймановы Острова, Закон об электронных сделках (2000 год), статья 39 *a*); Маврикий, Закон об электронных сделках (2000 год), статья 35, пункт 1 *a*) и *b*); Мексика, Торговый кодекс, Декрет об электронной подписи (2003 год), статья 99 II); Сингапур, Закон об электронных сделках (глава 88), статья 39; Таиланд, Закон об электронных сделках (2001 год), статья 27, пункт 1; а также Эквадор, Закон об электронной торговле, электронных подписях и сообщениях данных (2002 год), статья 17 *b*).

на небольшие суммы, это может быть экономически неоправданным. Вместо этого Типовой закон обязывает поставщика сертификационных услуг лишь предоставить "разумно доступные средства", которые позволят полагающейся стороне установить по сертификату, в частности, существуют ли средства для направления подписавшим лицом уведомления о том, что данные для создания подписи были скомпрометированы, и предлагается ли услуга по своевременному аннулированию[307]. В случаях, когда услуга по своевременному аннулированию предусмотрена, поставщик сертификационных услуг должен обеспечить фактическое наличие возможности ее использования[308].

230. Режим, установленный Директивой Европейского союза об электронных подписях, обязывает государства – члены Европейского союза "как минимум" обеспечить, чтобы поставщик сертификационных услуг, выдавший сертификат, который был представлен населению как отвечающий установленным требованиям, нес ответственность за возмещение ущерба, причиненного любому субъекту или юридическому или физическому лицу, разумно полагающемуся на такой сертификат, вследствие непринятия мер по регистрации аннулирования сертификата, за исключением случаев, когда поставщик сертификационных услуг может доказать отсутствие небрежности в своих действиях[309]. Законы некоторых стран предписывают поставщику сертификационных услуг принимать меры для недопущения подделки сертификатов[310] или аннулировать сертификат, как только станет известно, что информация, на основании которой он был выдан, является неточной или ложной[311].

231. Аналогичная обязанность может также быть установлена для подписавшего и других уполномоченных лиц. В частности, Типовой закон ЮНСИТРАЛ об электронных подписях требует, чтобы подписавший без неоправданных задержек использовал средства, предоставленные в его распоряжение поставщиком сертификационных услуг, или иным образом предпринимал разумные усилия для уведомления любого лица, которое, как подписавший может разумно предполагать, полагается на электронную подпись или предоставляет услуги в связи с ней, если подписавшему стало известно, что данные для создания подписи были скомпрометированы, или если обстоятельства, известные подписавшему, обусловливают существенный риск того, что данные для создания подписи могли быть скомпрометированы[312].

232. Во внутреннем законодательстве нередко предусмотрена обязанность подписавшего ходатайствовать об аннулировании сертификата при любых обстоятельствах, когда секретность данных для создания подписи могла быть нарушена[313], хотя в некоторых случаях закон обязывает подписавшего лишь сообщать об этом

---

[307] Статья 9, подпункт 1 *d*), v) и vi).

[308] Статья 9, подпункт 1 *e*).

[309] European Union directive on electronic signatures …, article 6, paragraph 2; см. также paragraph (*b*) of annex II to the directive.

[310] Панама, Закон о цифровой подписи (2001 год), статья 49, пункт 6.

[311] Аргентина, Закон о цифровой подписи (2001 год), статья 19 *e*) 2).

[312] Статья 8, подпункт 1 *b*), i) и ii).

[313] Аргентина, Закон о цифровой подписи (2001 год), статья 25 *c*); Доминиканская Республика, Закон об электронной торговле и цифровых документах и подписях (2002 год), статьи 49 и 53 *e*); Колумбия, Закон № 527 об электронной торговле, статья 39, пункт 4; Маврикий, Закон об электронных сделках (2000 год), статья 36; Панама, Закон о цифровой подписи (2001 год), статья 37, пункт 5; Российская Федерация, Федеральный закон об электронной цифровой подписи (2002 год), статья 12, пункт 1; Сингапур, Закон об электронных сделках (глава 88), статья 40; а также Эквадор, Закон об электронной торговле, электронных подписях и сообщениях данных, статья 17 *f*).

поставщику сертификационных услуг[314]. В законах нескольких стран принята формулировка Типового закона ЮНСИТРАЛ об электронных подписях, который обязывает подписавшего уведомлять также любое лицо, которое, как может разумно предполагать владелец устройства для создания подписи, полагается на электронную подпись или предоставляет услуги в связи с ней[315]. Хотя в ряде правовых систем последствия неисполнения этой обязанности могут прямо не оговариваться, в некоторых странах закон прямо предусматривает ответственность подписавшего за несообщение об утрате контроля над частным ключом или необращение с просьбой об аннулировании сертификата[316].

Заключение

233. Широкое внедрение электронных методов подписания и удостоверения подлинности может стать важным шагом, способствующим сокращению объемов коммерческой документации и связанных с ней операционных издержек в международной торговле. Хотя темпы изменений в этой сфере во многом определяются прежде всего качеством и надежностью технических решений, правовые нормы могут внести существенный вклад в создание благоприятных условий для использования электронных методов подписания и удостоверения подлинности.

234. Во многих странах уже приняты внутренние меры в этом направлении в форме законодательства, подтверждающего юридическую значимость электронных сообщений и определяющего критерии их эквивалентности сообщениям, составленным на бумаге. Важной составляющей таких законов часто являются положения, регулирующие применение электронных методов подписания и удостоверения подлинности. Наиболее авторитетным образцом законодательства в этой области стал Типовой закон ЮНСИТРАЛ об электронной торговле, широкое внедрение положений которого способствует обеспечению весьма важной согласованности на международном уровне. Еще большей согласованности позволила бы достичь широкая ратификация Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах, в которой предложен ряд конкретных правил, касающихся международных сделок.

235. Принятие этих норм ЮНСИТРАЛ может способствовать и международному применению электронных методов подписания и удостоверения подлинности. Так, содержащиеся в Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах гибкие критерии функциональной эквивалентности электронных подписей и подписей под бумажными

---

[314] Индия, Закон об информационных технологиях (2000 год), статья 42, пункт 2; а также Турция, Указ о процедурах и принципах, связанных с исполнением Закона об электронной подписи (2005 год), статья 15 *f*) и *i*).

[315] Вьетнам, Закон об электронных сделках, статья 25, пункт 2 *b*); Каймановы Острова, Закон об электронных сделках (2000 год), статья 31 *b*); Китай, Закон об электронных подписях, статья 15; а также Таиланд, Закон об электронных сделках (2001 год), статья 27, пункт 2.

[316] Венесуэла (Боливарианская Республика), Закон о сообщениях данных и электронных подписях, статья 40; Доминиканская Республика, Закон об электронной торговле и цифровых документах и подписях (2002 год), статья 55; Китай, Закон об электронных подписях, статья 27; Панама, Закон о цифровой подписи (2001 год), статья 39; Российская Федерация, Федеральный закон об электронной цифровой подписи (2002 год), статья 12, пункт 2; а также Эквадор, Закон об электронной торговле, электронных подписях и сообщениях данных, статья 17 *e*).

документами могут составить единую международную основу для обеспечения соответствия электронных методов подписания и удостоверения подлинности иностранным требованиям в отношении формы подписи. Однако при этом могут оставаться нерешенными некоторые проблемы, в частности связанные с международным использованием электронных методов подписания и удостоверения подлинности, требующих участия доверенной третьей стороны в процессе такого удостоверения или подписания.

236. Возникающие в данной области проблемы в очень большой степени обусловлены расхождениями в технических стандартах или несовместимостью оборудования либо программного обеспечения, что сужает возможности взаимодействия между системами, существующими в разных странах. Усилия по согласованию стандартов и повышению технической совместимости могут позволить преодолеть имеющиеся на сегодняшний день трудности. Однако использование электронных методов подписания и удостоверения подлинности наталкивается и на трудности юридического характера, связанные, в частности, с внутренним законодательством, предписывающим или поощряющим использование тех или иных конкретных технологий электронного подписания, как правило цифровых подписей.

237. Законы, определяющие юридическую значимость цифровых подписей, обычно признают такую же юридическую значимость за подписями, подкрепляемыми иностранными сертификатами, лишь в той мере, в какой эти сертификаты рассматриваются как эквивалентные сертификатам, выданным внутри страны. Анализ, проведенный в рамках настоящего исследования, указывает на то, что для правильной оценки юридической эквивалентности необходимо сравнивать между собой не только технические стандарты и стандарты защиты, присущие каждой конкретной технологии подписания, но и нормы, регулирующие ответственность различных сторон, вовлеченных в этот процесс. В Типовом законе ЮНСИТРАЛ об электронных подписях сформулирован общий комплекс основных правил, определяющих некоторые обязанности сторон в процессе подписания и удостоверения подлинности, которые могут влиять на их индивидуальную ответственность. Существуют также тексты, принятые на региональном уровне, – такие, как Директива Европейского союза об электронных подписях, – создающие аналогичную законодательную основу для ответственности поставщиков сертификационных услуг, которые действуют в соответствующем регионе. Однако ни один из этих текстов не охватывает все вопросы ответственности, связанные с международным использованием некоторых электронных методов подписания и удостоверения подлинности.

238. Законодателям и лицам, ответственным за выработку политики, важно уяснить для себя различия между внутренними режимами ответственности, существующими в разных странах, а также те элементы, которые их объединяют, с тем чтобы разработать надлежащие методы и процедуры признания подписей, подкрепляемых иностранными сертификатами. Возможно, уже сегодня во внутреннем законодательстве различных стран даются в основном аналогичные ответы на вопросы, рассмотренные в настоящей публикации, что может объясняться общностью правовых традиций этих стран или их участием в региональных механизмах интеграции. Для таких стран могут быть целесообразными выработка единых стандартов ответственности и даже взаимное согласование внутренних правил в целях содействия трансграничному использованию электронных методов подписания и удостоверения подлинности.

United Nations publication
ISBN: 978-92-1-433058-5
Sales No. R.09.V.4

FOR UNITED NATIONS USE ONLY

Printed in Austria
V.08-55700—March 2009—215