ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ

A

Генеральная Ассамблея

Distr.
GENERAL

A/CN.9/446
11 February 1998

RUSSIAN
Original: ENGLISH

КОМИССИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ
ПО ПРАВУ МЕЖДУНАРОДНОЙ ТОРГОВЛИ
Тридцать первая сессия
Нью-Йорк, 1-12 июня 1998 года

ДОКЛАД РАБОЧЕЙ ГРУППЫ ПО ЭЛЕКТРОННОЙ ТОРГОВЛЕ О РАБОТЕ ЕЕ ТРИДЦАТЬ ВТОРОЙ СЕССИИ (Вена, 19-30 января 1998 года)

СОДЕРЖАНИЕ

V.98-50893

СОДЕРЖАНИЕ (продолжение)

ВВЕДЕНИЕ

1. На своей двадцать девятой сессии (1996 год) Комиссия приняла решение включить в свою повестку дня вопросы о подписях в цифровой форме и сертификационных органах. Рабочей группе по электронной торговле было предложено рассмотреть целесообразность и возможность подготовки единообразных правил по этим темам. Было выражено согласие с тем, что работа, которая должна быть проведена Рабочей группой на ее тридцать первой сессии, может охватывать подготовку проекта правил по определенным аспектам вышеуказанных тем. Рабочей группе было предложено представить Комиссии достаточные элементы для принятия обоснованного решения в отношении рамок единообразных правил, которые будут разрабатываться. В отношении более четкого мандата для Рабочей группы было достигнуто согласие о том, что единообразные правила, которые следует подготовить, должны охватывать такие вопросы, как: правовая основа, поддерживающая процессы сертификации, включая появляющуюся технологию удостоверения подлинности и сертификации в цифровой форме; применимость процесса сертификации; распределение риска и ответственности пользователей, поставщиков и третьих сторон в контексте использования методов сертификации; конкретные вопросы сертификации через применение регистров; и включение путем ссылки[1].

2. На тридцатой сессии (1997 год) Комиссии был представлен доклад Рабочей группы о работе ее тридцать первой сессии (A/CN.9/437). Что касается целесообразности и возможности подготовки единообразных правил по вопросам подписей в цифровой форме и сертификационных органов, Рабочая группа сообщила Комиссии, что она достигла консенсуса в отношении важного значения и необходимости работы в направлении согласования норм права в этой области. Хотя она не приняла окончательного решения в отношении формы и содержания такой работы, она пришла к предварительному выводу о том, что практически можно подготовить проект единообразных правил по крайней мере по вопросам подписей в цифровой форме и сертификационных органов и, возможно, по связанным с этими вопросами проблемам. Рабочая группа напомнила о том, что наряду с подписями в цифровой форме и сертификационными органами в рамках будущей работы в области электронной торговли, возможно, также потребуется рассмотреть следующие темы: вопросы технических альтернатив криптографии публичных ключей; общие вопросы о функциях, выполняемых поставщиками услуг, являющимися третьими сторонами; и заключение контрактов в электронной форме (A/CN.9/437, пункты 156-157). В отношении вопроса включения путем ссылки Рабочая группа пришла к выводу о том, что необходимость в проведении Секретариатом дальнейшего исследования отпала, поскольку основополагающие вопросы хорошо известны и поскольку ясно, что многие аспекты "войны форм" и договоров присоединения необходимо будет оставить на урегулирование на основе применимых национальных законов в силу причин, связанных, в частности, с защитой потребителей и другими соображениями публичного порядка. Рабочая группа решила, что этот вопрос должен быть рассмотрен в качестве первого основного пункта ее повестки дня в начале следующей сессии (A/CN.9/437, пункт 155).

3. Комиссия дала высокую оценку работе, выполненной Рабочей группой на ее тридцать первой сессии, одобрила заключения Рабочей группы и поручила ей подготовить единообразные правила по правовым вопросам подписей в цифровой форме и сертификационных органов (далее в тексте - "единообразные правила").

4. В отношении конкретной сферы применения и формы таких единообразных правил было выражено общее мнение, что на данном начальном этапе принятие решения невозможно. Было сочтено, что, хотя Рабочая группа может надлежащим образом сосредоточить свое внимание на вопросах подписей в цифровой форме с учетом очевидной ведущей роли криптографии публичных ключей в зарождающейся практике электронной торговли, подготавливаемые единообразные правила должны соответствовать нейтральному с точки зрения носителей информации подходу, который взят за основу в Типовом законе ЮНСИТРАЛ об электронной торговле (далее в тексте - "Типовой закон"). Таким образом, единообразные правила не должны препятствовать использованию других методов удостоверения подлинности. Кроме того, при решении вопросов, связанных с криптографией публичных ключей, в этих единообразных правилах, возможно, необходимо будет учесть различия в уровнях обеспечения надежности и признать

различные юридические последствия и уровни ответственности, соответствующие различным видам услуг, оказываемых в контексте подписей в цифровой форме. Что касается сертификационных органов, то Комиссия, хотя она и признала ценность стандартов, определяемых рыночными отношениями, в целом согласилась с тем, что Рабочая группа может надлежащим образом предусмотреть разработку минимального свода стандартов, которые должны будут строго соблюдаться сертификационными органами, особенно в случае необходимости трансграничной сертификации.

5. В качестве дополнительного вопроса, подлежащего рассмотрению в контексте будущей работы в области электронной торговли, было указано на то, что Рабочей группе, возможно, придется на более позднем этапе обсудить вопросы юрисдикции, применимого права и урегулирования споров применительно к сети "Интернет"[2].

6. Рабочая группа по электронной торговле, в состав которой входят все государства - члены Комиссии, провела свою тридцать вторую сессию в Вене с 19 по 30 января 1998 года. В работе сессии приняли участие представители следующих государств - членов Рабочей группы: Австралии, Австрии, Алжира, Болгарии, Бразилии, Венгрии, Германии, Египта, Индии, Ирана (Исламской Республики), Испании, Италии, Китая, Мексики, Нигерии, Польши, Российской Федерации, Сингапура, Словакии, Соединенного Королевства Великобритании и Северной Ирландии, Соединенных Штатов Америки, Судана, Таиланда, Финляндии, Франции и Японии.

7. В работе сессии приняли участие наблюдатели от следующих государств: Анголы, Беларуси, Боснии и Герцеговины, Гватемалы, Греции, Дании, Индонезии, Ирака, Ирландии, Канады, Колумбии, Коста-Рики, Кувейта, Ливана, Малайзии, Марокко, Нидерландов, Пакистана, Парагвая, Республики Кореи, Турции, Украины, Чешской Республики, Швейцарии и Швеции.

8. На сессии присутствовали наблюдатели от следующих международных организаций: Международного торгового центра ЮНКТАД/ВТО, Конференции Организации Объединенных Наций по торговле и развитию (ЮНКТАД), Организации Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО), Организации Объединенных Наций по промышленному развитию (ЮНИДО), Всемирной организации интеллектуальной собственности (ВОИС), Европейской комиссии, Организации экономического сотрудничества и развития (ОЭСР), Всемирной торговой организации (ВТО), Каирского регионального центра по международного торговому арбитражу, Международного морского комитета (ММК), Международной ассоциации портов и гаваней (МАПГ), Международной ассоциации адвокатов (МАА), Международной торговой палаты (МТП), Форума по вопросам права и политики, связанным с "Интернет" (ФППИ), и Европейской международной ассоциации студентов-юристов (ЕАСЮ).

9. Рабочая группа избрала следующих должностных лиц:

Председатель: г-н Мадс Брюд АНДЕРСЕН (Дания);

Заместитель Председателя: г-н ПАН Кан Чау (Сингапур);

Докладчик: г-н Гритсана ЧАНГГОМ (Таиланд).

10. Рабочей группе были представлены следующие документы: предварительная повестка дня (A/CN.9/WG.IV/WP.72); подготовленная Секретариатом для тридцать первой сессии Рабочей группы записка под названием "Планирование будущей работы в отношении электронной торговли: подписи в цифровой форме, сертификационные органы и связанные с этим правовые вопросы" (A/CN.9/WG.IV/WP.71), в которой, в частности, резюмируются обсуждения, ранее проведенные Рабочей группой по вопросу о включении путем ссылки; записка, содержащая текст предложенного проекта положения о включении путем ссылки и пояснительные примечания Соединенного Королевства Великобритании и Северной Ирландии (A/CN.9/WG.IV/WP.74); и записка Секретариата, содержащая

проект единообразных правил о подписях в цифровой форме и других электронных подписях, сертификационных органах и соответствующих правовых вопросах (A/CN.9/WG.IV/WP.73).

11. Рабочая группа утвердила следующую повестку дня:

1. Выборы должностных лиц

2. Утверждение повестки дня

3. Правовые аспекты электронной торговли: включение путем ссылки

4. Правовые аспекты электронной торговли: проект единообразных правил о подписях в цифровой форме, других электронных подписях, сертификационных органах и соответствующих правовых вопросах

5. Прочие вопросы

6. Утверждение доклада.

I. ХОД РАБОТЫ И РЕШЕНИЯ

12. Рабочая группа обсудила вопрос о включении путем ссылки на основе записки, подготовленной Секретариатом (A/CN.9/WG.IV/WP.71), и предложения, внесенного Соединенным Королевством Великобритании и Северной Ирландии (A/CN.9/WG.IV/WP.74). Ход работы и заключения Рабочей группы по этому вопросу отражены в разделе II ниже. После обсуждения Рабочая группа приняла текст проекта статьи о включении путем ссылки. Секретариату было поручено подготовить на основе обсуждений и решений Рабочей группы краткое руководство для оказания помощи государствам в принятии и применении этого проекта статьи. Было отмечено, что проект статьи вместе с соответствующим руководством по его принятию будет представлен на рассмотрение Комиссии на ее тридцать первой сессии, которая будет проведена в Нью-Йорке 1-12 июня 1998 года, для заключительного рассмотрения и возможного включения в Типовой закон и Руководство по его принятию.

13. Рабочая группа также обсудила вопросы о подписях в цифровой форме, других электронных подписях и сертификационных органах и другие соответствующие правовые вопросы на основе записки, подготовленной Секретариатом (A/CN.9/WG.IV/WP.73). Ход работы и заключения Рабочей группы по этим вопросам отражены в разделе III ниже. Секретариату было поручено подготовить на основе этих обсуждений и заключений свод пересмотренных положений, с возможными вариантами, для рассмотрения Рабочей группой на одной из будущих сессий.

II. ВКЛЮЧЕНИЕ ПУТЕМ ССЫЛКИ

14. С учетом состоявшегося ранее обсуждения вопроса о включении путем ссылки, а также проектов текстов, представленных на предыдущих сессиях (A/CN.9/WG.IV/WP.71, пункты 77-93), Рабочей группе было предложено рассмотреть вопрос о включении путем ссылки в электронном контексте на основе следующего предложенного проекта положения (A/CN.9/WG.IV/WP.74, приложение):

"1) Настоящая статья применяется в случае, когда сообщение данных содержит ссылку на - или когда его содержание может быть полностью установлено только при помощи ссылки на - информацию, записанную в другом месте ("дальнейшая информация").

2) С учетом положений пункта 5 сообщение данных имеет ту же силу, как если бы дальнейшая информация была полностью изложена в сообщении данных, и любая ссылка на сообщение данных будет представлять собой ссылку на это сообщение, включающее всю дальнейшую информацию, если соблюдены условия, изложенные в пункте 3.

3) Условия, упомянутые в пункте 2, состоят в том, чтобы в сообщении данных:

a) идентифицировалась дальнейшая информация

i) с помощью общего наименования или описания или кода; и

ii) с помощью достаточного указания на запись и части такой записи, в которой или в которых содержится дальнейшая информация, и, если эта запись не является общедоступной, на место, в котором - и в случаях, когда средства доступа либо не являются очевидными, либо ограничены тем или иным образом, на средства, с помощью которых - она может быть получена; и

b) прямо указывается или ясно подразумевается, что этому сообщению данных предполагается придать ту же силу, как если бы дальнейшая информация была полностью изложена в сообщении данных.

4) Идентификация, упомянутая в пункте 3(a), может быть произведена косвенно с помощью ссылки на записанную в другом месте информацию, в которой содержатся необходимые идентификационные данные, при соблюдении применительно к этой ссылке условий, установленных в пункте 3.

5) Ничто в настоящей статье не затрагивает

a) никакой нормы права, которая требует, чтобы адресат был достаточным образом уведомлен о содержании дальнейшей информации или о записи или месте, где - или о средствах, с помощью которых - такая информация может быть получена, или которая требует, чтобы соответствующее место или запись были доступны для другого лица; или

b) никакой нормы права, касающейся действительности условий для целей заключения контрактов, включая акцепт оферты;

c) никакой нормы права, предписывающей признание силы включаемой дальнейшей информации или действительность процедур включения".

15. Было отмечено следующее: предполагается, что данный проект положения будет применяться в том случае, когда в сообщении данных используется включение путем ссылки (пункт 1); общий принцип заключается в том, что включенная информация (для описания которой термин "условия" не используется, поскольку не вся информация ведет к возникновению обязательства) должна иметь ту же силу, как если бы она была полностью изложена в сообщении данных (пункт 2); общие условия включения путем ссылки должны состоять в том, чтобы включаемая информация была ясно и конкретно идентифицирована (что имеет особую важность для защиты потребителей и прочих третьих сторон), чтобы были указаны место и способ, в котором или с помощью которого такая информация может быть получена, и чтобы было указано на намерение включить такую информацию (пункт 3); косвенная идентификация источника информации путем ссылки на другой источник должна быть приемлемой при соблюдении тех же условий (пункт 4); и любые существующие нормы права, применимые к вопросам включения путем ссылки при использовании бумажных сообщений, должны распространяться также и на электронные сообщения (пункт 5).

16. Было достигнуто общее согласие в отношении необходимости урегулирования данного вопроса, поскольку включение путем ссылки неразрывно связано с использованием электронных сообщений. Было отмечено, что при использовании электронных сообщений большой объем данных обязательно включается путем ссылки (например, записи сообщений, заявления о принципах, подписи в цифровой форме в сертификатах). Кроме того, было отмечено, что включение путем ссылки в электронном контексте может осуществляться различными методами, включая унифицированные указатели ресурсов (URLs), идентификаторы объекта (OIDs) или другие записи, к которым имеется разумный доступ по указанному адресу, но не ограничиваясь ими.

17. Хотя было признано, что включение путем ссылки создает определенный риск, например для потребителей, в то же время отмечалось, что такая практика позволяет потребителям использовать возможности, обеспечиваемые исключительно через сети электронных сообщений. Указывалось, что главная цель положения, касающегося включения путем ссылки, должна состоять в обеспечении сбалансированности в положении заинтересованных сторон. Для достижения этой цели Рабочей группе было предложено параллельно с вышеупомянутым проектом положения рассмотреть проект положения следующего содержания:

"Вариант А Если иное не согласовано сторонами, информация считается составной частью сообщения данных, если это прямо указано или ясно подразумевается [и если в сообщении данных указана процедура, в соответствии с которой к такой информации можно получить доступ на разумной и своевременной основе]. Такая информация имеет силу в той степени, в какой это допускается законом.

Вариант В Информация не может быть лишена юридической силы на том лишь основании, что она включена в сообщение данных путем ссылки".

18. В отношении варианта А было отмечено, что материальные факторы, определяющие разумную доступность того или иного условия, включают: возможности доступа (часы работы архива данных, простота доступа и приемлемые уровни избыточности); стоимость доступа (исключая расходы на соответствующие услуги по связи; если взимается определенная плата, такая плата должна быть разумной и пропорциональной стоимости контракта); формат (широко используемый в рамках заинтересованного сообщества); целостность (проверка содержания, установление личности отправителя и механизм исправления ошибок при передаче); и степень, в которой такое условие может быть впоследствии изменено (договор, не предусматривающий права на такое изменение; уведомление относительно обновления условий; уведомление о принципах внесения изменений). Было также указано, что такие факторы могут быть изложены в руководстве по принятию положений о включении путем ссылки (см. пункты 23-24 ниже).

19. Рабочая группа продолжила обсуждения данного вопроса на основе вышеупомянутых предлагаемых альтернативных положений. Было отмечено, что предлагаемые проекты положений обладают рядом общих преимуществ, одно из которых заключается в том, что эти положения призваны облегчить включение путем ссылки в электронном контексте путем устранения существующей во многих правовых системах неопределенности, в отношении того, являются ли положения, касающиеся традиционного включения путем ссылки, применимыми к включению путем ссылки в электронной среде. В этой связи было предложено избрать иной подход, в рамках которого широкое использование включения путем ссылки в электронной среде поощряться не будет, что позволит снизить риск возможного воспроизведения в сфере электронной торговли такого вызывающего большие трудности явления, которое в сфере традиционной торговли с использованием бумажных документов известно как "война форм". В поддержку этого предложения было высказано мнение о том, что, хотя в контексте бумажных документов включение путем ссылки необходимо из соображений экономии времени, места и затрат, в электронном контексте большой объем данных может быть отражен в сообщении данных простым, оперативным и недорогим образом. Против этого предложения были высказаны возражения на том основании, что придание единообразному закону функций кодекса поведения является неуместным,

поскольку это будет препятствовать использованию широко распространенной и важной практики, присущей применению электронных сообщений.

20. Как отмечалось, еще одним преимуществом вышеупомянутых предложений является то, что в них признается необходимость не затрагивать действия правовых норм, касающихся защиты потребителей, и других национальных и международных императивных норм (например, норм, обеспечивающих защиту более слабых сторон в контексте договора присоединения). Было подчеркнуто следующее: первое предложение призвано обеспечить достижение требуемого результата путем перечисления таких норм права, которые остаются незатронутыми (пункт 5); второе предложение обеспечивает достижение того же результата, поскольку в нем упоминается, что информация имеет силу "в той степени, в какой это допускается законом" (вариант A), и не исключается, что информация будет лишена юридической силы на иных основаниях, чем то, что она включена путем ссылки (вариант B). В целях четкого указания на то, что любая из предложенных формулировок не затрагивает существующие нормы права, было предложено увязать любое положение о включении путем ссылки с формулировкой, аналогичной той, которая использована во второй сноске к статье 1 Типового закона, где однозначно провозглашается принцип, согласно которому Типовой закон не имеет преимущественной силы по отношению к нормам права, предназначенным для защиты потребителей.

21. В то же время было выражено мнение о том, что первое предложение и вариант A второго предложения имеют ряд недостатков. Один из недостатков заключается в том, что оба предложения могут нарушить сложившуюся или складывающуюся практику путем установления завышенных стандартов. Было отмечено, что на практике во многих случаях окажется невозможным соблюсти требования о том, чтобы намерение включить информацию путем ссылки было прямо выраженным или ясно подразумевалось и чтобы существовали разумные возможности доступа к такой информации. Был приведен пример включения путем ссылки основной чартер-партии в коносамент, выданный в соответствии с субчартер-партией; как отмечалось, такая практика была бы затруднена в случае необходимости соблюдения требований о том, чтобы намерение включить информацию путем ссылки было прямо выраженным или ясно подразумевалось и чтобы существовали разумные возможности доступа к такой информации. Другой недостаток состоит в том, что указанные положения могут непреднамеренно противоречить императивным нормам права и приводить к возникновению несправедливых результатов. В этой связи было отмечено, что помимо двух условий, изложенных в первом предложении и в варианте A второго предложения, следует включить третий элемент, предусматривающий, что включение путем ссылки зависит от согласия сторон. В частности, было отмечено, что в случае открытого ЭДИ согласие сторон абсолютно необходимо.

22. В ответ было заявлено, что пункт 5 первого предложения и вторая фраза варианта A второго предложения как раз и призваны устранить такую озабоченность и обеспечить, чтобы положение о включении путем ссылки не вступало в противоречие со сложившейся практикой или императивными нормами внутригосударственного права. В то же время было высказано мнение о том, что эти положения могут вызвать сложности толкования. Было указано, что вариант B не имеет этого недостатка, поскольку в нем лишь излагается общий принцип недискриминации, закрепленный в статье 5 Типового закона. Было высказано общее мнение о том, что согласно варианту B включение путем ссылки будет действительным только в той мере, в которой оно допускается законом. Исходя из этого Рабочая группа пришла к выводу о предпочтительности варианта B.

23. В редакционном отношении было предложено привести вариант B в соответствие с формулировками статьи 5 Типового закона и в этих целях сослаться не только на юридическую силу, но и на действительность и исковую силу. Что касается конкретного места, в которое следует поместить положение о включении путем ссылки, то было предложено, учитывая тот факт, что данный вопрос связан с электронной торговлей в целом, а не только с подписями в цифровой форме, включить его в Типовой закон в качестве новой статьи 5 бис. В целях оказания помощи лицам, использующим Типовой закон, и законодателям в толковании положения о включении путем ссылки было также предложено включить в Руководство по принятию Типового закона справочную и пояснительную информацию,

касающуюся положения о включении путем ссылки. Было предложено отразить в Руководстве факторы, на основании которых государства, возможно, пожелают принять расширенный вариант предложения о включении путем ссылки. Такие факторы могут быть сформулированы на основе текста первого предложения и варианта A второго предложения. Это предложение было сочтено в целом приемлемым. В то же время было высказано опасение, что подобный подход может оказаться несоответствующим подходу, использованному в статье 5 Типового закона. Была высказана точка зрения, заключавшаяся в том, что вышеупомянутые факторы не следует излагать в качестве вариантов, альтернативных положениям Типового закона. По общему мнению, при подготовке раздела Руководства по принятию, касающегося включения путем ссылки, внимание следует уделить тому, чтобы избежать непреднамеренного создания впечатления о том, что ограничения, касающиеся включения путем ссылки, должны быть внесены в отношении электронной торговли в дополнение к ограничениям, которые уже могут применяться в рамках торговли на основе бумажных документов.

24. После обсуждения Рабочая группа приняла вариант B, постановила представить его Комиссии для рассмотрения и возможного включения в качестве статьи 5 бис в Типовой закон и просила Секретариат подготовить пояснительную записку для добавления в Руководство по принятию Типового закона.

III. РАССМОТРЕНИЕ ПРОЕКТА ЕДИНООБРАЗНЫХ ПРАВИЛ О ПОДПИСЯХ В ЭЛЕКТРОННОЙ ФОРМЕ

РАЗДЕЛ I. СФЕРА ПРИМЕНЕНИЯ И ОБЩИЕ ПОЛОЖЕНИЯ

25. Рабочая группа пришла к общему мнению о том, что взаимосвязь между единообразными правилами и Типовым законом (в особенности, что касается вопроса о том, следует ли принять единообразные правила о подписях в цифровой форме в качестве отдельного юридического документа или же их следует включить в расширенный вариант Типового закона) потребуется прояснить на более позднем этапе. Хотя было достигнуто согласие с тем, что на нынешнем этапе какого-либо конкретного решения принято быть не может, Рабочая группа подтвердила свою рабочую гипотезу, заключающуюся в том, что единообразные правила должны быть подготовлены в качестве проекта законодательных положений, должны согласовываться с положениями Типового закона в целом и должны включать те или иные положения, аналогичные статьям 1 (Сфера применения), 2(a), (c) и (d) (Определения терминов "сообщение данных", "составитель" и "адресат"), 3 (Толкование) и 7 (Подпись) Типового закона.

26. Что касается сферы применения единообразных правил, то было высказано мнение о том, что ее следует ограничить подписями в цифровой форме и исключить другие способы удостоверения подлинности. В ответ было отмечено, что в связи с предварительным выводом о том, что подготовка проекта единообразных правил о подписях в цифровой форме практически осуществима, Рабочая группа на своей предыдущей сессии также согласилась с тем, что, наряду с подписями в цифровой форме и сертификационными органами, в рамках работы в области электронной торговли, возможно, также потребуется рассмотреть вопросы технических альтернатив криптографии публичных ключей (A/CN.9/437, пункты 156-157). Было также напомнено о том, что на тридцатой сессии Комиссии было сочтено, что, хотя Рабочая группа может надлежащим образом сосредоточить свое внимание на вопросах подписей в цифровой форме с учетом предполагаемой ведущей роли криптографии публичных ключей в зарождающейся практике электронной торговли, единообразные правила должны соответствовать нейтральному с точки зрения носителей информации подходу, который взят за основу в Типовом законе (см. пункт 4 выше). После обсуждения Рабочая группа подтвердила свое решение о том, что, хотя она будет уделять первоочередное внимание подготовке специальных положений, касающихся способов подписания в цифровой форме, ей также следует выделить из этих специальных положений те правила, которые имеют более общее применение, с тем, чтобы учесть альтернативные способы удостоверения подлинности.

РАЗДЕЛ II. ЭЛЕКТРОННЫЕ ПОДПИСИ

Часть I. Защищенные электронные подписи

Статья 1. Определения

27. Рабочая группа рассмотрела следующий текст проекта статьи 1:

"Для целей настоящих Правил:

a) "Подпись" означает любой символ или любые виды процедур обеспечения защиты, используемые или принятые каким-либо лицом [или от имени какого-либо лица] с целью идентификации этого лица и указания на то, что это лицо согласно с информацией, к которой данная подпись прилагается;

b) "Электронная подпись" означает [подпись] [данные], исполненные в электронной форме и внесенные в текст либо приложенные к тексту, либо ассоциируемые с текстом сообщения [и используемые каким-либо лицом [или от имени какого-либо лица] с целью идентификации этого лица и указания на то, что это лицо согласно с информацией, содержащейся в сообщении данных] [и используемые с целью удовлетворения условиям [статьи 7 Типового закона ЮНСИТРАЛ об электронной торговле]];

c) "Защищенная электронная подпись" означает электронную подпись, которая

i) представляет собой подпись в цифровой форме в значении статьи 4 и удовлетворяет требованиям, предусмотренным статьей 5; или

ii) на время ее исполнения может быть каким-либо иным образом удостоверена как подпись соответствующего конкретного лица посредством процедуры обеспечения защиты, а именно: связана исключительно с использующим ее лицом; дает возможность быстрой, объективной и автоматизированной идентификации этого лица; исполнена таким образом или с применением таких средств, которые подконтрольны лишь использующему ее лицу; и связана с сообщением данных, к которому она относится, таким образом, что изменение сообщения делает данную электронную подпись недействительной; или

iii) [во взаимоотношениях сторон, причастных — в ходе своей обычной работы — к созданию, отправлению, получению, хранению или обработке сообщений данных каким-либо иным способом] является разумной с коммерческой точки зрения в обстоятельствах, оговоренных заранее, и должным образом применяется сторонами".

Общие замечания

28. Было указано, что положения, содержащиеся в проекте статьи 1, не только являются определениями, но также и предназначены для того, чтобы служить средством, которое позволит установить сферу действия единообразных правил. Хотя было отмечено, что такой же редакционный подход был использован в контексте Типового закона, было высказано общее мнение о том, что Рабочей группе, возможно, потребуется вернуться к рассмотрению проекта статьи 1 в ходе обсуждения вопроса о сфере применения единообразных правил.

Подпункт (a)

29. Широкую поддержку получило мнение о том, что подпункт (a) следует исключить. Хотя включение в единообразные правила определения понятия "подпись" на основе статьи 7 Типового закона может послужить полезным ориентиром для тех стран, в которых в настоящее время отсутствует определение

"подписи", было указано, что для целей единообразных правил такое определение не является необходимым. Один из доводов, приведенных в пользу исключения этого определения, состоял в том, что включение всеобъемлющего определения "подписи" может нанести ущерб приемлемости документа в тех странах, в которых положение, содержащееся в подпункте (a), может вступить в коллизию с уже имеющимися определениями.

Подпункт (b)

30. Широкую поддержку получило мнение о том, что формулировка подпункта (b) должна зеркально воспроизводить текст статьи 7 Типового закона. Этот результат может быть достигнут либо путем воспроизведения этой статьи полностью в подпункте (b), либо с помощью ссылки на "условия, установленные в статье 7 Типового закона". После обсуждения Рабочая группа отдала предпочтение последней формулировке. В редакционном плане было достигнуто общее согласие с тем, что вместо слова "подпись" следует использовать слово "данные".

Подпункт (c): общие замечания

31. Было выражено мнение, что определение электронной подписи в качестве "защищенной" ("secure") может быть неуместным. Вопрос о том, является ли тот или иной способ "надежным" ("secure"), представляет собой не вопрос определения, а вопрос факта, который должен быть установлен с учетом обстоятельств, при которых применяется этот способ. Критические замечания в отношении использования слова "надежный" ("secure") были высказаны также на том основании, что оно приносит субъективный критерий и подразумевает, что подписи, не подпадающие под эту категорию, уже по своей сути являются ненадежными. В ответ было указано, что хотя ссылку на "защищенную" ("secure") подпись, возможно, потребуется заменить более удачной формулировкой, этот термин используется в единообразных правилах только как средство выделения категории электронных подписей такого качества, что за ними могут быть признаны специальные правовые последствия. Что касается вопроса о том, может ли использование слова "secure" устанавливать субъективный критерий, то было указано, что способы удостоверения подлинности разрабатываются отнюдь не в вакууме. Для оценки степени надежности любого конкретного способа могут быть применены стандарты, установленные либо на основании принятых в порядке регулирования правил, либо на основании добровольной, разработанной в соответствующем секторе практики. После обсуждения Рабочая группа решила продолжить свою работу на основе той предпосылки, что для урегулирования различных методов, за которыми единообразные правила будут признавать определенные правовые последствия, будет использована соответствующая категория (для описания которой в предварительном порядке будет использоваться термин "защищенный" ("secure")).

32. Было высказано мнение о том, что было бы неуместно предусматривать такой порядок, при котором одни и те же правовые последствия будут устанавливаться для использования самых разнообразных способов удостоверения подлинности - от, как это было указано, надежных по своей сути (например, электронных подписей) до тех, которые по своей сути являются ненадежными (например, некоторые методы удостоверения подлинности, которые могут быть согласованы сторонами). В ответ было указано, что подпункт (c) как раз и направлен на создание такой категории, в рамках которой наиболее надежные подписи в цифровой форме могут быть приравнены к использованию других способов, при условии, что такие способы удовлетворяют жесткому стандарту, устанавливаемому в подпункте (c)(ii). Что касается подпункта (c)(iii), то может быть рассмотрен вопрос о его выделении в отдельное положение, касающееся автономии сторон. Было принято решение о том, что обсуждение определений, возможно, потребуется возобновить после рассмотрения положений, касающихся правовых последствий объектов этих определений.

Подпункт (c)(i)

33. Содержание подпункта (c)(i) было сочтено в целом приемлемым. В то же время было высказано мнение, что требования проекта статьи 5, на которые дается ссылка в подпункте c(i), недостаточно обеспечивают качество подписей в цифровой форме как защищенных электронных подписей. Было высказано предположение о том, что к рассмотрению этого вопроса, возможно, потребуется вернуться в контексте обсуждения проекта статьи 5.

Подпункт (c)(ii)

34. Была выражена обеспокоенность в связи с тем, что предусматриваемое согласно подпункту (c)(ii) бремя доказывания является настолько тяжелым, что презумпции, устанавливаемые в статье 2(1), будут практически лишаться смысла в случае, когда используются нецифровые электронные подписи. В ответ было указано, что подпункт (c)(ii) и проект статьи 2 преследуют различные цели. В то же время было достигнуто общее согласие с тем, что взаимосвязь между подпунктом (c)(ii) и проектом статьи 2, возможно, потребуется прояснить в пересмотренном проекте единообразных правил, который должен быть подготовлен Секретариатом.

35. В целом было сочтено, что содержание подпункта (c)(ii) является важным для того, чтобы гарантировать нейтральность единообразных правил с точки зрения носителей информации. Было высказано мнение о том, что, поскольку цель подпункта (c)(ii) состоит в определении некоторых критериев, которым должен удовлетворять тот или иной конкретный способ для того, чтобы обусловить применимость презумпций, устанавливаемых в проекте статьи 1, вопрос о том, был ли использован тот или иной конкретный способ с намерением поставить подпись, является неуместным. Соответственно, было предложено исключить слова "может быть каким-либо иным образом удостоверена как подпись соответствующего конкретного лица".

36. Дополнительные предложения были высказаны относительно конкретной формулировки подпункта (c)(ii). Одно из них состояло в том, что следует исключить слова "быстрой" и "автоматизированной". Было указано, что "быстрая" и "автоматизированная" идентификация лица отнюдь не является фактором, неотъемлемо присущим использованию большинства способов удостоверения подлинности (включая некоторые способы подписания в цифровой форме), и не имеет явно выраженной связи с надежностью процедуры удостоверения подлинности и с неприкосновенностью данных, подписанных в электронной форме. Другое предложение состояло в том, чтобы дополнить слова "посредством процедуры обеспечения защиты" словами "или комбинации процедур обеспечения защиты". После обсуждения эти предложения были приняты Рабочей группой.

Подпункт (c)(iii)

37. Было предложено исключить подпункт (c)(iii). Было указано, что предоставление статуса "защищенной электронной подписи" любой процедуре, которая может быть согласована сторонами, вызовет опасность того, что для создания правовых последствий могут быть применены любые процедуры, не обеспечивающие достаточную надежность. В этой связи было высказано мнение, что в настоящее время единственным "надежным" ("secure") способом удостоверения подлинности является подпись в цифровой форме. В ответ было отмечено, что - исходя из принципа свободы договора - должна быть признана свобода сторон договариваться о том, что в отношениях между собой они будут полагаться на способ удостоверения подлинности, который является менее надежным, чем тот вид электронной подписи, который описан в подпункте (c)(ii), и что при использовании этого способа удостоверения подлинности они будут признавать презумпции, устанавливаемые в проекте статьи 2. Было также отмечено, что ссылка на то, что способ подписания должен быть "разумным с коммерческой точки зрения", предназначена для того, чтобы служить защитительной оговоркой против неограниченного признания - на основании принципа автономии сторон, -возможно, ненадежных способов удостоверения подлинности. В то же время были высказаны сомнения относительно того, что для такой защитительной оговорки может быть использована концепция "коммерческой разумности". В ряде стран уже тот факт, что "коммерческие" стороны согласовали ту или иную процедуру, будет достаточным для того, чтобы такая процедура была признана "коммерчески разумной". В редакционном плане был поднят вопрос о возможном несоответствии между словами "коммерчески разумный" и формулировкой, использованной в статье 7 Типового закона. Хотя было напомнено о том, что слова "commercially reasonable" ("коммерчески обоснованный") были использованы в статье 5 Типового закона ЮНСИТРАЛ о международных кредитовых переводах, Рабочая группа сочла, что для того, чтобы избежать изложенного выше толкования, формулировку, возможно, потребуется изменить. Было высказано предположение о

том, что в подпункт (c)(iii) следует, возможно, включить ссылку на прямо оговоренное сторонами положение о том, что согласованный способ будет влечь за собой те последствия, которые признаются согласно проекту статьи 2 за защищенной электронной подписью. Было также предложено сохранить в подпункте (c)(iii) слова "во взаимоотношениях сторон" без квадратных скобок.

38. Был задан вопрос о том, могут ли стороны использовать подпункт (c)(iii) для того, чтобы обойти императивные нормы, касающиеся формы некоторых юридических актов. Было указано, что такое толкование будет неприемлемым с учетом того факта, что в условиях применения бумажных документов такой свободы договора не существует. Хотя в целом было достигнуто согласие с тем, что согласно закону ряда стран отход от некоторых императивных требований к форме на основании частного соглашения не допускается, такие императивные требования к форме обычно применяются лишь к весьма узкой категории сделок, и этот вопрос, по всей вероятности, может быть урегулирован с помощью прямо выраженного исключения, касающегося сферы действия общего положения по вопросу об автономии сторон.

39. В центре внимания обсуждения стоял вопрос о том, каким образом в единообразных правилах будет регулироваться принцип автономии сторон. Было напомнено о том, что одной ссылки на статью 4 (Изменение по договоренности) Типового закона будет, возможно, недостаточно для удовлетворительного решения этого вопроса с учетом того факта, что в статье 4 проводится разграничение между теми положениями Типового закона, которые могут быть свободно изменены на основании договора, и теми положениями, которые должны рассматриваться в качестве императивных, если только изменение по договоренности не допускается правом, применимым за пределами Типового закона. Что касается электронных подписей, то практическая важность "закрытых" сетей обуславливает необходимость в широком признании автономии сторон. В то же время, возможно, потребуется принять во внимание и основывающиеся на публичном порядке ограничения свободы договора, включая законы, направленные на защиту потребителей от уловок, связанных с договорами присоединения. Было предложено включить в единообразные правила положение, аналогичное статье 4(1) Типового закона и устанавливающее, что, если иное не предусмотрено единообразными правилами или другим применимым законом, за электронными подписями и сертификатами, которые были выданы или получены или на которые стороны сделки полагаются в соответствии с согласованными ими процедурами, будут признаваться последствия, указанные в соглашении сторон. Кроме того, Рабочей группе было предложено рассмотреть вопрос о выработке правила толкования, предусматривающего, что при определении того, является ли сертификат, электронная подпись или сообщение данных, проверенное со ссылкой на сертификат, достаточно надежными для той или иной конкретной цели, во внимание принимались все соответствующие соглашения, в которых участвовали стороны, любая установившаяся в их отношениях практика и любой применимый торговый обычай.

40. В качестве альтернативы на рассмотрение Рабочей группы было внесено предложение о следующей новой статье:

> "1) Если законодательство требует наличие подписи лица, это требование считается выполненным с помощью электронной подписи, если
>
> a) использование этой электронной подписи было согласовано сторонами сделки или
>
> b) эта электронная подпись представляла собой способ, являющийся как надежным, так и соответствующим цели, для которой электронная подпись была использована.
>
> 2) При определении того, является ли электронная подпись достаточно надежной для какой-либо конкретной цели, принимаются во внимание любая практика в отношениях между сторонами и любые соответствующие торговые обычаи".

41. Обсуждение было продолжено на основе предложенной новой статьи. Было указано, что цель предложенного текста состоит в том, чтобы развить и расширить подход, использованный в статье 7 Типового закона. В частности, было указано следующее: цель пункта 1(a) состоит в том, чтобы дать сторонам возможность определить тот вид электронной подписи, который они желают использовать в своих деловых операциях; пункт 1(a) построен на основе статьи 7(1)(b) Типового закона; и в пункте 2 предпринимается попытка разъяснить пункт 1(b). Было высказано мнение о том, что если предлагаемая новая статья будет включена в единообразные правила, то необходимость в пункте 2 проекта статьи 2 единообразных правил отпадет и его можно будет исключить.

42. Против этого предложения были высказаны возражения, в целом, на том основании, что оно очевидно противоречит статье 7 Типового закона по ряду аспектов, включая следующие: оно не включает элементов идентификации и согласия, и, таким образом, подписью называется нечто, что по смыслу Типового закона подписью не является; оно разрешает сторонам отходить от императивных норм, касающихся подписей, и, таким образом, устанавливает преимущественный порядок по отношению к нормам, в силу которых в соответствии со статьей 7(2) Типового закона могут создаваться обязательства в отношении подписи или устанавливаться правовые последствия в случае ее отсутствия; и оно не включает положения, аналогичного статье 7(3) Типового закона, которая позволяет государствам исключить применение статьи 7 в ряде случаев (например, применительно к оборотным документам).

43. Широкое распространение получило мнение о том, что основной недостаток предлагаемой новой статьи заключается в том факте, что в отличие от статьи 7 Типового закона и вразрез с нормами, применимыми в условиях использования бумажных документов, она позволяет сторонам отступать от императивных норм права. Таким образом, предлагаемая новая статья может непреднамеренно привести к подрыву Типового закона и национального законодательства, регулирующего подписи, и ненадлежащим образом затронуть права третьих сторон. Кроме того, широкую поддержку получило мнение о том, что в предлагаемой новой статье без какой-либо необходимости повторяются элементы, содержащиеся в проекте статьи 1 единообразных правил.

44. С тем чтобы привести предложенную новую статью в соответствие со статьей 7 Типового закона и устранить вышеупомянутые недостатки, был внесен ряд предложений. Одно из них состояло в том, чтобы включить ссылку на основные характеристики подписи, а именно на функции, связанные с идентификацией лица и согласием с содержанием сообщения, путем включения в конце вводных слов в пункте 1 предложенной новой статьи формулировки примерно следующего содержания: "она является подписью этого лица и". Другое предложение заключалось в том, чтобы признать преимущественную силу применимого права путем включения в начало пункта 1(a) примерно следующей формулировки: "с учетом соответствующего законодательства". Еще одно предложение заключалось в том, чтобы в соответствии со статьей 7 Типового закона между подпунктами (a) и (b) был поставлен союз "и", а не "или". Другое предложение состояло в том, что учет практики сторон и торговых обычаев, которые предусматриваются в пункте 2 новой статьи, должен допускаться, а не признаваться обязательным и что этого результата можно достичь с помощью замены слова "принимаются" словами "могут приниматься". Еще одно предложение состояло в том, чтобы включить в предлагаемую новую статью основные элементы статьи 7(2) и (3) Типового закона.

45. Широкое распространение получило мнение о том, что вместо изменения формулировки предложенной новой статьи Рабочей группе следует попытаться установить базовые принципы в вопросе о том, в каких масштабах автономия сторон должна признаваться в единообразным правилах. В целом было выражено согласие с тем, что, как правило, в единообразных правилах не следует ограничивать автономию сторон в том, что касается взаимоотношений между самими сторонами. Было также достигнуто согласие относительно того, что усилия Рабочей группы должны быть направлены на определение тех видов сделок (и - применительно к подписям в цифровой форме - тех видов сертификатов), которые будут предполагать высокий уровень надежности и которые, таким образом, могут быть обусловлены соблюдением императивных норм, содержащихся в действующем в ряде стран законодательстве. Что касается юридических требований к форме, которые могут ограничивать

автономию сторон, то широкую поддержку получило мнение о том, что можно провести полезное разграничение между теми требованиями к подписи, цель которых заключается в обеспечении доказательств (и которые могут быть поставлены в зависимость от автономии сторон), и теми требованиями к форме, которые предписываются для целей действительности (и которые, как правило, будут носить императивный характер).

46. После обсуждения Рабочая группа постановила предложить Секретариату подготовить пересмотренный проект статьи 1, с учетом вышеизложенных обсуждений и решений.

Статья 2. Презумпции

47. Рабочая группа рассмотрела следующий текст проекта статьи 2:

"1) В отношении сообщения данных, подлинность которого удостоверяется при помощи защищенной электронной подписи, исходят из опровержимой презумпции, что:

a) сообщение данных не было изменено с момента приложения к нему защищенной электронной подписи;

b) защищенная электронная подпись является подписью лица, к которому она относится; и

c) защищенная электронная подпись была приложена этим лицом с намерением подписать сообщение.

2) В отношении сообщения данных, подлинность которого удостоверяется при помощи электронной подписи, не являющейся защищенной, ничто в настоящих Правилах не затрагивает действующие юридические или доказательные нормы, относящиеся к бремени доказывания подлинности или целостности сообщения данных или электронной подписи.

3) Положения настоящей статьи не применяются к следующему: [...].

[4) Презумпции, содержащиеся в пункте 1, могут быть опровергнуты:

a) доказательствами того, что защитная процедура, примененная для проверки электронной подписи, не должна быть в целом признана как заслуживающая доверия в силу развития техники, использованной процедуры обеспечения защиты или по каким-либо иным причинам;

b) доказательствами того, что процедура обеспечения защиты, согласованная сторонами в соответствии со статьей 1(c)(iii), не была проведена заслуживающим доверия образом; или

c) доказательствами, связанными с фактами, о которых доверяющая сторона была осведомлена, что они могут свидетельствовать о неразумности проявления доверия к данной защитной процедуре. Коммерческая разумность процедуры обеспечения защиты, согласованной сторонами в соответствии со статьей 1(c)(iii), должна определяться с учетом целей процедуры и коммерческих обстоятельств на момент достижения сторонами согласия о принятии этой процедуры, включая характер сделки, опыт сторон, объем аналогичных сделок, заключенных одной или обеими сторонами, наличие альтернативных вариантов, предложенных соответствующей стороне, но отвергнутых ею, стоимость альтернативных процедур, а также характер процедур, обычно используемых в аналогичных видах сделок.]"

48. Хотя признано, что принцип нейтральности с точки зрения носителей информации должен быть отражен в единообразных правилах через признание тех правовых последствий, которые будут связаны с применением электронных подписей при использовании нецифровых методов, Рабочая группа постановила отложить обсуждение проекта статьи 2 до завершения рассмотрения оставших проектов статей единообразных правил.

Статья 3. Атрибуция

49. Рабочая группа рассмотрела следующий текст проекта статьи 3:

"1) Вариант A Согласно [статье 13 Типового закона ЮНСИТРАЛ об электронной торговле] составитель сообщения данных, на котором проставлена защищенная электронная подпись составителя, [связан содержанием] [считается лицом, подписавшим] сообщения таким же образом, как если бы это сообщение существовало в [собственноручно] подписанной форме в соответствии с законом, применимым к содержанию этого сообщения.

Вариант B Во взаимоотношениях держателя частного ключа с любой третей стороной, доверяющей подписи в цифровой форме, которая поддается [проверке] [удостоверению] с помощью соответствующего сертифицированного публичного ключа, такая подпись в цифровой форме [считается подписью данного держателя ключа] [удовлетворяет условиям, предусмотренным [статьей 7(1) Типового закона ЮНСИТРАЛ об электронной торговле]].

2) Пункт 1 не применяется, если:

a) [составитель] [держатель ключа] сможет доказать, что [защищенная электронная подпись] [частный ключ] использовалась(лся) без его разрешения и что [составитель] [держатель ключа] не имел возможности предотвратить такое использование в пределах разумной осмотрительности; или

b) доверяющая сторона узнала или должна была узнать, если бы она запросила информацию у [составителя] [сертификационного органа] или как-либо иначе проявила разумную осмотрительность, что данная [защищенная электронная] [в цифровой форме] подпись не является подписью [составителя] [держателя частного ключа]".

Общие замечания

50. Рабочая группа в первую очередь рассмотрела цели и сферу действия проекта статьи 3 и его взаимосвязь со статьями 7 и 13 Типового закона.

51. Относительно того, следует ли в этом проекте статьи урегулировать только вопрос об атрибуции защищенных электронных подписей (или подписей в цифровой форме) или же следует также рассмотреть вопрос об ответственности предполагаемого подписавшегося перед доверяющими сторонами, были высказаны различные мнения. Одна из точек зрения состояла в том, что проект статьи 3 должен быть направлен на увязывание подписи с предполагаемым подписавшимся и на обеспечение целостности сообщения данных. Другое мнение состояло в том, что основная цель проекта статьи 3 должна заключаться в создании стимула для использования подписей в цифровой форме за счет надлежащего распределения ответственности за убытки, причиненные доверяющей стороне в результате неспособности предполагаемого подписавшегося проявить разумную осмотрительность и не допустить несанкционированного использования его подписи (см. пункт 58 ниже). Возобладало мнение о том, что следует рассмотреть оба этих вопроса. В этом контексте было высказано предостережение, что попытка урегулировать вопросы ответственности может не соответствовать использованному в Типовом законе подходу, согласно которому договорные вопросы оставлены на урегулирование на основании иного применимого права за рамками Типового закона. В ответ было отмечено, что единообразные правила разрабатываются на основе несколько иного подхода, так как, в частности, в них уже регулируется вопрос об ответственности сертификационных органов. После обсуждения Рабочая группа решила рассмотреть возможность урегулирования обоих вопросов, возможно, в отдельных положениях (см. пункты 55 и 60 ниже).

52. Что касается сферы действия проекта статьи 3, то было высказано мнение о том, что ее следует ограничить подписями в цифровой форме и что следует соответствующим образом изменить место проекта статьи 3 в тексте единообразных правил. В поддержку этого мнения было указано, что подписи в цифровой форме известны и применяются настолько широко, что они заслуживают того, чтобы быть рассмотренными в первоочередном порядке. Кроме того, было отмечено, что вопрос об атрибуции подписей в цифровой форме является достаточно важным для того, чтобы быть рассмотренным отдельно от вопроса об атрибуции других видов электронных подписей. Еще одна точка зрения заключалась в том, что правила, устанавливаемые в проекте статьи 3, должны применяться как к подписям в цифровой форме, так и к другим электронным подписям. Возобладало мнение о том, что - в той мере, в которой это возможно, - вопросы, рассматриваемые в проекте статьи 3, должны быть урегулированы при использовании нейтрального с точки зрения носителей информации подхода с тем, чтобы охватить широкий диапазон электронных подписей.

53. Что касается взаимосвязи между проектом статьи 3 и статьями 7 и 13 Типового закона, то было отмечено, что статья 7 касается требований к подписи, а статья 13 - атрибуции сообщений. Была выражена обеспокоенность в связи с тем, что в проекте статьи 3, возможно, просто воспроизводятся положения статьи 13 Типового закона. В ответ было указано, что в проекте статьи 3 рассматривается атрибуция электронных подписей, отличающаяся от атрибуции сообщения данных, и предусматривается специальная защита предполагаемого подписавшегося в случаях, когда его подпись используется несанкционированно и предполагаемый подписавшийся, даже если бы он проявил разумную осмотрительность, не смог бы предотвратить такое несанкционированное использование.

Пункт 1

54. Поддержка была выражена как варианту A, так и варианту B. В поддержку варианта A было указано, что он основывается на подходе, являющимся нейтральным с точки зрения носителя информации, и, таким образом, учитывает различные виды технологий, используемые в международной торговле. В этой связи было отмечено, что необходимо также обеспечить нейтральный подход к вопросам о порядке применения той или иной конкретной технологии (например, подписи в цифровой форме с сертификатом или без него). Такой нейтральный подход с точки зрения вопросов применения может быть обеспечен, как это было указано, с помощью общего правила, предусматривающего, что получатель сообщения данных, который разумно доверяет защищенной электронной подписи, имеет право рассматривать это сообщение как сообщение предполагаемого подписавшегося (см. A/CN.9/WG.IV/WP.73, пункты 35-36). В поддержку варианта B было указано, что в этом варианте вполне обоснованно основное внимание уделяется подписям в цифровой форме, которые в отличие от других видов электронных подписей достаточно известны и широко используются.

55. В то же время в отношении обоих вариантов A и B были высказаны критические замечания в связи с тем, что в них неуместно смешиваются два различных вопроса: вопрос об атрибуции и вопрос об ответственности. Кроме того, ряд выступающих выразили обеспокоенность и высказали замечания в отношении обоих вариантов. Что касается варианта A, то было отмечено следующее: вступительная формулировка не является достаточно четкой; использование термина "составитель" является неуместным по целому ряду причин, включая тот факт, что лицо, подписывающее сообщение данных, необязательно является его составителем; формулировка "связан содержанием" относится к общему обязательственному праву, а не только к атрибуции электронных подписей предполагаемому подписавшемуся; и ссылка на применимый закон должна относиться к закону, применимому к сообщению данных в целом, а не только к его содержанию.

56. Что касается варианта B, то было отмечено следующее: с тем чтобы не нанести ущерба исключениям, содержащимся в других положениях единообразных правил, касающихся, например, скомпрометированных частных ключей, в начале варианта B следует добавить формулировку примерно следующего содержания: "с учетом положений статей..."; в соответствии с подходом, используемым в статье 13 Типового закона, следует дать ссылку на фактическую проверку того, было ли использование

цифровой подписи санкционировано, а не только на способность держателя частного ключа провести такую проверку; с тем чтобы избежать ситуации, когда может быть произведена атрибуция подписи в цифровой форме предполагаемому подписавшемуся, даже если он аннулировал сертификат, следует использовать формулировку примерно следующего содержания: "частный ключ, указанный в действительном сертификате"; никаких ссылок на статью 7 Типового закона включать не следует, поскольку эта статья касается требований к подписи, а не ее атрибуции.

Пункт 2

57. Хотя Рабочая группа согласилась с тем, что пункт 2 является в целом приемлемым, была выражена обеспокоенность тем, что использование термина "разумная осмотрительность" может привнести неопределенность. С тем чтобы устранить эту обеспокоенность, был внесен ряд предложений. Одно из них состояло в том, что атрибуция подписи предполагаемому подписавшемуся должна быть произведена в том случае, если он не сможет доказать, что использование подписи было несанкционированным. Другое предложение состояло в том, что подпись должна считаться подписью предполагаемого подписавшегося, если, кроме того, он не сможет доказать, что он был не в состоянии предотвратить несанкционированное использование, причем каких-либо ссылок на концепцию "разумной осмотрительности" делать не следует. Против обоих этих предложений были высказаны возражения на том основании, что они могут непреднамеренно повысить уровень ответственности предполагаемого подписавшегося.

Предложение о включении новой статьи 3

58. С тем чтобы снять вопросы, вызвавшие обеспокоенность в связи с проектом статьи 3, и исходя из той предпосылки, что вопрос об атрибуции защищенных электронных подписей достаточно урегулирован в проекте статьи 2 единообразных правил, было внесено предложение о том, что в центр внимания проекта статьи 3 следует поставить вопрос об ответственности предполагаемого подписавшегося и что, таким образом, статья 3 должна гласить примерно следующее:

> "1) В отношениях между держателем частного ключа и любым лицом, доверяющим подписи в цифровой форме, держатель не связан сообщением, если он не подписывал его.
>
> 2) Если держатель ключа не проявил разумной осмотрительности с тем, чтобы избежать такого положения, когда доверяющая сторона доверяет несанкционированно использованной подписи в цифровой форме, он несет ответственность за компенсацию доверяющей стороне за причиненный ей ущерб. Доверяющая сторона имеет право на такую компенсацию только в том случае, если она запросила информацию у сертификационного органа или иным образом проявила разумную осмотрительность с тем, чтобы установить, что подпись в цифровой форме не является подписью держателя".

59. Хотя Рабочая группа в целом согласилась с тем, что в предложенной редакции правомерно разграничиваются атрибуция подписи и ответственность (или материальная ответственность) за ущерб, причиненный несанкционированным использованием подписи, было отмечено, что она не позволяет достаточным образом урегулировать вопросы, вызывавшие обеспокоенность в связи с вариантами A и B. Кроме того, было указано, что бремя доказывания переносится на доверяющую сторону, которой необходимо показать, что она проявила разумную осмотрительность, с тем чтобы доказать, что подпись является подписью предполагаемого подписавшегося. Было выражено общее согласие с тем, что подход, нейтральный с точки зрения носителя информации, был бы более предпочтительным и что вопросы атрибуции и ответственности следует рассмотреть по отдельности.

60. В рамках такого подхода Рабочей группе было предложено рассмотреть альтернативную формулировку примерно следующего содержания:

"Атрибуция защищенной электронной подписи

В отношениях между предполагаемым подписавшим лицом и доверяющей стороной защищенная электронная подпись считается подписью предполагаемого подписавшего лица, если предполагаемое подписавшее лицо не сможет доказать, что защищенная электронная подпись была использована без разрешения.

Ответственность за защищенную электронную подпись

В том случае, если защищенная электронная подпись использовалась без разрешения и предполагаемое подписавшее лицо не проявило разумной осмотрительности для предупреждения использования такого сообщения адресатом, предполагаемое подписавшее лицо обязано возместить убытки для компенсации доверяющей стороне причиненного вреда, за исключением тех случаев, когда доверяющая сторона не запрашивала информации у соответствующей третьей стороны или когда она иным образом узнала или должна была узнать, что данная подпись не является подписью предполагаемого подписавшего лица".

61. После обсуждения Рабочая группа просила Секретариат отразить предложенную альтернативную формулировку в пересмотренном проекте единообразных правил для дальнейшего рассмотрения Рабочей группой на одной из будущих сессий. Ряд делегаций выразили обеспокоенность в связи с возможными противоречиями между предложенной формулировкой и положениями внутреннего права их стран, касающимися деликтов.

Часть II. Подписи в цифровой форме

Статья 4. Определение

62. Рабочая группа рассмотрела следующий текст проекта статьи 4:

"Для целей настоящих Правил,

Вариант А "подпись в цифровой форме" означает тип электронной подписи, состоящей в таком преобразовании сообщения данных с использованием резюмирующей функции сообщения и асимметрической криптосистемы, что любое лицо, располагающее первоначальным, не подвергшимся преобразованию, сообщением данных и публичным ключом подписавшегося может точно определить:

a) было ли такое преобразование осуществлено с использованием частного ключа подписавшегося, соответствующего его публичному ключу; и

b) было ли первоначальное сообщение данных изменено после произведенного преобразования.

Вариант В a) "подпись в цифровой форме" представляет собой числовую величину, которая добавлена к сообщению данных и которая при использовании известной математической процедуры, связанной с частным криптографическим ключом составителя, дает возможность определить, что эта числовая величина была получена с помощью частного ключа составителя;

b) математические процедуры, используемые для подготовки подписей в цифровой форме в соответствии с настоящими Правилами, основываются на кодировании с помощью публичного ключа. При применении к какому-либо сообщению данных эти

математические процедуры производят преобразование сообщения таким образом, что лицо, располагающее первоначальным сообщением и публичным ключом составителя, может точно определить:

i) было ли такое преобразование осуществлено с использованием частного ключа, который соответствует публичному ключу составителя; и

ii) было ли первоначальное сообщение изменено после произведенного преобразования".

63. Хотя определенная поддержка была высказана как в отношении варианта A, так и в отношении варианта B, ни один из них не был принят Рабочей группой.

64. В пользу варианта A было указано, что, поскольку основное внимание в этом варианте уделяется созданию подписи в цифровой форме без ссылки на ту или иную конкретную технологию, этот вариант является достаточно гибким для охвата различных видов подписей в цифровой форме. Тем не менее было выражено беспокойство в связи с тем, что вариант A не учитывает различных методов, при помощи которых может использоваться инфраструктура для применения публичных ключей (например, с использованием или без использования резюмирующей функции сообщения), а также различные функции, которые могут выполняться благодаря использованию подписи в цифровой форме (например, функция идентификации подписавшего лица ("защищенные подписи"), функция установления целостности сообщения данных ("защищенные записи") или же определенное сочетание этих двух функций). В контексте этого обсуждения для обеспечения трансграничного признания различных видов подписей и сертификатов в цифровой форме Рабочей группе было предложено рассмотреть возможность подготовки конвенции вместо добавления к Типовому закону (см. пункт 212 ниже).

65. В ответ на упомянутое выше беспокойство было указано, что включение элементов идентификации подписавшего лица и проверки целостности сообщения в определение термина "подпись в цифровой форме" является общепринятым подходом. Кроме того, было указано, что такой подход, цель которого состоит в выявлении функционального эквивалента подписи в контексте бумажных документов, соответствует подходу, применяемому в Типовом законе. Указывалось также, что попытка охватить все виды подписей в цифровой форме является чрезмерно амбициозной задачей и будет препятствовать достижению прогресса в одной из областей, в которой необходимо срочно обеспечить регулирование, с тем чтобы избежать дисгармонии права в результате применения различных подходов в национальном законодательстве. В этой связи было отмечено, что в соответствии с вариантом A, согласно которому подпись в цифровой форме определяется в качестве типа электронной подписи, этот термин будет относиться только к различным видами применения криптографии публичных ключей, которые предназначены служить функциональным эквивалентом подписи в контексте использования бумажных документов, в то время как вариант B является достаточно широким для того, чтобы охватить все виды технологии цифровых подписей, включая те из них, которые не предназначены служить функциональными эквивалентами подписей.

66. В пользу варианта B было указано, что он обеспечивает большую определенность, поскольку он состоит из более технических формулировок и содержит конкретную ссылку на кодирование с помощью публичного ключа, что, как отмечалось, является широко распространенной технологией. В то же время было выражено беспокойство в связи с тем, что вариант B носит чрезмерно ограничительный характер, поскольку в нем содержится ссылка на определенную математическую процедуру для создания подписи в цифровой форме, что, возможно, не позволяет учесть потенциальные технические изменения, в результате которых принятая в настоящее время процедура устареет. Было высказано предложение сделать в этом проекте положения ссылку на "наиболее совершенную математическую процедуру".

67. Как в отношении варианта A, так и в отношении варианта B были высказаны возражения на том основании, что "подпись в цифровой форме" необоснованно определяется в них с помощью ссылки на

"преобразование сообщения данных". В порядке разъяснения было указано, что в результате обработки сообщения с использованием определенного алгоритма изменяется не сообщение в целом, а только его представление в цифровой форме. Для решения этой проблемы была предложена формулировка примерно следующего содержания:

> "Подпись в цифровой форме представляет собой такое криптографическое преобразование (с использованием асимметрического криптографического метода) цифровой формы сообщения данных, что любое лицо, располагающее сообщением данных и надлежащим публичным ключом, может определить:
>
> a) что такое преобразование осуществлено с использованием частного ключа, соответствующего надлежащему публичному ключу; и
>
> b) что сообщение данных не было изменено после криптографического преобразования".

68. В поддержку предложенного текста было указано, что такой текст, не содержащий ссылки на частный ключ подписавшего лица, позволяет учесть необходимость обеспечения охвата в единообразных правилах подписей в цифровой форме, используемых для различных целей, а не только для идентификации подписавшего лица. Было также указано, что предлагаемый текст, не содержащий ссылки на резюмирующую функцию сообщения, позволит также охватить подписи в цифровой форме, созданные с помощью использования другой процедуры.

69. В ходе обсуждения было высказано предложение о том, что Рабочей группе следует рассмотреть - исключительно в целях сопоставления - текст, который был принят в 1988 году Международной организацией по стандартизации (ИСО) и который гласит следующее: "Сообщение данных: прилагаемые данные или криптографическое преобразование единицы данных, которые позволяют получателю единицы данных подтвердить источник и целостность единицы данных, а также обеспечить защиту от подлога, например, получателем" (ISO 7498/2). Другое предложение состояло в том, чтобы включить определение ИСО в единообразные правила. Хотя было решено, что определение ИСО основано на техническом подходе, многие члены Рабочей группы выразили скептицизм в отношении того, что такое определение может оказаться приемлемым для целей единообразных правил.

70. После обсуждения Рабочая группа решила, что ей следует отложить принятие решения относительно определения термина "подпись в цифровой форме" до завершения рассмотрения существенных положений единообразных правил и принятия решения относительно сферы применения этих положений. Определение термина "подпись в цифровой форме" может, в частности, зависеть от того, будут ли единообразные правила охватывать только использование компьютерных методов, призванных обеспечить воспроизведение в условиях применения электронных средств тех функций, которые традиционно выполняются в международных торговых сделках с помощью использования выполненных от руки подписей, или же сфера применения единообразных правил будет распространяться на дополнительные виды использования "подписей в цифровой форме". Секретариату было предложено подготовить для дальнейшего рассмотрения данного вопроса на одной из будущих сессий альтернативные формулировки, основанные на вариантах A и B и на вышеизложенном предложении (см. пункт 67 выше) и учитывающие высказанные замечания.

Статья 5. Правовые последствия

71. Рабочая группа рассмотрела следующий текст проекта статьи 5:

> "1) В случаях, когда сообщение данных или какая-либо его часть подписываются с использованием подписи в цифровой форме, эта подпись считается, по отношению к данной части сообщения, защищенной электронной подписью, если:

a) подпись в цифровой форме проставлена в течение срока действия [имеющего юридическую силу] сертификата и проверена путем ссылки на публичный ключ, указанный в сертификате; и

b) сертификат считается устанавливающим четкую связь между публичным ключом и личностью соответствующего лица в силу того, что:

i) сертификат был выдан сертификационным органом, лицензированным [уполномоченным] ... [принимающее государство указывает орган или ведомство, компетентное лицензировать сертификационные органы и принимать постановления в отношении функционирования лицензированных сертификационных органов]; или

ii) сертификат был выдан каким-либо иным образом сертификационным органом в соответствии со стандартами, установленными ... [принимающее государство указывает орган или ведомство, компетентное устанавливать признанные стандарты функционирования лицензированных сертификационных органов].

2) В случаях, когда сообщение данных или какая-либо его часть подписываются с использованием подписи в цифровой форме, не удовлетворяющей требованиям, изложенным в пункте 1, подпись в цифровой форме считается, по отношению к данной части сообщения, защищенной электронной подписью, если имеются достаточные доказательства того, что данный сертификат устанавливает четкую связь между публичным ключом и личностью его держателя.

3) Положения настоящей статьи не применяются по отношению к следующему: [...]".

Общие замечания

72. Уже в начале обсуждения было высказано получившее широкую поддержку мнение о том, что Рабочей группе будет необходимо провести дальнейшее рассмотрение проекта статьи 5 по существу в свете решений, которые будут приняты относительно сферы действия единообразных правил. В частности, существует непосредственная связь между проектом статьи 5 и решением о том, будет ли в единообразных правилах использована концепция "защищенной электронной подписи". Правовые последствия, которые будут увязаны с использованием сертификатов в контексте подписей в цифровой форме, будут также зависеть от определения "сертификата" в соответствии с проектом статьи 8. Если единообразные правила будут регулировать только те случаи, когда подписи в цифровой форме используются для целей международных торговых сделок с намерением поставить подпись (т.е. идентифицировать подписавшего и установить связь между подписавшим и подписанной информацией), то может быть приемлемым такой подход, при котором функции сертификата будут ограничиваться установлением связи между парой ключей и личностью какого-либо лица. В подобном случае следует конкретно указать, что единообразные правила регулируют только вопросы особого вида сертификатов ("сертификаты личности"), что является важным, в связи, в частности, с тем, что в практике электронной торговли могут использоваться и другие виды сертификатов, например, в целях определения уровня полномочий того или иного лица ("сертификаты полномочий"). Было выражено мнение, что проект статьи 5 должен охватывать как сертификаты личности, так и сертификаты полномочий. В контексте обсуждения этого вопроса было предложено включить в проект статьи 5 ссылку на сертификат, используемый для проверки целостности информации, содержащейся в сообщении данных. В ответ было указано, что, хотя проверка целостности данных является важным результатом использования сертификата в контексте процесса подписания в цифровой форме, она не является характерным элементом собственно сертификата.

73. После обсуждения Рабочая группа постановила продолжить рассмотрение проекта статьи 5. В то же время было достигнуто общее согласие с тем, что обсуждение потребуется возобновить после того, как Рабочая группа завершит рассмотрение материально-правовых положений единообразных правил.

Название

74. Широкую поддержку получило мнение о том, что название проекта статьи 5 недостаточно полно отражает содержание этой статьи и может быть неправильно истолковано. Было принято решение о том, чтобы сформулировать название примерно следующим образом: "Подписи в цифровой форме, подтвержденные сертификатами".

Пункт 1

Вступительная формулировка

75. Было поддержано мнение о том, что ссылка на концепцию "защищенной подписи в цифровой форме" в проекте статьи 5 не является необходимой и что ее следует заменить ссылкой на условия, устанавливаемые в статье 7 Типового закона. В ответ было указано, что такая ссылка на статью 7 Типового закона может непреднамеренно ограничить сферу действия проекта статьи 5, поскольку будет предполагаться существование юридических требований к подписи, которые будет необходимо удовлетворить в условиях применения электронных сообщений. Проект статьи 5 преследует более широкую цель: он прямо направлен на то, чтобы создать определенность в отношении юридических последствий подписей в цифровой форме при условии соблюдения некоторых технических стандартов, независимо от того, существуют ли какие-либо конкретные требования к подписи.

76. После обсуждения Рабочая группа постановила сохранить ссылки на "защищенную электронную подпись" и на условия, устанавливаемые в статье 7 Типового закона, в качестве альтернативных формулировок для рассмотрения Рабочей группой на одной из будущих сессий. Вступительная формулировка проекта статьи 5 должна гласить примерно следующее: "В отношении всего сообщения данных или какой-либо его части в случаях, когда составитель идентифицирован подписью в цифровой форме, подпись в цифровой форме [является защищенной цифровой подписью] [удовлетворяет условиям, установленным в статье 7 Типового закона ЮНСИТРАЛ об электронной торговле], если:".

Подпункт (a)

77. Содержание подпункта (a) было сочтено в целом приемлемым. С тем чтобы более точно отразить концепцию необходимой надежности процесса подписания в цифровой форме, было решено включить слово "надежно", которое будет относиться как к проставлению подписи в цифровой форме, так и к ее проверке путем использования публичного ключа, указанного в сертификате. Было также решено сохранить в этом проекте положения в квадратных скобках ссылку на юридическую силу сертификата.

Подпункт (b)

78. Что касается подпункта (b)(i), то широкую поддержку получило мнение о том, что в положении, касающемся случая, когда государства для урегулирования вопросов, связанных с инфраструктурой публичных ключей, примут подход, основывающийся на регулировании, предпочтительно использовать не слово "аккредитованный", а слова "имеющий лицензию" или "зарегистрированный". Что касается подпункта (b)(ii), то было высказано мнение о том, что это положение следует исключить, поскольку сферу действия проекта статьи 5 следует ограничить использованием сертификатов, выданных сертификационными органами, получившими лицензию от государства, принимающего единообразные правила. Возобладало, однако, мнение о том, что ссылка должна быть сделана на отраслевые стандарты и на механизмы, которые могут быть разработаны на практике для обеспечения надежности таких стандартов. В целом было сочтено, что такая ссылка является необходимой для отражения "двойного" подхода к подписям в цифровой форме и инфраструктурам публичных ключей, принятого Рабочей группой на ее предыдущей сессии (см. A/CN.9/437, пункт 69). Согласно этому подходу наравне с правительственным регулированием будут признаваться отраслевые стандарты. Было указано, что в ряде стран правительственные органы, возможно, и не пожелают участвовать в создании стандартов защиты

для подписей в цифровой форме. В этой связи было отмечено, что в проекте статьи 5 следует не только упомянуть о "стандартах защиты", но и более широко охватить различные виды стандартов, которые могут быть разработаны участниками практической деятельности.

79. Что касается ссылки на признанные отраслевые стандарты, то было предложено использовать формулировку статьи 9(2) Конвенции Организации Объединенных Наций о договорах международной купли-продажи товаров: "обычай, о котором стороны знали или должны были знать и который в международной торговле широко известен и постоянно соблюдается сторонами в договорах данного рода в соответствующей области торговли". В то же время согласно широко распространенному мнению более уместной была бы ссылка на "коммерчески обоснованные и международно признанные стандарты".

80. С учетом вышеупомянутого обсуждения для целей дальнейшего рассмотрения было решено сформулировать подпункт (b) примерно следующим образом:

> "b) сертификат устанавливает связь между публичным ключом и личностью соответствующего лица в силу того факта, что:
>
> i) сертификат был выдан сертификационным органом, получившим лицензию от... [принимающее государство указывает орган или ведомство, компетентное выдавать лицензии сертификационным органам и принимать правила, регулирующие функционирование получивших лицензию сертификационных органов]; или
>
> ii) сертификат был выдан сертификационным органом, аккредитованным ответственным аккредитационным органом, применяющим коммерчески обоснованные и международно признанные стандарты, относящиеся к вопросам надежности технологии, практики и других соответствующих характеристик функционирования сертификационного органа. Неисчерпывающий перечень таких аккредитационных органов или стандартов, удовлетворяющих условиям настоящего пункта, может быть опубликован ... [принимающее государство указывает орган или ведомство, компетентное устанавливать признанные стандарты функционирования получивших лицензию сертификационных органов]; или
>
> iii) сертификат был иным образом выдан в соответствии с коммерчески обоснованными и международно признанными стандартами".

Пункт 2

81. В связи с пунктом 2 был отмечен ряд моментов, вызвавших обеспокоенность. Один из них состоял в том, что пункт 2 является, возможно, излишним, если учитывать проект статьи 2, в котором устанавливаются юридические презумпции, связанные со статусом "защищенной электронной подписи". В ответ было отмечено, что пункт 2 является необходимым для установления связи между подписью в цифровой форме, которая может быть признана (например, решением суда) в качестве связывающей публичный ключ и держателя, хотя она формально и не удовлетворяет требованиям, установленным в пункте 1, и другими положениями единообразных правил (например, пересмотренным проектом статьи 3 в отношении вопроса об "ответственности за защищенную электронную подпись"). В этом контексте было высказано мнение о том, что в проект статьи 3, возможно, потребуется включить слова "независимо от положений статьи 5".

82. Еще один момент, вызвавший обеспокоенность, заключался в том, что в пункте 2 устанавливается чрезвычайно низкий стандарт для признания подписей в цифровой форме, которые в иных отношениях не удовлетворяют требованиям, установленным в пункте 1. Пункт 2 в его нынешней редакции может привести к тому, что статус "защищенных" будет предоставлен цифровым подписям, применение которых основывается на ненадежных процедурах, например, по причине недостаточной "длины" ключа. В ответ было указано, что, хотя в проект статьи 5 или в определение понятия "защищенная электронная подпись",

возможно, и потребуется включить дополнительную ссылку на надежность технических процедур, положение, аналогичное пункту 2, является необходимым для того, чтобы сохранить для сторон возможность доказать в суде или в третейском суде, что подпись в цифровой форме, которую они используют, является достаточно надежной для того, чтобы ее юридическая сила была признана, хотя ее применение и не отвечает условиям пункта 1. В то же время была высказана обеспокоенность в связи с тем, что предоставление статуса "защищенных" создает презумпции и устанавливает распределение ответственности из деликта на основании проектов статей 2 и 3. Было указано на необходимость того, чтобы такие серьезные последствия могли быть установлены с помощью четких правил и стандартов еще до проставления подписи, а не накладывались на не подозревающую о них сторону решением суда на каком-либо более позднем этапе.

83. По вопросу о том, как сформулировать содержащуюся в пункте 2 ссылку на общие правила доказывания, были высказаны различные предложения. Одно из мнений состояло в том, что сфера действия пункта 2 должна быть расширена и что он должен охватывать не только ситуацию, когда используется сертификат, но и любую другую ситуацию, когда применяется подпись в цифровой форме или любая другая электронная подпись. Согласно этой точке зрения из пункта 2 следует исключить ссылку на "сертификат" и перенести этот пункт в раздел, касающийся электронных подписей в целом. Другое мнение состояло в том, что сфера действия пункта 2 должна быть сужена и что это положение должно применяться только в том случае, когда цифровая подпись проставлена в течение срока действия сертификата, имеющего юридическую силу. Согласно этой точке зрения, правило, содержащееся в пункте 2, следует изложить в пункте 1(b) в примерно следующей формулировке:

> "iv) достаточные доказательства показывают, что сертификат устанавливает четкую связь между публичным ключом и личностью его держателя".

84. После обсуждения Рабочая группа не достигла консенсуса по вопросам о сфере действия положения, содержащегося в пункте 2, и о его месте в тексте единообразных правил. К Секретариату была обращена просьба подготовить пересмотренный проект положения с вариантами, отражающими обсуждение, проведенное по пункту 2, для рассмотрения Рабочей группой на одной из будущих сессий.

Статья 6. Подписи, проставляемые юридическими лицами

85. Рабочая группа рассмотрела следующий текст проекта статьи 6:

"[Юридическое лицо может идентифицировать сообщение данных путем добавления к этому сообщению публичного криптографического ключа, сертифицированного для этого юридического лица. Юридическое лицо рассматривается как [составитель] [одобрившее направление] сообщения только в том случае, если это сообщение также подписано в цифровой форме физическим лицом, уполномоченным действовать от имени этого юридического лица.]"

86. Было напомнено о том, что на предыдущей сессии Рабочей группы широкую поддержку получило мнение о целесообразности исключения проекта статьи 6. Этот проект был оставлен в квадратных скобках в качестве напоминания о том, что Рабочей группе может понадобиться более глубоко обсудить вопрос о параметрах, в пределах которых единообразные правила должны признавать действительность операций "электронных агентов" в целях удостоверения подлинности сообщений данных в автоматическом режиме (см. A/CN.9/437, пункты 115-117). Рабочая группа приняла решение о том, что вопрос об "электронных агентах" потребуется обсудить на более позднем этапе. В то же время было решено исключить проект статьи 6, поскольку может быть сочтено, что он ненадлежащим образом затрагивает другие своды правовых норм (например, агентское право и нормы акционерного права, касающиеся представительства компаний физическими лицами).

Часть III. Другие электронные подписи

87. Согласно общему мнению, раздел III следует оставить в единообразных правилах до принятия решения о том, следует ли принцип недискриминации, закрепленный в определениях понятий "подпись" и "защищенная электронная подпись" (и выраженный через признание правового статуса любых способов удостоверения подлинности, которые будут отвечать требованиям к "защищенной электронной подписи"), выразить также и с помощью более специальных положений, касающихся иных способов удостоверения подлинности, чем подписи в цифровой форме.

88. С тем чтобы более подробно проинформировать Рабочую группу о том, как могут применяться подписи в цифровой форме и различные другие способы удостоверения подлинности, были сделаны несколько сообщений технического характера. Эти сообщения резюмируются ниже (пункты 89-105).

89. Было напомнено, что для надежности электронной торговли требуется, чтобы стороны сделки были в состоянии провести удостоверение личности друг друга. Во многих случаях электронного взаимодействия (например, при покупках через сеть "Интернет") традиционные способы удостоверения либо не могут быть применены, либо не являются надежными. Эта необходимость в надежных методах электронного удостоверения вышла за рамки потребностей коммерческой деятельности и затрагивает практически каждый вид взаимодействия в сфере применения цифровых средств.

90. Было указано, что для удовлетворения этих потребностей в настоящее время предлагаются самые разнообразные решения. Эти решения состоят как из технологического, так и из методологического компонентов. Хотя существует тенденция к тому, чтобы уделять значительно более пристальное внимание различным технологическим подходам, воздействие методологии или бизнес-модели, лежащей в основе вариантов электронного удостоверения, недооценивать не следует. Помимо многочисленных различных технологических подходов рынок предлагает также самые разнообразные методологии применения этих технологий. Эти многочисленные решения отражают различные виды удостоверения, требующиеся в самых различных ситуациях, возникающих в условиях применения цифровых средств. По мере развития этого сектора будут возникать потребности в новых решениях вопроса об удостоверении.

91. Способы удостоверения могут быть разбиты на категории в зависимости от удостоверяемой характеристики. Были описаны три следующие базовые категории характеристик: 1) "то, что вам известно"; 2) "кто вы"; и 3) "то, что у вас есть". Многие решения используют комбинацию этих трех характеристик.

92. Первая категория ("то, что вам известно") является одной из характеристик, наиболее часто используемых для удостоверения личности отдельных лиц. В эту категорию входят пароли, фразы-пароли и личные идентификационные номера (ЛИН). Большинство компьютерных систем имеют программы допуска, которые позволяют получить доступ к ресурсам тем лицам, которые знают действующий пароль. Например, для автоматизированного доступа к информации о состоянии банковского счета пользователям необходимо знать правильный ЛИН, связанный со счетом, информация о котором запрашивается. Другой вид удостоверения, подпадающий под эту категорию, основывается на личной информации, предположительно известной только соответствующему конкретному лицу. Например, в некоторых странах банки при открытии счета часто просят клиентов сообщить девичью фамилию матери. Эта информация может быть использована впоследствии для удостоверения личности владельца счета. Хотя такая категория удостоверения в настоящее время широко используется в практике, она имеет ряд недостатков. Во-первых, обычно требуется, чтобы информация, совместно известная сторонам, была либо тайной, либо трудной для получения. Во-вторых, требуется, чтобы отношения между сторонами уже были установлены и чтобы ранее они уже могли "обменяться" тайным элементом информации (например, паролем, ЛИН или информацией о девичьей фамилии матери).

93. Вторую категорию способов удостоверения ("кто вы") часто называют биометрикой. При этом подходе для удостоверения личности индивидуума используются его природные качества. В число используемых в биометрике природных элементов входят: отпечатки пальцев, сетчатая и радужная

оболочки глаза, отпечатки ладони, характеристики голоса и собственноручные подписи. Поскольку все эти характеристики являются уникальными, их использование представляет собой прекрасный способ удостоверения личности. Если может быть обеспечено публичное распространение информации об этих характеристиках, то для этого вида удостоверения личности не потребуется наличия ранее установленных отношений. Кроме того, с помощью этих подходов часто можно добиться надежного удостоверения, поскольку манипулирование такими системами или махинации с ними весьма затруднены. К недостаткам этих подходов относится тот факт, что их применение связано с высокими затратами, поскольку требуется определенное оборудование для получения информации о соответствующем элементе. Другой вызывающий обеспокоенность фактор в связи с применением способов, относящихся к этой категории, касается устройств, применяемых для сбора биометрической информации. В некоторых случаях эти устройства считаются причиняющими излишние неудобства (например, для применения устройства, сканирующего сетчатую оболочку глаза, требуется, чтобы пользователи приложили глаз к прорези, через которую с помощью красного цвета сканируется сетчатая оболочка). В других случаях информация, полученная в ходе сканирования в целях удостоверения личности, может раскрывать личную информацию о состоянии здоровья, которую соответствующее лицо не хочет обнародовать публично (например, на основании некоторых нарушений в состоянии радужной оболочки глаза могут быть диагностицированы некоторые характеристики состояния здоровья и, таким образом, хотя сканирование радужной оболочки и не причиняет излишних физических неудобств, некоторые считают, что оно представляет собой вторжение в частную жизнь). И наконец, некоторые из этих устройств могут быть не всегда надежными, особенно в "анормальных" условиях использования (например, отпечатки с порезанных пальцев). Тем не менее широко признается, что биометрические решения являются одним из самых надежных способов удостоверения личности, и они используются в практике в настоящее время. Были приведены примеры страны, в которой службы иммиграции и натурализации опробывают технологию снятия отпечатков ладони для ускорения паспортного контроля, и страховых компаний, которые используют биометрику подписи для удостоверения личности клиентов при обработке требований о выплате возмещения.

94. Третья категория способов удостоверения ("то, что у вас имеется") была описана в качестве одной из наиболее активно развивающихся областей в сфере электронного удостоверения. "То, что" может быть в материальной форме (например, устройство типа "запрос-ответ") или может представлять собой информацию (например, криптографический ключ). Применение устройств типа "запрос-ответ" аналогично использованию подхода совместного обладания тайной информацией, который используется в категории "то, что вам известно", за тем исключением, что это решение реализуется через машинное обеспечение. Для этого решения требуется, чтобы в распоряжение соответствующих лиц было предоставлено устройство, которое является уникальным и которое резервируется только за конкретным отдельным пользователем. Когда это лицо пытается получить доступ к какой-либо услуге, центральная система просит его идентифицировать себя (обычно с помощью имени), а затем составляет цифровой запрос на основе имеющейся в системе информации относительно уникального устройства, зарезервированного за этим лицом. Затем это лицо вводит этот номер в устройство, которое составляет цифровой ответ. Этот цифровой ответ может быть затем введен в систему, к которой пытается получить доступ владелец устройства. Центральная система "знает" о том, что на цифровой запрос, посланный этому лицу, может быть представлен только один приемлемый ответ и что приемлемый ответ может быть подготовлен только уникальным устройством, зарезервированным за этим лицом. Поэтому, если был введен правильный цифровый ответ, то центральная система "знает", что лицо, пытающееся получить доступ, является именно тем лицом, как оно утверждает. Такой вид устройств широко используется для удостоверения личности лиц, пытающихся получить дистанционный доступ к компьютерным системам. Такие устройства также применяются одним из банков в экспериментальном проекте "банк на дому", который был назван проектом "осуществления банковских операций с помощью браузера", поскольку он предоставляет любому лицу возможность получить доступ к банковскому счету с помощью любой программы просмотра, установленной на любой машине. Эта прикладная программа продемонстрировала одну из сильных сторон этого подхода. Хотя он и требует наличия компонента машинного обеспечения, не возникает необходимости в системной модификации, подобной той, которая требуется в случае использования плат для установки интегральных схем.

95. Другая подкатегория третьей категории охватывает использование подписей в цифровой форме. Важным аспектом технологии подписей в цифровой форме является использование частного ключа для создания цифровой подписи и использование публичного ключа для удостоверения подлинности этой подписи. Частный ключ, используемый для создания подписей в цифровой форме, может быть записан на жестком диске или на интеллектуальной карточке и должен храниться в большой тайне использующим его лицом. Информация о публичном ключе распространяется на широкой основе. Имеется ряд различных парадигм для использования технологии подписей в цифровой форме, каждая из которых связана с особым подходом к обеспечению того, чтобы получатель доверял цифровой подписи.

96. Один из первых подходов состоит в создании директории с указанием соответствующих лиц и публичных ключей. Согласно этой модели получатель документа, подписанного в цифровой форме, проверяет публичный ключ лица, подписавшего документ, путем сверения с публичным ключом, указанным в заслуживающей доверия директории. Было сообщено о ряде случаев применения этой модели в настоящее время.

97. В рамках другого подхода, разработанного на основе подхода, предусматривающего использование директорий, применяются цифровые сертификаты. Цифровые сертификаты представляют собой электронные документы, подписанные доверенной структурой в цифровой форме. Когда документ подписан в цифровой форме, к нему прилагается копия цифрового сертификата подписавшего его лица. В ней содержится информация об этом лице и о его публичном ключе. Когда получатель получает сообщение и цифровой сертификат, он использует указанный в цифровом сертификате публичный ключ для удостоверения подлинности сообщения.

98. Широко распространено использование цифровых сертификатов при применении стандарта (ISO X.509), который позволяет для удостоверения личности сторон использовать иерархию доверенных структур. Такой подход часто называют моделью "кредитной карты", поскольку он отражает бизнес-модель, лежащую в основе сектора кредитных карт. Например, торговцу клиент может быть неизвестен, однако торговец принимает платеж с помощью кредитной карты, поскольку он знает, что эта карта выдана потребителю банком (название банка всегда указывается на карте), который уполномочен выдавать такие карты компанией, занимающейся организацией расчетов по кредитным картам. Даже если торговцу неизвестен банк, выдавший эту карту, он может оказать доверие клиенту, поскольку ему известно, что личность клиента удостоверена банком, а сам банк удостоверен компанией, занимающейся организацией расчетов по этой кредитной карте. Аналогично, иерархия доверия в соответствии со стандартом X.509 позволяет производить удостоверение цифровых сертификатов иерархической цепочкой доверенных структур (известных под названием "Certificate Authorities" (сертифицирующие органы), которые в настоящем докладе называются "сертификационные органы" (certification authorities)), которые могут быть проверены получателем сертификата. Последний сертификационный орган в этой доверительной системе известен под названием "базы" ("root"). Таким образом, подписание какого-либо документа в цифровой форме при использовании подхода на основе стандарта X.509 предполагает рассылку цифрового сертификата лица, поставившего свою подпись, и всех подтверждающих цифровых сертификатов, связанных с доверительной иерархией, на которую полагается получатель. Согласно этой модели получатель может проверить всю доверительную цепочку без необходимости сверяться с директорией он-лайн. Этот подход был описан в качестве особенно подходящего для создания возможностей обмена заслуживающими доверия сообщениями между очень многочисленной группой людей, которые могут практически или вовсе не иметь контактов друг с другом. Одно из преимуществ такого подхода - возможность связать многие сертификаты в обратном порядке вплоть до доверенной "базы" - является также и одним из его недостатков. Если "база" скомпрометирована, все находящееся ближе к началу цепочки также становится ненадежным.

99. Другой вариант использования цифровых сертификатов обычно называется сетевой моделью доверия. При такой модели сертификационных органов не имеется. Цифровые сертификаты составляются отдельными лицами. Не имеется также и доверенной базы. Отдельные лица сами

принимают решения о том, кому и в какой степени они будут доверять. Эта модель предназначена для небольших сообществ пользователей, которые поддерживают регулярные контакты, и реализовать ее в широких масштабах трудно. Тем не менее эта модель в настоящее время используется в различных условиях.

100. Было указано, что важное соображение для понимания принципов использования цифровых сертификатов X.509 связано с историческим смещением акцента в направлении идентификации личности. Поскольку стандарт X.509 вытекает из директории X.500, то первоочередное внимание, естественно, уделяется связыванию публичных ключей с личностью соответствующих лиц. Было указано, что такой изначальный акцент на личности вызывает трудности применительно ко многим вопросам публичного порядка, связанным с использованием подписей в цифровой форме. Хотя ясно, что некоторые цифровые сертификаты удостоверяют личность соответствующего лица, также ясно, что другие цифровые сертификаты выполняют иные функции, чем удостоверение личности. Цифровые сертификаты могут также использоваться для удостоверения прав или отношений какого-либо лица без какой-либо информации относительно его личности. Во многих случаях информация о личности соответствующего лица не является необходимой или даже желательной. Имеются многочисленные специальные целевые сертификаты, которые могут быть использованы только для выполнения некоторых функций, точно так же, как личная кредитная карта не может быть использована для подтверждения личности соответствующего лица, а его паспорт не может быть использован для покупки товаров. Склонность постоянно учитывать фактор личности, хотя и является логичной, может существенно ограничить использование этой технологии. Если при каждом виде применения подписей в цифровой форме будет необходимо выполнять строгие требования общецелевого сертификата личности, то использование такой технологии будет весьма затруднено и будет связано с большими затратами. Важно помнить о том, что диапазон требований к удостоверению всегда будет весьма широк и что технология является достаточно гибкой для удовлетворения всех таких требований.

101. Когда несколько компаний, занимающихся организацией расчетов по кредитным картам, приняли решение о разработке надежного метода для электронной торговли по публичным сетям, таким как "Интернет", они выделили три основные деловые цели: решение должно быть надежным; решение должно быть открытым для любого поставщика технологии, заинтересованного в разработке продукта, который мог бы выполнять принятый протокол; и должно быть обеспечено взаимодействие между всеми элементами реализации. Для целей сектора платежей в понятие "надежный" входят три следующих компонента: 1) конфиденциальность платежной информации, в том числе информации о номере счета клиента; 2) целостность информации о заказе и 3) удостоверение личности сторон сделки. В целях обеспечения требуемого уровня "надежности" был разработан протокол надежных электронных операций ("НЭО"). Этот протокол использует подписи в цифровой форме (на основе модели X.509) для выполнения функций обеспечения целостности данных и удостоверения личности сторон.

102. Было дано краткое описание протокола НЭО. Потребитель, который желает осуществлять надежные электронные коммерческие операции при использовании НЭО, должен в первую очередь приобрести программное обеспечение, прошедшее проверку на соблюдение соответствующих требований при помощи процедур, установленных Базовым сертификационным органом НЭО. С помощью этого программного обеспечения составляется пара ключей и прикладная программа, которые потребитель направляет структуре, выдавшей предназначенную для использования платежную карту. Программное обеспечение вводит публичный ключ в прикладную программу сертификата и направляет потребителю запрос о предоставлении идентификационной информации с тем, чтобы финансовое учреждение могло проверить, имеет ли лицо, запрашивающее сертификат, полномочия на это. Эта прикладная программа направляется финансовому учреждению через "Интернет". Если прикладная программа принимается, финансовое учреждение подписывает в цифровой форме сертификат потребителя и направляет его обратно потребителю через "Интернет". Программное обеспечение потребителя обеспечивает хранение этого цифрового сертификата в памяти компьютера потребителя. Эта прикладная процедура применяется только один раз для получения сертификата.

103. Затем потребитель может начать производить покупки в режиме он-лайн и может заключать надежные сделки с торговцами, использующими программное обеспечение, отвечающее требованиям НЭО. На первоначальных этапах заключения сделки программное обеспечение потребителя запрашивает удостоверяющую информацию у торговца. Программное обеспечение удостоверяет личность торговца путем проверки всех подписей в цифровой форме и цифровых сертификатов, направленных торговцем. Если в какой-либо момент процесса удостоверения выявляется какое-либо несоответствие, то потребителю дается предупреждение. Затем потребитель выбирает товары или услуги, которые он хотел бы приобрести, выбирает метод платежа и начинает процесс заключения сделки. Программное обеспечение потребителя отделяет платежную информацию от информации о заказе. Затем производится кодирование платежной информации при использовании защищенной криптографической системы с тем, чтобы финансовое учреждение торговца было единственным, которое сможет расшифровать платежную информацию. Информация о заказе, оговаривающая предмет покупки и другие детали сделки, и зашифрованная платежная информация подписываются в цифровой форме и направляются торговцу. Торговец, по получении этого сообщения, производит отделение зашифрованной платежной информации, подписывает в цифровой форме это новое сообщение и направляет его своему финансовому учреждению. Финансовое учреждение проводит проверку цифровой подписи торговца, расшифровывает платежную информацию, а затем представляет платежную информацию на обработку существующей платежной инфраструктуре. Финансовое учреждение подписывает в цифровой форме содержащий разрешение ответ и направляет его торговцу. Затем торговец направляет подписанный в цифровой форме ответ потребителю. Если сделка разрешена, торговец выполняет заказ.

104. Было указано, что система НЭО является примером доверия к технологии цифровых подписей при удостоверении подлинности сообщений и личности сторон. В то же время важно отметить, что сертификаты НЭО не являются сертификатами личности. Они не удостоверяют личность какого-либо лица, а также не могут использоваться для выполнения этой функции, как это прямо указывается в заявлении с изложением принципов, которое прилагается к этим сертификатам. Сертификаты НЭО лишь удостоверяют связь частного ключа с номером счета. Применительно к НЭО технология цифровых подписей используется для обеспечения дополнительной надежности в отношении сделки, а не для установления личности какого-либо лица. Кроме того, в системе НЭО не используются перечни аннулированных сертификатов ("ПАС") как в отношении сертификатов потребителей, так и торговцев. В контексте бизнес-модели НЭО в таких перечнях нет необходимости. В этой системе по-прежнему требуется разрешение на сделку, которое должно быть получено через существующую платежную инфраструктуру, и, таким образом, создание дополнительного ПАС для держателей карточек не даст каких-либо выгод и приведет к дополнительным значительным затратам на создание и поддержание системы.

105. Было указано, что НЭО является примером: 1) не связанного с удостоверением личности использования цифровых подписей и сертификатов; 2) выдачи сертификатов рыночными сертификационными органами без какой-либо лицензии; 3) выдачи сертификатов в рамках системы, в которой стороны определяют свои права и обязательства на основании соглашения; и 4) практики, при которой в ряде случаев полагающаяся сторона (банк, который производит платеж на основе информации, подписанной потребителем в цифровой форме) может быть эмитентом сертификата. НЭО является лишь одним из примеров применения технологии цифровых подписей. Было указано, что в будущем появятся другие многочисленные виды применения, которые будут основываться на технологиях и бизнес-моделях, которые еще только предстоит создать.

106. Рабочая группа выразила свою признательность за сделанные сообщения. Было выражено общее мнение о том, что примеры технологических решений, которые применяются в настоящее время или которые рассматриваются на предмет применения, помогают лучше понять правовые вопросы, которые необходимо урегулировать в единообразных правилах. Рабочая группа выразила надежду, что в рамках ее будущих сессий смогут быть сделаны дополнительные сообщения о новых моментах в области цифровых подписей и других способов удостоверения.

РАЗДЕЛ III. СЕРТИФИКАЦИОННЫЕ ОРГАНЫ И СООТВЕТСТВУЮЩИЕ ВОПРОСЫ

Статья 7. Сертификационный орган

107. Рабочая группа рассмотрела следующий текст проекта статьи 7:

"1) Для целей настоящих Правил "сертификационный орган" означает:

a) любые лицо или организацию, лицензированные [уполномоченные] ... *[*принимающее государство указывает орган или ведомство, компетентное лицензировать сертификационные органы и принимать постановления в отношении функционирования лицензированных сертификационных органов*]* действовать в соответствии с настоящими Правилами; или

b) любые лицо или организацию, которые в порядке своей обычной деловой практики занимаются выдачей сертификатов по криптографическим ключам, используемым для подписи в цифровой форме.

[2) Сертификационный орган может предлагать или облегчать регистрацию и фиксацию времени передачи и приема сообщений данных, а также выполнять другие функции в отношении сообщений, защищенных с помощью подписей в цифровой форме.]"

Пункт 1

108. Было высказано мнение, что в пункте 1 делается излишний акцент на ситуации, когда функцию сертификационного органа выполняет независимая третья сторона (которую часто называют "доверенной третьей стороной"), а эта ситуация отнюдь не является единственно возможной. Было указано, что в практике использования подписей в цифровой форме стороны все более часто используют системы "самосертификации" (или "взаимосертификации"), в которых участвуют только составители и адресаты сообщений, подписанных в цифровой форме. Соответственно, определение понятия "сертификационный орган" следует расширить для охвата всех видов практики. Было предложено заменить слова "в порядке своей обычной деловой практики" в пункте 2 словами "в рамках своих деловых операций". Это предложение было сочтено в целом приемлемым.

109. Другое предложение заключалось в том, что Рабочей группе наряду с определением "сертификационного органа", возможно, потребуется рассмотреть определение "регистрационного органа". Хотя поддержки этому предложению выражено не было, было в целом сочтено, что этот вопрос, возможно, потребуется обсудить на одном из последующих этапов.

110. Еще одно предложение состояло в том, чтобы исключить подпункт (a), поскольку он касается лишь одной из составных частей категории, рассматриваемой в подпункте (b). В поддержку этого предложения было указано, что любая ссылка в единообразных правилах на "сертификационные органы, получившие лицензию" может быть истолкована как поощряющая принимающее эти правила государство к созданию систем лицензирования, что может противоречить "двойному подходу", принятому Рабочей группой на ее предыдущей сессии (см. A/CN.9/437, пункт 69). Было также указано, что исключение подпункта (a) позволит не только сохранить необходимую гибкость, но и должным образом сконцентрировать внимание единообразных правил на использовании подписей в цифровой форме для целей международных торговых сделок в отличие от применения подписей в цифровой форме для административных целей. Возобладала, однако, точка зрения о том, что положения подпункта (a) следует сохранить. Было указано, что в некоторых контекстах сертификационные органы, действующие на основании лицензии, могут и не осуществлять "деловых" операций. Кроме того, проведение различия между сертификационными органами, действующими на основании лицензии, и теми сертификационными органами, которые функционируют на исключительно частной основе, является оправданным с точки зрения необходимости отразить различные правовые режимы, которые могут

распространяться на эти два вида сертификационных органов. В качестве примера такого различия было указано, что антимонопольное законодательство, которое может применяться в отношении функционирующих под частным контролем сертификационных органов, может и не распространяться на сертификационные органы, выполняющие публичные функции. Кроме того, даже если категория, рассматриваемая в подпункте (a), охватывается положением, содержащимся в подпункте (b), подпункт (a) будет по-прежнему служить полезной цели, поскольку он будет отвечать потребностям тех государств, которые намереваются использовать систему лицензирования, и, таким образом, способствует сохранению нейтрального характера единообразных правил.

111. С учетом вышеизложенного обсуждения было принято решение о том, что для цели дальнейшего рассмотрения редакция пункта 1 должна быть изменена примерно следующим образом:

> "1) Для целей настоящих Правил "сертификационный орган" означает любое лицо или организацию, которые в рамках своих деловых операций занимаются выдачей сертификатов в отношении криптографических ключей, используемых для целей подписей в цифровой форме.
>
> 2) Пункт 1 применяется с учетом любого применимого закона, который требует, чтобы сертификационный орган получил лицензию, был аккредитован или функционировал таким образом, который указан в этом законе".

Пункт 2

112. Сохранению пункта 2 была выражена определенная поддержка. Было высказано мнение, что функции, перечисленные в пункте 2, должны быть дополнены прямой ссылкой на такие другие функции, как составление, внесение соответствующих изменений, приостановление действия и аннулирование сертификатов с тем, чтобы лучше проиллюстрировать связь между различными вспомогательными услугами, предоставляемыми сертификационными органами, и функционированием системы подписей в цифровой форме, обеспечение которого представляет собой для сертификационного органа основной вид деятельности. Возобладало, однако, получившее широкое распространение мнение о том, что пункт 2 следует исключить и что его существенные положения могут быть рассмотрены на более позднем этапе на предмет возможного включения в руководство по принятию, если Рабочая группа примет решение о том, что такое руководство должно быть подготовлено.

Статья 8. Сертификат

113. Рабочая группа рассмотрела следующий текст проекта статьи 8:

> "Для целей настоящих Правил "сертификат" означает сообщение данных [или какую-либо иную запись], в котором по меньшей мере:
>
> a) идентифицируется выдавший его сертификационный орган;
>
> b) называются или идентифицируются его держатель либо соответствующие устройство или электронный агент, находящиеся под контролем держателя;
>
> c) содержится публичный ключ, соответствующий частному ключу, находящемуся под контролем держателя;
>
> d) указываются срок действия [и существующие ограничения, если таковые имеются, относительно сферы использования публичного ключа]; и
>
> e) подписан [в цифровой форме] сертификационным органом, выдавшим сертификат".

Общие замечания

114. Было высказано общее мнение о том, что проект статьи 8 следует разделить на две части (или на две отдельные статьи), в одной из которых будет содержаться общее определение сертификатов, охватываемых единообразными правилами, а в другой будут перечисляться минимальные требования к содержанию таких сертификатов, как это делается в подпунктах (a)-(e). Отмечалось, что такой подход надлежащим образом расширит сферу применения единообразных правил, которая будет более ограниченной, если все элементы, содержащиеся в проекте статьи 8, будут включены в определение термина "сертификат".

Определение термина "сертификат"

115. С самого начала было решено, что использование технических определений сертификатов может оказаться неприемлемым, поскольку они, вероятно, будут пересматриваться по мере изменения потребностей и развития технологии. После этого Рабочая группа рассмотрела определение термина "сертификат" на основе формулировки следующего содержания: "Для целей настоящих правил "сертификат" означает сообщение данных или какую-либо иную запись, выдаваемую сертификационным органом для целей идентификации лица или структуры, являющихся держателями частного ключа".

116. Было указано, что такое определение охватывает только сертификаты личности и не включает в сферу применения единообразных правил различные другие сертификаты, которые широко используются и которые, возможно, необходимо признать. В связи с этим были высказаны различные мнения. Согласно одному мнению, единообразные правила должны охватывать только сертификаты личности. Согласно другому мнению, должны охватываться также другие виды сертификатов (например, сертификаты полномочий). Хотя это мнение получило определенную поддержку, было выражено беспокойство в связи с тем, что если будут охватываться другие сертификаты, то в положениях, касающихся подтверждений сертификационного органа и, следовательно, его ответственности, необходимо будет установить различные правовые режимы для охвата различных видов выдаваемых сертификатов, что может оказаться чрезмерно сложной задачей для Рабочей группы.

117. Что касается редакционных аспектов, то было предложено подготовить для охвата различных видов сертификатов общее определение, которое будет охватывать все виды сертификатов, а в последующих положениях указать конкретные цели каждого вида сертификатов. Для иллюстрации такого подхода была предложена формулировка примерно следующего содержания: "Для целей настоящих правил "сертификат" означает сообщение данных, которое позволяет проверить сообщение данных, соответствующее публичному ключу, содержащемуся в сертификате". После этого для каждого вида сертификатов необходимо будет предусмотреть положение, указывающее на его цели, например положение следующего содержания: "Сертификат личности предназначен для удостоверения личности". Альтернативно для отражения мнения о том, что сертификаты могут выполнять различные функции, предлагалось изменить определение, включив в него ссылку на сообщение данных, "... которое предназначено для проверки личности или другой существенной характеристики определенного лица". Кроме того, предлагалось заменить слова "подтверждение", "установление" или другой аналогичный термин словом "проверка", которому в некоторых случаях можно придать конкретное техническое значение.

118. Основное внимание в ходе дальнейшего обсуждения было уделено последнему из предложенных определений. Было высказано несколько предложений относительно конкретной формулировки определения "сертификата личности". Согласно одному предложению, следует избегать ссылки на "иные записи". Для обоснования этого предложения было указано, что ссылка на "записи" в единообразных правилах может создать проблемы в отношении толкования статьи 2(a) Типового закона. В ответ было указано, что такая ссылка на "записи" позволит избежать создания любой неопределенности относительно того, будут ли единообразные правила охватывать сертификат в чисто бумажной форме. Согласно

другому предложению, для избежания проблем толкования субъективных намерений сторон слова "для целей идентификации" следует заменить словами "которая идентифицирует".

119. Против предложенной формулировки были высказаны возражения на основании того, что она может привести к возникновению ситуации, в которой сертификационный орган сможет избегать ответственности, не указывая то лицо, которому выдан сертификат. Поэтому необходимо включить формулировку примерно следующего содержания: "который предназначен для идентификации". Согласно другому предложению, слово "лицо" следует заменить термином "предмет", который широко используется в практике и позволит надлежащим образом охватить ситуацию, когда предметом сертификата является не лицо, а определенное "устройство или электронный агент". Против этого предложения были высказаны возражения на том основании, что термин "предмет", если он будет использован, необходимо будет определить на основе ссылки на определенное "лицо"; любое "устройство или электронный агент" будет в любом случае находиться под контролем определенного лица; и термин "предмет" не будет соответствовать терминологии, используемой в Типовом законе, а также в других текстах ЮНСИТРАЛ. Хотя ссылка на определенное "лицо" была сочтена приемлемой, было указано, что следует четко указать, что она означает предмет сертификата и охватывает также "структуру". Что касается ссылки на "структуру", то было решено, что ее можно оставить до принятия Рабочей группой окончательного решения по вопросу о том, может ли предметом сертификата быть какое-либо "устройство или электронный агент". Согласно другому предложению, формулировку "частный ключ" следует заменить формулировкой "пара ключей".

120. После обсуждения Рабочая группа постановила изменить формулировку определения следующим образом:

"Сертификат [личности]

Для целей настоящих правил "сертификат" [личности] означает сообщение данных или иную запись, которые выдаются сертификационным органом и которые предназначены для подтверждения личности [или другой существенной характеристики] лица или структуры, которые являются держателем определенной пары ключей".

121. Было решено, что слово "личность" или слова "другая существенная характеристика", заключенные в квадратные скобки, позволят Рабочей группе рассмотреть на более позднем этапе вопрос о том, должны ли охватываться помимо сертификатов личности другие виды сертификатов.

Положение о минимальных требованиях к содержанию сертификата личности

122. После этого Рабочая группа приступила к рассмотрению подпунктов (a)-(e), сосредоточив внимание на вопросе о том, насколько четко в них описаны минимальные требования к содержанию сертификата личности.

Общие замечания

123. Было выражено общее согласие в отношении того, что практическая цель положения, определяющего минимальные требования к содержанию сертификата, заключается в установлении стандартов, которые должен будет соблюдать сертификационный орган для выполнения своей функции и для того, что избежать ответственности за ущерб, причиненный в результате того, что сертификационный орган не включил в сертификат все необходимые элементы. Было высказано общее мнение, что окончательное решение в отношении минимальных требований к содержанию сертификата не может быть принято до решения вопроса об ответственности сертификационного органа и вопроса о видах сертификатов, которые будут охватываться единообразными правилами. Рабочая группа решила перейти к рассмотрению подпунктов (a)-(e) при том понимании, что предварительный обмен мнениями может облегчить возобновление обсуждения на более позднем этапе.

124. В ходе обсуждения был поднят вопрос о том, следует ли рассматривать сертификат, не отвечающий минимальным требованиям, определенным в проекте статьи 8, в качестве недействительного сертификата, или же следует применять проект статьи 8 в качестве субсидиарной нормы, в результате чего такой сертификат может быть действительным, если это будет согласовано сторонами. Было высказано мнение, что в последнем случае в проект статьи 8 следует включить положение, аналогичное проекту статьи 5(2).

Вводная формулировка

125. Хотя было выражено согласие с тем, что сертификат может быть выдан в чисто бумажной форме, была поставлена под сомнение целесообразность использования формулировки "или иная запись" (см. пункт 118 выше).

Подпункт (a)

126. Подпункт (a) был признан по существу в целом приемлемым.

Подпункт (b)

127. Было отмечено, что в связи с использованием слова "держатель" возникает вопрос о том, имеется ли в виду лицо, которому выдан сертификат, или лицо, которое располагает экземпляром сертификата и полагается на него. Кроме того, было указано, что термин "держатель" создает неопределенность, поскольку в проекте статьи 8 этот термин используется применительно как к лицу, являющемуся держателем сертификата, так и к лицу, являющемуся держателем соответствующей пары ключей. Хотя, исходя из вышеупомянутых соображений, было высказано мнение, что следует отдать предпочтение термину "предмет", Рабочая группа в целом отдала предпочтение термину "лицо" (см. пункт 119 выше). Тем не менее было принято решение, что оба термина следует заключить в квадратные скобки и продолжить рассмотрение этого вопроса. Что касается ссылки на "устройство или электронного агента", использование которой, по мнению некоторых участников, создает неопределенность, то было принято решение заключить эту формулировку в квадратные скобки до возобновления рассмотрения этого вопроса Рабочей группой (см. пункт 119 выше).

Подпункт (c)

128. Подпункт (c) был признан по существу в целом приемлемым. Что касается слова "держатель", то было принято решение заменить его словами "предмет" и "лицо" в квадратных скобках (см. пункт 127 выше).

Подпункт (d)

129. Было достигнуто согласие в отношении того, что срок действия является одним из наиболее важных элементов сертификата. Что касается ссылки на сферу использования сертификата и любые существующие в этом отношении ограничения, то было предложено исключить такую ссылку или по крайней мере изменить ее, указав, что положения о сфере использования и любых соответствующих ограничениях могут быть включены в сертификат с помощью ссылки. В поддержку этого предложения было указано, что в сертификат, вероятно, невозможно будет включить полный перечень всех ограничений. Кроме того, было отмечено, что непреднамеренным результатом такой ссылки может быть возложение на сертификационный орган ответственности за то, что он не включил в сертификат все возможные ограничения. Против этого предложения были высказаны возражения на том основании, что сфера использования и любые соответствующие ограничения являются ключевыми элементами, на основе которых можно оценить функции и целостность сертификата. Кроме того, было отмечено, что ссылка на сферу использования сертификата и любые соответствующие ограничения позволяет учесть необходимость указания на то, что сертификаты могут выполнять различные функции. В этой связи было

высказано предложение включить такую ссылку в новый подпункт (g) в квадратных скобках для дальнейшего рассмотрения этого вопроса Рабочей группой. С учетом этого изменения Рабочая группа одобрила подпункт (d) по существу.

Подпункт (e)

130. Хотя было выражено общее согласие с тем, что подпись сертификационного органа является одним из основных элементов сертификата, были высказаны различные мнения в отношении того, должна ли такая подпись быть в цифровой форме. Согласно одному мнению, подпись должна быть в цифровой форме для обеспечения целостности сертификата. Другое мнение заключалось в том, что, если подпись сертификационного органа является криптографической, полагающиеся на сертификат стороны, возможно, не смогут определить, что эта подпись является подписью соответствующего конкретного сертификационного органа, свидетельствующей о его намерении нести ответственность по сертификату. Кроме того, было указано, что, если подпись сертификационного органа не является результатом транспарентной процедуры, такой сертификат может оказаться недействительным. Рабочая группа согласилась с тем, что необходимо обеспечить защищенность подписи сертификационного органа и транспарентность соответствующей процедуры. Поэтому было принято решение сохранить без скобок формулировку "в цифровой форме" и добавить формулировку "или защищен иным образом" в целях устранения причин для беспокойства, выраженного в связи с формулировкой "в цифровой форме".

Новый подпункт (g)

131. Было высказано мнение, что применяемые сертификационным органом алгоритмы должны быть включены в перечень минимальных элементов сертификата. В поддержку этого предложения было указано, что алгоритмы имеют принципиально важное значение для обеспечения идентификации подписавшего лица и целостности сообщения данных. Против этого предложения были высказаны возражения на том основании, что, если указание соответствующих алгоритмов будет определено в качестве обязательного требования действительности сертификата, сертификационный орган сможет избегать ответственности, не включив этого указания в сертификат. С учетом необходимости обеспечить целостность данных было отмечено, что более эффективно эта задача может быть решена путем включения элемента целостности данных в определение подписи в цифровой форме. Противоположная точка зрения заключалась в том, что, если в сертификат не будут включены применяемые алгоритмы, сертификационный орган будет нести ответственность за неспособность выдать действительный сертификат. После обсуждения Рабочая группа приняла решение включить ссылку на применяемые алгоритмы в квадратных скобках в проект статьи 8 для дальнейшего рассмотрения этого вопроса на одной из будущих сессий.

Статья 9. Заявление о практике сертификации

132. Рабочая группа рассмотрела следующий текст проекта статьи 9:

> "Для целей настоящих Правил "заявление о практике сертификации" означает заявление, опубликованное сертификационным органом, указавшим те виды практики, которые этот орган применяет при выдаче или каком-либо ином использовании сертификатов".

133. Рабочая группа отметила, что проект статьи 9 связан с целым рядом вопросов, рассматриваемых в других положениях единообразных правил, например, с вопросом о подтверждениях, представляемых при выдаче сертификата (проект статьи 10), и вопросом об ответственности сертификационного органа (проект статьи 12), и постановила отложить рассмотрение проекта статьи 9 до тех пор, пока она не завершит рассмотрение единообразных правил.

Статья 10. Подтверждения, представляемые при выдаче сертификата

134. Рабочая группа рассмотрела следующий текст проекта статьи 10:

"Вариант A

1) Выдавая сертификат, сертификационный орган подтверждает любому лицу, разумно полагающемуся на сертификат либо на подпись в цифровой форме, подлинность которой может быть проверена публичным ключом, указанным в этом сертификате, что:

a) при выдаче сертификата сертификационный орган выполнил все применимые требования настоящих Правил и — если сертификационный орган опубликовал сертификат или иным образом предоставил его в распоряжение любого такого полагающегося на сертификат лица — указанный в этом сертификате держатель [являющийся и правомерным держателем соответствующего частного ключа] согласился с ним;

b) указанный в сертификате держатель [правомерно] владеет частным ключом, соответствующим указанному в сертификате публичному ключу;

c) публичный и частный ключи держателя составляют действующую пару ключей;

d) вся содержащаяся в сертификате информация является точной на момент его выдачи, если сертификационный орган не указал в сертификате [или не включил путем ссылки в сертификате указание на то], что точность определенной информации не подтверждена; и

e) насколько известно сертификационному органу, в сертификате не упущены никакие существенные факты, которые, если бы об их существовании было известно, могли бы отрицательно сказаться на достоверности указанных выше подтверждений.

2) При условии соблюдения положений пункта 1 сертификационный орган, выдавший сертификат, подтверждает любому лицу, разумно полагающемуся на сертификат либо на подпись в цифровой форме, подлинность которой может быть проверена публичным ключом, указанным в этом сертификате, что сертификационный орган выдал данный сертификат в соответствии с любым применимым заявлением о практике сертификации [включенным путем ссылки в сертификат, или], уведомление о котором было направлено полагающемуся на сертификат лицу.

Вариант B

1) Выдавая сертификат, сертификационный орган подтверждает держателю и любому лицу, [добросовестно и] в течение срока действия сертификата полагающемуся на содержащуюся в нем информацию, что:

a) сертификационный орган [обработал] [подтвердил] [выдал] и будет обслуживать, а также, в случае необходимости, аннулирует данный сертификат в соответствии с:

i) настоящими Правилами;

ii) любым другим применимым законом, регулирующим выдачу данного сертификата; и

iii) любым применимым заявлением о практике сертификации, сделанным или включенным путем ссылки в сертификат либо уведомление о котором было направлено такому лицу (если было направлено);

b) сертификационный орган проверил личность держателя в пределах, указанных в сертификате или в каком-либо применимом заявлении о практике сертификации, либо — в отсутствие такого заявления о практике сертификации — соответствующим [надежным] [заслуживающим доверия] образом;

c) сертификационный орган проверил, что лицо, ходатайствующее о выдаче сертификата, является держателем частного ключа, соответствующего публичному ключу, указанному в сертификате;

d) за исключением того, что указано в сертификате или каком-либо применимом заявлении о практике сертификации, вся прочая информация, содержащаяся в сертификате, является, насколько это известно сертификационному органу, точной на момент выдачи сертификата;

e) если сертификационный орган опубликовал сертификат, идентифицированный в сертификате держатель согласился с ним.

[2) Если сертификационный орган выдал сертификат в соответствии с положениями закона какой-либо иной страны, то этот сертификационный орган должен также предоставить все гарантии и подтверждения — если такие необходимы, — которые требуются согласно закону, регулирующему выдачу сертификата.]"

135. Название проекта статьи было предложено изменить примерно следующим образом: "процедуры выдачи сертификата". В самом начале обсуждения было отмечено, что проект статьи 10, устанавливающий стандарт, на основе которого будет оцениваться ответственность сертификационного органа, тесно связан с проектом статьи 12, в котором применительно к этому стандарту устанавливается соответствующая санкция. При обсуждении варианта A в центре внимания стоял вопрос о том, следует ли рассматривать подтверждения, перечисленные в подпунктах (a)-(e) пункта 1, в качестве обязательных требований (т.е. минимальных стандартов, от которых стороны не могут отходить на основании соглашения) или в качестве "субсидиарных" правил. Что касается содержания понятия "субсидиарные правила", то на различных этапах обсуждения такие возможные "субсидиарные" нормы характеризовались либо как правила, "предназначенные для заполнения пробелов" (т.е. как требования, которые будут иметь обязательную силу только в отсутствие соглашения о противном), либо как правила, которые будут применяться только в том случае, если между сторонами вообще не имеется договорных отношений.

136. В поддержку установления в пункте 1 субсидиарной нормы указывалось на следующее: необходимо, чтобы предусматриваемое правило было гибким, с тем чтобы обеспечить возможность учета будущих изменений в технологии; установление высокого стандарта ответственности для всех сертификационных органов приведет только к созданию препятствий для развития этого сектора и будет одновременно поощрять к выходу на рынок менее надежные сертификационные органы; установление минимальных стандартов для относительно малонадежных сертификатов может ограничить глобальное использование таких сертификатов в различных важных контекстах; в целом ожидания держателя сертификата и сторон, полагающихся на сертификат, относительно его содержания должны определяться только со ссылкой на принятые сертификационным органом - в заявлении о практике сертификации или иным образом -обязательства относительно того, что будет подтверждаться в сертификате; и принятие обязательных минимальных стандартов для сертификатов может привести к изоляции единообразных правил от коммерческой практики, фактически применяющейся на основных рынках. Соответственно ответственность сертификационного органа должна определяться только со ссылкой на те обязательства, которые сертификационный орган согласился на себя принять. Было указано, что этот подход позволяет добиться такого уровня гибкости, который необходим для учета самых разнообразных сертификатов, имеющихся на рынке. Была предложена следующая возможная новая формулировка проекта статьи 10, который может быть объединен с проектом статьи 12:

"1) Сертификационный орган прямо указывает в сертификате те виды услуг, которые он предоставляет. Если обязательство сертификационного органа в сертификате не указывается, то сертификационный орган считается гарантировавшим личность держателя ключа.

2) Если сертификационный орган не выполнил услуг, указанных в сертификате, или проявил небрежность при гарантировании личности держателя ключа, он несет ответственность перед стороной, положившейся на сертификат, за причиненные убытки.

3) Сертификационный орган может ограничить свою ответственность по возмещению убытков путем включения в сертификат оговорок об освобождении от ответственности.

4) Настоящая статья применяется, если сертификационный орган и сторона, полагающиеся на сертификат, не договорились об ином".

137. Против этого предложения были высказаны возражения на том основании, что в некоторых правовых системах возникнет несоответствие между определением критериев, на основании которых может быть признан правовой статус сертификата, с одной стороны, и таким порядком, при котором, с другой стороны, может допускаться использование общей оговорки об освобождении от ответственности, противоречащей важнейшим элементам этих критериев. Было также указано, что между стороной, полагающейся на сертификат, и сертификационным органом, как правило, не будет существовать договорной связи. В этой связи было высказано мнение о том, что было бы, возможно, целесообразно разъяснить, охватывает ли понятие "сторона, полагающаяся на сертификат" держателя пары ключей, указанных в сертификате. Было высказано мнение, что размеры сертификатов могут быть весьма ограниченными, что затруднит включение в них "прямо выраженных оговорок об освобождении от ответственности". В ответ было указано, что установление минимального стандарта относительно предполагаемого содержания сертификата отвечает необходимости сократить размеры собственно сертификата.

138. В поддержку сохранения пункта 1 варианта A в качестве минимального стандарта, от которого сторонам не будет разрешаться отходить на основании частного соглашения, было напомнено, что Рабочая группа на своей предыдущей сессии приняла решение, непосредственно касающееся этого вопроса (см. A/CN.9/437, пункты 70-71). Кроме того, было указано, что установление минимальных требований будет не только защищать держателя сертификата и других полагающихся на него сторон, но также и укрепит доверие к механизмам использования подписей в цифровой форме и их коммерческую приемлемость, что будет полезным и для сертификационных органов. В ответ на возражение, заключавшееся в том, что установление минимального стандарта приведет к наложению обременительных обязательств на сертификационные органы, было указано, что цель проекта статьи 10 состоит не в том, чтобы наложить какие-либо обязательства на сертификационный орган, а лишь в том, чтобы определить специальный правовой режим для некоторых сертификатов, которые при соблюдении определенных требований будут удовлетворять условиям предоставления специального правового статуса. Сертификационный орган по-прежнему сможет по своему усмотрению предлагать сертификаты более низкого качества, хотя выдача таких сертификатов и не повлечет за собой аналогичных юридических последствий. Выступавшие в защиту сохранения минимального стандарта в целом признали, что предусматриваемые в проекте статьи 12 механизмы ограничения объема ответственности создают надлежащий баланс, что позволит сертификационным органам согласиться на обязательные требования, устанавливаемые в проекте статьи 10. В этой связи была проведена параллель с режимом ответственности в секторе морских перевозок, в котором, как это показывает история, взаимодействие ничем не ограниченных рыночных сил привело к созданию такой общей колоссальной неопределенности, что стороны стали неохотно заключать сделки, связанные с морской перевозкой, что вызвало необходимость в скорейшем принятии международных документов в этой области, таких, как Гаагские правила.

139. Было высказано предположение о том, что ограничение сферы действия этого положения за счет определения конкретного вида сертификатов (например, сертификатов личности, выдаваемых для целей сделок с большим стоимостным объемом), к которым будет применяться проект статьи 10, возможно, повысит приемлемость проекта статьи 10 в виде обязательного стандарта. В качестве альтернативы было высказано предположение о том, что принятие более низкого обязательного стандарта может способствовать приемлемости применения проекта статьи 10 к более широкой категории сертификатов. В целях объединения этих двух возможных подходов было внесено предложение сохранить в качестве минимального стандарта только подпункты (a), (d) и (e) пункта 1. Хотя включению этого предложения в число вопросов для дальнейшего обсуждения была выражена общая поддержка, в целом было сочтено, что по ряду аспектов требуются дополнительные разъяснения.

140. Один из вопросов, требующих разъяснений, касается точной категории сертификатов, к которым будет применяться такой более низкий обязательный стандарт. Согласно одной из точек зрения, более низкий стандарт должен применяться только к ограниченной категории высокозащищенных сертификатов личности. Было поддержано мнение о том, что для тех сертификатов, за которыми будет признаваться высокий уровень правовой надежности, потребуется более жесткий стандарт. В частности, если цель сертификата будет состоять в том, чтобы установить юридическую обязательность подписи, то потребуется предусмотреть дополнительные гарантии относительно связи между сертификатом и личностью держателя пары ключей. В то же время было также поддержано мнение о том, что предложенный минимальный стандарт на основе подпунктов (a), (d) и (e) сокращен до таких пределов, что можно предусмотреть его применение к широкому диапазону сертификатов.

141. Другой вопрос, требующий дальнейшего разъяснения, касается соответствия предложенного текста пункта 1 другим положениям единообразных правил, касающимся идентификационной функции сертификата. Было напомнено о том, что для целей подписей в цифровой форме основная функция сертификата состоит в идентификации держателя пары ключей и что именно по этой причине ранее было предложено, чтобы Рабочая группа сконцентрировала свое внимание на концепции сертификатов "личности". Если будет принят предлагаемый более низкий стандарт, то сертификационный орган более не будет давать каких-либо заверений относительно личности держателя, а будет просто гарантировать, что процедуры, установленные самим сертификационным органом, были выполнены. Хотя было признано, что такие процедуры могут косвенно вести к идентификации держателя пары ключей, было предложено более подробно рассмотреть вопрос о сохранении положений подпунктов (b) и (c), касающихся прямой (или "дефинитивной") идентификации держателя, в единообразных правилах, возможно, в качестве части проекта статьи 2.

142. Хотя в целях установления стандарта для сертификатов личности было предложено использовать подпункты (a), (d) и (e), после обсуждения Рабочая группа в целом согласилась с тем, что такой ограниченный стандарт более целесообразно применять к широкому диапазону сертификатов. Было также решено, что необходимо еще раз проанализировать вопрос о том, каким образом следует отразить идентификационную функцию - либо в проекте статьи 10, либо в какой-то более ранней статье единообразных правил - в качестве одной из важнейших функций более узкой категории сертификатов, для которых необходим более высокий уровень правовой надежности. Было достигнуто согласие с тем, что этот вопрос потребуется еще раз рассмотреть на одной из будущих сессий. До завершения этого обсуждения подпункты (a), (d) и (e) будут сохранены в пункте 1, а подпункты (b) и (c) будут заключены в квадратные скобки. Было также внесено предложение о том, чтобы альтернативная формулировка на основе пункта 1(b) варианта B была также заключена в квадратные скобки в пункте 1 для рассмотрения Рабочей группой на одной из будущих сессий. Что касается подпункта (d), то широкое распространение получило мнение о том, что ссылка на возможную оговорку сертификационного органа об освобождении от ответственности применительно к точности информации, содержащейся в сертификате, будет приемлемой только в том случае, если подпункты (b) и (c) будут включены в пункт 1.

143. Что касается пункта 2, то, согласно общему мнению, принцип, заключающийся в том, что сертификационный орган должен выполнять обязательства, принятые на себя в заявлении о практике сертификации, должен быть сохранен.

144. С тем чтобы отразить вышеизложенное обсуждение, было внесено следующее предложение о пересмотренном варианте проекта статьи 10:

"В случаях, когда выдается сертификат, считается, что:

a) лицо или учреждение, выдавшие сертификат, выполнили все применимые требования Правил;

[b) в момент выдачи сертификата частный ключ является ключом держателя и соответствует публичному ключу, указанному в сертификате;]

[c) публичный и частный ключи держателя составляют действующую пару ключей;]

d) вся содержащаяся в сертификате информация является точной на момент его выдачи [, если сертификационный орган не указал в сертификате, что точность определенной информации не подтверждается];

e) насколько известно сертификационному органу, в сертификате не упущены никакие существенные факты, которые, если бы они были известны, могли бы отрицательно сказаться на надежности информации в сертификате; и

[f) если сертификационный орган опубликовал заявление о практике сертификации - сертификат был выдан сертификационным органом в соответствии с этим заявлением о практике сертификации".]

145. После обсуждения Рабочая группа просила Секретариат подготовить, с возможными вариантами, пересмотренный проект статьи 10, отражающий вышеизложенное обсуждение.

Статья 11. Договорная ответственность

146. Рабочая группа рассмотрела следующий текст проекта статьи 11:

"1) Во взаимоотношениях между сертификационным органом, выдавшим сертификат, и держателем этого сертификата [или какой-либо иной стороной, находящейся в договорных отношениях с сертификационным органом] права и обязательства сторон определяются достигнутым между ними соглашением.

2) При условии соблюдения статьи 10 сертификационный орган может, по соглашению между сторонами, снять с себя ответственность за любой ущерб, вызванный дефектами информации, указанной в сертификате, техническими ошибками или аналогичными обстоятельствами. Однако на оговорку, ограничивающую или снимающую ответственность сертификационного органа, нельзя ссылаться, если такие снятие или ограничение договорной ответственности будут, учитывая цель договора, в высшей степени несправедливыми.

3) Сертификационный орган не имеет права ограничивать свою ответственность, если будет доказано, что убытки последовали в результате действия или бездействия сертификационного органа, совершенных с намерением причинить ущерб или по грубой неосторожности и при понимании того, что ущерб может быть причинен."

147. Было отмечено, что в пункте 1 воспроизводится принцип автономии сторон в связи с режимом ответственности, применимым к сертификационному органу. Кроме того, было отмечено, что в пункте 2 речь идет об оговорках об освобождении от ответственности, которые в целом объявляются допустимыми при двух исключениях. Первое исключение обусловлено ссылкой на проект статьи 10, в котором устанавливается минимальный стандарт, от которого сертификационные органы не вправе отходить. Второе исключение основывается на Принципах международных коммерческих контрактов МИУЧП (статья 7.1.6) и представляет собой попытку установить единообразный стандарт оценки общей приемлемости оговорок об освобождении от ответственности. Было отмечено также, что в пункте 3 регулируется ситуация, при которой убытки или иной ущерб возникают в результате преднамеренного неправомерного поведения сертификационного органа или его агентов (этот пункт сформулирован на основе статьи 18 Типового закона ЮНСИТРАЛ о международных кредитовых переводах).

148. Сначала Рабочая группа рассмотрела вопрос о том, следует ли сохранить проект статьи 11 в качестве части единообразных правил. В поддержку предложения о его исключении было указано, что в нем рассматриваются вопросы, которые было бы целесообразнее решать на основе договора и применимого права. В частности, было отмечено, что пункт 1 является излишним, поскольку в нем лишь излагается принцип автономии сторон, который уже охвачен в статье 4 Типового закона; а пункты 2 и 3 вступают в коллизию с национальным правом по вопросам, возможность унификации которых проблематична. Кроме того, было отмечено, что предмет проекта статьи 11 достаточно полно охватывается в проекте статьи 10. Хотя решение, состоящее в том, чтобы оставить вопросы договорной ответственности на урегулирование на основании договора и закона, применимого вне рамок единообразных правил, было признано приемлемой альтернативой, возобладало мнение о том, что имеет смысл попытаться достигнуть определенной степени единообразия в урегулировании этого важного предмета.

149. Было внесено несколько предложений относительно возможных путей достижения этого результата. Предлагалось, в частности, сохранить проект статьи 11 в его нынешней формулировке. В поддержку этого предложения было отмечено, что, хотя в пункте 1, как может показаться, излагаются очевидные вещи, в пункте 2 содержится чрезвычайно важный принцип, согласно которому основные обязательства по договору не могут быть сняты с помощью оговорок об освобождении от ответственности. Кроме того, было отмечено, что пункт 3 имеет чрезвычайно важное значение и охватывает не только договорные, но и внедоговорные отношения.

150. Предлагалось также включить в пункт 1 ссылку на недопустимость заключения сторонами соглашений на "в высшей степени несправедливых" условиях и исключить пункты 2 и 3. Хотя предложение об исключении пунктов 2 и 3 получило поддержку, против него были высказаны возражения, в частности, на следующих основаниях: использование формулировки "в высшей степени несправедливые" является неприемлемым, поскольку она неизвестна многим правовым системам; вопрос защиты прав более слабой стороны, на урегулирование которого направлена эта формулировка, должен регулироваться другими законами (например, законом о защите прав потребителей); и исключение пунктов 2 и 3 может непреднамеренно привести к тому, что у сторон появится возможность свести на нет саму суть договора и снять с себя ответственность за преднамеренное неправомерное поведение.

151. Другое связанное с этим предложение заключалось в том, чтобы в пункт 1 после слова "обязательства" добавить формулировку "и любые их ограничения", а в конец этого пункта формулировку "в соответствии с применимым правом", а также исключить пункты 2 и 3. В поддержку этого предложения было заявлено, что такой подход позволит сформулировать приемлемое заявление общего характера, основанное на принципе автономии сторон и применимом праве. Тем не менее было отмечено, что в случае применения такого подхода единообразие не будет достигнуто.

152. Было предложено также заменить проект статьи 11 положением, указывающим, что ответственность сертификационного органа должна определяться на основании стандартов, установленных в заявлении о практике сертификации. Против этого предложения были высказаны

возражения на том основании, что это положение заменит как договорные, так и минимальные стандарты, установленные в проекте статьи 10 в качестве исходной точки для оценки ответственности сертификационного органа. Тем не менее было высказано мнение, что это предложение может обеспечить выработку приемлемого правила для слабозащищенных сертификатов, к которым не будут применяться минимальные стандарты проекта статьи 10.

153. В ходе обсуждения был внесен ряд предложений редакционного характера. Что касается пункта 1, то было отмечено, что содержащаяся в квадратных скобках ссылка на "какую-либо иную сторону" является слишком общей и нечеткой и ее следует заменить ссылкой на "какую-либо доверяющую сторону". Предлагалось также изменить пункт 1, с тем чтобы уточнить, что в нем не ставится цели ограничить урегулирование отношений между сторонами исключительно их соглашением, поскольку такой подход лишит смысла содержащиеся в пунктах 2 и 3 положения об исключении права сторон договариваться об оговорках об освобождении от ответственности. Что касается пункта 2, то было предложено после слова "ущерб" добавить слова "связанный с сертификатом" и исключить остальную часть первого предложения пункта 2.

154. После обсуждения Рабочая группа не смогла достичь согласия относительно конкретной формулировки проекта статьи 11 и поручила Секретариату подготовить альтернативные варианты, отражающие различные высказанные мнения, для рассмотрения на одной из будущих сессий.

Статья 12. Ответственность сертификационного органа перед сторонами, полагающимися на сертификаты

155. Рабочая группа рассмотрела следующий текст проекта статьи 12:

"1) В отсутствие соглашения об обратном, выдающий сертификат сертификационный орган несет ответственность перед любым лицом, разумно полагающимся на сертификат, за:

a) [нарушение гарантии, предусмотренной статьей 10] [небрежность, проявившуюся в неправильном подтверждении достоверности информации, указанной в сертификате];

b) регистрацию аннулирования сертификата сразу же после получения уведомления о его аннулировании; и

c) [последствия неприменения] [небрежность в применении] следующего:

i) любой процедуры, указанной в заявлении о практике сертификации, опубликованном сертификационным органом; или

ii) любой процедуры, предусмотренной применимым законом.

2) Независимо от положений пункта 1) сертификационный орган не несет ответственности, если может доказать, что он или его агенты приняли все необходимые меры для избежания ошибок в сертификате или что ни он, ни его агенты не имели возможности принять такие меры.

3) Независимо от положений пункта 1) сертификационный орган вправе ограничить в сертификате [или каким-либо иным образом] цели, в которых данный сертификат может использоваться. Сертификационный орган не будет считаться ответственным за ущерб, возникший в результате использования данного сертификата в каких-либо иных целях.

4) Независимо от положений пункта 1) сертификационный орган вправе ограничить в сертификате [или каким-либо иным образом] стоимостной объем сделок, по которым данный сертификат будет действительным. Сертификационный орган не будет считаться ответственным

за ущерб, возникший в результате совершения сделок и превышающий установленный предел стоимости."

Общие замечания

156. Была выражена широкая поддержка положению об ответственности сертификационного органа перед сторонами, полагающимися на сертификаты, которое было бы сформулировано по аналогии с проектом статьи 12. Тем не менее многие участники отметили, что сфера действия такого положения должна быть ограничена только теми случаями, когда сертификационный орган гарантирует личность держателя ключа и целостность сообщения данных, подписанного держателем ключа. Такой подход позволил бы облегчить применение некоторых видов практики, при которых требуется обеспечить высокий стандарт надежности, не оказывая при этом отрицательного воздействия на другие виды практики, в которых такие высокие стандарты надежности и ответственности могут быть неуместными.

157. В то же время были выражены определенные сомнения относительно возможности и целесообразности установления специального режима ответственности. Было указано, что установление такого режима ответственности может воспрепятствовать применению различных видов практики сертификации, если это не будет сопровождаться соответствующей количественной оценкой рисков, связанных с предоставлением сертификационных услуг, поскольку сертификационные органы будут сталкиваться с рисками, в отношении которых они не смогут получить страхового покрытия. Кроме того, отмечалось, что такой режим ответственности может оказаться ненужным, поскольку в отсутствие конкретного режима применяются общие принципы деликтного права. Тем не менее было указано, что в некоторых правовых системах, в которых ответственность сертификационных органов специально не регулируется, сертификационные органы в принципе не будут нести ответственности перед доверяющими сторонами. Кроме того, отмечалось, что регулирование таких вопросов в соответствии с применимым правом может оказаться неприемлемым по целому ряду причин, включая следующие: неопределенность, существующая во многих правовых системах, может оказать отрицательное воздействие на развитие электронной торговли; полное отсутствие ответственности может привести к тому, что стороны коммерческих сделок не смогут воспользоваться услугами сертификационных органов; а также тот факт, что в связи с определением применимого права возникает целый ряд весьма сложных вопросов. Что касается той формы, которую следует придать подготовленному документу, то было высказано мнение о том, что применение единообразного режима ответственности может быть более эффективно обеспечено через принятие не типового закона, а конвенции (см. пункт 212 ниже).

158. После обсуждения Рабочая группа постановила, что необходимо предпринять максимальные усилия для урегулирования вопроса об ответственности сертификационных органов перед полагающимися сторонами в рамках единообразных правил, и приступила к подробному рассмотрению проекта статьи 12. Было высказано предложение о том, что в рамках дальнейшего обсуждения проекта статьи 12 Рабочей группе, возможно, следует рассмотреть вопрос о характере и предсказуемости убытков, которые может понести доверяющая сторона.

Пункт 1

Вводная формулировка

159. Были высказаны различные мнения относительно целесообразности сохранения вводной формулировки. Согласно одному мнению, если в проекте статьи 10 будут устанавлены минимальные стандарты, которые должны соблюдаться сертификационным органом, то вступительную формулировку следует исключить. Согласно другому мнению, вводная формулировка является полезной, поскольку она позволяет сторонам согласовать условия своей ответственности, и поэтому ее следует сохранить. В ответ было указано, что стороны не могут согласовывать такие условия, поскольку проект статьи 12 касается деликтной ответственности в тех случаях, когда, как правило, не существует какого-либо соглашения.

В то же время было указано, что доверяющие стороны в рамках замкнутых систем связи обычно будут иметь определенное соглашение с сертификационным органом. Отмечалось также, что условия ответственности, согласованные между сертификационными органами и держателями ключей, могут быть включены в договоры между держателями ключей и доверяющими сторонами.

160. Преобладающее мнение состояло в том, что упомянутые случаи представляют собой исключения и что их урегулирование и не должно наносить ущерба основной цели проекта статьи 12, которая состоит в том, чтобы установить режим деликтной ответственности сертификационных органов перед третьими сторонами. Поэтому дополнительную потребность учесть соглашения об обратном между сертификационными органами и клиентами или доверяющими сторонами, в тех случаях, когда такие соглашения существуют, было предложено отразить путем включения соответствующей формулировки в конце проекта статьи 12.

Подпункты (a)-(c)

161. Было указано, что вторая заключенная в квадратные скобки формулировка в подпунктах (a) и (c), по-видимому, отражает принцип строгой ответственности и поэтому ее следует исключить. Было выражено беспокойство в связи с тем, что использование понятия "неправильное подтверждение" может привести к возникновению неопределенности, поскольку, хотя оно и имеет конкретное значение в некоторых правовых системах, в других правовых системах оно неизвестно. В качестве альтернативной формулировки было предложено использовать слова "неверное заявление".

Пункт 2

162. Были высказаны различные мнения относительно того, следует ли возлагать бремя доказывания небрежности на сертификационный орган или же на доверяющую сторону. Согласно одному мнению, такое бремя доказывания должно быть возложено на доверяющую сторону. Для обоснования этого мнения было указано, что доверяющая сторона может доказать, что была допущена небрежность, поскольку доказательства в отношении соблюдения сертификационным органом стандарта осмотрительности, изложенного в проекте статьи 10, могут быть беспрепятственно получены доверяющей стороной. Кроме того, отмечалось, что возложение бремени доказывания на сертификационный орган будет уместно лишь в том случае, если Рабочая группа будет придерживаться принципа строгой ответственности. Согласно другому мнению, хотя небрежность должна служить основанием для возникновения ответственности, бремя доказывания должно быть возложено на сертификационный орган, поскольку любые соответствующие доказательства будут находиться под контролем сертификационного органа. Было указано, что это имеет место, в частности, в том случае, если сертификат касается не личности держателя ключа, а процедуры, применяемой сертификационным органом для определения личности держателя ключа.

Пункты 3 и 4

163. Была выражена поддержка принципу ограничения ответственности сертификационного органа, который закрепляется в пунктах 3 и 4. Тем не менее было высказано мнение о том, что пределы ответственности следует устанавливать лишь в том случае, если соответствующий режим основан на строгой ответственности сертификационного органа в отличие от режима ответственности, основанного на небрежности.

164. В отношении характера возможных пределов ответственности было указано, что установление пределов в денежном выражении по каждой сделке не будет обеспечивать надлежащей защиты сертификационных органов, особенно в контексте сертификатов личности, поскольку, независимо от пределов ответственности, такие сертификаты могут быть использованы несколько раз в течение весьма короткого срока, без какой-либо возможности установить, были ли превышены пределы ответственности. Поэтому было предложено включить в проект статьи 12 положение о совокупном пределе

ответственности примерно следующего содержания: "Сертификационный орган может указать в сертификате или каким-либо иным образом предел ответственности на срок действия сертификата в отношении всех случаев его применения в объеме совокупной стоимости сертификата. Сертификационный орган не будет считаться ответственным за ущерб, превышающий такой совокупный предел, независимо от количества требований, представленных в отношении такого сертификата". В то же время было высказано мнение о невозможности функционирования совокупных пределов ответственности, поскольку доверяющая сторона, принимая во внимание нынешний уровень развития прикладной технологии, будет не в состоянии узнать, был ли достигнут определенный предел.

Предложения в отношении нового проекта статьи 12

165. Для учета упомянутых выше замечаний были высказаны различные предложения относительно альтернативной формулировки проекта статьи 12. Согласно одному предложению, проект статьи 12 должен гласить следующее:

"1) В том случае, если сертификационный орган выдает сертификат, он несет ответственность перед любым лицом, разумно полагающимся на сертификат, если он проявляет небрежность в результате:

a) представления в сертификате неверной информации;

b) неспособности [представить уведомление или] опубликовать информацию об аннулировании [или приостановлении действия] сертификата сразу же после того, как ему стало известно о необходимости аннулировать сертификат [или приостановить его действие] [; или

c) неспособности выполнить процедуру, предусмотренную в заявлении о практике сертификации, которое было опубликовано сертификационным органом и которое было доведено до сведения полагающегося лица].

2) Сертификационный орган может указать в сертификате [или в каком-либо ином документе] ограничение цели или целей, в которых данный сертификат может использоваться, и сертификационный орган не несет ответственности за ущерб, возникающий в результате использования данного сертификата в каких-либо иных целях.

3) Сертификационный орган может указать в сертификате [или в каком-либо ином документе] предел в отношении стоимости сделок, до которого данный сертификат будет действительным, и сертификационный орган не несет ответственности за ущерб, превышающий такой предел.

[4) Пункт 1 настоящей статьи не применяется, в том случае и в той степени, в которых в соглашении между сертификационным органом и лицом, полагающимся на сертификат, содержатся обратные условия]".

166. Согласно другому предложению, проект статьи 12 необходимо изменить следующим образом:

"1) Если сертификационный орган не докажет, что он или его агенты приняли все разумные меры для избежания ошибок в сертификате, он несет ответственность перед любым лицом, разумно полагающимся на сертификат, выданный этим сертификационным органом, за:

[включить подпункты (a)-(c)]

2) Независимо от пункта 1, доверие к сертификату не является разумным в той мере, в какой оно противоречит информации, содержащейся в сертификате".

167. Хотя к первому предложению был проявлен определенный интерес, Рабочая группа сосредоточила внимание на втором предложении. Было указано, что пункт 1 предназначен для установления ответственности за ошибки в сертификате в соответствии с принципом разумного доверия без каких-либо ссылок на подтверждения и небрежность. Кроме того, отмечалось, что цель пункта 2 состоит в том, чтобы предоставить сертификационному органу право устанавливать в сертификате стандарты, в соответствии с которыми можно оценить, насколько разумно то или иное лицо полагается на сертификат. В порядке разъяснения было указано, что пункт 2 не призван обеспечить исчерпывающего перечня всех ситуаций, в которых доверие к сертификату можно расценить как неразумное. Хотя пункты 1 и 2 были сочтены в целом приемлемыми в качестве основы для дальнейших обсуждений, по ряду вопросов было выражено беспокойство и высказаны предложения.

Новый пункт 1

168. Было, в частности, выражено беспокойство в связи с тем, что на практике сертификационный орган практически не в состоянии принять "все разумные меры" на рентабельной и оперативной основе. В целях устранения оснований для такого беспокойства было внесено несколько предложений. Согласно одному предложению, слово "все" следует заменить словом "коммерчески". В поддержку этого предложения было указано, что ссылка на "коммерчески разумные меры" позволит отразить практически возможные методы в конкретных обстоятельствах. Кроме того, отмечалось, что такая ссылка будет соответствовать терминологии, использованной в других текстах ЮНСИТРАЛ (например, в статье 5(2)(a) Типового закона ЮНСИТРАЛ о международных кредитовых переводах). Против этого предложения были высказаны возражения на том основании, что такая ссылка привнесет неопределенность с учетом того факта, что универсального понимания термина "коммерчески разумный" не существует. Согласно другому предложению, следует просто исключить слово "все". Против этого предложения также были высказаны возражения на том основании, что в результате этого неизбежно произойдет необоснованное занижение стандарта осмотрительности, который должен соблюдаться сертификационным органом. Согласно еще одному предложению, в новом пункте 1 следует использовать формулировку статьи 7(1)(b) Типового закона.

169. Было также выражено беспокойство в связи с тем, что новый пункт 1 не позволяет учесть ошибок, допускаемых сертификационным органом при выдаче сертификата. В целях устранения оснований для такого беспокойства предлагалось включить после слова "сертификате" в новом пункте 1 слова "или при его выдаче". Было указано, что информация, содержащаяся в перечне аннулированных сертификатов (ПАС) или в аналогичном перечне, также должна быть охвачена в новом пункте 2.

170. Было решено заключить подпункт (c) в квадратные скобки до решения вопроса о функции заявления о практике сертификации.

Новый пункт 2

171. В качестве редакционного замечания было предложено исключить вводную формулировку и добавить в начале нового пункта 1 слова "при условии соблюдения пункта 2". Было выражено беспокойство в связи с тем, что новый пункт 2 может непреднамеренно излишне ограничить основания, исходя из которых разумность доверия к сертификату может подвергаться сомнению. Было также выражено беспокойство в связи с тем, что новый пункт 2 может не охватывать ситуацию, при которой на сертификат могут полагаться в рамках сделки с чрезмерно большим стоимостным объемом, поскольку термин "информация" может не охватывать понятие стоимости. В целях устранения оснований для такого беспокойства было предложено перечислить пункты 3 и 4 проекта статьи 12 в качестве примеров ситуаций, при которых доверие к сертификату не будет считаться разумным. В этих же целях предлагалось привести аналогичные примеры, касающиеся, например, ситуаций, при которых сертификационный орган может указать в сертификате, какие упомянутые стороны или виды сторон могут полагаться на такой сертификат. Кроме того, предлагалось лишить сертификационный орган права

полагаться на пределы ответственности, если ущерб причиняется в результате преднамеренного или неосторожного поведения сертификационного органа.

172. Кроме того, было выражено беспокойство в связи с тем, что из-за наличия ссылки на информацию, "содержащуюся" в сертификате, новый пункт 2 может непреднамеренно привести к необоснованному увеличению объема информации, которую необходимо включать в сертификат. В целях устранения оснований для такого беспокойства было предложено разрешить включать такую информацию в сертификат путем ссылки. Против этого предложения были высказаны возражения на том основании, что было бы несправедливо определять права третьих сторон, исходя из условий, включаемых в соглашение между сертификационным органом и держателем ключа, т.е. условий, к которым третьи стороны могут даже не иметь доступа.

173. После обсуждения Рабочая группа постановила изменить формулировку проекта статьи 12 примерно следующим образом:

"1) При условии соблюдения пункта 2, если сертификационный орган не докажет, что он или его агенты приняли [все разумные] [коммерчески разумные] меры [, которые являлись соответствующими цели, для которой был выдан сертификат, с учетом всех обстоятельств] для избежания ошибок в сертификате [или при его выдаче], он несет ответственность перед любым лицом, разумно доверяющим сертификату, выданному этим сертификационным органом, за:

a) ошибки в сертификате; [или]

b) регистрацию аннулирования сертификата сразу же после получения уведомления о его аннулировании [; или

c) последствия неприменения следующего:

i) любой процедуры, указанной в заявлении о практике сертификации, опубликованном сертификационным органом; или

ii) любой процедуры, предусмотренной применимым правом].

2) Доверие к сертификату не является разумным в той мере, в которой оно противоречит информации, содержащейся в сертификате [или включенной в него путем ссылки] [или в перечне аннулирования] [или в информации об аннулировании]. [Доверие не является разумным, в частности, если:

a) оно противоречит цели, для которой выдан сертификат;

b) оно оказано в превышение стоимости, в отношении которой сертификат является действительным; или

c) [...].]"

Было высказано мнение, что проект статьи 12 должен применяться только в отношении сертификационных органов, выдающих сертификаты личности.

Статьи 13-16

174. По причине нехватки времени Рабочая группа отложила рассмотрение проектов статей 13-16 до своей будущей сессии. Была высказана точка зрения о том, что эти проекты статей должны применяться только в отношении сертификационных органов, выдающих сертификаты личности. Согласно другому

мнению, Рабочей группе следует рассмотреть вопрос о том, должны ли единообразные правила применяться только к сертификатам личности или же также и к любым другим видам сертификатов.

РАЗДЕЛ IV. ПРИЗНАНИЕ ИНОСТРАННЫХ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

Статья 17. Иностранные сертификационные органы, предлагающие услуги на основании настоящих Правил

175. Рабочая группа рассмотрела следующий текст проекта статьи 17:

"Вариант A

1) Иностранные [лица] [организации] могут получить местную регистрацию в качестве сертификационных органов либо могут оказывать сертификационные услуги, находясь в другой стране и не получая местную регистрацию, если они удовлетворяют тем же объективным стандартам и следуют тем же процедурам, что и местные организации и лица, имеющие право стать сертификационными органами.

2) Вариант X Правило, изложенное в пункте 1, не применяется к следующему: [...].

Вариант Y Исключения из правила, изложенного в пункте 1, могут быть сделаны в пределах, которые диктуются соображениями национальной безопасности.

Вариант B

... [принимающее государство указывает орган или ведомство, компетентное устанавливать правила в связи с одобрением иностранных сертификатов] управомочен одобрять иностранные сертификаты и устанавливать конкретные правила, касающиеся такого одобрения".

Общие замечания

176. В отношении названия раздела IV было отмечено, что содержащаяся в нем ссылка на признание иностранных электронных подписей является неуместной, поскольку этот раздел касается оказания услуг иностранными сертификационными органами (т.е. проект статьи 17), подтверждения иностранных сертификатов местными сертификационными органами (т.е. проект статьи 18) и признания иностранных сертификатов (т.е. проект статьи 19). Рабочая группа рассмотрела ряд предложений, представленных в целях более четкого отражения в названии раздела рассматриваемого в нем вопроса (например, "трансграничное признание сертификатов", "признание электронных подписей и сертификатов", "признание иностранных сертификационных органов и сертификатов"). Вместе с тем было выражено общее мнение, что рассмотрение соответствующего названия раздела IV следует отложить до тех пор, пока Рабочая группа не проведет детальное обсуждение юридических последствий сертификатов.

177. В отношении двух вариантов, предложенных в проекте статьи 17, было в целом признано, что вариант B, согласно которому определенный указанный орган принимающего государства устанавливает правила одобрения иностранных сертификатов, не является надлежащей основой для разработки единообразных правил. Была достигнута договоренность о том, что вариант B следует исключить и что в ходе обсуждений Рабочей группе следует сосредоточить внимание на варианте A.

Сфера действия проекта статьи 17

178. Было отмечено, что проект статьи 17 преследует две цели: во-первых, признается право иностранного сертификационного органа создать местное предприятие в соответствии с условиями, изложенными в этой статье; во-вторых, иностранным сертификационным органам предоставляется право оказывать услуги в принимающем государстве, не создавая местного предприятия. В такой редакции проект статьи 17 затрагивает вопросы торговой политики, а именно вопрос о том, в какой степени принимающее государство будет отменять ограничения в отношении предприятий иностранных сертификационных органов и оказания услуг иностранными сертификационными органами. Вместо этого предлагалось, чтобы Рабочая группа сосредоточила внимание на разработке типовых положений о юридических последствиях иностранных сертификатов и взаимоотношениях между держателями сертификатов и сертификационными органами. В поддержку этого предложения были высказаны различные мнения. Было, в частности, указано, что вопросы торговой политики входят в компетенцию других форумов и что рассматривать их в проекте единообразных правил было бы нецелесообразно.

179. В ответ на эти мнения было отмечено, что в проекте статьи 17, в котором иностранным организациям разрешается создавать местные предприятия в качестве сертификационного органа, просто излагается принцип, согласно которому иностранные организации, удовлетворяющие установленным для местных сертификационных органов стандартам, не должны подвергаться дискриминации. Этот принцип, как отмечалось, имеет особое значение в отношении сертификационных органов, поскольку такие органы могут функционировать, не создавая при этом физических отделений или другого коммерческого предприятия в той стране, в которой они действуют. Было также отмечено, что в самом Типовом законе рассматривается ряд трансграничных вопросов, которые можно рассматривать как затрагивающее принципы торговой политики.

180. Заслушав различные мнения, Рабочая группа в целях ускорения рассмотрения проекта единообразных правил приступила к обсуждению ряда поправок к проекту статьи 17 без ущерба для оговорок, высказанных по существу проекта статьи 17.

Пункт 1

181. Был задан вопрос о том, касается ли пункт 1 только признания сертификационных органов, которые действуют в соответствии с разрешением, выданным органом или правительственным ведомством иностранного государства. В ответ на этот вопрос было отмечено, что пункт 1 в существующей редакции

не касается вопроса о том, требуется ли сертификационному органу правительственное разрешение в иностранном государстве. Вместе с тем было также высказано мнение, что положение, подобное проекту статьи 17, должно основываться на режиме лицензирования в соответствии с законодательными требованиями.

182. Было высказано мнение, что некоторые проблемы, возникшие в связи с пунктом 1, обусловлены тем, что в этом положении, как представляется, чрезмерное внимание уделяется не способности сертификационного органа выдавать сертификаты, которые будут использоваться в принимающем государстве, а признанию самого сертификационного органа. Кроме того, слова "удовлетворяют тем же объективным стандартам и следуют тем же процедурам, что и местные организации и лица, имеющие право стать сертификационными органами" могут стать препятствием для применения новых технологий, поскольку это положение может быть истолковано как основание для отказа в признании иностранных сертификационных органов, которые применяют процедуры, являющиеся технически более совершенными, чем процедуры, используемые в принимающем государстве. Было отмечено, что вместо существующей формулировки было бы целесообразно сделать ссылку на "объективные требования", которым должны удовлетворять сертификационные органы в принимающем государстве. В качестве альтернативы было предложено заключить слова "и следуют тем же процедурам" в квадратные скобки.

183. В отношении условий, которым должен удовлетворять иностранный сертификационный орган, было отмечено, что цель проекта пункта 1 заключается в обеспечении того, чтобы эти условия были по существу такими же, как и условия, установленные для национальных сертификационных органов. Поэтому было предложено изменить формулировку пункта 1 таким образом, чтобы признание иностранных сертификационных органов регулировалось законами принимающего государства. Вопросы, связанные с определением стандартов, которым должен удовлетворять иностранный сертификационный орган, могут быть рассмотрены Рабочей группой на более позднем этапе. Кроме того, такая поправка позволит более четко указать, что в отношении такого признания будут действовать также любые исключения в принимающем государстве, что устранит необходимость в любом из вариантов пункта 1. Формулировка предлагаемого текста была следующей:

> "В соответствии с законодательством принимающего государства иностранное [лицо] [организация] может:
>
> a) создать местное предприятие в качестве сертификационного органа; или
>
> b) оказывать сертификационные услуги, не создавая местного предприятия, если [оно] [она] удовлетворяет тем же объективным стандартам и следует тем же процедурам, что и местные организации и лица, имеющие право стать сертификационными органами".

184. В ответ на это предложение было отмечено, что ссылка на внутреннее законодательство не является удовлетворительным решением, поскольку законы принимающего государства могут содержать дискриминационные положения, которые могут противоречить духу проекта статьи 17. Кроме того, в связи с предлагаемой поправкой возникают вопросы о том, кто в принимающем государстве будет определять, что иностранный сертификационный орган удовлетворяет тем же объективным стандартам и следует тем же процедурам, что и местные организации и лица, и каким образом это будет определяться.

185. Было высказано мнение, что существующая формулировка пункта 1 может означать, что иностранным сертификационным органам необходимо не только получить разрешение в соответствии с собственным законодательством, но и необходимо также выполнить требования принимающего государства. Было отмечено, что такое правило может иметь нежелательные ограничительные последствия и не будет содействовать развитию электронной торговли. В связи с последним замечанием было предложено уточнить смысл пункта 1, сформулировав его в виде недискриминационного правила примерно следующего содержания:

"1) Иностранным [лицам] [организациям] не может быть отказано в праве на создание местного предприятия или на оказание сертификационных услуг лишь на том основании, что они являются иностранными, если они удовлетворяют тем же объективным стандартам и следуют тем же процедурам, что и местные организации и лица, имеющие право стать сертификационными органами".

186. Против этого предложения были высказаны возражения по той причине, что в связи с предлагаемым правилом недискриминации возникают такие же общие основания для беспокойства, на которые было указано в общих замечаниях в отношении сферы действия проекта статьи 17 (см. пункты 178-180 выше).

187. Рассмотрев различные предложения и приняв во внимание различные высказанные мнения, Рабочая группа отметила, что требуется дополнительное время для проведения консультаций по вопросам, рассматриваемым в проекте статьи 17. Секретариату было предложено представить пересмотренный проект статьи 17 с возможными вариантами, отражающими результаты вышеизложенных обсуждений, для рассмотрения Рабочей группой на более позднем этапе.

Пункт 2

188. В связи с двумя предлагаемыми вариантами исключений в пункте 2, было высказано мнение, что вариант X следует исключить, поскольку он может послужить открытым механизмом ограничения сферы действия пункта 1. Согласно этому мнению, если и допускать какие-либо исключения, они должны быть обусловлены только соображениями национальной безопасности, как это предусматривается в варианте Y. Вместе с тем было отдано общее предпочтение сохранению варианта X, в соответствии с которым принимающее государство вправе формулировать любые исключения из общего правила пункта 1. Хотя вариант Y позволяет ограничить возможные исключения только теми исключениями, которые обусловлены соображениями национальной безопасности, было высказано мнение, что государства, возможно, пожелают включить в свое законодательство другие возможные основания для исключений, обусловленные соображениями публичного порядка. После обсуждения было решено оставить для дальнейшего рассмотрения оба варианта X и Y, заключив их в квадратные скобки.

Статья 18. Подтверждение иностранных сертификатов местными сертификационными органами

189. Рабочая группа рассмотрела следующий текст проекта статьи 18:

"Сертификаты, выданные иностранными сертификационными органами, могут использоваться для подписей в цифровой форме на тех же условиях, что и сертификаты, подпадающие под действие настоящих Правил, если они признаются сертификационным органом, функционирующим на основании... [закона принимающего государства], и этот сертификационный орган гарантирует - в той же мере, что и в отношении своих собственных сертификатов - правильность содержащейся в сертификате информации, а также его действительность и законную силу".

190. В качестве общего замечания было отмечено, что значительным шагом по пути укрепления доверия к сертификатам является включение положений, касающихся вопросов их трансграничного признания. Было указано, что сертификаты все шире используются в коммерческой практике и что доверие к новой технологии можно укрепить путем принятия международных стандартов. Рабочей группе было предложено рассмотреть международные механизмы для аккредитации сертификационных органов, действующих в соответствии с международными стандартами. Была высказана поддержка предложению включить предлагаемую тему в число других вопросов для обсуждения Рабочей группой на более позднем этапе. Вместе с тем было отмечено, что предлагаемая тема касается не только

вопросов, поднятых в проекте статьи 18, и что Рабочая группа может ее рассмотреть, например, при возобновлении обсуждения вопроса о регистрации сертификатов.

191. Что касается проекта статьи 18, то было отмечено, что цель содержащегося в нем правила заключается лишь в том, чтобы предоставить возможность национальному сертификационному органу гарантировать правильность атрибутов иностранного сертификата в тех же пределах, что и для своих собственных сертификатов, а также гарантировать, что иностранный сертификат является действительным и что срок его действия не истек. В соответствии с проектом статьи 18 ответственность в случае порока иностранного сертификата налагается на национальный сертификационный орган, предоставивший такую гарантию. Однако наличие гарантии, предоставляемой на основании проекта статьи 18, не является обязательным условием для признания сертификатов, выдаваемых иностранными сертификационными органами, удовлетворяющими в других отношениях условиям, изложенным в проекте статьи 19. В связи с тем, что положение о гарантии, предусмотренное в проекте статьи 18, носит лишь добровольный характер, было предложено исключить из текста проект статьи 18, поскольку в нем нет необходимости. Далее было высказано предложение, что в единообразных правилах решение вопроса о том, могут ли, и если да, то на каких условиях, национальные сертификационные органы предоставлять такую гарантию в отношении сертификатов, выданных иностранными сертификационными органами, должно быть оставлено на усмотрение принимающего государства. Ссылку на выдачу таких гарантий, которые предусматриваются в проекте статьи 18, можно было бы сделать в руководстве по принятию единообразных правил или в прилагаемых к нему пояснительных примечаниях в зависимости от характера документа, который в конечном итоге будет принят.

192. Рабочей группе было сделано напоминание о том, что ранее на тридцать первой сессии обсуждались различные уровни доверия, которые мог бы обеспечить национальный сертификационный орган в отношении иностранного органа. Было отмечено, что эти уровни могут варьироваться от самого высшего, при котором национальный сертификационный орган по просьбе стороны, полагающейся на иностранный сертификат, гарантирует содержание этого сертификата исходя из объявленного им знания процедур, предшествовавших выдаче данного сертификата, и принимает тем самым на себя полную ответственность за любые содержащиеся в сертификате ошибки или иные пороки, до самого низшего уровня доверия, при котором национальный сертификационный орган лишь гарантирует личность иностранного сертификационного органа на основании проверки его публичного ключа и цифровой подписи (см. A/CN.9/437, пункты 81-82). Было указано, что эти различные уровни доверия не отражены должным образом в проекте статьи 18 и что, если это положение будет сохранено, четко следует указать, что оно не исключает других вариантов помимо предоставления полной гарантии в отношении правильности и действительности сертификата, выданного иностранным сертификационным органом.

193. В ответ на эти замечания было заявлено, что проект статьи 18 выполняет полезную роль, поскольку он допускает обращение и трансграничное использование сертификатов без необходимости в двусторонних или многосторонних международных соглашениях о признании сертификатов, которые, по мнению некоторых государств, возможно, потребуются для того, чтобы предоставить признание на основании проекта статьи 19. Кроме того, ввиду принятого Рабочей группой решения рассмотреть в единообразных правилах не только сертификационные органы, получившие лицензию от государственных структур, но и сертификационные органы, функционирующие вне рамок государственной системы лицензирования (см. A/CN.9/437, пункты 48-50), проект статьи 18 имеет дополнительное преимущество, поскольку он допускает принятие коммерческого решения в тех ситуациях, когда признание на основании положений проекта статьи 19 не может быть получено автоматически. В этой связи было предложено уточнить сферу действия проекта статьи 18, изменив его формулировку примерно следующим образом:

> "Сертификаты, выданные иностранными сертификационными органами, могут использоваться для подписей в цифровой форме на тех же условиях, что и сертификаты, подпадающие под действие настоящих Правил, если в их отношении сертификационным органом, функционирующим на основании ... [закон принимающего государства], выдана соответствующая гарантия".

194. Было высказано мнение в поддержку сохранения в единообразных правилах положения, в соответствии с которым национальный сертификационный орган уполномочивается предоставлять гарантии в связи с сертификатами, выдаваемыми иностранными сертификационными органами. Такое положение может основываться на проекте статьи 18 и учитывать предложения, внесенные в Рабочей группе. Вместе с тем было заявлено, что нынешнее место проекта статьи 18 в главе IV является неправильным, поскольку в этом положении не идет речи о признании сертификатов, выдаваемых за рубежом.

195. После обсуждения Рабочая группа приняла решение сохранить проект статьи 18 в квадратных скобках, с предложенными поправками, и предложила Секретариату подготовить с учетом высказанных мнений альтернативные варианты этого положения для дальнейшего рассмотрения Рабочей группой.

Статья 19. Признание иностранных сертификатов

196. Рабочая группа рассмотрела следующий текст проекта статьи 19:

"1) Сертификаты, выданные иностранным сертификационным органом, признаются имеющими такую же юридическую силу, что и сертификаты, выданные сертификационными органами, функционирующими на основании... [закона принимающего государства], если практика иностранного сертификационного органа обеспечивает степень надежности, по меньшей мере эквивалентную той, которая требуется от сертификационных органов в соответствии с настоящими Правилами. [Такое признание может быть осуществлено путем опубликования соответствующего государственного решения либо путем заключения двустороннего или многостороннего соглашения между заинтересованными государствами.]

2) Подписи и записи, соответствующие законам другого государства в отношении подписей в цифровой форме и других электронных подписей, признаются имеющими такую же юридическую силу, что и подписи и записи, соответствующие настоящим Правилам, если законы этого другого государства требуют степени надежности, по меньшей мере эквивалентной той, которая требуется от подобных записей и подписей согласно... [праву принимающего государства]. [Такое признание может быть осуществлено путем опубликования соответствующего государственного решения либо путем заключения двустороннего или многостороннего соглашения с другими государствами.]

3) За подписями в цифровой форме, проверяемыми путем сверки с сертификатом, выданным иностранным сертификационным органом, [суды и другие органы, занимающиеся установлением фактов] должны признавать юридическую силу в том случае, если такой сертификат является, с учетом всех обстоятельств, надежным в той мере, насколько это требуется для цели, для которой он был выдан.

4) Независимо от положений предыдущего пункта правительственные ведомства могут указать [путем публикации], что в оформлении представляемых этим ведомствам подписей должны участвовать какой-либо конкретный сертификационный орган, определенная категория сертификационных органов или категория сертификатов".

Пункты 1 и 2

197. Было отмечено, что в пунктах 1 и 2 рассматриваются возможности для установления степени надежности иностранных сертификатов и подписей до совершения какой-либо сделки (и до возникновения какого-либо спора относительно степени надежности подписи). С этой целью в пунктах 1 и 2 сформулированы критерии, которые могут применяться в принимающем государстве в целях признания сертификатов, выдаваемых иностранными сертификационными органами, а также подписей и записей, отвечающих требованиям закона другого государства.

198. Были подняты различные вопросы относительно объема признания на основании положений пунктов 1 и 2. Что касается пункта 1, то было высказано мнение, что понятие юридической эквивалентности сертификатов, выдаваемых иностранными сертификационными органами, и сертификатов, выдаваемых сертификационными органами, функционирующими на основании правил принимающего государства, не является достаточно четким. Было указано, что термин "признание", как он обычно используется в частном международном праве, означает признание правовых последствий актов, совершенных в рамках другой юрисдикции. Однако это понятие не может быть применено в контексте пункта 1, поскольку сертификат представляет собой содержащий констатацию фактов документ, который выполняет лишь функцию декларирования. Кроме того, как в пункте 1, так и в пункте 2 подразумевается, что принимающее государство должно применять свои собственные законы для установления степени надежности сертификатов, выдаваемых иностранными сертификационными органами, а также подписи и записей, отвечающих требованиям закона другого государства. В этой связи было заявлено, что пункты 1 и 2 не соответствуют общим принципам частного международного права, согласно которым действительность актов, совершенных за рубежом, должна устанавливаться в соответствии с применимым правом той правовой системы, в которой они были совершены. В качестве добавления было указано, что статья 5 Типового закона и проекты статей 3 и 5 единообразных правил уже предусматривают нормы для атрибуции сообщений данных и для установления степени надежности электронной подписи.

199. В ответ на эти замечания было указано, что пункты 1 и 2 выполняют полезную функцию применительно к тем национальным режимам регулирования, которые для осуществления определенных сделок требуют использования определенных классов сертификатов, обеспечивающих высокую степень надежности. В принимающих государствах, имеющих подобные режимы регулирования, пункт 1 предусматривает минимальные стандарты для признания выдаваемых иностранными сертификационными органами сертификатов, которые используются в связи с осуществлением иных сделок чем те, в отношении которых требуется специальный класс сертификатов. Аналогичным образом в пункте 2 для этих принимающих государств устанавливается субсидиарное правило, в соответствии с которым создается презумпция действительности подписей и записей, которые отвечают требованиям закона другого государства и которые, как это сочтено, обеспечивают разумную степень надежности для всех тех ситуаций, когда на основании законов принимающего государства не предписывается соблюдения более жестких требований. К Рабочей группе был обращен настоятельный призыв не оставлять вопрос о минимальных стандартах, которые применяются к иностранному сертификату, на урегулирование исключительно в соответствии с нормами коллизионного права принимающего государства.

200. Рабочая группа обсудила возможные поправки к пунктам 1 и 2 в целях устранения оснований для выраженного беспокойства. Было, в частности, предложено объединить пункты 1 и 2 и сформулировать правило недискриминации примерно следующим образом:

> "Сертификаты, выдаваемые иностранными сертификационными органами, не могут быть лишены такого же признания, как и сертификаты, выдаваемые внутренними сертификационными органами, на том основании, что они были выданы иностранными сертификационными органами".

201. Тем не менее в отношении предложенной формулировки, составленной в отрицательной форме, были высказаны возражения, поскольку она не устанавливает стандартов, на основе которых должно предоставляться признание. Кроме того, отмечалось, что в отношении предлагаемого правила недискриминации могут быть высказаны такие же оговорки, как и в отношении проекта статьи 17 (см. пункты 185-186 выше).

202. После обсуждения было высказано общее мнение о том, что было бы желательно сформулировать материально-правовую норму, в которой будет указан метод установления степени надежности иностранных сертификатов и подписей до заключения какой-либо сделки. Секретариату было предложено подготовить с учетом высказанных мнений пересмотренный текст пунктов 1 и 2, включая текст, объединяющий оба пункта, с возможными вариантами.

Пункт 3

203. Было указано, что цель пункта 3 состоит в установлении стандарта для оценки иностранных подписей и сертификатов, если их надежность не была предварительно определена. В то же время отмечалось, что это положение в его существующей формулировке может оказаться ненужным, поскольку в нем лишь подтверждается принцип, в соответствии с которым в случае возникновения спора относительно аутентичности подписи и надежности сертификата, выданного иностранным сертификационным органом, суды принимающего государства должны признать за этой подписью или сертификатом такую доказательственную силу, которая будет сочтена надлежащей в соответствующих обстоятельствах.

204. В ответ на эти замечания было указано, что пункт 3, который основывается на статье 7 Типового закона, обеспечивает полезные руководящие принципы для судов принимающего государства в отношении оценки надежности иностранного сертификата. Этот важный принцип желательно вновь подтвердить в единообразных правилах с учетом того факта, что государство, принимающее единообразные правила, может не включить статью 7 Типового закона в свое внутреннее законодательство. Для более четкого изложения цели пункта 3 было предложено изменить его формулировку примерно следующим образом:

> "Подписи в цифровой форме, проверяемые путем сверки с сертификатом, выданным иностранным сертификационным органом, не могут быть лишены признания юридической силы [судами и другими органами, занимающимися установлением фактов], если такой сертификат является, с учетом всех обстоятельств, как надежным, так и соответствующим цели, для которой был выдан сертификат".

205. После обсуждения Рабочая группа постановила сохранить положения пункта 3 для дальнейшего рассмотрения Рабочей группой на более позднем этапе.

Пункт 4

206. Были подняты вопросы, касающиеся необходимости такого положения, как пункт 4, в котором за правительственными ведомствами сохраняется право определять процедуры, которые должны использоваться при поддержании с ними связи при помощи электронных средств. С одной стороны, было выражено беспокойство в связи с тем, что пункт 4 может вызвать нежелательные ограничительные последствия и может быть истолкован таким образом, что лица и организации, иные чем правительственные ведомства, не имеют права выбирать какой-либо конкретный сертификационный орган, определенную категорию сертификационных органов или категорию сертификатов, которые они хотели бы использовать в связи с получаемыми ими сообщениями или подписями. Было указано, что подобная ситуация противоречила бы принципу автономии сторон, закрепленному в различных положениях Типового закона. С другой стороны, если цель пункта 4 состоит в установлении особой прерогативы правительственных ведомств, то это положение нуждается в дополнительном уточнении, поскольку его можно толковать таким образом, что в отсутствие четкого указания со стороны правительственного ведомства на какой-либо конкретный сертификационный орган, определенную категорию сертификационных органов или категорию сертификатов, которые оно желает использовать в связи с получаемыми им сообщениями или подписями, такое правительственное ведомство обязано признать любую категорию сертификационных органов или сертификатов.

207. Было высказано общее мнение о том, что не только за правительственными ведомствами, но также и за сторонами коммерческих и других сделок следует признать право выбирать конкретный сертификационный орган, определенную категорию сертификационных органов или категорию сертификатов, которые они желают использовать в связи с получаемыми ими сообщениями или подписями. Рабочая группа просила Секретариат изменить формулировку пункта 4, с тем чтобы отразить

это понимание, и постановила рассмотреть вопрос о надлежащем месте этого пересмотренного положения в тексте единообразных правил, на более позднем этапе.

IV. КООРДИНАЦИЯ РАБОТЫ

208. Рабочая группа заслушала сообщения о работе, проводимой в области электронной торговли Организацией Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО) и Конференцией Организации Объединенных Наций по торговле и развитию (ЮНКТАД).

209. Было указано, что на двадцать девятой сессии Генеральной конференции ЮНЕСКО получила мандат в отношении разработки международно-правового документа, касающегося использования кибернетического пространства. В связи с этим было высказано мнение о том, что ЮНЕСКО и ЮНСИТРАЛ следует объединить усилия в области электронной торговли. Было указано, что такие усилия должны определяться необходимостью содействовать развитию электронной торговли таким образом, чтобы это приносило выгоды как развитым, так и развивающимся странам и чтобы одновременно гарантировались основные права человека, включая право на частную жизнь. Было особо указано на необходимость сосредоточения внимания Рабочей группы в ее работе в связи с подписями в цифровой форме и другими электронными подписями на вопросах атрибуции сообщений данных их составителям, целостности сообщений данных и отчетности сторон, участвующих в электронной торговле.

210. В сообщении о деятельности ЮНКТАД было указано, что в целях оказания помощи развивающимся странам, стремящимся получить выгоды от новых достижений в области электронной связи, была создана Глобальная сеть торговых точек. Кроме того, было объявлено о том, что в настоящее время ЮНКТАД организует выставку, в которой будут участвовать изготовители оборудования, производители программного обеспечения и поставщики услуг в области электронной торговли (Лион, 8-13 ноября 1998 года). Было указано, что в ходе этой выставки будут организованы показы средств и оборудования по широкому кругу вопросов, касающихся электронной торговли.

211. Рабочая группа приняла к сведению эти сообщения и выразила благодарность заинтересованным организациям за участие в ее работе. Секретариату было предложено продолжить работу по наблюдению за деятельностью других международных организаций в области правовых аспектов электронной торговли и представить Рабочей группе доклад о результатах такой деятельности.

V. БУДУЩАЯ РАБОТА

212. При закрытии сессии было внесено предложение о том, что Рабочая группа, возможно, пожелает рассмотреть в предварительном порядке вопрос о проведении работы по подготовке международной конвенции, основанной на положениях Типового закона и единообразных правил. Было решено, что этот вопрос, возможно, необходимо будет рассмотреть в рамках отдельного пункта повестки дня на следующей сессии Рабочей группы на основе более подробных предложений, которые, возможно, будут представлены заинтересованными делегациями. Тем не менее предварительный вывод Рабочей группы состоял в том, что подготовку конвенции следует в любом случае рассматривать в качестве отдельного проекта по отношению к подготовке единообразных правил и любых других возможных дополнений к Типовому закону. До принятия какого-либо окончательного решения относительно формы единообразных правил предложение относительно подготовки конвенции на более позднем этапе не должно отвлекать внимание Рабочей группы от ее текущей задачи, которая состоит в том, чтобы сосредоточить внимание на подготовке проекта единообразных правил о подписях в цифровой форме и других электронных подписях, а также от реализации решения, согласно которому Рабочая группа исходит в рабочем порядке из предположения о том, что единообразные правила будут подготовлены в форме проекта законодательных положений. Было высказано общее мнение о том, что возможность подготовки проекта конвенции не следует использовать в качестве повода для возобновления рассмотрения вопросов, урегулированных в Типовом законе, поскольку это может оказать отрицательное воздействие на процесс расширения использования этого уже весьма успешного документа.

213. Было указано, что следующую сессию Рабочей группы планируется провести в Нью-Йорке с 29 июня по 10 июля 1998 года и что эти сроки должны быть подтверждены Комиссией на ее тридцать первой сессии (Нью-Йорк, 1-12 июня 1998 года).

Примечания

[1]Официальные отчеты Генеральной Ассамблеи, пятьдесят первая сессия, Дополнение № 17 (A/51/17), пункты 223-224.

[2]Там же, пятьдесят вторая сессия, Дополнение № 17 (A/52/17), пункты 249-251.