**ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ**

**A**

**Генеральная Ассамблея**

Distr.
GENERAL

A/CN.9/437
12 March 1997

RUSSIAN
Original: ENGLISH

КОМИССИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ
ПО ПРАВУ МЕЖДУНАРОДНОЙ ТОРГОВЛИ
Тридцатая сессия
Вена, 12-30 мая 1997 года

# ДОКЛАД РАБОЧЕЙ ГРУППЫ ПО ЭЛЕКТРОННОМУ ОБМЕНУ ДАННЫМИ О РАБОТЕ ЕЕ ТРИДЦАТЬ ПЕРВОЙ СЕССИИ (Нью-Йорк, 18-28 февраля 1997 года)

СОДЕРЖАНИЕ


| | | Пункты | Страница |
|---|---|---|---|
| ВВЕДЕНИЕ | | 1-15 | 2 |
| I. | ХОД РАБОТЫ И РЕШЕНИЯ | 16 | 4 |
| II. | ПРАВОВЫЕ ВОПРОСЫ И ВОЗМОЖНЫЕ ПОЛОЖЕНИЯ ДЛЯ ВКЛЮЧЕНИЯ В ЕДИНООБРАЗНЫЕ ПРАВИЛА В ОТНОШЕНИИ ПОДПИСЕЙ В ЦИФРОВОЙ ФОРМЕ | 17-150 | 5 |
| | A. Общие замечания | 17-24 | 5 |
| | B. Конкретные правовые вопросы и проекты положений, касающиеся подписей в цифровой форме | 25-150 | 7 |
| | 1. Определения | 29-50 | 8 |
| | a) Подписи в цифровой форме | 30-38 | 8 |
| | b) Уполномоченные сертификационные органы | 39-50 | 10 |
| | 2. Ответственность | 51-73 | 14 |
| | 3. Вопросы трансграничной сертификации | 74-89 | 20 |
| | 1. Определения (продолжение) | 90-113 | 24 |
| | b) Уполномоченные сертификационные органы (продолжение) | 90-97 | 24 |
| | c) Сертификаты | 98-113 | 26 |
| | 4. Подписи, проставляемые физическими и юридическими лицами | 114-117 | 30 |
| | 5. Атрибуция сообщений, подписанных в цифровой форме | 118-124 | 31 |
| | 6. Аннулирование сертификатов | 125-139 | 32 |
| | 7. Регистр сертификатов | 140-148 | 35 |
| | 8. Отношения между пользователями и сертификационным органом | 149-150 | 37 |
| III. | ВКЛЮЧЕНИЕ ПУТЕМ ССЫЛКИ | 151-155 | 38 |
| IV. | БУДУЩАЯ РАБОТА | 156-157 | 39 |


V.97-21492

## ВВЕДЕНИЕ

1. После принятия Типового закона ЮНСИТРАЛ об электронной торговле (далее в тексте - "Типовой закон") Комиссия на своей двадцать девятой сессии (1996 год) приступила к рассмотрению будущей работы в области электронной торговли на основе предварительного обсуждения, проведенного Рабочей группой по электронному обмену данными на ее тридцатой сессии (A/CN.9/421, пункты 109-119). Было достигнуто общее согласие в отношении того, что ЮНСИТРАЛ должна продолжать свою работу по разработке правовых норм, которые могли бы внести предсказуемость в область электронной торговли и тем самым активизировать торговлю во всех регионах.

2. Были высказаны новые предложения в отношении возможных тем и приоритетных направлений будущей работы. Одно из предложений заключалось в том, что Комиссии следует приступить к разработке правил, касающихся подписей в цифровой форме. Было отмечено, что принятие законов о подписях в цифровой форме вместе с законами, признающими действия "заверяющих органов" (далее именуемых "сертификационными органами") или иных лиц, уполномоченных выдавать электронные сертификаты или иные формы гарантий в отношении происхождения или атрибуции сообщений данных, "подписанных" в цифровой форме, рассматривается во многих странах как необходимое условие для развития электронной торговли. Было отмечено, что возможность полагаться на подписи в цифровой форме будет одним из ключевых факторов, способствующих увеличению числа заключенных контрактов, а также возможности передавать права на товары или другие вещные права при помощи электронных средств. В ряде стран в настоящее время готовятся новые законы, регулирующие вопросы подписи в цифровой форме. Было отмечено, что в этой сфере развития законодательства уже сейчас нет единообразия. Если Комиссия решит заняться работой в этой области, она будет иметь возможность унифицировать новые законы или по крайней мере установить общие принципы в области электронной подписи и тем самым обеспечить международную инфраструктуру для такой коммерческой деятельности.

3. Это предложение получило значительную поддержку. Однако было высказано общее мнение, что, если Комиссия решит заняться работой в области подписей в цифровой форме через свою Рабочую группу по электронному обмену данными, она должна установить для этой группы четкий мандат. Также было высказано мнение, что, поскольку ЮНСИТРАЛ не может взяться за подготовку технических стандартов, необходимо позаботиться о том, чтобы она не оказалась вовлеченной в технические аспекты вопроса о подписях в цифровой форме. Было отмечено, что, как признала Рабочая группа на своей тридцатой сессии, возможно, потребуется провести работу по вопросам, связанным с сертификационными органами, и что такую работу необходимо будет, вероятно, проводить в контексте рассмотрения регистров и поставщиков услуг. Однако Рабочая группа также сочла, что ей не следует заниматься рассмотрением каких-либо технических аспектов вопроса о приемлемости использования того или иного конкретного стандарта (там же, пункт 111). Была высказана обеспокоенность в отношении того, что работа по подписям в цифровой форме может выйти за рамки торгового права и затронуть общие вопросы гражданского и административного права. В ответ на это было указано, что то же самое относится и к положениям Типового закона и что Комиссия не должна уклоняться от разработки полезных правил по той причине, что такие правила могут также оказаться полезными за пределами сферы торговых отношений.

4. Другое предложение, выдвинутое на основе результатов предварительного обсуждения, проведенного в Рабочей группе, заключалось в том, что будущая работа должна быть сконцентрирована на поставщиках услуг. В качестве вопросов, которые могут быть затронуты при обсуждении проблем, связанных с поставщиками услуг, были упомянуты следующие: минимальные стандарты, которые должны соблюдаться в отсутствие договоренности сторон; объем риска, который принимают на себя "конечные" стороны; последствия таких правил или соглашений для третьих сторон; распределение рисков, сопряженных с неправомерным вторжением в операции или иными несанкционированными действиями; и объем обязательных гарантий, если таковые предусматриваются, или иных обязательств при предоставлении платных услуг (там же, пункт 116).

5. Было высказано общее мнение о том, что ЮНСИТРАЛ было бы целесообразно проанализировать отношения между поставщиками услуг, пользователями и третьими сторонами. Было отмечено, что весьма важно направить такие усилия на разработку международных норм и стандартов коммерческого поведения в этой области в целях оказания содействия развитию торговли с помощью электронных средств, а не ставить перед собой задачу установить режим, регламентирующий деятельность поставщиков услуг, или другие правила, которые могли бы повлечь за собой расходы, неприемлемые для рыночного применения электронного обмена данными (ЭДИ) (там же, пункт 117). Вместе с тем было выражено мнение, что тема поставщиков услуг может оказаться слишком широкой и охватывать слишком много совершенно отличных друг от друга фактических ситуаций, чтобы ее можно было рассматривать как одно направление деятельности. В целом было решено, что вопросы, относящиеся к поставщикам услуг, уместно было бы рассматривать в контексте каждой новой области деятельности, которой будет заниматься Рабочая группа.

6. Еще одно предложение заключалось в том, чтобы Комиссия приступила к подготовке новых общих правил, необходимых для разъяснения того, как традиционные договорные функции могут выполняться через посредство электронной торговли. Как было отмечено, существует большая неопределенность в отношении того, что означают термины "исполнение", "поставка" и другие в контексте электронной торговли, когда оферта, акцепт и поставка товаров могут осуществляться через открытые компьютерные сети по всему миру. Быстрый рост компьютеризированной торговли, а также числа сделок через "Интернет" и другие системы обусловил первостепенное значение этой темы. Была высказана мысль о том, что проведение Секретариатом исследования по этой теме могло бы внести ясность в вопрос о масштабах такой работы. Если Комиссия после изучения такого исследования решит продолжать свою работу, одним из вариантов могло бы быть включение таких правил в раздел "Специальные положения" Типового закона.

7. Еще одно предложение состояло в том, чтобы Комиссия сосредоточила свое внимание на вопросе включения путем ссылки. Было напомнено о принятом Рабочей группой решении о том, что эту тему было бы целесообразно рассмотреть в контексте более общей работы над вопросами регистров и поставщиков услуг (там же, пункт 114). Комиссия достигла общей договоренности о том, что этим вопросом можно заняться в контексте работы над вопросами сертификационных органов.

8. После обсуждения Комиссия признала уместность включения вопроса о подписях в цифровой форме и сертификационных органах в повестку дня Комиссии при условии, что это даст возможность заняться и другими темами, предложенными Рабочей группой для будущей работы. Что касается более четкого мандата Рабочей группы, то было также принято решение о том, что единообразные правила, которые планируется подготовить, должны охватывать такие вопросы, как правовая база процессов сертификации, включая новейшую технологию удостоверения подлинности и сертификации в цифровой форме; применимость процесса сертификации; распределение риска и ответственности пользователей, поставщиков услуг и третьих сторон в контексте использования методов сертификации; конкретные вопросы сертификации на основе применения регистров; и включение путем ссылки.

9. Комиссия просила Секретариат подготовить справочное исследование по вопросам подписей в цифровой форме и поставщиков услуг на основе анализа законов, которые готовятся сейчас в различных странах. На базе этого исследования Рабочая группа должна рассмотреть желательность и целесообразность подготовки единообразных правил по вышеупомянутым темам. Было решено, что работа, которая должна быть проведена Рабочей группой на ее тридцать первой сессии, может охватывать подготовку проектов правил по определенным аспектам вышеуказанных тем. Рабочей группе было предложено представить Комиссии достаточную информацию для принятия обоснованного решения в отношении сферы применения единообразных правил, которые будут разрабатываться. Ввиду широкого круга вопросов, охватываемых Типовым законом и возможной будущей работой в области электронной

торговли, было решено переименовать Рабочую группу по электронному обмену данными в Рабочую группу по электронной торговле[1].

10. Рабочая группа по электронной торговле, в состав которой входят все государства - члены Комиссии, провела свою тридцать первую сессию в Нью-Йорке с 18 по 28 февраля 1997 года. В работе сессии приняли участие представители следующих государств - членов Рабочей группы: Австралии, Австрии, Аргентины, Болгарии, Венгрии, Германии, Египта, Индии, Ирана (Исламской Республики), Испании, Италии, Кении, Китая, Мексики, Польши, Российской Федерации, Сингапура, Словакии, Соединенного Королевства Великобритании и Северной Ирландии, Соединенных Штатов Америки, Таиланда, Уганды, Финляндии, Франции и Японии.

11. В работе сессии приняли участие наблюдатели от следующих государств: Габона, Дании, Индонезии, Ирландии, Канады, Колумбии, Кувейта, Мавритании, Монголии, Республики Корея, Турции, Чешской Республики, Швейцарии и Швеции.

12. На сессии присутствовали наблюдатели от следующих международных организаций: Конференции Организации Объединенных Наций по торговле и развитию (ЮНКТАД), Европейской комиссии, Международной ассоциации адвокатов (МАА), Международной торговой палаты (МТП) и Международного союза адвокатов (МСА).

13. Рабочая группа избрала следующих должностных лиц:

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

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

Докладчик: г-н Петр АУСТЕН (Польша).

14. Рабочей группе были представлены следующие документы: предварительная повестка дня (A/CN.9/WG.IV/WP.70) и записка Секретариата (A/CN.9/WG.IV/WP.71).

15. Рабочая группа утвердила следующую повестку дня:

1. Выборы должностных лиц

2. Утверждение повестки дня

3. Планирование будущей работы по правовым аспектам электронной торговли: подписи в цифровой форме, сертификационные органы и смежные правовые вопросы

4. Прочие вопросы

5. Утверждение доклада.

## I. ХОД РАБОТЫ И РЕШЕНИЯ

16. Рабочая группа обсудила вопросы подписи в цифровой форме, сертификационных органов и смежные правовые вопросы на основе записки, подготовленной Секретариатом (A/CN.9/WG.IV/WP.71). Ход обсуждения и выводы Рабочей группы по этим вопросам изложены в разделе II ниже. Рабочая группа

---

[1]Официальные отчеты Генеральной Ассамблеи, пятьдесят первая сессия, Дополнение № 17 (A/51/17), пункты 216-224.

также провела предварительное обсуждение вопросов о включении путем ссылки и о будущей работе. Это обсуждение изложено в разделах III и IV ниже.

## II. ПРАВОВЫЕ ВОПРОСЫ И ВОЗМОЖНЫЕ ПОЛОЖЕНИЯ ДЛЯ ВКЛЮЧЕНИЯ В ЕДИНООБРАЗНЫЕ ПРАВИЛА В ОТНОШЕНИИ ПОДПИСЕЙ В ЦИФРОВОЙ ФОРМЕ

### A. Общие замечания

17. До обсуждения возможных положений для включения в единообразные правила в отношении подписей в цифровой форме и смежных правовых вопросов Рабочая группа обменялась мнениями относительно сферы охвата своей работы и рассмотрела инициативы, которые предпринимаются в настоящее время на национальном уровне для урегулирования правовых вопросов, касающихся подписей в цифровой форме и сертификационных органов.

18. Рабочая группа заслушала сообщения об усилиях, которые предпринимаются в настоящее время на национальном уровне для урегулирования правовых вопросов, касающихся подписей в цифровой форме. В настоящее время в ряде стран рассматривается вопрос о надлежащем правовом режиме механизмов, которые могут выполнять в электронной среде функции, аналогичные функциям собственноручной подписи на бумажных документах. В одних странах рассмотрение этого вопроса находится на предварительных стадиях, а в других, как об этом было сообщено, уже приняты законы о подписях в цифровой форме или идет процесс подготовки законодательства по этому вопросу на базе Типового закона. В таком законодательстве зачастую предусматривается использование подписей в цифровой форме на основе применения публичных криптографических ключей и сертификационных органов. Объем и степень детализации таких законодательных актов носят разный характер - от общих законов, принятых в целях создания возможности использования подписей в цифровой форме в качестве средства установления аутентичности электронных сообщений, до более подробного законодательства, в котором устанавливаются правовые рамки функционирования сертификационных органов, а также могут регулироваться некоторые вопросы, затрагивающие соображения публичного порядка, как то: создание административных рамок, требующихся для инфраструктуры для использования публичных ключей (ИПК); использование криптографии для подписей в цифровой форме или для целей конфиденциальности; вопросы защиты потребителей; и возможность государственных органов получать доступ к закодированной информации, например через механизм обязательного депонирования ключей. Рабочая группа также заслушала сообщения об усилиях по унификации регулирования, предпринимаемых в настоящее время на региональном уровне рядом международных организаций.

19. Вопрос правового режима механизмов, используемых для выполнения функций, эквивалентных функциям собственноручных подписей, например подписей в цифровой форме и других видов электронных подписей, был сочтен одним из наиболее важных вопросов, который нуждается в решении в целях укрепления правовой инфраструктуры электронной торговли. Было выражено общее мнение о том, что отсутствие правового режима подписей в цифровой форме и других электронных подписей может создать препятствие для экономических сделок, осуществляемых с помощью электронных средств. Было также выражено мнение, что разнообразие подходов и возможных решений, рассматриваемых на национальном уровне, обуславливает целесообразность усилий по унификации со стороны ЮНСИТРАЛ применительно к этой теме. Было выражено мнение, что помимо подготовки рекомендаций относительно правовых рамок, которые может установить принимающее правила государство в отношении подписей в цифровой форме и других видов электронных подписей, ЮНСИТРАЛ было бы целесообразно уделить внимание и вопросу о критериях признания сертификатов, выданных иностранными сертификационными органами. Было отмечено, что ЮНСИТРАЛ сможет, вероятно, содействовать этому процессу путем установления международно признанных минимальных стандартов лицензирования сертификационных органов.

20. Рабочая группа рассмотрела вопрос о том, следует ли ей заниматься только "подписями в цифровой форме" (т.е. методами, связанными с применением "криптографии с использованием публичных ключей", которая называется также "криптографией с использованием парных ключей") или же охватить и другие виды электронных подписей. Было отмечено, что в настоящее время разрабатываются также и другие технологии, которые в целом называются "электронные подписи" и которые не связаны с криптографией

с использованием публичных ключей, с тем чтобы они могли выполнять функции, которые обычно выполняют собственноручные подписи. К числу таких технологий относится использование кодов или "паролей", или биометрических идентификационных механизмов, причем эти технологии могут использоваться одновременно с системой подписей в цифровой форме на базе инфраструктуры для использования публичных ключей. Было отмечено, что при использовании бумажных документов необходимости в соблюдении формальностей и требований в отношении удостоверения подлинности и сертификации применительно к ряду операций не возникает. Отмечалось, что хотя подписи в цифровой форме в рамках инфраструктуры для использования публичных ключей позволяют обеспечить высокую степень правовой определенности, можно найти и другие способы идентификации и удостоверения подлинности в целом ряде ситуаций, когда в такой степени правовой определенности нет необходимости. Было высказано мнение, что Рабочая группа не должна создавать ошибочного впечатления о том, что она не рекомендует использовать такие другие технологии, сосредоточив свое внимание только на подписях в цифровой форме. В контексте этого обсуждения было отмечено, что применение подписей в цифровой форме с помощью криптографии с использованием публичных ключей отнюдь не всегда означает, что ставится цель добиться наивысшей степени правовой определенности. Способы использования подписей в цифровой форме являются достаточно гибкими и позволяют также снизить уровень надежности, а, соответственно, и расходы.

21. Было выражено общее мнение о том, что цель единообразных правил в отношении электронных подписей должна заключаться в предоставлении законодателям ориентиров в отношении того, каким образом самые разнообразные функции, связанные с удостоверением подлинности, могут осуществляться в электронной среде. Диапазон этих функций, если использовать так называемую "скользящую шкалу", весьма широк: от обеспечения максимальной степени надежности (аналогичной нотариально или иным образом заверенным подписям применительно к бумажным документам) до низкого уровня надежности, обеспечиваемого пометками от руки или факсимильными подписями. Однако одна из трудностей проведения работы в области электронных подписей обусловлена тем, что если цель единообразных правил, которые будут подготовлены, заключается в представлении таких рекомендаций, которые позволили бы осуществить принципы, закрепленные в статье 7 Типового закона, то, возможно, придется отойти от сугубо функционального подхода и относительно подробно изложить в этих правилах то, каким образом конкретные методы могут выполнять вышеназванные функции.

22. Было выражено общее мнение о том, что в соответствии с нейтральным с точки зрения носителей информации подходом, который был принят в Типовом законе, единообразные правила, разрабатываемые Рабочей группой, не должны препятствовать использованию любого метода, который в соответствии со статьей 7 Типового закона являлся бы "как надежным, так и соответствующим" в качестве альтернативы собственноручным и другим подписям на бумажных документах. Однако в целях содействия обсуждению Рабочая группа решила, что сначала она сосредоточит внимание на вопросах подписей в цифровой форме, которые, благодаря законодательству и правовой литературе, лучше известны, нежели другие способы. Было достигнуто общее понимание относительно того, что при необходимости в ходе обсуждения может быть принят более общий подход и будут рассмотрены вопросы, касающиеся других способов использования электронных подписей.

23. Что касается сферы охвата работы, то общее мнение членов Рабочей группы заключалось в том, что она не должна распространяться на вопросы, касающиеся применения криптографии для целей безопасности. Эти вопросы, которые уже рассматривались на других международных форумах, например в Организации экономического сотрудничества и развития (ОЭСР), весьма сложны, не имеют непосредственного отношения к механизму подписей в цифровой форме и могли бы препятствовать прогрессу в обсуждениях Рабочей группы, которой следует направить свою работу на содействие электронной торговле. В более общем плане было решено, что не следует пытаться урегулировать в разрабатываемых единообразных правилах каких-либо вопросов национальной безопасности, публичного порядка, уголовного или административного права, которые могут возникать при использовании механизмов подписей в цифровой форме.

24. Был высказан целый ряд мнений относительно того, должна ли Рабочая группа также заниматься вопросами правовых норм о защите потребителей. Согласно одной точке зрения, вопросы потребителей следует исключить из сферы текущей работы, которая должна быть сосредоточена сугубо на коммерческих сделках. Другое мнение заключалось в том, что, хотя основные рассматриваемые вопросы по своей сути не имеют непосредственной связи с проблемами потребителей, при подготовке единообразных правил, касающихся подписей в цифровой форме, было бы уместно рассмотреть вопрос о том, есть ли необходимость в разработке отдельных стандартов для потребительских сделок. В то же время было высказано предположение о том, что подготовить конкретные положения по вопросам, касающимся норм о защите потребителей, будет, возможно, особенно сложно, так как природа электронных сообщений делает практически невозможной идентификацию какой-либо стороны в качестве потребителя. После обсуждения было решено, что Рабочая группа, занимаясь в первую очередь коммерческими сделками, будет учитывать возможные последствия обсуждаемых ею вопросов для потребительских сделок.

## B. Конкретные правовые вопросы и проекты положений, касающиеся подписей в цифровой форме

25. При обсуждении вопроса о том, в какой форме должна вестись работа Рабочей группы, были высказаны различные мнения. Одно из них заключалось в том, что было бы преждевременно принимать решение о том, что результаты рассмотрения вопросов подписей в цифровой форме и смежных вопросов, которое будет проведено Рабочей группой, должны быть оформлены в виде типового законодательства. Согласно другому мнению, Рабочей группе следует в качестве рабочей гипотезы принять решение о том, что ее будущая деятельность по вопросам подписей в цифровой форме и смежным вопросам должна рассматриваться как дополнение к Типовому закону. Было напомнено о том, что на своей двадцать девятой сессии Комиссия просила Рабочую группу рассмотреть вопрос о желательности и целесообразности подготовки единообразных правил по вопросам подписей в цифровой форме и сертификационных органов. Комиссия постановила, что работа, которую предстоит провести Рабочей группе на ее нынешней сессии, могла бы включать подготовку проекта правил по определенным аспектам вышеупомянутых тем (см. пункт 9 выше).

26. После обсуждения Рабочая группа отложила принятие решения о форме своей будущей работы до завершения рассмотрения ею связанных этой темой правовых вопросов существа. Рабочая группа также отложила рассмотрение вопроса о конкретной взаимосвязи между такой будущей работой и Типовым законом. Было решено, что возможные единообразные правила, касающиеся подписей в цифровой форме, должны быть подготовлены на основе статьи 7 Типового закона и должны рассматриваться как устанавливающие порядок, при котором может использоваться надежный метод "для идентификации лица" и "указания на то, что это лицо согласно" с информацией, содержащейся в сообщении данных. В целом будущая работа над вопросом о подписях в цифровой форме должна проводиться при обеспечении соответствия с закрепленными в Типовом законе принципами и использованной в нем терминологии.

27. Для того чтобы содействовать проведению дальнейших обсуждений, Рабочая группа приняла в качестве первоначальной рабочей гипотезы решение о том, что ее работа в области подписей в цифровой форме будет вестись в виде подготовки проекта законодательных положений. Вместе с тем было высказано мнение, что Рабочей группе, возможно, следует рассмотреть необходимость подготовки дополнительных пояснений - возможно, для включения в преамбулу или в руководство по принятию единообразных законодательных положений или в виде разработки отдельных руководящих принципов, - в частности в отношении вопросов, которые могут быть сочтены неподходящими для унификации. Например, было указано, что исходящие от ЮНСИТРАЛ пояснительные комментарии по различным вопросам, связанным с созданием инфраструктуры для использования публичных ключей, могли бы иметь большое познавательное значение.

28. Было решено, что Рабочая группа будет строить обсуждение на основе проекта единообразных положений, содержащегося в записке Секретариата (A/CN.9/WG.IV/WP.71, пункты 52-76). Было отмечено, что эти проекты положений носят весьма предварительный характер, и в целом было решено, что при

их обсуждении Рабочей группе следует сосредоточить свое внимание не на рассмотрении формулировок каждой конкретной статьи, а на том, чтобы использовать эту возможность для обсуждения концептуального подхода, который мог бы лечь в основу единообразных правил, касающихся подписей в цифровой форме. Было высказано общее мнение, что в ходе обсуждения каждого из вопросов, регулируемых проектами положений, Рабочей группе, возможно, следует рассмотреть следующие аспекты: a) необходимо ли обеспечение единообразия; b) достаточно ли полно урегулирован этот вопрос в Типовом законе или же желательно разработать более подробные положения; c) касается ли этот вопрос только подписей в цифровой форме или же его можно урегулировать на более общем уровне; d) имеет ли этот вопрос непосредственное отношение к праву международной торговли, мандату ЮНСИТРАЛ и сфере ее компетенции; и e) имеется ли потребность в императивном правиле или же преимущественную силу должен иметь принцип автономии сторон.

## 1. Определения

29. С самого начала было высказано мнение, что в дополнение к проектам определений "подписи в цифровой форме", "уполномоченных сертификационных органов" и "сертификатов", содержащимся в записке Секретариата (A/CN.9/WG.IV/WP.71, пункты 52-60), Рабочей группе, возможно, потребуется рассмотреть дополнительные определения. Были предложены следующие определения: ""частный ключ" означает один из пары ключей, используемых для создания подписи в цифровой форме"; "публичный ключ" означает один ключ из пары ключей, используемых для проверки подлинности подписи в цифровой форме"; "пара ключей" в асимметрической криптосистеме означает частный ключ и математически соотносящийся с ним публичный ключ, причем этот публичный ключ позволяет проверить подлинность подписи в цифровой форме, созданной частным ключом". Рабочая группа приняла к сведению это предложение. Было высказано мнение, что, как представляется, предложенные определения в определенной степени объясняются друг через друга. Как замечание более общего характера было высказано опасение, что включение в единообразные правила нормативного характера большого числа определений может войти в противоречие с законодательной традицией многих стран. После обсуждения было в целом решено, что на более позднем этапе, возможно, потребуется вернуться к вопросу о добавлении ограниченного числа определений.

### a) Подписи в цифровой форме

30. Рабочая группа обсудила определение понятия "подпись в цифровой форме" на основе следующего проекта положения:

"Проект статьи A

1) 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 достоверно определить, что эта числовая величина была получена с помощью частного криптографического ключа составителя.

2) Математические процедуры, используемые для подготовки санкционированных подписей в цифровой форме в соответствии с [настоящим Законом] [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 криптографическим ключом составителя, может точно определить,

a) было ли такое преобразование произведено с использованием частного криптографического ключа, который соответствует частному криптографическому ключу составителя; и

b) было ли первоначальное сообщение изменено после произведенного преобразования.

3) Подпись в цифровой форме, добавленная к какому-либо сообщению данных, считается санкционированной, если ее подлинность можно проверить в соответствии с процедурами, установленными сертификационным органом, уполномоченным согласно [настоящему Закону] [настоящим Правилам].

4) [Соответствующий орган принимающего государства] устанавливает конкретные правила в отношении технических требований, которым должны отвечать подписи в цифровой форме и порядок проверки их подлинности".

Пункты 1 и 2

31. Было высказано мнение о необходимости расширения определения "подписи в цифровой форме", с тем чтобы оно охватывало не только криптографию с использованием публичных ключей, но и другие виды электронных подписей. Однако большинство членов Группы сочли нецелесообразным пытаться разработать определение "подписи в цифровой форме", которое выходило бы за рамки существующей практики. Было решено ограничить понятие "подписи в цифровой форме" исключительно случаями асимметрической криптографии, однако при необходимости рассмотреть другие определения для охвата иных методов, которые могут в целом пониматься под понятием "электронные подписи".

32. В отношении пункта 1 было предложено заменить слова "достоверно определить, что эта числовая величина была получена" выражением "определить, что эта числовая величина была получена лишь". Рабочая группа решила, что на столь раннем этапе обсуждения ей не следует заниматься сколь-нибудь углубленным обсуждением содержащихся в тексте формулировок. Было высказано общее мнение, что пункты 1 и 2 отражают суть понятия "подписи в цифровой форме" в том виде, в каком оно может использоваться для определения сферы будущей работы. После обсуждения Рабочая группа сочла содержание пунктов 1 и 2 в целом приемлемым, однако согласилась с тем, что на более позднем этапе ей, возможно, потребуется вновь рассмотреть вопрос об их конкретной формулировке.

Пункт 3

33. Был поднят целый ряд вопросов в отношении цели пункта 3. Было высказано мнение, что пункт 3 не позволяет решить задачу введения понятий инфраструктуры для использования публичных ключей и проверки подлинности подписей в цифровой форме и что в нем, напротив, затрагиваются вопросы существа, не относящиеся к определению "подписи в цифровой форме". Было высказано мнение, что пункт 3 может толковаться как означающий введение понятия процедур проверки подлинности подписи в цифровой форме в качестве одного из условий ее действительности. Было высказано предположение о том, что пункт 3 было бы целесообразно исключить и заменить описательным определением понятия "проверка подлинности" подписей.

34. Было указано, что пункт 3 может толковаться как касающийся лишь проверки подлинности подписей в цифровой форме, которые применяются в рамках инфраструктуры для использования публичных ключей, созданной государственными органами. Было высказано мнение, что в своей нынешней формулировке это положение излишне жестко, поскольку может препятствовать признанию использования подписей в цифровой форме в любых других условиях, как, например, в случае инфраструктур для использования публичных ключей, созданных организациями, которые не являются государственными органами. Было высказано общее мнение о том, что было бы нежелательно принимать положение, которое может отрицательно сказаться на возможных операциях между входящими в замкнутую группу сторонами, которые не испытывают потребности прибегать к услугам сертификационного органа. Было отмечено, что на этапе, когда государства еще только рассматривают различные варианты инфраструктуры для использования публичных ключей, было бы преждевременно отдавать в проекте единообразных правил предпочтение какой-либо конкретной системе инфраструктуры для использования публичных ключей в ущерб всем прочим вариантам.

35. Было высказано мнение о том, что, хотя пункт 3 должен толковаться с учетом статьи 7 Типового закона, эти два положения, возможно, не полностью соответствуют друг другу. Например, в пункте 3 понятие "подписи в цифровой форме" ограничивается ссылкой на "санкционированную" подпись в цифровой форме, а это слово не используется в контексте статьи 7 Типового закона или в других положениях статей A-J, как они изложены в записке Секретариата (A/CN.9/WG.IV/WP.71). Кроме того, в статье 7 Типового закона содержится ссылка на использование метода подписи, который является "как надежным, так и соответствующим цели, для которой сообщение данных было подготовлено или передано", то есть статья 7 допускает различную степень надежности в зависимости от целей подготовки или передачи сообщения данных, в том числе от любой договоренности сторон. Было указано, что в соответствии со статьей 7 Типового закона стороны сделки, достаточно доверяющие друг другу, могут договориться об уровне защиты, который они считают надлежащим в сложившихся обстоятельствах, и не обязательно должны прибегать к услугам сертификационного органа. С точки зрения сторон, важным моментом является то, насколько они доверяют используемой ими системе. Было отмечено, что доверие к аппаратным средствам, программному обеспечению и процедурам, используемым сторонами, определяется рядом факторов (например, тем, обеспечивают ли они достаточную защиту от вмешательства и злоупотребления; являются ли они достаточно легкодоступными, надежными и хорошо работающими; достаточно ли они подходят для выполнения намеченной функции; и соответствует ли их функционирование общепринятым принципам защиты). Таким образом, стороны должны сами решать, должен ли требующийся им стандарт надежности предусматривать процедуру проверки подлинности, применяемую сертификационным органом. В то же время из пункта 3 вытекает, что подпись в цифровой форме является надежной лишь в случае, если она может быть удостоверена при помощи сертификационного органа. Поэтому было сочтено, что пункт 3 носит более ограничительный характер, чем статья 7 Типового закона. Было указано, что для приведения пункта 3 в соответствие со статьей 7 Типового закона в его положения потребуется внести существенные изменения.

36. Были также подняты вопросы в отношении указания в пункте 3 на проверку подлинности подписи в цифровой форме в соответствии с процедурами, установленными сертификационным органом. Было высказано мнение, что указание на эти процедуры затрагивает вопрос технических инструкций, применяемых при проверке подлинности подписей в цифровой форме, и других оперативных критериев, соблюдаемых сертификационным органом, или правовых последствий несоблюдения этих процедур в каждом конкретном случае. Однако эти вопросы относятся к вопросам существа, которые не могут быть надлежащим образом рассмотрены в рамках ограниченной сферы применения проекта статьи A. Поэтому было предложено исключить из пункта 3 указание на процедуры проверки подлинности.

37. Рассмотрев различные высказанные мнения, Рабочая группа постановила исключить пункт 3. Было решено, что к обсуждению возможных вариантов инфраструктуры для использования публичных ключей, возможно, придется вернуться после изучения вопроса о правовых последствиях подписи в цифровой форме.

Пункт 4

38. Было высказано мнение, что в той мере, в какой пункт 4 предусматривает установление государством технических требований в отношении подписей в цифровой форме, он, как представляется, исключает возможность создания организациями, не являющимися государственными органами, инфраструктур для использования публичных ключей. В соответствии с решением исключить пункт 3 и ввиду наличия логической связи между этими двумя положениями Рабочая группа постановила исключить и пункт 4.

b) Уполномоченные сертификационные органы

39. Рабочая группа обсудила определение понятия "уполномоченный сертификационный орган" на основе следующего проекта положения:

"Проект статьи B

1) ... [принимающее государство указывает орган или ведомство, компетентное уполномочивать сертификационные органы] может предоставлять сертификационным органам полномочия действовать в соответствии с [настоящим Законом] [настоящими Правилами]. Такие полномочия могут быть отозваны.

2) ... [принимающее государство указывает орган или ведомство, компетентное принимать постановления в отношении уполномоченных сертификационных органов] может устанавливать правила, регулирующие условия, на которых такие полномочия могут быть предоставлены, и принимать постановления, касающиеся функционирования сертификационных органов.

3) Уполномоченные сертификационные органы могут выдавать сертификаты в отношении криптографических ключей физических и юридических лиц.

4) Уполномоченные сертификационные органы могут предлагать или облегчать регистрацию и фиксацию времени передачи и приема сообщений данных, а также выполнять другие функции в отношении сообщений, запущенных с помощью подписей в цифровой форме.

5) ... [принимающее государство указывает орган или ведомство, компетентное устанавливать конкретные правила в отношении функций, которые должны выполняться уполномоченными сертификационными органами] может устанавливать более конкретные правила в отношении функций, которые должны выполняться уполномоченными сертификационными органами в связи с выдачей сертификатов отдельным физическим или юридическим лицам."

40. Рабочая группа провела общий обмен мнениями о том подходе, которым следует руководствоваться в вопросе о сертификационных органах. Согласно одной точке зрения, проект статьи B в нынешней формулировке устанавливает, как представляется, конкретный способ создания инфраструктуры для использования публичных ключей, а решение этого вопроса было бы предпочтительнее оставить на усмотрение каждого принимающего государства, чтобы оно само приняло свои собственные правила в этой области. Было отмечено, что, хотя сертификационные органы могут играть ключевую роль в установлении доверия в отношении надежности подписей в цифровой форме, вполне возможно существование систем подписей в цифровой форме, функционирующих и без сертификационных органов. Отмечалось также, что создание публично-правовой системы, в рамках которой могут выдаваться полномочия на деятельность сертификационных органов, отнюдь не обязательно укрепит доверие к подписям в цифровой форме, так как это может быть скорее достигнуто путем назначения сертификационных органов в частном порядке или же с помощью других форм механизмов рыночного типа. Другая точка зрения сводилась к тому, что проект статьи B в целом приемлем для целей определения сертификационных органов, поскольку он сформулирован в разрешительной форме, особенно пункт 2, который не препятствует принимающему государству иным образом организовать свою инфраструктуру для использования публичных ключей.

41. Для цели рассмотрения возможных подходов к вопросу функционирования сертификационных органов Рабочей группе было предложено изучить две возможные цели, на достижение которых может быть направлено определение понятия "сертификационный орган". Одна из них может заключаться в представлении принимающим государствам ориентиров в отношении ключевых элементов, которые необходимо учитывать при создании национальных инфраструктур для использования публичных ключей. Было указано, что проект статьи B является недостаточно подробным, чтобы являться надлежащим руководством в этой связи. Альтернативная цель могла бы состоять в том, чтобы оставить решение вопроса создания внутренних инфраструктур для использования публичных ключей на усмотрение каждого принимающего государства, установив при этом в определении термина "сертификационный орган" критерии, которые каждое принимающее государство должно применять при признании сертификатов, выданных иностранными сертификационными органами. Было отмечено, что если Рабочая группа пожелает ограничить сферу применения проекта единообразных правил достижением последней цели, то в проект статьи B, возможно, потребуется включить вводный пункт следующего содержания: "Настоящие единообразные положения применяются к сертификатам, выданным в соответствии с

правовым режимом, обладающим следующими атрибутами:". Было отмечено, однако, что такое предложение, если оно будет принято, потребует существенной переработки остальных положений проекта статьи B. Другое мнение заключалось в том, что в проекте статьи B не следует устанавливать конкретных критериев, ограничившись на этот счет лишь общим заявлением, содержащимся в пункте 2. Другие комментарии, в том числе примерный перечень возможных критериев, которые следует учесть принимающим государствам, можно было бы включить в руководство по принятию проекта единообразных правил.

42. Рабочая группа решила, что вопрос о том, нужно ли включать определение понятия "сертификационный орган" в проект единообразных правил для иных целей, помимо установления критериев, которые следует применять каждому принимающему государству при признании сертификатов, выданных иностранными сертификационными органами, будет, вероятно, необходимо обсудить позднее. Большинство поддержало мнение о том, что, хотя установление стандартов или критериев может помочь сертификационным органам в установлении уровня доверия, необходимого для их функционирования, необходимо, вероятно, проводить разграничение между общими вопросами доверия к сертификационным органам, которые могут зависеть от того правового режима, на основании которого они были учреждены, и более конкретными вопросами, связанными с уровнем доверия, которым пользуются конкретные сертификаты, выданные сертификационным органом.

43. Было высказано мнение о том, что положения относительно функционирования и обязанностей сертификационных органов, такие как положения, изложенные в проекте статьи B, могут быть использованы не только как структурные элементы системы сертификационных органов (например, инфраструктуры для использования публичных ключей). Положения этого вида могут быть использованы также и для целей определения последствий постановки подписей в цифровой форме, а также действий, связанных с подписями в цифровой форме, или предусматривающих их использование. С учетом этого было отмечено, что при обсуждении данного вопроса Рабочей группе было бы полезно иметь в виду весь спектр факторов, относящихся к определению правовых последствий использования подписей в цифровой форме. Рабочая группа могла бы проанализировать следующие факторы: a) виды подписей (к числу которых, если идти от общего случая к специальному, относятся электронные подписи; подписи в цифровой форме; подписи в цифровой форме с сертификатом и подписи в цифровой форме с сертификатом, выданным официально уполномоченным сертификационным органом); b) затрагиваемые стороны (т.е. непосредственно стороны контракта, включая сертификационные органы; третьи стороны, например, грузоотправители и банки; государственные органы; другие лица, например, поставщики услуг, коммуникационные компании); c) действия или события, с которыми связываются правовые последствия (т.е. использование подписей в цифровой форме; выдача сертификата, включая несанкционированную выдачу; истечение срока действия сертификата; отзыв сертификата; отзыв полномочий, выданных сертификационному органу); d) сфера работы ЮНСИТРАЛ в этой области (применение только на международном уровне; применение на международном уровне плюс предложения в отношении национальных законов; предложения в отношении национальных законов); e) правовые последствия (т.е. действительность; обязательства органа, выдающего сертификаты, и лица, пользующегося сертификатами; способы правовой защиты; материальная ответственность, включая ее пределы; доказательства); f) техника составления (т.е. установление стандартов; правовые последствия, если стандарты соблюдены; правовые последствия, если стандарты не соблюдены). Рабочая группа выразила мнение, что предлагаемый перечень факторов является полезным инструментом в плане содействия проведения ею анализа цели и последствий положений, касающихся сертификационных органов.

44. В ходе последующего обсуждения Рабочая группа рассмотрела вопрос о том, целесообразно ли включать в проект единообразных правил оперативные критерии, которые должны соблюдаться сертификационными органами, будь то уполномоченными или нет.

45. Было отмечено, что в дополнение к уже содержащимся в проекте статьи B положениям в него необходимо добавить единообразные правила, где прямо указываются критерии, которые должны учитываться при выдаче полномочий на деятельность сертификационных органов, или иным образом определяются минимальные стандарты, которые должны соблюдаться сертификационными органами для

обеспечения правового признания выдаваемых ими сертификатов. Если в проекте единообразных правил будут регулироваться вопросы, связанные с деятельностью сертификационных органов, то указать такие критерии необходимо. Было напомнено, что в пункте 44 записки Секретариата (A/CN.9/WG.IV/WP.71) перечисляется ряд факторов, которые могут учитываться при оценке надежности какого-либо сертификационного органа. Было отмечено в целом, что такой перечень представляет собой хорошую основу для обсуждения, если Рабочая группа решит продолжить рассмотрение этого вопроса. Указывалось, что некоторые из этих критериев могут быть расширены, с тем чтобы охватить такие факторы, как компетентность персонала на управленческом уровне или полное выделение сертификационной функции из любых других операций, которые может осуществлять сертификационный орган.

46. Против включения в проект единообразных правил оперативных критериев для сертификационных органов были высказаны возражения. Рабочей группе было напомнено о состоявшемся ранее обсуждении роли государственных органов в создании инфраструктур для использования публичных ключей и возможности того, что в некоторых государствах сертификационные функции будут выполнять частные компании, при этом получение предварительного разрешения от государства требоваться не будет (см. пункт 40 выше). Кроме того, можно бы было рассмотреть другие приемлемые альтернативы устанавливаемым государством критериям, например, международно признанные торговые обыкновения и практику или квалификационные стандарты, разработанные авторитетными неправительственными органами, как это имеет место в ряде областей коммерческой деятельности. Было выражено мнение, что предлагаемое включение критериев, которые должны учитываться при выдаче полномочий на деятельность сертификационных органов, будет и ненужным, и неуместным в случае сертификационных органов, которые функционируют не на основе выданных государством полномочий. Кроме того, включение любых таких критериев потребует указания на то, какой орган или учреждение компетентны определять, удовлетворяет ли тот или иной сертификационный орган указанным критериям. В связи с такой системой могут возникнуть трудности применительно к сертификационным органам, функционирующим за пределами инфраструктуры для использования публичных ключей, созданной государственными органами.

47. В ответ на эти возражения было напомнено, что положение, содержащее общеприемлемые критерии функционирования сертификационных органов, может быть важным шагом на пути к повышению доверия к подписям в цифровой форме. Такие критерии, вероятно, не требуются, когда электронные сделки совершаются между сторонами, действующими в рамках замкнутой системы, которую они считают достаточно надежной. Доверяющие друг другу партнеры, осуществляющие операции в рамках таких замкнутых систем, по сути могут и не использовать сертификатов, выдаваемых сертификационными органами. Однако в целях создания возможностей для более широкого использования подписей в цифровой форме необходимо содействовать повышению доверия общества в целом к подлинности таких подписей и надежности методов, используемых для их проверки. Один из важных способов достижения этой цели заключается в том, чтобы продемонстрировать обществу в целом, что органы, осуществляющие сертификацию подлинности публичных ключей, должны соответствовать определенным критериям, разработанным для обеспечения их надежности. Было отмечено, что, хотя Рабочая группа не должна пренебрегать возможной ролью торговых обыкновений и практики или неправительственных органов в деле выработки приемлемых оперативных стандартов любой конкретной области коммерческой деятельности, пока еще нет устойчивой практики определения приемлемых критериев функционирования сертификационных органов.

48. Было указано, что два осуждаемых альтернативных варианта, а именно установление критериев для выдачи государством полномочий на деятельность сертификационных органов и признание оперативных критериев сертификационных органов, действующих за пределами созданной государством инфраструктуры для использования публичных ключей, могут и не быть взаимоисключающими. Различие между этими двумя ситуациями может заключаться в правовых последствиях, признаваемых за подписями в цифровой форме в одном и другом случае. Что касается сертификационных органов, уполномоченных государством, то выполнение сертификационным органом применимых оперативных критериев будет представлять собой предварительное условие для выдачи полномочий такому

сертификационному органу, что, в свою очередь, будет условием признания юридической действительности сертификатов, выдаваемых этим сертификационным органом. Во второй ситуации сертификационному органу до начала его деятельности не нужно будет доказывать, что оперативные критерии выполнены. Однако, если выдаваемые им сертификаты будут оспариваться (например, в суде или арбитраже), разрешающему спор органу необходимо будет дать оценку надежности сертификата путем определения того, был ли он выдан сертификационным органом, удовлетворяющим этим критериям.

49. Было высказано мнение, что надежность сертификата может зависеть от действий сертификационного органа в отношении этого конкретного сертификата, а не от институциональных факторов. Такая "оперативная" надежность не обязательно будет зависеть от того факта, является ли сертификационный орган уполномоченным или нет, или от международно признанных торговых обыкновений и практики. Было высказано предположение о том, что критерии надежности будут определяться целью, для которой проводится оценка надежности (например, в целях перекрестной сертификации, выдачи лицензии, установления ответственности).

50. Учитывая, что обсуждение находится на раннем этапе и что по этому вопросу были высказаны противоречивые мнения, общую поддержку получило предложение о том, чтобы Рабочая группа приняла к сведению вышеупомянутые предложения в качестве возможных рабочих гипотез и вернулась к изучению этих проблем на более позднем этапе после рассмотрения других неразрывно связанных с ними вопросов, таких как вопрос об ответственности сертификационных органов и вопросы трансграничной сертификации.

## 2. Ответственность

51. Рабочая группа обсудила вопрос об ответственности сертификационных органов на основе следующего проекта положения:

"Проект статьи H

1) Уполномоченный сертификационный орган несет ответственность перед любым лицом, которое действовало добросовестно, полагаясь на сертификат, выданный этим сертификационным органом, за любой ущерб, вызванный пороками в регистрации, произведенной сертификационным органом, техническими поломками и аналогичными обстоятельствами [,[даже если этот ущерб не возник в результате] [,если этот ущерб возник в результате] небрежности сертификационного органа].

2) Вариант X Ответственность за любой отдельный ущерб не превышает [сумма]. ... [принимающее государство указывает орган или ведомство, компетентное пересмотреть размер максимальной суммы] может регулировать размер этой суммы один раз в два года с целью отразить изменение цен.

Вариант Y ... [принимающее государство указывает орган или ведомство, компетентное принимать постановления в отношении ответственности] может принимать постановления в отношении ответственности сертификационных органов.

3) В случае, если сторона, которая понесла ущерб, содействовала этому преднамеренно или в результате небрежности, размер компенсации может быть уменьшен или же она может не предоставляться.

[4) Если уполномоченный сертификационный орган получил уведомление об аннулировании сертификата, этот орган немедленно регистрирует такое аннулирование. Если данный орган не делает этого, то он несет ответственность за любой ущерб, понесенный в результате этого пользователем.]"

Пункты 1 и 2

Общие замечания

52. Рабочая группа обсудила сферу применения и последствия предлагаемых правил об ответственности сертификационных органов. Было отмечено, что вопрос об ответственности сертификационных органов связан с двумя различными видами ответственности: "структурной" ответственностью, наступающей в результате нарушения сертификационным органом условий функционирования, и "оперативной" ответственностью, наступающей в результате действий сертификационного органа при выдаче, приостановлении действия или отзыве сертификата. В первом случае сертификационный орган подрывает возложенное на него публичное доверие, и было бы целесообразно, чтобы выдающий полномочия государственный орган взимал штрафы или налагал другие санкции, соразмерные тяжести нарушения. Во втором случае сертификационный орган нарушает свои профессиональные обязательства перед клиентом. Между тем зачастую ущерб будет нести торговый партнер последнего, который в большинстве случаев не будет иметь договорных отношений с сертификационным органом. В этих обстоятельствах был задан вопрос о том, целесообразно ли предоставлять потерпевшей стороне возможность требовать возмещения от сертификационного органа или же потерпевшая сторона должна иметь право требовать возмещения только от своего торгового партнера, который, в свою очередь, может потребовать возмещения от сертификационного органа. Было высказано предположение о том, что установить адекватный режим ответственности, при котором пользователь сертификата будет наделен правом предъявлять требования непосредственно к сертификационному органу, будет весьма сложно.

53. Была высказана точка зрения о том, что Рабочей группе было бы предпочтительнее не заниматься вопросом ответственности сертификационных органов, поскольку этот тонкий и сложный вопрос не может быть надлежащим образом урегулирован в проекте единообразных правил. Было напомнено, что в контексте Типового закона было решено совсем не затрагивать вопроса об ответственности поставщиков услуг, являющихся третьими сторонами. Было отмечено, что вопрос ответственности тесно связан с вопросом ущерба, который не столь легко поддается международной унификации. Рабочей группе было предложено рассмотреть возможную целесообразность исключения обоих вопросов из сферы проекта единообразных правил, с тем чтобы они решались на основе применимого национального права. Если такой подход будет принят, то можно было бы рассмотреть следующие альтернативы: оставить определение права, применимого к вопросам ответственности и ущерба, на усмотрение национальных коллизионных норм; разработать специальную единообразную коллизионную норму; или непосредственно определить, какая коллизионная норма должна применяться (например, коллизионная норма страны, в которой сертификационный орган зарегистрирован или иным образом наделен полномочиями функционировать). В поддержку этого предложения было отмечено, что вопрос об ответственности является по сути вопросом о гарантиях, предоставляемых сертификационным органом, а этот вопрос было бы лучше всего оставить на урегулирование сторонами контракта или же на урегулирование в соответствии с национальным правом, применимым к их договорным отношениям.

54. Однако предложение о включении в проект единообразных правил положения об ответственности сертификационных органов получило широкую поддержку. Вопрос ответственности был назван слишком важным, чтобы полностью оставлять его решение на усмотрение сторон, в особенности в свете того обстоятельства, что не все пользователи сертификатов могут состоять в непосредственных договорных отношениях с сертификационным органом. Ограничить права пользователей возможностью истребовать возмещение со своих торговых партнеров за ошибки сертификационного органа означало бы оставить без защиты тех лиц, которые являются жертвами обманных действий с использованием фиктивных наименований и идентификаций, при том, что сертификационный орган знал об этом или своей небрежностью содействовал этому. Кроме того, отсутствие единообразных правил об ответственности сертификационных органов может привести к нежелательной ситуации, когда некоторые страны будут предусматривать лишь ответственность на ничтожном уровне, с тем чтобы благоприятствовать или способствовать созданию сертификационных органов на своих территориях. Возможность возникновения "сертификационного рая" может вызвать колебания у торговых партнеров при решении вопроса о том, использовать ли подписи в цифровой форме, а такая ситуация не соответствует цели поощрения

электронной торговли. Большинство поддержало мнение о том, что каким бы сложным ни был вопрос об ответственности сертификационных органов, затрагивающий аспекты как договорной, так и деликтной ответственности, он должен быть урегулирован в единообразных правилах.

55. После обсуждения Рабочая группа решила, что в принципе в проекте единообразных правил должны содержаться положения относительно ответственности сертификационных органов в контексте их участия в механизмах использования подписей в цифровой форме.

Характер ответственности

56. Были подняты вопросы относительно характера ответственности сертификационных органов, в частности о том, должна ли такая ответственность быть основана на небрежности или она будет определяться как "абсолютная ответственность", называемая также "объективная ответственность" или "ответственность без вины". Были высказаны возражения против включения положений, которые бы возлагали на сертификационный орган абсолютную ответственность. Отмечалось, что абсолютная ответственность представляет собой отступление от общего принципа деликтного права, согласно которому лицо несет ответственность за свою собственную небрежность, и как таковая она признается в национальном праве в исключительных случаях, затрагивающих публичные интересы, например, в случае режима абсолютной ответственности лиц, осуществляющих неразумно опасную деятельность. Нет никаких убедительных причин для того, чтобы распространять на сертификационные органы режим абсолютной ответственности. Кроме того, нежелательным последствием такого режима будет создание препятствий для становления нового сектора сертификационных органов, что ограничит возможности использования подписей в цифровой форме. Было отмечено далее, что сертификационные органы могут предоставлять своим клиентам и обществу в целом услуги разного уровня - от простого перечня имен или наименований держателей публичных ключей и их соответствующих ключей до более индивидуализированных видов услуг, включающих гарантии подлинности публичных ключей и идентификацию их держателей. Уровень обязательств, принимаемых на себя сертификационными органами, а также взимаемая ими плата зависят от вида предоставляемых ими услуг. С учетом такого диапазона услуг было бы неразумно возлагать одинаковый уровень ответственности на все сертификационные органы во всех мыслимых обстоятельствах. В этой связи было отмечено, что режим ответственности, применимый к сертификационным органам, должен основываться на небрежности, как это предусматривается согласно одному из вариантов в пункте 1 проекта статьи H.

57. В ответ на это было отмечено, что было бы несправедливо требовать, чтобы потерпевшая сторона несла бремя доказывания небрежности сертификационного органа. С учетом высокого уровня технической оснащенности, которого можно ожидать от сертификационных органов, и высокого уровня доверия, который с их помощью предполагается создать, эти органы в обычных обстоятельствах должны нести ответственность во всех случаях, когда сертификаты выдаются с пороками, что приводит к возникновению ущерба. Было отмечено, что в некоторых правовых системах определенные профессиональные категории (например, государственные нотариусы в некоторых странах системы гражданского права) обязаны заключить договор о страховании ответственности перед третьими лицами или стать участником общего компенсационного фонда для выплаты возмещения лицам, понесшим ущерб в результате их действий. Было указано, что создание такого общего компенсационного фонда было бы облегчено, если бы сертификационные органы были организованы в каких-либо институциональных рамках, например в рамках механизма лицензирования.

58. Отмечалось, что расхождение во мнениях, выраженных в Рабочей группе, можно было бы устранить, если вместо позитивной нормы с указанием обстоятельств, при которых сертификационные органы несут ответственность, включить в единообразные правила норму, устанавливающую опровержимую презумпцию ответственности. Согласно такому предложению, например, в случае ошибочной идентификации лица или ошибочной атрибуции публичного ключа какому-либо лицу сертификационный орган будет нести ответственность за убытки, понесенные потерпевшей стороной, если только он не докажет, что сделал все возможное, чтобы не допустить такой ошибки. Сертификационный орган мог бы опровергнуть такую презумпцию, например, доказав, что он придерживался такого

стандарта поведения, который может быть установлен в единообразных правилах. Было отмечено, что такая схема ответственности, которая похожа на схемы, предусмотренные в некоторых национальных законах, касающихся ответственности за выпуск продукции, обеспечила бы дополнительную защиту пользователям услуг, не возлагая при этом абсолютной ответственности на сертификационный орган. Рабочая группа приветствовала это предложение, которое, по общему мнению, содержит перспективный подход для дальнейшего рассмотрения Рабочей группой при урегулировании сложной проблемы ответственности сертификационных органов.

59. Затем Рабочая группа приступила к рассмотрению обстоятельств, которые освобождали бы сертификационный орган от ответственности за допущенную ошибку. Было отмечено, что согласно предлагаемой схеме ответственности, сертификационный орган должен освобождаться от ответственности, если он сможет доказать, что он проявил разумную заботливость при идентификации держателя публичного ключа или при исполнении своих функций по удостоверению подлинности; что ошибки возникли по собственной вине пользователя, как указывается в пункте 3 проекта статьи H; или что ошибки связаны с обстоятельствами вне сферы контроля сертификационного органа. Было выражено общее мнение, что перечень подобных событий, освобождающий от ответственности, был бы приемлемым.

Типовые условия сертификации и автономия сторон

60. Было высказано мнение, что при рассмотрении вопроса об ответственности важно учитывать взаимные ожидания и интересы пользователя и сертификационного органа. Предполагается, что сертификационный орган должен будет сообщать свои типовые условия сертификации (ТУС), в которых пользователям, среди прочего, будет предоставляться информация о методах и процедурах, которые он применяет для идентификации держателя публичного ключа. Предполагается, что пользователь должен будет разумно ознакомиться с содержанием этого документа. Кроме того, следует предусмотреть обязанность пользователей убедиться в том, что сертификат остается в силе (например, в том, что сертификат не был отозван), прежде чем они будут полагаться на него. И наконец, предполагается, что пользователи должны действовать разумно на основе имеющейся у них информации. На вопросы о том, каким образом пользователи могут проверить действительность сертификата, было отмечено, что можно потребовать, чтобы сертификационные органы имели базы данных действующих сертификатов - как это уже и делают некоторые органы, - которые будут доступны заинтересованным сторонам для цели проверки действительности сертификатов. В ответ на это предложение было указано, что, хотя было бы целесообразно поощрять осмотрительность пользователей в плане обращения с сертификатами, главная ответственность за подлинность и действительность сертификата лежит на сертификационном органе и следует весьма осмотрительно подходить к вопросу возложения каких-либо обязанностей на пользователей, которые бы заставили их разделить эту ответственность. В большинстве случаев пользователи обычно будут не в состоянии установить ряд факторов, относящихся к действительности сертификата, например процедуры идентификации, применяемые сертификационным органом, или же вопрос о том, является ли держатель публичного ключа также держателем соответствующего частного ключа. Было неразумно перекладывать ответственность за какой-либо из этих вопросов на пользователя.

61. Рабочая группа провела обсуждение вопроса о значении типовых условий сертификации и о том, в какой степени они могут ограничивать или иным образом определять объем ответственности, принимаемой на себя сертификационными органами. Для целей защиты интересов пользователей можно потребовать, чтобы сертификационные органы сообщали о пределах ответственности с помощью включения соответствующих положений в свои типовые условия сертификации. С технической точки зрения можно было бы предусмотреть доступ к типовым условиям сертификации в электронной форме для лиц, пользующихся услугами сертификационного органа. Было высказано мнение, что сторона, обращающаяся к услугам сертификационного органа, должна давать свое согласие на обязательность положений, изложенных в типовых условиях сертификации; такое согласие будет выводиться из факта использования услуг сертификационного органа. Договорные отношения между двумя сторонами должны иметь преимущественную силу перед всеми нормами из других источников, и в этой связи важно обеспечить возможность принудительного исполнения согласованных условий. Было указано, однако,

что такие важные для полагающихся на сертификат сторон положения, как ограничения ответственности, должны включаться непосредственно в сертификат, а не только в документ, на который в сертификате сделана ссылка, каким бы доступным ни был такой документ.

62. Большинство членов Рабочей группы согласились с тем, что при разработке схемы ответственности сертификационных органов следует должным образом учитывать необходимость в сохранении автономии сторон. В то же время были высказаны оговорки относительно возможности того, чтобы сертификационный орган мог снять с себя ответственность за свою небрежность путем оговорок об освобождении от ответственности или отказов, содержащихся в типовых условиях сертификации или любом другом документе, исходящем от этого сертификационного органа. Было указано, что получатель сообщения, который пользуется сертификатом для проверки подлинности подписей в цифровой форме, зачастую не будет иметь непосредстенных юридических отношений с сертификационным органом и, таким образом, возможности оговорить с сертификационным органом содержание таких положений об ответственности. Даже составитель сообщения, который находится в договорных отношениях с сертификационным органом, не всегда будет иметь возможность оговаривать такие условия, которые во многих случаях будут представлять собой заранее составленные примерные коммерческие условия, не предусматривающие внесения изменений. В некоторых правовых системах одностороннее исключение ограничения ответственности противоречило бы публичному порядку. Если устанавливать пределы ответственности и исключения, то они должны соответствовать закону или быть санкционированы государственными органами.

Пределы ответственности

63. Рабочая группа рассмотрела вопрос о том, должны ли устанавливаться пределы ответственности сертификационных органов и как такие пределы могут определяться. В качестве возражения против установления пределов ответственности сертификационных органов было указано, что такие пределы, как правило, устанавливаются в областях деятельности, где в той или иной форме существует монополия, как в случае почтовых и телефонных служб в ряде стран. Однако в других областях деятельности, открытых для конкуренции, для установления подобных пределов ответственности нет оснований.

64. Вместе с тем были высказаны различные мнения в поддержку ограничения в какой-либо форме ответственности сертификационных органов. Были высказаны следующие аргументы: a) сертификационные органы представляют собой формирующийся сектор, развитие которого может быть затруднено, если ответственность этих органов будет неограниченной; b) важно дать сертификационным органам возможность самим определять степень ответственности, которую они готовы взять на себя, и это может явиться необходимым предварительным условием заключения ими договора страхования для обеспечения надлежащего покрытия рисков, связанных с их деятельностью; и c) в случае с подписями в цифровой форме может возникнуть ситуация, когда роль сертификационного органа будет ограничиваться выдачей сертификата, который сам по себе может иметь весьма незначительную поддающуюся исчислению ценность или вообще не иметь таковой. Далее было указано, что в случае выдачи сертификата, устанавливающего связь между публичным ключом и конкретным физическим лицом, этот сертификат может прилагаться к ряду сообщений в рамках самых разных операций, общую сумму которых сертификационный орган в большинстве случаев не в состоянии предвидеть. Было подчеркнуто, что в случае операций с кредитными карточками существуют средства санкционирования каждой операции в отдельности, так что во всех случаях, когда кредитная карточка используется для заключения сделки на сумму сверх заранее установленного лимита, компания, выдавшая кредитную карточку, в состоянии оценить свою потенциальную ответственность в случае несанкционированного использования этой кредитной карточки. У сертификационных органов, которые, как правило, не осведомлены об условиях операций, производимых их клиентами, такая возможность отсутствует. Поэтому было бы трудно установить "пороговый" или верхний предел ответственности путем включения ссылки на стоимостной объем операции, для целей которой используется подпись в цифровой форме. Ввиду неограниченного числа операций, в которых может использоваться один-единственный сертификат, сомнительно, чтобы сертификационные органы были в состоянии за разумную сумму застраховать себя от ответственности перед третьими лицами.

65. Что касается возможных методов ограничения объема ответственности, которую несут сертификационные органы, то Рабочая группа обсудила ряд предложений. Один возможный подход мог бы заключаться в установлении фиксированной суммы, как это предлагается сделать в варианте X пункта 2 проекта статьи H. Другие предложенные подходы предусматривали ограничение ответственности путем указания коэффициента, на который должна перемножаться плата подписчика, процентной доли от стоимостного объема операции или процентной доли от фактического ущерба, понесенного пострадавшей стороной. Вместе с тем было указано, что ущерб, который может возникнуть в результате действий сертификационного органа, с трудом поддается количественной оценке, что осложняет его использование в качестве объективного критерия для установления фиксированного объема ответственности. Кроме того, услуги, оказываемые сертификационным органом, и взимаемая им за это плата зачастую никак не связаны со стоимостным объемом операций, к которым эти услуги относятся, или с ущербом, который могут понести стороны. Другие механизмы ограничения ответственности, такие, как содержащиеся в Конвенции Организации Объединенных Наций о морской перевозке грузов ("Гамбургские правила") или в Типовом законе ЮНСИТРАЛ о международных кредитовых переводах, касаются операций, включающих поддающиеся количественной оценке элементы (например, стоимость груза, сумма кредитового перевода), которых в рассматриваемом случае может и не иметься.

66. Еще один возможный вариант ограничения ответственности заключается в освобождении от ответственности за определенные виды убытков, такие, как косвенные убытки. В отношении последней возможности было указано, что понятие "косвенные убытки", которые иногда именуются "непрямыми убытками", может по-разному толковаться в различных правовых системах. В связи с этим было высказано мнение о том, что предпочтительнее было бы конкретно указать охватываемые этим понятием виды убытков, за которые сертификационный орган не будет нести ответственности. Хотя некоторые члены Рабочей группы поддержали идею разработки подхода, освобождающего от ответственности за косвенные убытки, по аналогии с подходом, закрепленным в Типовом законе ЮНСИТРАЛ о международных кредитовых переводах, было указано, что в случаях подписей в цифровой форме и сертификационных органов применение подобного подхода может оказаться неуместным. Было указано, что убытки, как правило, возникают не непосредственно в результате, например, выдачи подложного сертификата, а скорее вследствие того, что на основе такого сертификата третье лицо положилось на недостоверную подпись в цифровой форме. В этом смысле большинство возможных убытков, понесенных в результате действий сертификационных органов, можно рассматривать как "косвенные" или "непрямые". Еще одно предложение заключалось в использовании в качестве критерия ограничения ответственности сертификационных органов элемента "предсказуемости". Было указано на возможную необходимость более углубленного изучения режима ответственности продавца товаров в соответствии с Конвенцией Организации Объединенных Наций о договорах международной купли-продажи товаров, который мог бы стать отправной точкой.

67. Рассмотрев широкий круг предложенных альтернатив, Рабочая группа обратилась к Секретариату с просьбой подготовить краткий доклад о существующих правовых режимах и используемых методах ограничения ответственности, в особенности в рамках международных конвенций, регулирующих вопросы грузовых и пассажирских перевозок. В этом докладе можно было бы также рассмотреть режим ответственности, установленный в соответствии с определенными национальными законами в отношении профессиональных категорий, которые в условиях использования бумажных документов выполняют функции, аналогичные тем, которые предусматриваются для сертификационных органов.

Минимальный стандарт ответственности

68. Было указано, что на нынешнем этапе обсуждения Рабочая группа еще не закончила рассмотрение вопроса о том, должны ли сертификационные органы предварительно получать полномочия от государственного ведомства. Было высказано мнение, что при возобновлении обсуждения этого вопроса в контексте продолжения рассмотрения проекта статьи B Рабочей группе следует также рассмотреть вопрос о том, должно ли такое государственное ведомство нести субсидиарную ответственность за действия уполномоченного им сертификационного органа.

69. В отношении пунктов 1 и 2 Рабочая группа пришла к предварительному выводу о том, что режим ответственности, применимый к сертификационным органам, должен быть основан на "двойном подходе": необходимо признать, что ответственность может варьироваться в зависимости от того, должен ли сертификационный орган действовать на основе стандартов, в обязательном порядке установленных государственным ведомством, или же он функционирует просто на основе стандартов, согласованных в частном порядке.

70. Было предложено предусмотреть возложение на любой сертификационный орган при выдаче сертификата обязательства, которое могло бы быть сформулировано следующим образом:

"Выдавая сертификат, сертификационный орган подтверждает, что он удостоверился в том, что:

1) 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 лица, которое разумно полагается на этот сертификат или на подпись в цифровой форме, подлинность которой может быть проверена публичным ключом, указанным в этом сертификате, - что указанный в этом сертификате держатель согласился с ним;

2) указанный в сертификате держатель владеет частным ключом, соответствующим указанному в сертификате публичному ключу;

3) публичный ключ держателя и частный ключ составляют действующую пару ключей;

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

и

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

Рабочая группа пришла к общему мнению, что большая часть предложенной формулировки по существу является приемлемой в качесте основы для дальнейшего обсуждения, поскольку устанавливает минимальный стандарт, от которого стороны не должны иметь возможность отходить по частной договоренности. В частности, никакая оговорка, ограничивающая ответственность сертификационного органа, не должна рассматриваться как подпадающая под защиту или льготы, которые предусматриваются единообразными правилами, если она противоречит вышеперечисленным требованиям. В случае заявлений об ответственности сертификационного органа этот орган будет считаться несущим ответственность за последствия выдачи сертификата, если он не сможет доказать, что он выполнил вышеперечисленные требования. Однако если сертификационный орган пожелает взять на себя более жесткие обязательства, чем перечисленные подтверждения, он должен иметь возможность сделать это путем включения соответствующих положений в типовые условия сертификации или иным способом.

71. Рабочая группа согласилась с тем, что описанный выше минимальный стандарт должен быть применим к выдаче сертификатов для целей подписей в цифровой форме, как они определены в проекте статьи A. В целом было решено, что в проекте единообразных правил не следует пытаться урегулировать другие действия, которые могут осуществляться сертификационными органами, или оказываемые ими услуги. Такие действия и услуги могут регулироваться любыми договорами между сертификационными органами и их клиентами или любыми другими применимыми нормами права (например, императивными нормами права, регулирующими допустимость оговорок об освобождении от ответственности).

Пункты 3 и 4

72. Рабочая группа сочла пункты 3 и 4 в целом приемлемыми по существу в качестве основы для дальнейшего обсуждения. В отношении пункта 3 было высказано общее мнение, что, хотя при подготовке пересмотренного варианта проекта статьи H, возможно, необходимо будет учесть принцип контрибутивной небрежности, конкретное положение, содержащееся в пункте 3, по-видимому, является теперь излишним ввиду решения Рабочей группы о том, что режим ответственности, применимый к сертификационным органам, не должен основываться лишь на небрежности. В пункте 4 было решено исключить слово "пользователем", с тем чтобы охватить этим положением и ущерб, понесенный любой заинтересованной стороной.

73. После обсуждения Рабочая группа обратилась к Секретариату с просьбой подготовить пересмотренный проект статьи H с учетом результатов вышеизложенного обсуждения и принятых решений.

## 3. Вопросы трансграничной сертификации

74. Рабочая группа провела обсуждение вопросов трансграничной сертификации на основе следующего проекта положения:

"Проект стати I

1) Сертификаты, выданные иностранными сертификационными органами, могут использоваться для подписей в цифровой форме на тех же условиях, что и подписи в цифровой форме, подпадающие под действие [настоящего Закона] [настоящих Правил], если они признаются уполномоченным сертификационным органом и этот уполномоченный сертификационный орган гарантирует в той же мере, что и свои собственные сертификаты, правильность пунктов сертификата, а также его действительность и законную силу.

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

75. Прежде чем Рабочая группа приступила к обсуждению вопросов трансграничной сертификации, было напомнено о том, что в соответствии с выданным ей Комиссией мандатом Рабочая группа должна проинформировать Комиссию о желательности и целесообразности подготовки единообразных правил в отношении подписей в цифровой форме, сертификационных органов и смежных вопросов (см. пункт 9 выше). В соответствии с этим мандатом от Рабочей группы на данном этапе не требуется завершения подготовки проекта текста для рассмотрения Комиссией на ее тридцатой сессии.

76. Рабочей группе было также напомнено о проведенном ею ранее в ходе рассмотрения проекта статьи B обсуждении вопроса о роли сертификационных органов, в частности о расхождении высказанных мнений относительно того, должны ли сертификационные органы получать у правительства разрешение на свою деятельность (см. пункты 40-50 выше). Рабочая группа в целом сочла, что она сможет продолжить обсуждение этого вопроса после рассмотрения вопросов ответственности сертификационных органов и трансграничной сертификации. В то же время было отмечено, что решение по вопросам, поднятым в проекте статьи B, будет также иметь последствия для режима трансграничной сертификации, предусматриваемого проектом единообразных правил.

77. В качестве общего замечания было высказано мнение, что пункты 1 и 2 несколько по-разному подходят к вопросу о соотношении сертификатов, выданных национальными сертификационными органами, и иностранных сертификатов. Пункт 1 позволяет национальным сертификационным органам гарантировать - в той же мере, что и в отношении своих собственных сертификатов - правильность содержащейся в иностранном сертификате информации, а также его действительность и законную силу.

В соответствии с пунктом 2 органу или ведомству, компетентному уполномочивать сертификационные органы в принимающем государстве, предоставляется возможность признавать сертификаты, выданные иностранными сертификационными органами, на устанавливаемых им самим условиях. Было высказано мнение, что вопросы, регулируемые пунктом 1, можно было бы назвать "перекрестной сертификацией", а ситуацию, регулируемую пунктом 2, точнее было бы назвать "трансграничным признанием". Эти различные вопросы правильнее было бы, по-видимому, рассмотреть по отдельности.

78. Было высказано мнение, что в пунктах 1 и 2 излагаются два различных альтернативных варианта возможного режима иностранных сертификатов в соответствии с проектом единообразных правил. Поддержку получили оба эти варианта. В то же время было высказано широко распространенное мнение, что эти два варианта отнюдь не обязательно следует рассматривать как взаимоисключающие. Хотя предложение изложить существо пунктов 1 и 2 в двух отдельных статьях получило поддержку, было высказано мнение о целесообразности более тщательного обсуждения вопроса о соответствующих сферах применения этих положений. Было указано, что пункт 1 по сути содержит положение о возложении ответственности на внутренний сертификационный орган в случае, если иностранный сертификат оказывается порочным, - ответственность, которая будет выводиться из проекта статьи Н. Пункт 2, в свою очередь, посвящен не вопросам ответственности, а правовым последствиям, которые могут проистекать непосредственно из иностранного сертификата, например в случаях, когда на иностранный сертификат будут ссылаться при рассмотрении спора в судах принимающего государства. Эти правовые последствия не обязательно будут основываться на существовании гарантии, предусмотренной в пункте 1, или зависеть от нее.

79. Ввиду принятого Рабочей группой решения рассмотреть в проекте единообразных правил не только сертификационные органы, лицензированные государственными ведомствами, но и "сертификационные органы рыночного типа" (см. пункты 48-50 выше), широкую поддержку получило мнение о том, что в проекте статьи I должны рассматриваться вопросы признания иностранных сертификатов, выдаваемых обоими видами сертификационных органов.

80. Было высказано мнение, что Рабочей группе следует также рассмотреть вопрос об условиях, на которых может производиться признание иностранных сертификатов. Такие условия могли бы устанавливаться в форме правительственных требований или закрепляться в соглашениях между национальными и иностранными сертификационными органами. Были представлены разъяснения в отношении возможного содержания таких соглашений между сертификационными органами. Было напомнено о том, что инфраструктура для использования публичных ключей нередко основывается на иерархии органов различного уровня. В рамках этих иерархических структур вполне могут существовать два этапа перекрестной сертификации. На начальном этапе, как предполагается, перекрестную сертификацию будут осуществлять лишь "основные органы" (т.е. органы, занимающиеся сертификацией технологии и методов в связи с использованием пар ключей и осуществляющие регистрацию подчиненных им сертификационных органов). На более позднем этапе, как предполагается, по мере развития этого сектора подчиненные сертификационные органы, занимающие более низкую ступень по сравнению с "основным органом", смогут принимать непосредственное участие в гарантировании правильности сертификатов, выданных иностранными сертификационными органами. Однако при разработке норм по вопросам перекрестной сертификации Рабочей группе следует учитывать возможность того, что - особенно в случае подписей в цифровой форме, предусматривающих наименьший уровень защиты, - может потребоваться обеспечить признание действительности иностранных сертификатов в отсутствие конкретного соглгашения между сертификационными органами. Поэтому было высказано мнение о необходимости разработки субсидиарного стандарта для признания поставленных в этих обстоятельствах иностранных подписей в цифровой форме.

81. Было указано, что включение положений, регулирующих вопросы трансграничного признания, может явиться важным шагом в направлении повышения доверия к сертификатам. Однако Рабочей группе необходимо тщательно проанализировать методы и процедуры такой трансграничной сертификации или признания. Было указано, что для того, чтобы определить, заслуживает ли иностранный сертификат доверия, получатель подписанного в цифровой форме сообщения, к которому

прилагается этот сертификат, должен рассмотреть ряд вопросов, например, следующие: уполномочен ли сертификационный орган, выдавший сертификат, совершать действия за границей; является ли цифровая подпись этого сертификационного органа подлинной; существуют ли правовые средства обжалования действий этого сертификационного органа; признается ли подпись в цифровой форме юридически значимой; и можно ли на основании подписи в цифровой форме привлечь поставившее ее лицо к ответственности.

82. Далее было указано, что с этой точки зрения перекрестная сертификация может по сути обеспечивать четыре различных уровня надежности. На самом высоком уровне внутренний сертификационный орган по просьбе стороны, полагающейся на иностранный сертификат, будет гарантировать содержание этого сертификата на основе декларированного им знания процедур, приведших к выдаче сертификата, и тем самым принимать на себя всю ответственность за любые ошибки или иные пороки в сертификате. На уровне, непосредственно следующем за этим, внутренний сертификационный орган будет гарантировать содержание иностранного сертификата на основе полученной им информации о надежности иностранного сертификационного органа. На следующем уровне надежности внутренний сертификационный орган будет ограничивать свои обязательства гарантией надежности иностранного сертификационного органа, не беря при этом на себя никакой ответственности за содержание иностранного сертификата. На самом низком уровне внутренний сертификационный орган будет просто гарантировать, что он идентифицировал иностранный сертификационный орган на основании проверки подлинности его публичного ключа и подписи в цифровой форме. Рабочей группе было предложено при разработке положений о перекрестной сертификации или признании иностранных сертификатов обратить внимание на вопрос об уровне, устраивающем получателя сообщения.

83. В этой связи был проведен сравнительный анализ положения сертификационного органа, гарантирующего правильность и действительность иностранного сертификата, и финансового учреждения, гарантирующего аккредитив, выставленный иностранным банком. Приемлемость аккредитива для его бенефициара определяется такими факторами, как надежность иностранного банка, выставившего аккредитив, и возможность принудительного взыскания по этому аккредитиву в стране бенефициара. В некоторых случаях бенефициар может настаивать на предоставлении местным банком контргарантии. Адекватный уровень защиты по этим операциям устанавливается бенефициаром аккредитива с учетом степени риска, который готов принять на себя бенефициар. Точно так же стороне сделки, связанной с использованием иностранного сертификата, может быть достаточно знать, например, что этот сертификат выдан солидным иностранным сертификационным органом, и она не будет испытывать необходимости в получении гарантии от внутреннего сертификационного органа. Было высказано опасение, что проект статьи I может пониматься как сдерживающий или не допускающий использование сертификатов, которые не гарантированы внутренним сертификационным органом, даже в случае операций, участники которых вполне готовы согласиться и на меньший уровень защиты и правовой определенности. Важно обеспечить, чтобы проект статьи I предусматривал гибкое регулирование вопросов перекрестной сертификации и трансграничного признания.

84. В связи с приведенным выше сопоставительным анализом роли сертификационных органов и роли банков в контексте операций с аккредитивами было высказано общее мнение, что при подготовке единообразных правил в отношении признания сертификатов следует учитывать, что подписи в цифровой форме могут использоваться не только для передачи прав, но и для передачи обязательств, например в случае использования подписи в цифровой форме в уведомлении об уступке долга. Соответственно, риск, связанный с доверием к подписи в цифровой форме, возможно, необходимо будет переносить на получателя или на автора подписи в цифровой форме, в зависимости от вида сделки.

85. В связи с возможной сферой охвата перекрестной сертификации и признания было указано, что функции, выполняемые сертификационным органом, в какой-то мере напоминают функции, выполняемые в некоторых правовых системах государственным нотариусом. Так, в ряде правовых систем определенные виды операций требуют, чтобы государственный нотариус - или другое официальное лицо, выполняющее аналогичные функции, - удостоверил определенные факты (например, личность одной из

сторон) или засвидетельствовал элементы сделки (например, подписи сторон или подлинность документа). Однако круг сделок, требующих такого нотариального удостоверения, в разных правовых системах различен, и было бы нецелесообразно пытаться унифицировать существующие в разных странах требования в отношении оформления основных сделок.

86. Было высказано мнение, что признание иностранных сертификатов нередко будет предоставляться на основе взаимности и что поэтому полномочия по такому признанию будут вытекать из двусторонних и многосторонних международных соглашений. Были высказаны оговорки в отношении включения в проект единообразных правил ссылки на взаимность ввиду различного понимания "взаимности" в разных правовых системах. С другой стороны, предложение добавить ссылки на двусторонние и многосторонние международные соглашения вызвало самую разную реакцию. В поддержку этого предложения было указано, что включение ссылки на двусторонние или многосторонние международные соглашения позволит пояснить, что проект единообразных правил не затрагивает международных обязательств, которые могут быть приняты на себя государствами, например, в рамках региональных соглашений об экономической интеграции и сотрудничестве. Вместе с тем было также указано, что никакой специальной ссылки на такие соглашения не требуется, поскольку ничто в пункте 1 не препятствует осуществлению принимающим государством перекрестной сертификации и признания иностранных сертификатов посредством таких соглашений. Далее было высказано мнение, что вместо того, чтобы включать в проект статьи I ссылку на международные соглашения, Рабочей группе следует рассмотреть вопрос о разработке материальных норм о признании иностранных сертификатов. Было также отмечено, что включение в статью I ссылки на двусторонние и многосторонние международные соглашения будет оправдано лишь в двух случаях: a) если Рабочая группа придет к выводу, что разработка унифицированных правил в отношении признания является невозможной; или b) если такая ссылка будет относиться к соглашениям, обеспечивающим более благоприятный уровень признания иностранных сертификатов, чем предусмотренный в проекте единообразных правил.

87. Было указано, что пункты 1 и 2 содержат два различных варианта, имеющихся в распоряжении принимающего государства, в зависимости от того, требует ли функционирование сертификационного органа предварительной правительственной санкции. Вместе с тем было высказано опасение, что при прочтении проекта этой статьи в сочетании с проектом статьи B, требующим от сертификационных органов, учрежденных в принимающем государстве, предварительного получения такой санкции, пункт 1 может быть истолкован как допускающий признание сертификатов, выданных иностранными сертификационными органами, которые в соответствии с национальным законодательством не уполномочены осуществлять свою деятельность, и при этом лишающий юридической силы сертификаты, выданные внутренними сертификационными органами, не получившими в принимающем государстве требуемых полномочий. В этой связи был задан вопрос о том, заключается ли цель проекта статьи I в том, чтобы позволить уполномоченному правительством сертификационному органу придавать правовую силу сертификатам, выданным другими, не уполномоченными сертификационными органами, будь то внутренними или иностранными. Если предполагаемая цель проекта статьи I заключается именно в этом, то его текст, возможно, необходимо изменить с учетом решения, которое будет принято Рабочей группой в отношении проекта статьи B.

88. Что касается гарантии, предусмотренной в пункте 1, то было указано, что в некоторых правовых системах могут возникнуть трудности при урегулировании этого вопроса посредством принятия общего положения без добавления более подробных положений, ввиду того, что предоставляемые сертификационными органами гарантии могут в разных странах весьма значительно различаться. При отсутствии какого-то общего понимания в отношении видов гарантий, предлагаемых сертификационными органами, внутренним сертификационным органам будет трудно взять на себя ответственность за сертификаты, выданные за границей.

89. После обсуждения различных точек зрения, высказанных в Рабочей группе, сложилось общее мнение о целесообразности урегулирования вопросов трансграничной сертификации в проекте единообразных правил. Хотя Рабочая группа сочла закрепленные в проекте статьи I принципы в целом приемлемыми, она решила, что на столь раннем этапе обсуждения этой темы было бы преждевременно

пытаться сформулировать конкретные положения, регулирующие эти вопросы. Секретариату было предложено подготовить пересмотренный проект статьи I с учетом вышеизложенного хода обсуждения и необходимости охвата как лицензированных государством, так и нелицензированных сертификационных органов. Секретариату было предложено провести различие между условиями и последствиями признания подписи в цифровой форме и сертификата, с одной стороны, и признанием сертификационного органа - с другой, а также представить соответствующие предложения, возможно, в форме вариантов, по регулированию этих различных вопросов.

1. Определения (продолжение)

b) Уполномоченные сертификационные органы (продолжение)

90. Завершив предварительное обсуждение проектов статей H и I, посвященных вопросам ответственности и перекрестной сертификации, Рабочая группа вернулась к обсуждению вопросов, связанных с определением "сертификационного органа" в проекте статьи B (см. пункты 40-49 выше). Было напомнено о том, что для того, чтобы учесть как случаи, когда сертификационные органы действуют на чисто частной основе, так и ситуации, когда от сертификационных органов требуется получение лицензии или иных полномочий от государственных органов, прежде чем им будет разрешено заниматься своей деятельностью, Рабочая группа в предварительном порядке постановила принять "двойной подход" (см. пункты 48-50 выше), который предполагает необходимость разработки широкого определения "сертификационного органа", охватывающего оба вида ситуаций. В этой связи было высказано мнение, что Рабочая группа могла бы рассмотреть возможность замены термина "сертификационный орган" ("certification authority") выражением "сертификационное предприятие" ("certification entity"), с тем чтобы избежать возможного толкования, будто функции сертификации обязательно выполняются лишь государственными органами. Хотя это предложение получило определенную поддержку, было напомнено, что понятие "сертификационный орган" ("certification authority") уже широко используется как государственными, так и частными субъектами. Рабочей группе было настоятельно предложено проявлять осторожность при утверждении терминологии, которая может идти вразрез с формирующейся практикой в области сертификации.

91. Было указано на то, что положения, закрепленные в настоящее время в проекте статьи B, регулируют различные аспекты вопроса о сертификационных органах. Некоторые пункты, такие, как пункт 3, по своей природе представляют собой чистое определение, тогда как другие положения, такие, как пункт 4, носят более оперативный характер и посвящены описанию функций, выполняемых сертификационными органами. В этой связи было предложено разбить проект статьи B на различные статьи, касающиеся, соответственно, определения сертификационных органов и описания их функций. Многие члены Рабочей группы придерживались мнения, что при изменении структуры проекта статьи B было бы целесообразно в дополнение к функции фиксации времени указать и другие функции, которые могут выполняться сертификационными органами, такие, как выдача пар ключей, ведение реестров, хранение записей и оказание других услуг, которые были охарактеризованы как "вспомогательные" по отношению к основным функциям, выполняемым сертификационными органами применительно к подписям в цифровой форме. Однако Рабочая группа в целом пришла к выводу о том, что рассмотрение таких вспомогательных услуг не должно вести к расширению сферы действия единообразных правил, которая определяется с помощью ссылки на "подписи в цифровой форме" в проекте статьи A.

92. В качестве одного из возможных способов разграничения правовых режимов, применимых к сертификационным органам, лицензированным или иным образом уполномоченным принимающим государством, и к неуполномоченным сертификационным органам, было предложено перечислить в проекте единообразных правил конкретные правовые последствия, которых можно ожидать от выдачи сертификатов уполномоченными сертификационными органами. В ответ на заданный вопрос о правовых последствиях, которые могут вытекать из выдачи сертификатов неуполномоченными сертификационными органами, было предложено урегулировать этот вопрос просто путем включения ссылки на статью 7 Типового закона. Хотя это предложение получило определенную поддержку, было указано, что в единообразных правилах было бы, возможно, целесообразно подробнее остановиться на правовых

последствиях сертификатов, выдаваемых чисто частными сертификационными органами. Согласно другому предложению, разграничение между уполномоченными и неуполномоченными органами можно было бы провести на основе различного набора функций, которые могут выполняться этими двумя видами органов. Было высказано общее мнение, что Рабочей группе на одной из будущих сессий, возможно, потребуется продолжить изучение этих вопросов.

93. В контексте обсуждения пункта 3 был поднят вопрос о том, обеспечивает ли упоминание "ключей физических и юридических лиц" достаточную ясность в ситуациях, когда криптографические ключи выдаются непосредственно электронным устройствам или используются такими устройствами в отсутствие прямого вмешательства со стороны человека. Рабочая группа напомнила о том, что этот вопрос уже обсуждался в контексте подготовки Типового закона, и в целом согласилась с возможной необходимостью продолжения обсуждения этого вопроса на более позднем этапе в связи с вопросами подписей в цифровой форме.

94. Что касается возможной структуры пересмотренного проекта статьи B, то внимание Рабочей группы было обращено на использовавшийся при подготовке Типового закона метод, в основе которого лежит сочетание нормативных положений и руководства по принятию таких положений. Использование этого метода позволило включить более подробные разъяснения содержания нормативных положений и иллюстрирующие их примеры, что облегчит их рассмотрение законодательными органами. Было предложено избрать такой же подход и в отношении единообразных правил. Было бы целесообразно включить в руководство по принятию пояснительный материал, особенно в отношении различных функций, выполняемых сертификационными органами. Рабочая группа сочла это предложение в целом приемлемым в качесте рабочей гипотезы, однако отложила принятие решения об окончательной форме единообразных правил.

95. После обсуждения Рабочая группа постановила изложить положения, содержащиеся в настоящее время в проекте статьи B, в двух отдельных статьях, посвященных, соответственно, расширенному определению "сертификационного органа" и функциям, выполняемым сертификационными органами. Было решено, что общее определение "сертификационного органа" должно основываться на тексте пункта 3 проекта статьи B. Было решено добавить к ссылке на "физические и юридические лица" и ссылку на "электронные устройства", заключив ее в квадратные скобки до будущего обсуждения этого вопроса Рабочей группой. В дополнение к общему определению "сертификационного органа" пересмотренная статья с определением должна включать определение "лицензированных", "уполномоченных" или "аккредитованных" сертификационных органов, которое могло бы быть подготовлено на основе пункта 1 проекта статьи B. Что касается элементов, содержащихся в пунктах 2 и 5 этого проекта статьи, то их следует отразить в той части руководства по принятию проекта единообразных правил, которая будет посвящена определению "уполномоченных" сертификационных органов.

96. Было достигнуто общее согласие в отношении того, что отдельная статья, в которой должны рассматриваться различные функции, выполняемые сертификационными органами, могла бы быть подготовлена на основе текста пункта 4 проекта статьи B. Было также решено, что объем будущей статьи о функциях сертификационных органов было бы, по-видимому, целесообразно расширить путем указания в ней и других функций. В этих целях можно было бы использовать элементы, содержащиеся в имеющихся или рассматриваемых на предмет принятия законодательных актах, руководящих принципах и типовых контрактах, касающихся сертификационных органов. В редакционном плане было высказано общее мнение о том, что содержащуюся в пункте 4 ссылку на "сообщения, защищенные с помощью подписей в цифровой форме", по-видимому, следует изменить, с тем чтобы она не могла толковаться как устанавливающая какие-либо особые последствия применительно к вопросу о приемлемости методов защиты, используемых сертификационными органами.

97. Секретариату было предложено подготовить пересмотренный вариант проекта статьи B с учетом изложенного выше хода обсуждения и принятых решений.

c) Сертификаты

98. Рабочая группа провела обсуждение определения сертификатов на основе следующего проекта положения:

"Проект статьи C

В сертификате, выдаваемом уполномоченным сертификационным органом в форме сообщения данных или как-либо иначе, по меньшей мере указываются:

a) имя пользователя [и адрес и место нахождения коммерческого предприятия];

b) [день и год рождения] [достаточные идентификационные данные] пользователя, если пользователем является физическое лицо;

c) если пользователем является юридическое лицо, то название компании и любая соответствующая информация для идентификации этой компании;

d) название, адрес или место нахождения сертификационного органа;

e) публичный криптографический ключ пользователя;

f) любая необходимая информация, указывающая, каким образом проверка подлинности публичного криптографического ключа пользователя может быть произведена получателем подписи в цифровой форме, представленной в соответствии с сертификатом;

g) серийный номер сертификата; и

h) [дата выдачи и дата истечения срока действия] [срок действия] сертификата".

99. С самого начала Рабочей группе было напомнено о том, что в ходе обсуждения определения "сертификационного органа" она договорилась в качестве рабочей гипотезы использовать гибкий подход, который охватывал бы сертификаты, выданные как сертификационными органами, уполномоченными правительствами, так и сертификационными органами, действующими за пределами правительственной инфраструктуры для использования публичных ключей, не исключая на нынешнем этапе никакую из этих альтернатив. В соответствии с этой рабочей гипотезой во вводной части проекта статьи C следует исключить слово "уполномоченным".

100. Были высказаны общие замечания в отношении используемой в проекте статьи C терминологии, в частности в отношении употребления слова "пользователь" применительно к держателю частного ключа пары криптографических ключей. Было высказано мнение, что может возникнуть ошибочное понимание, будто под этим словом имеется в виду получатель сообщения, которого можно рассматривать как "пользователя" сертификата или публичного ключа, используемого для проверки подлинности подписи в цифровой форме. Был предложен ряд альтернативных формулировок, включая выражения "владелец пары ключей", "держатель сертификата", "держатель частного ключа". Было решено поручить Секретариату пересмотреть терминологию, используемую в проекте статьи C и в остальных положениях проекта единообразных правил, и подготовить предложения в целях устранения возможных неясностей.

101. Многие члены Рабочей группы высказались за то, что в проекте статьи C следует сначала определить понятие "сертификат", прежде чем устанавливать, каким должно быть его содержание. В частности, была предложена следующая формулировка определения: "Сертификатом является сообщение данных, которое предназначено в качестве сертификата, в котором указывается сертификационный орган, публичный ключ пользователя и имя пользователя и которое подписано в цифровой форме сертификационным органом". Другое предложение заключалось в разработке определения на основе

элементов сертификата, изложенных в записке Секретариата, где сертификат определяется как электронная запись, в которой указывается публичный ключ и имя подписчика сертификата в качестве "субъекта" сертификата и подтверждается, что предполагаемое подписывающее лицо, указанное в сертификате, является держателем соответствующего частного ключа (A/CN.9/WG.IV/WP.71, пункт 36). Было высказано мнение, что определение, построенное по типу изложенного в последнем предложении, было бы в целом приемлемым. Однако в таком определении следует конкретно указать, что если сертификат передается по электронным средствам связи, то он должен быть подписан сертификационным органом в цифровой форме, чтобы гарантировать подлинность этого сертификата в отношении как его содержания, так и источника.

102. Был задан вопрос о том, не означают ли слова "по меньшей мере", использованные во вводной части проекта статьи C в связи с содержанием сертификата, что сертификат, который не содержит всю информацию и данные, перечисленные в проекте статьи C, не будет считаться сертификатом по смыслу проекта единообразных правил. В ответ на это было указано, что в проекте статьи C в ее нынешнем виде перечисляется ряд обязательных элементов, которые должны содержаться в сертификате, чтобы он мог считаться таковым в соответствии с проектом единообразных правил. Для обеспечения большей ясности было предложено сделать определение "сертификата" самостоятельным положением, выделив перечень информации, которая должна указываться в сертификате, в отдельное положение.

103. Рабочая группа обсудила объем информации, которая должна содержаться в сертификате. В качестве общего замечания было высказано мнение, что число обязательных элементов должно быть минимальным и что к ним должна относиться в основном информация, которая требуется пользователю сертификата для проверки подлинности используемой в сообщении данных подписи в цифровой форме. Была высказана обеспокоенность в связи с тем, что включение в перечень данных, которые должны содержаться в сертификате, ненужных элементов может привести к непреднамеренному исключению из сферы действия проекта единообразных правил ряда сертификатов, которые в остальном могут быть достаточны для тех целей, в которых они были выданы. Было высказано мнение о важности учета разницы между информацией, содержащейся в сертификате, и мерами, которые должны приниматься сертификационным органом для установления точности этой информации. Чем больше информации содержится в сертификате, тем больше опасность того, что сертификационному органу придется нести ответственность. В соответствии с этим было предложено не устанавливать в проекте единообразных правил минимальных требований в отношении содержания сертификата.

104. Был предложен другой подход, основанный на результатах обсуждения вопроса ответственности сертификационных органов, в ходе которого Рабочая группа пришла к выводу, что в случае ошибочной идентификации лица или ошибочной атрибуции публичного ключа какому-либо лицу сертификационный орган должен нести ответственность за убытки, понесенные любой потерпевшей стороной, если этот сертификационный орган не сможет доказать, что он сделал все возможное для недопущения ошибки (см. пункт 58 выше). Было высказано общее мнение, что установление в отношении сертификационного органа требования соблюдать адекватные процедуры удостоверения точности информации или надлежащей идентификации держателей частных ключей при одновременном предоставлении этому сертификационному органу возможности уклоняться от ответственности путем выдачи сертификатов, не содержащих минимального объема информации, которая должна быть изложена в сертификате, не будет отвечать цели защиты конечных пользователей.

105. Было высказано мнение, что если сертификат должен будет отвечать ряду определенных обязательных требований в отношении его содержания, то сертификационный орган не сможет уклониться от ответственности указанным выше способом. В этой связи было напомнено о том, что в ходе обсуждения вопроса ответственности сертификационных органов было выдвинуто предложение, согласно которому на любом сертификационном органе при выдаче сертификата должна лежать обязанность подтвердить, что он проверил ряд элементов (см. пункт 70 выше). Это предложение получило широкую поддержку. После обсуждения Рабочая группа пришла к выводу, что этот вопрос не удастся углубленно рассмотреть на нынешней сессии. Было решено при первой же возможности возобновить

обсуждение этого вопроса на основе вариантов, которые должны быть подготовлены Секретариатом с учетом хода вышеизложенного обсуждения.

106. В отношении, в частности, данных, которые могут требоваться для идентификации держателя частного ключа, было предложено объединить подпункты (a), (b) и (c) в отдельное положение. В этой связи было отмечено, что во многих странах информация, к примеру, о дате рождения лица охраняется как носящая личный характер, и ее раскрытие с помощью электронных средств может регулироваться специальными нормами. Поэтому было предложено отказаться от требования указания в сертификате такого рода информации личного характера. В ответ на это было указано, что в определенных обстоятельствах лицо, обращающееся за выдачей сертификата, может дать согласие на передачу определенных сведений личного характера или источников дополнительной информации или быть заинтересовано в этом. Проект единообразных правил не должен исключать такую возможность в случаях, когда передача сведений личного характера с согласия соответствующего лица не противоречит применимым нормам в отношении защиты данных или публичному порядку в государстве, в котором подается заявка на выдачу сертификата или выдается такой сертификат. Было высказано общее мнение о том, что вопросы, касающиеся защиты данных, выходят за рамки проекта единообразных правил и что проект статьи C должен ограничиваться требованием обеспечения достаточной идентификации в соответствии с применимыми законами о защите данных.

107. Было предложено указать в подпункте (a) "имя или идентификацию" пользователя, с тем чтобы охватить ситуации, когда для идентификации пользователя используется не имя или название, а другие средства, такие, как номер счета - ситуация, возможная в случае сертификатов в связи с операциями с кредитными карточками. Против этого предложения были выдвинуты возражения на том основании, что это может стимулировать использование анонимных сообщений и сертификатов, что будет идти вразрез с целью содействия повышению правовой определенности в сфере электронной торговли. Рабочей группе было настоятельно рекомендовано сохранить в качестве одного из важнейших элементов сертификата указание на имя держателя частного ключа.

108. Для целей обеспечения надлежащей идентификации держателя частного ключа было предложено сохранить в проекте статьи C указание на дополнительные элементы идентификации, такие, как адрес в случае физических лиц и регистрационный номер в случае юридических лиц, поскольку одного имени физического лица или названия компании может оказаться недостаточно для идентификации этого лица или компании.

109. Было высказано мнение, что в некоторых случаях использование подписи в цифровой форме может ограничиваться определенными видами сделок, например в результате ограниченности полномочий лица, поставившего свою подпись, на принятие обязательств от лица компании, от имени которой заключается эта сделка. В связи с этим было высказано мнение, что в сертификате должна содержаться информация о таких ограничениях или пределах или указание на их источник. В ответ на это предложение было отмечено, что вопрос о том, в каких пределах можно доверять подписи в цифровой форме, затрагивает ряд сложных правовых проблем, которые касаются не только электронной торговли. В условиях использования документов в бумажной форме к документу, подписанному от руки, отнюдь не обязательно должна прилагаться декларация с изложением ограничений полномочий автора подписи, если таковые имеются. Рабочей группе было настоятельно рекомендовано не устанавливать в отношении подписи в цифровой форме более жестких требований, чем те, которые применяются к собственноручным подписям.

110. Рабочей группе было напомнено о проведенном ею ранее обсуждении вопросов о потребителях и об ответственности сертификационного органа, а также о возможных ограничениях ответственности и случаях освобождения от нее в соответствии с национальным законодательством или типовыми условиями сертификации соответствующего сертификационного органа. Было предложено обязать сертификационный орган указывать такие ограничения или включать ссылку на доступный пользователю документ, из которого можно получить информацию об этих ограничениях. Было также предложено предусмотреть в проекте единообразных правил последствия отсутствия такого указания в сертификате.

Наряду с этим было высказано мнение, что в тех случаях, когда срок действия сертификата ограничен, информация о таком ограничении должна указываться в сертификате в форме даты истечения срока действия или операционного периода. Было высказано мнение, что для защиты пользователей сертификатов важно обеспечить получение ими информации о сроке действия сертификатов и не накладывать на них риск возможной выдачи сертификата, не содержащего такого указания. Поэтому в проект единообразных правил следует включить субсидиарное положение, устанавливающее срок действия сертификата в случаях, когда в самом сертификате такое указание отсутствует. Однако в ответ на это было указано, что наличие такого правила может быть истолковано как означающее, что сертификационный орган вправе не указывать срок действия, или операционный период сертификата.

111. Были подняты вопросы в отношении характера информации, которую сертификационные органы в состоянии предоставлять пользователям их услуг в доступной форме с учетом существующей в настоящее время технологии. В ответ на это было указано, что существующая технология позволяет сертификационным органам прилагать к выдаваемым им сертификатам или иным образом увязывать с ними дополнительную информацию, такую, как их собственные типовые условия сертификации или информация, которая по их выбору может предоставляться для этих целей держателями частных ключей. Однако многие компьютерные системы, используемые в настоящее время клиентами сертификационных органов, по-прежнему не в состоянии обеспечить доступ ко всей такой информации. Помимо наличия этих технических трудностей, важно учитывать, что определенная информация, которая может прилагаться к сертификатам, может изначально поступать от держателей частных ключей и передаваться по их просьбе. В этих случаях важно проводить различие между элементами сертификата, которые удостоверены сертификационным органом (например, личность держателя частного ключа), и другими элементами, сообщенными клиентами без проверки их подлинности (например, информация об ограничениях на использование частных ключей в рамках корпорации). Сертификационный орган не должен нести ответственности за точность такой непроверенной информации.

112. Многие члены Рабочей группы высказались за то, что без ущерба для другой возможной информации, которую сертификационные органы могут предоставлять своим клиентам, они должны подтверждать и гарантировать проведение ими проверки точности и полноты информации, которая должна включаться в сертификат в обязательном порядке.

113. Обсудив мнения, высказанные в связи с проектом статьи C, Рабочая группа постановила добавить в этот проект статьи определение "сертификата". Обязательные элементы содержания сертификата должны быть изложены в отдельном положении, которое также должно регулировать последствия отсутствия этих обязательных элементов сертификата. Это положение должно отражать элементы, которые указаны в подпунктах (a), (b) и (c), сведенных в единое пересмотренное положение, и включать также информацию, упомянутую в подпунктах (d), (e) и (h) проекта статьи C. Рабочая группа пришла к выводу, что сертификационный орган не в состоянии сертифицировать информацию, указанную в подпункте (f), и поэтому постановила исключить этот подпункт. Было решено заключить подпункт (g) в квадратные скобки и рассмотреть его на более позднем этапе в качестве одного из возможных вариантов, поскольку не все сертификаты могут идентифицироваться серийным номером. В пересмотренном проекте статьи C должна содержаться прямая ссылка на применимость норм внутреннего права, касающихся защиты данных, к информации, которая должна содержаться в сертификате. Секретариату было предложено подготовить пересмотренный проект статьи C, отразив в нем в качестве возможных вариантов различные высказанные мнения и выводы, к которым пришла Рабочая группа.

### 4. Подписи, проставляемые физическими и юридическими лицами

114. Рабочая группа провела обсуждение этого вопроса на основе следующего проекта положения:

"Проект статьи D

1. Физические и юридические лица могут на равных основаниях получать сертификацию криптографических публичных ключей, используемых исключительно для целей идентификации.

2. 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".

115. Ряд делегаций выразили мнение, что проект статьи D следует исключить. Было указано на нецелесообразность проведения разграничения между юридическими и физическими лицами для целей подписей в цифровой форме ввиду того, что в Типовом законе, где понятие "лицо" охватывает как физических, так и юридических лиц, такое разграничение не проводится. Кроме того, было указано, что положения пункта 2 могут необоснованно противоречить другим сводам правовых норм, например агентскому праву, и нормам акционерного права, касающимся представительства компаний физическими лицами. В дополнение к этому было указано, что содержащаяся в пункте 2 норма, как представляется, возлагает на пользователей подписями в цифровой форме бремя, выходящее за рамки существующих требований в отношении собственноручных подписей.

116. В то же время было высказано мнение, что проект статьи D, и в частности пункт 2, преследует полезную цель. В частности, в тех случаях, когда ни одна из применимых норм права не определяет конкретно форму, в которой физическое лицо может ставить от имени юридического лица юридически значимую подпись, субсидиарное правило, подобное закрепленному в пункте 2, может дать полезное представление о том, в каких обстоятельствах можно доверять подписи в цифровой форме, считающейся подписью юридического лица. Была выражена поддержка сохранению пункта 2 при условии изменения формулировки этого положения, с тем чтобы четко указать, что, хотя в нем и содержится ссылка на "физическое лицо, уполномоченное действовать от имени" юридического лица, его цель не заключается в подмене собой положений внутреннего агентского права. Таким образом, вопрос о том, имеет ли физическое лицо фактические и юридические полномочия действовать от имени юридического лица, будет регулироваться соответствующими правовыми нормами за рамками единообразных правил.

117. После обсуждения Рабочая группа постановила заключить проект статьи D в квадратные скобки, с тем чтобы продолжить его обсуждение на одной из следующих сессий.

## 5. Атрибуция сообщений, подписанных в цифровой форме

118. Рабочая группа провела обсуждение этого вопроса на основе следующего проекта положения:

"Проект статьи E

1. Составитель сообщения данных, на котором проставлена подпись составителя в цифровой форме, связан содержанием сообщения таким же образом, как если бы это сообщение существовало в [собственноручно] подписанной форме в соответствии с законом, применимым к содержанию этого сообщения.

2. Адресат сообщения данных, на котором проставлена подпись в цифровой форме, имеет право считать это сообщение данных сообщением составителя и действовать на основании этого предположения, если:

a) для установления того, что это сообщение данных является сообщением составителя, адресат надлежащим образом применил публичный ключ составителя к сообщению данных в полученном виде и применение публичного ключа составителя показало, что полученное сообщение данных было закодировано с помощью частного криптографического ключа составители и что первоначальное сообщение не было изменено после его кодирования посредством использования публичного криптографического ключа составителя;

или

b) сообщение данных, полученное адресатом, явилось результатом действий лица, взаимоотношения которого с составителем или любым представителем составителя дали такому лицу возможность получить доступ к частному криптографическому ключу составителя.

3. Пункт 2 не применяется:

a) с момента, когда адресат узнал или должен был узнать, если бы он запросил информацию у уполномоченного сертификационного органа или как-либо иначе проявил разумную осмотрительность, что срок действия публичного криптографического ключа составителя истек или что сертификат, выданный этим сертификационным органом, был аннулирован или его действие было приостановлено;

или

b) в случае, предусмотренном пунктом 2(b), с момента, когда адресат узнал или должен был узнать, если бы он проявил разумную осмотрительность или использовал любую согласованную процедуру, что данное сообщение данных не являлось сообщением данных составителя".

119. Было высказано мнение, что проект статьи E следует исключить. В поддержку этого мнения было указано, что этот проект статьи лишь содержит конкретизированный применительно к данному сектору вариант статьи 13 Типового закона и может создать неопределенность в отношении возможной взаимосвязи двух положений. Другое мнение заключалось в том, что этот проект статьи необходимо исключить, поскольку он может быть неверно истолкован как вторгающийся в сферу права, применимого к коммерческой сделке, для которой была использована подпись в цифровой форме. Например, положения пункта 1, согласно которым составитель сообщения данных "связан содержанием сообщения" могут быть неверно истолкованы как касающиеся общего договорного права.

120. Возобладала точка зрения о том, что, хотя конкретные формулировки проекта статьи E, возможно, потребуется изменить, содержащийся в пункте 1 принцип полезен, поскольку он устанавливает правовые последствия использования подписи в цифровой форме. Что же касается того, каким образом этот принцип может быть выражен, то было предложено изменить формулировку пункта 1, придав ей форму опровержимой презумпции, согласно которой держатель подписи в цифровой форме будет считаться лицом, подписавшим сообщение данных, на котором проставлена подпись в цифровой форме.

121. В отношении возможности урегулирования вопроса об атрибуции сообщений, подписанных в цифровой форме, с помощью презумпций, опровержимых или неопровержимых, было указано, что, возможно, необходимо провести дальнейшее разграничение на основе вида сделок, в которых могут использоваться подписи в цифровой форме. Например, один и тот же стандарт не может применяться и для сугубо коммерческих сделок между долгосрочными торговыми партнерами, и для представления налоговых деклараций государственным органам.

122. Было указано, что в положении, аналогичном тому, которое содержится в пункте 1, может потребоваться провести разграничение между различными видами подписей в цифровой форме (например, на основе различных уровней надежности, достигаемых с помощью разных алгоритмов, и соответствующей разницы в расходах в связи с подписью в цифровой форме) и различными обстоятельствами, при которых подписи в цифровой форме могут использоваться. Было отмечено, что при подготовке пересмотренного проекта пункта 1 можно было бы учесть следующие категории: используется ли подпись в цифровой форме вне рамок любого существовавшего ранее контракта между сторонами; используется ли подпись в цифровой форме в рамках договорных отношений; связана ли подпись в цифровой форме с выдачей сертификата неаккредитованным сертификационным органом; или был ли выдан сертификат полномочным сертификационным органом. Было отмечено также, что при рассмотрении различных степеней риска, связанных с процессом использования подписи в цифровой форме в случае подлога, особое внимание следует уделить ситуации, когда подлог имеет место до выдачи пары ключей. В таких ситуациях в отсутствие какого-либо соглашения между сторонами бремя

доказывания наличия связи между подписью в цифровой форме и отправителем должен нести получатель. Если сертификат был выдан и он является надлежащим и действительным, то бремя доказывания может быть перенесено. Другое предложение заключалось в том, что применительно к сообщениям, сертифицированным сертификационным органом, сторона, назначившая конкретный сертификационный орган, должна нести риск, связанный с использованием сертификатов, выданных этим сертификационным органом.

123. Были высказаны сомнения в отношении того, следует ли при пересмотре проекта статьи E принимать во внимание все вышеназванные категории. Было напомнено, в частности, о том, что в контексте обсуждения вопросов ответственности Рабочая группа решила сосредоточить внимание на ситуациях, когда сертификат был выдан. Однако было выражено общее мнение о том, что при подготовке пересмотренного проекта статьи E для его рассмотрения Рабочей группой на одной из будущих сессий необходимо учесть все или некоторые из предложенных категорий.

124. После обсуждения Рабочая группа решила, что необходимо пересмотреть положение об атрибуции сообщений, подписанных в цифровой форме, для дальнейшего рассмотрения Рабочей группой и что такое положение может быть разработано на основе пункта 1 проекта статьи E. Было выражено общее мнение, что для уточнения связи между статьей E и статьями 7 и 13 Типового закона могут потребоваться соответствующие комментарии. Секретариату было предложено подготовить пересмотренный проект статьи E с возможными вариантами, отражающими вышеизложенное обсуждение.

### 6. Аннулирование сертификатов

125. Рабочая группа обсудила вопрос аннулирования сертификатов на основе следующего проекта положения:

"Проект статьи F

1. Держатель сертифицированной пары ключей может аннулировать соответствующий сертификат. Аннулирование вступает в силу с момента его [регистрации] [получения] сертификационным органом.

2. Держатель сертифицированной пары ключей обязан аннулировать соответствующий сертификат, если держатель узнает, что частный криптографический ключ был утерян или скомпрометирован или подвергается опасности неправильного использования в других отношениях. Если держатель не аннулирует сертификат в такой ситуации, то держатель несет ответственность за любой ущерб, понесенный третьими сторонами, которые полагались на содержание сообщений, в результате того, что держатель не произвел аннулирования".

Пункт 1

126. Были высказаны общие замечания по поводу смысла пункта 1. Отмечалось, что держатель частного ключа всегда должен иметь право требовать, чтобы сертификационный орган аннулировал сертификат. То обстоятельство, что аннулирование вступает в силу по получении или регистрации сертификационным органом, не должно толковаться как ограничение этого права. Кроме того, тот факт, что аннулирование вступает в силу по получении или регистрации сертификационным органом, не должен толковаться в том смысле, что третьи стороны обязаны удостовериться в действительности сертификата (например, в том, что сертификат не был аннулирован), прежде чем они будут полагаться на сертификат; это предложение вызвало целый ряд возражений в Рабочей группе (см. пункт 60 выше).

127. Были высказаны различные мнения по поводу момента вступления аннулирования в силу. Согласно одной точке зрения, аннулирование должно вступать в силу с момента регистрации сертификационным органом, поскольку момент получения в некоторых случаях будет трудно установить, в результате чего возникнет неопределенность в отношении момента прекращения действия сертификата. Другое мнение сводилось к тому, что при аннулировании сертификата сертификационный орган должен быть обязан действовать оперативно, с тем чтобы не допустить любого ущерба, который может понести держатель частного ключа или третьи стороны, например, в результате случайного принятия сертификата, после того, как держатель от него отказался. Таким образом, вступление в силу аннулирования сертификата следует поставить в зависимость от мер, которые должен принять сертификационный орган, действия которого находятся вне сферы контроля держателя частного ключа.

128. Был поднят вопрос о возможных последствиях регистрации аннулирования сертификата. В этой связи было высказано мнение, что понятие регистрации аннулирования сертификата может быть неполностью адекватным для целей проекта статьи F, который предназначен, среди прочего, для обеспечения того, чтобы третьи стороны в соответствующих случаях были уведомлены о том, что тот или иной сертификат был аннулирован. Было отмечено, что по получении требования об аннулировании сертификационному органу в некоторых случаях придется проверить подлинность такого требования, а эта процедура в зависимости от обстоятельств может повлечь определенные задержки. Таким образом, надлежащим моментом полного вступления в силу такого аннулирования является момент опубликования соответствующей информации путем введения ее в общедоступную базу данных, которую ведет сертификационный орган, или с помощью другого соответствующего способа.

129. В свете последних замечаний было указано, что для цели установления момента, с которого сертификат считается аннулированным, момент получения требования об аннулировании все же предпочтительнее момента регистрации. Однако, если понятие получения таких требований будет сочтено недостаточно точным, получение может быть совмещено с какой-либо мерой, которую сертификационный орган впоследствии должен будет принять для придания силы такому аннулированию, например, с опубликованием аннулирования или уведомления о нем.

130. Для содействия обсуждению этого вопроса Рабочей группе было предложено изучить общие последствия выбора момента вступления аннулирования в силу, а также вопрос о том, какие стороны могут быть затронуты таким аннулированием. Момент вступления аннулирования в силу будет иметь ключевое значение для определения ответственности соответственно держателя частного ключа и сертификационных органов как в отношениях между собой, так и в отношении третьих сторон. Было указано, что Рабочей группе было бы целесообразно рассмотреть каждую из этих ситуаций в отдельности. В поддержку этого предложения отмечалось, что каждый из альтернативных вариантов, содержащихся в настоящее время в пункте 1, имеет свои достоинства. Применительно к отношениям держателя частного ключа и сертификационного органа было бы целесообразно предусмотреть, что аннулирование должно вступать в силу по получении сертификационным органом требования об аннулировании от держателя частного ключа. Что же касается третьих сторон, то было бы более целесообразно предусмотреть требование о том, что для вступления уведомления в силу необходима предварительная регистрация или опубликование.

131. Было отмечено, что момент вступления аннулирования в силу имеет значительные последствия для ответственности сертификационного органа и что оба эти вопроса следует урегулировать согласованно. Было указано, что в пункте 4 проекта статьи H предусматривается, что, если уполномоченный сертификационный орган получил уведомление об аннулировании сертификата, он немедленно регистрирует такое аннулирование. Если сертификационный орган не делает этого, он несет ответственность за любой ущерб, понесенный в результате этого пользователем. Таким образом, если в проекте единообразных правил будет предусмотрено, что аннулирование сертификата вступает в силу в момент его получения, то пункт 4 проекта статьи H будет необходимо исключить, поскольку отпадает возможное основание для ответственности сертификационного органа за вину или небрежность при регистрации аннулирования. С другой стороны, если аннулирование сертификата будет вступать в силу в момент его регистрации, то никакого другого положения, помимо пункта 4 проекта статьи H, возможно, не потребуется.

132. В ответ на это замечание было указано, что содержащееся в пункте 4 проекта статьи H правило необходимо сохранить, независимо от того, какой выбор из двух альтернативных вариантов, предусматриваемых в настоящее время в пункте 1 статьи F, сделает Рабочая группа. Задержка в регистрации требования об аннулировании может послужить причиной определенного ущерба либо для собственника, либо для полагающейся на сертификат стороны, и поэтому правило об ответственности за последствия задержки в регистрации будет необходимо.

133. В этой связи было указано, что международные стандарты и рекомендации, касающиеся электронной сертификации и удостоверения подлинности, например подготавливаемые Международной торговой палатой руководящие принципы единообразной международной практики удостоверения подлинности и сертификации, отражают принцип, согласно которому сертификационный орган должен принимать незамедлительные меры в связи с требованием об аннулировании сертификата. Однако, как было отмечено ранее, в осуществлении такого требования может возникнуть определенная задержка, особенно в том случае, когда обстоятельства заставят сертификационный орган провести ту или иную проверку, например подтвердить полномочия лиц, затребовавших аннулирование от имени держателя частного ключа. Во избежание непреднамеренного использования сертификата в тот период, когда сертификационный орган осуществляет проверку требования о его аннулировании, было предложено включить в проект единообразных правил положение, согласно которому сертификационный орган должен приостановить действие сертификата немедленно по получении требования держателя частного ключа. Было пояснено, что в отличие от аннулирования, которое прекращает действие сертификата, приостановление является временной мерой, которая приостанавливает его действие лишь на определенный срок.

134. Предложение о том, чтобы помимо понятия полного аннулирования ввести понятие приостановления действия сертификата, получило поддержку. В то же время было указано, что вопросы такого приостановления необходимо урегулировать в отдельном положении, поскольку понятие и последствия приостановления отличаются от понятия и последствий аннулирования.

135. Обсудив различные высказанные мнения, Рабочая группа решила, что вопрос об аннулировании сертификатов является важной частью надлежащего правового режима подписей в цифровой форме заслуживает дальнейшего обсуждения Рабочей группой. Было выражено общее мнение о том, что в положение по этому вопросу необходимо добавить новые элементы, и Секретариату было предложено подготовить пересмотренное положение с учетом результатов обсуждений в Рабочей группе, включая возможные варианты, касающиеся момента вступления аннулирования в силу. Было решено также, что пересмотренный проект должен содержать положения о приостановлении действия сертификата.

Пункт 2

136. Было отмечено, что употребление слова "obligation" в первом предложении этого пункта на английском языке не вполне уместно и что лучше было бы в этом контексте употребить другие слова, например "onus" или "duty".

137. Было отмечено, что, помимо держателя сертифицированной пары ключей, сертификационный орган также должен быть обязан аннулировать соответствующий сертификат, если ему станет известно, что частный криптографический ключ был утерян, скомпрометирован или подвергается опасности неправильного использования в других отношениях. В поддержку этого предложения было отмечено, что такая обязанность предусматривается в ряде международных стандартов и рекомендаций, касающихся электронной сертификации и удостоверения подлинности, например в подготавливаемых Международной торговой палатой руководящих принципах единообразной международной практики удостоверения подлинности и сертификации.

138. В ответ на вопросы о том, может ли сертификационный орган выполнять такую обязанность, было указано, что имеющаяся в настоящее время технология позволяет сертификационному органу оперативно реагировать на подобные ситуации. Однако время, необходимое для принятия таких мер, зависит не только от имеющейся технологии, но и от уровня услуг, предоставляемых сертификационным органом своим клиентам в соответствии с условиями их договорных отношений (например, от того, выделил ли сертификационный орган сотрудников для урегулирования ситуаций, когда частные ключи были утеряны, скомпрометированы или неправильно используются; осуществляет ли сертификационный орган обслуживание клиентов в выходные дни или только в обычное рабочее время).

139. Рабочая группа приняла к сведению высказанные мнения и решила учитывать их в ходе будущего обсуждения вопроса об аннулировании сертификатов.

## 7. Регистр сертификатов

140. Рабочая группа провела обсуждение вопроса о регистре сертификатов на основе следующего проекта положения:

"Проект статьи G

1) Уполномоченный сертификационный орган ведет общедоступный электронный регистр выданных сертификатов, указывающий, когда отдельный сертификат был выдан, когда истекает срок его действия и когда его действие было приостановлено или он был аннулирован.

2) Регистр хранится сертификационным органом в течение по меньшей мере [10] лет после даты аннулирования или истечения срока действия любого сертификата, выданного этим сертификационным органом".

141. Рабочей группе было предложено начать обсуждение вопроса о регистре сертификатов с рассмотрения того, насколько нужно включить положение по этому вопросу в проект единообразных норм, и, в случае положительного ответа на этот вопрос, рассмотреть элементы такого регистра и продолжительность срока хранения, если таковой будет предусмотрен.

142. Хотя принципиальных возражений по поводу включения положения о регистре сертификатов не прозвучало, было отмечено, что Рабочая группа должна продолжить изучение вопроса о том, действительно ли такое положение необходимо в контексте проекта единообразных правил и применимо ли оно ко всем разнообразным видам сертификатов, которые могут быть выданы сертификационными органами.

143. В отношении структуры такого регистра было заявлено, что сертификационные органы, относящиеся к одной и той же инфраструктуре для использования публичных ключей, могли бы вести не каждый свой собственный регистр сертификатов, а пользоваться централизованным регистром, в который они будут заносить данные о выдаваемых ими сертификатах. Вопрос о такой структуре, преследующей цель устранения множественности регистров, в настоящее время рассматривается в ряде стран. Отмечалось, что Рабочей группе было бы целесообразно глубже проработать такую возможность.

144. В отношении пункта 1 было указано, что в регистре нет нужды указывать дату выдачи сертификата и что в этой связи слова "указывающий, когда отдельный сертификат был выдан" следует исключить. Другое предложение заключалось в том, чтобы сертификационные органы вели отдельную базу данных для аннулированных сертификатов, с тем чтобы облегчить обработку запросов заинтересованных сторон, касающихся действительности сертификатов.

145. Были высказаны противоположные мнения относительно необходимости и адекватности срока хранения, о котором говорится в пункте 2. Было заявлено, что установление минимальных сроков хранения вполне уместно для цели обеспечения доступности данных для заинтересованных сторон, что имеет особое значение в контексте установленных в национальных законах сроков давности для осуществления или защиты прав или предъявления требований об исполнении обязательств. Вместе с тем в национальных законах устанавливаются различные сроки давности для разных видов прав и обязательств. В них также предусматриваются различные сроки хранения публичных и частных документов в зависимости от предмета соответствующего документа. В данных обстоятельствах было бы предпочтительно оставить вопрос об определении надлежащего срока хранения на урегулирование в национальном праве, а не устанавливать произвольный срок, который может и не подойти ко всем обстоятельствам. Кроме того, Рабочая группа должна учитывать расходы на содержание регистра сертификатов в течение того или иного конкретного срока. В зависимости от уровня услуг, предоставляемых сертификационным органом, и способа сдачи сертификатов на хранение сертификационному органу может оказаться экономически невыгодно брать на себя обязательства по хранению отдельных видов сертификатов дольше определенного срока. Было бы нецелесообразно пытаться установить общий срок хранения, не имея информации о практических последствиях такой нормы для этого сектора.

146. Однако другое мнение заключалось в том, что вопрос о сроке хранения записей и информации, позволяющих заинтересованной стороне идентифицировать своих торговых партнеров и удостоверить подлинность их подписей, затрагивает целый ряд соображений публичного порядка, которые Рабочая группа не может оставить без внимания. Этот вопрос заслуживает того, чтобы он был отражен в проекте единообразных правил. Что касается надлежащего срока хранения, то было отмечено, что сертификационные органы нельзя наделять правом в одностороннем порядке устанавливать срок хранения исходя исключительно из соображений затрат. Кроме того, расходы на хранение сами по себе не должны быть решающим фактором для сокращения или неустановления срока хранения. Сертификационные органы, направляющие на хранение выданные ими сертификаты в один и тот же регистр в рамках какой-либо инфраструктуры для использования публичных ключей, могли бы создать тот или иной общий механизм совместного покрытия расходов.

147. Было внесено предложение о том, чтобы заинтересованные стороны, направляющие запросы в регистр сертификатов, оставляли какой-то след, свидетельствующий о том, что такой запрос был сделан. Было пояснено, что наличие такого свидетельства может оказаться важным в случае возникновения проблем между сертификационным органом и такой заинтересованной стороной в отношении того,

проверила ли заинтересованная сторона действительность сертификата до того, как она стала полагаться на сообщение, подписанное в цифровой форме.

148. Рабочая группа приняла к сведению различные высказанные мнения и просила Секретариат провести обзор поднятых вопросов и подготовить альтернативные проекты положений, отражающие обсуждения, которые были проведены в Рабочей группе.

8. Отношения между пользователями и сертификационным органом

149. Рабочей группе был представлен следующий проект положения:

"Проект статьи J

1) Сертификационному органу разрешено запрашивать только такую информацию, которая является необходимой для идентификации пользователя.

2) По просьбе юридических или физических лиц, сертификационный орган предоставляет информацию о следующем:

a) условиях, на которых сертификат может использоваться;

b) условиях, связанных с использованием подписей в цифровой форме;

c) расходах, связанных с использованием услуг сертификационного органа;

d) политике или практике сертификационного органа в отношении использования, хранения и передачи информации личного характера;

e) технических требованиях сертификационного органа в отношении оборудования связи пользователя;

f) условиях, на которых сертификационный орган может направлять пользователям предупреждения в случае сбоев или неисправностей в функционировании оборудования связи;

g) любом ограничении ответственности сертификационного органа;

h) любых ограничениях, налагаемых сертификационным органом на использование сертификата;

i) условиях, на которых пользователь имеет право устанавливать ограничения в отношении использования сертификата.

3) Информация, указанная в пункте 1, предоставляется пользователю до заключения окончательного соглашения о сертификации. [Такая информация может быть предоставлена сертификационным органом в виде заявления о практике сертификации.]

4) При условии направления уведомления за [один месяц] пользователь может расторгнуть соглашение о связи с сертификационным органом. Такое уведомление о расторжении вступает в силу в момент его получения сертификационным органом.

5) При условии направления уведомления [за три месяца] сертификационный орган может расторгнуть соглашение о связи с сертификационным органом. Такое уведомление о расторжении вступает в силу в момент его получения".

150. Рабочая группа отметила, что в той мере, в какой проект статьи J касается отношений между пользователями и сертификационными органами, он предвосхищает решения по целому ряду вопросов, которые еще рассматриваются Рабочей группой. Рабочая группа решила заключить весь проект статьи J в квадратные скобки и рассмотреть его на более позднем этапе.

## III. ВКЛЮЧЕНИЕ ПУТЕМ ССЫЛКИ

151. Завершив предварительное обсуждение правовых вопросов и возможных положений для рассмотрения в единообразных правилах, касающихся подписей в цифровой форме, как это отражено в части II настоящего доклада, Рабочая группа отметила, что из-за недостатка времени она не сможет провести на нынешней сессии подробное обсуждение вопросов, связанных с включением путем ссылки.

152. Рабочая группа напомнила, что вопрос о включении путем ссылки кратко обсуждался на различных этапах подготовки Типового закона (см. A/CN.9/406, пункты 90 и 178, и A/CN.9/407, пункты 100-105 и 117). На своей предыдущей сессии Рабочая группа в целом согласилась с тем, что работа по вопросу о включении путем ссылки в контексте электронной торговли является необходимой. Было выражено мнение о том, что в ходе любых попыток выработки правовых норм, касающихся включения в сообщения данных таких положений о ссылке, необходимо выполнить следующие три условия: a) положение о ссылке должно быть включено в сообщение данных; b) содержание документа, на который делается ссылка, например, общих условий, должно быть фактически известно стороне, против которой может использоваться документ, на который делается ссылка; и c) данная сторона должна выразить согласие с документом, на который делается ссылка, помимо того, что он должен быть ей известен. По общему мнению, тема о включении путем ссылки может быть надлежащим образом рассмотрена в контексте общей работы по вопросам регистров и поставщиков услуг (A/CN.9/421, пункт 114). На своей двадцать девятой сессии Комиссия достигла общей договоренности о том, что этим вопросом можно заняться в контексте работы по сертификационным органам[2].

153. На нынешней сессии было достигнуто общее согласие в отношении того, что приемлемость включения путем ссылки имеет существенно важное значение для развития электронной торговли в целом. Хотя этот вопрос, возможно, потребуется рассмотреть и в контексте работы, связанной с подписями в цифровой форме и сертификационными органами, он также заслуживает обсуждения на более общем уровне. Даже если впоследствии будет сочтено уместным разработать конкретные правила, регулирующее включение путем ссылки в контексте подписей в цифровой форме, общее обсуждение и, возможно, общий свод правил являются необходимыми.

154. Было выражено мнение о том, что разработка правил для включения путем ссылки в электронной среде может оказаться трудной задачей ввиду сложности связанных с этим вопросов. В условиях использования бумажных документов включение путем ссылки и смежные вопросы, такие, как договоры присоединения и проблемы "войны форм", обусловили появление широкого спектра правовых норм, причем не все смежные правовые вопросы были решены удовлетворительным образом. Эта тема обусловила необходимость в обеспечении сбалансированности различных вступающих в коллизию интересов. С одной стороны, необходимо признавать автономию сторон. С другой стороны, необходимо ограничить возможные злоупотребления, связанные с договорами присоединения. С учетом тех трудностей, которые, как ожидается, встретятся в области включения путем ссылки, было предложено уделить более приоритетное внимание другим вопросам, которые также могут потребовать дополнительной работы в контексте электронной торговли. Еще одно мнение сводилось к тому, что обсуждение вопроса о включении путем ссылки можно начинать лишь на основе дополнительных исследований Секретариата, касающихся сравнительных правовых аспектов договоров присоединения, "войны форм" и смежных вопросов ответственности.

---

[2]Там, же, пятьдесят первая сессия, Дополнение № 17 (A/51/17), пункт 222.

155. Превалировало мнение о том, что необходимости в дальнейшем исследовании нет, 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. После обсуждения Рабочая группа решила, что этот вопрос должен быть рассмотрен в качестве первого основного пункта ее повестки дня в начале следующей сессии.

## IV. БУДУЩАЯ РАБОТА

156. Рабочая группа напомнила, что Комиссия просила ее рассмотреть желательность и целесообразность подготовки единообразных правил по вопросам подписей в цифровой форме и сертификационных органов. Закрывая свою сессию, Рабочая группа считает, что в ее докладе Комиссии должно быть указано, 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 подготовка проекта единообразных правил по вопросам подписей в цифровой форме практически осуществима.

157. В контексте обсуждения будущей работы было еще раз указано на то, 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 (см. A/51/17, пункты 219-221).