



Генеральная Ассамблея

Distr.: Limited
1 February 2019
Russian
Original: English

Комиссия Организации Объединенных Наций
по праву международной торговли
Рабочая группа IV (Электронная торговля)
Пятьдесят восьмая сессия
Нью-Йорк, 8–12 апреля 2019 года

Пояснительные замечания по проекту положений
о трансграничном признании услуг по управлению
идентификационными данными и удостоверительных
услуг

Записка Секретариата

Содержание

	Стр.
I. Введение.....	2
II. Основополагающие цели проектов положений.....	2
III. Пояснительные замечания по проектам положений.....	3
A. Глава I — Сфера применения (проекты статей 1–3).....	3
B. Глава II — Общие положения (проекты статей 4–7).....	4
C. Глава III — УИД (проекты статей 8–13).....	6
D. Глава IV — Удостоверительные услуги (проекты статей 14–18).....	11
E. Глава V — Международные аспекты (проекты статей 19–20).....	14



I. Введение

1. В настоящей записке излагаются замечания по проектам положений о трансграничном признании услуг по управлению идентификационными данными (УИД) и удостоверительных услуг, которые содержатся в документе [A/CN.9/WG.IV/WP.157](#). Справочная информация о работе Рабочей группы по правовым вопросам, касающимся УИД и удостоверительных услуг, приводится в документе [A/CN.9/WG.IV/WP.156](#), пункты 6–15.

II. Основополагающие цели проектов положений

2. В течение последних двадцати лет наблюдается экспоненциальный рост онлайн-активности. Увеличение коммерческой деятельности в режиме онлайн, т.е. электронных операций между предприятиями, между предприятиями и потребителями, а также между предприятиями и правительствами, является особенно значительным с точки зрения стоимостного объема, которую он представляет. Мировой объем электронной торговли увеличился с 64 млрд долл. в 1999 году до более 25 трлн долл. в 2015 году¹. Этот рост совпадает с расширением доступа к Интернету среди частных лиц и предприятий. Например, доля домохозяйств, имеющих доступ к Интернету, выросла с 35 процентов в 2002 году до 83,6 процента в 2017 году². Соответственно возросла доступность услуг электронного правительства (включая услуги, связанные с торговлей), электронных банковских услуг и электронных платежей.

3. Такой рост должен подкрепляться чувством доверия к онлайн-пространству. Одним из важных компонентов такого доверия является способность надежно идентифицировать каждую сторону, особенно в отсутствие какого-либо предварительного личного взаимодействия. В течение ряда лет предлагались различные решения для проблем, связанных с необходимостью идентификации в режиме онлайн. Это привело к быстрому распространению методов, технологий и устройств, используемых для управления идентификационными данными (УИД). Рассмотрение правовых аспектов УИД на глобальном уровне может способствовать не только согласованию таких различных решений, но также стимулировать взаимодействие между системами УИД независимо от их частной или государственной принадлежности.

4. Существует несколько препятствий на пути расширения использования УИД и удостоверительных услуг. Некоторые препятствия носят правовой характер и включают: 1) отсутствие законодательства, придающего юридическую силу УИД и удостоверительным услугам; 2) различия в законах и подходах к УИД, в том числе наличие законов, основанных на специфических технологических требованиях; 3) наличие законодательства, требующего представления бумажных идентификационных документов для заключения коммерческих сделок в режиме онлайн; и 4) отсутствие механизмов трансграничного юридического признания УИД и удостоверительных услуг ([A/CN.9/965](#), пункт 52).

5. Основная цель работы Рабочей группы заключается в устранении этих препятствий путем разработки единообразных правовых норм. Такие нормы служат нескольким целям: повысить эффективность; снизить операционные издержки; повысить безопасность и правовую определенность электронных сделок, обеспечив тем самым доверие; и преодолеть отставания в сфере цифровых технологий.

¹ Источник: UNCTAD, E-Commerce and Development Report 2001, UN Doc UNCTAD/SDTE/ECB/1, p. 44; UNCTAD, Information Economy Report 2017, UN Doc UNCTAD/IER/2017, p. 28.

² Источник: ITU, ICT Statistics, Global ICT Developments, 2001–2018, размещено по адресу <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>.

6. Таким образом, работа Рабочей группы способствует достижению Целей в области устойчивого развития. Важность идентификационных данных признается, в частности, в цели 16 в области устойчивого развития, задача 9 которой предусматривает обеспечение наличия у всех людей законных удостоверений личности. В цифровой экономике это превращается в право на наличие идентификационных данных в цифровой форме. Правовая основа для УИД и удостоверительных услуг будет способствовать безопасному внедрению идентификационных данных в цифровой форме. Поощряя доверие к онлайн-пространству, такая правовая основа будет способствовать также устойчивому развитию и социальной интеграции в соответствии с целью 9 в области устойчивого развития, которая касается (среди прочего) содействия инновациям.

III. Пояснительные замечания по проектам положений

A. Глава I — Сфера применения (проекты статей 1–3)

1. Цель использования УИД (проект статьи 1(1))

7. Идентификация может потребоваться для различных целей, а именно для соблюдения нормативных требований, для установления действительности коммерческого документа и выполнения договорных обязательств ([A/CN.9/965](#), пункты 82–83; см. также [A/CN.9/WG.IV/WP.153](#), пункты 32–34). **Рабочая группа, возможно, пожелает рассмотреть вопрос о порядке применения проектов положений в целях соблюдения нормативных требований.**

2. Трансграничное и внутригосударственное юридическое признание (проект статьи 1(1))

8. Признанию иностранных систем УИД и удостоверительных услуг способствует наличие внутригосударственной правовой основы. Это связано с тем, что такая основа устанавливает правовые понятия, которые имеют отношение к механизму признания. Трансграничное признание облегчается также, когда внутреннее законодательство содержит согласованные нормы, основанные на общих принципах, или даже идентичные положения. Более того, трансграничное признание систем УИД и взаимное признание систем УИД независимо от какого-либо трансграничного или иностранного элемента в определенной степени аналогичны. По этим причинам проект положений был составлен с целью предложить основу как международного соглашения, так и типового законодательства для принятия на внутригосударственной основе.

3. Соответствующие субъекты (проекты статей 1(2) и (3))

a) Публичные субъекты

9. Хотя основное внимание в работе Рабочей группы уделяется сделкам между коммерческими предприятиями, следует также учитывать системы УИД, созданные в других контекстах, имеющих отношение к коммерческим операциям, особенно в контексте связанных с торговлей государственных услуг, таких как механизмы единого обслуживания для таможенных операций ([A/CN.9/965](#), пункт 83). По этим причинам включение публичных субъектов в качестве субъектов, к которым может применяться проект положения, является оправданным.

10. **Рабочая группа, возможно, пожелает рассмотреть вопрос о том, приводит ли участие публичных субъектов в операциях, связанных с УИД, или в предоставлении удостоверительных услуг к возникновению особых вопросов, принимая во внимание применение принципов технологической нейтральности (см. ниже, пункт 23) и автономии сторон (см. ниже, пункт 24).**

b) Идентификация объектов

11. Было высказано мнение, что работа Рабочей группы должна способствовать надежной идентификации как субъектов (т.е. физических и юридических лиц), так и объектов (т.е. физических и цифровых объектов) сделок и что идентификация объекта может быть полезной для выявления субъектов сделки. В любом случае следует проводить четкое различие между субъектами и объектами, поскольку объекты не имеют правосубъектности и не могут нести ответственность ([A/CN.9/965](#), пункт 11).

12. Ссылка в пункте 3 на «проверку идентификационных данных» отражает решение Рабочей группы о том, что ее работа должна быть сосредоточена на транзакционной идентичности и, в этом контексте, на вопросах признания, а не на присвоении идентификационных данных ([A/CN.9/965](#), пункт 10). Вопросы транзакционной (или вторичной) идентичности и фундаментальной (или первичной) идентичности более подробно рассматриваются в пунктах 7–10 документа [A/CN.9/WG.IV/WP.153](#).

4. Отсутствие нового обязательства идентифицировать (проект статьи 2(1))

13. Общий принцип, характерный для текстов ЮНСИТРАЛ об электронной торговле, состоит в том, что материальное право, например законодательство, применимое к коммерческим сделкам в целом, не затрагивается.

14. В контексте УИД и удостоверительных услуг этот принцип требует, чтобы законодательство об УИД не вводило никакой новой обязанности по идентификации, чтобы законодательство о удостоверительных услугах не вводило никакой новой обязанности использовать какой-либо конкретный вид удостоверительных услуг и чтобы существующие обязанности оставались неизменными.

15. Было указано, что существует тесная связь между принципом отсутствия нового обязательства по идентификации и принципом автономии сторон ([A/CN.9/965](#), пункт 110). Было отмечено также, что новые обязательства по идентификации могут возникнуть из-за использования конкретной удостоверительной услуги, но в любом случае использование такой удостоверительной услуги должно осуществляться на добровольной основе (там же).

5. Ссылка на нормы права о конфиденциальности и защите данных (проект статьи 2(2))

16. Рабочая группа подчеркнула важность режимов защиты данных для УИД и удостоверительных услуг. Проект статьи 2(2) содержит конкретную ссылку на нормы права о конфиденциальности и защите данных, чтобы отразить то значение, которое Рабочая группа придает таким нормам.

В. Глава II — Общие положения (проекты статей 4–7)**1. Определения (проект статьи 4)**

17. Проекты определений в проекте статьи 4 были подготовлены на основе терминологии, используемой в существующих текстах ЮНСИТРАЛ об электронной торговле.

18. На своей пятьдесят седьмой сессии Рабочая группа просила Секретариат включить в список основных определений для будущей ссылки несколько определений, взятых из статьи 3 Постановления об eIDAS³. К их числу относятся следующие определения:

³ Постановление (ЕС) № 910/2014 Европейского парламента и Совета от 23 июля 2014 года об услугах по электронной идентификации и удостоверительных услугах для электронных сделок на внутреннем рынке и отмене Директивы 1999/93/ЕС.

а) «электронная идентификация» означает процесс использования персональных идентификационных данных в электронной форме, уникально представляющих физическое или юридическое лицо, либо физическое лицо, представляющее юридическое лицо;

б) «средства электронной идентификации» означают материальную и/или нематериальную единицу, содержащую идентификационные данные лица и используемую для аутентификации для целей онлайн-услуги;

с) «идентификационные данные лица» означают набор данных, позволяющих идентифицировать физическое или юридическое лицо или же физическое лицо, представляющее учреждаемое юридическое лицо;

д) «схема электронной идентификации» означает систему электронной идентификации, в которой средства электронной идентификации выдаются физическим или юридическим лицам или же физическим лицам, представляющим юридические лица;

е) «аутентификация» означает электронный процесс, который позволяет производить электронную идентификацию физического или юридического лица или же подтверждение происхождения и целостности данных в электронной форме;

ф) «авторитетный источник» означает любой источник независимо от его формы, который может быть задействован для предоставления точных данных, информации и/или доказательств, которые могут быть использованы для удостоверения идентификационных данных;

г) «полагающаяся сторона» означает физическое или юридическое лицо, которое полагается на электронную идентификацию или удостоверительную услугу.

19. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, должны ли эти определения, которые не соответствуют терминам, которым даны определения ЮНСИТРАЛ, заменить или дополнить определения в проекте статьи 4.

2. Общие принципы и единообразное толкование (проекты статей 5–7)

20. В текстах ЮНСИТРАЛ обычно содержится положение, в котором говорится об их равной аутентичности и обязанности единообразного толкования. Пункт 2 статьи 5 призван обеспечить сохранение единообразия при толковании и применении данного законодательного текста.

21. Рабочая группа определила следующие общие принципы как относящиеся к ее работе по правовым аспектам УИД и удостоверительных услуг: 1) недопущение дискриминации в отношении использования электронных средств; 2) функциональная эквивалентность; 3) технологическая нейтральность; и 4) автономия сторон ([A/CN.9/936](#), пункт 67).

22. Хотя эти общие принципы были закреплены в существующих текстах ЮНСИТРАЛ об электронной торговле для применения на национальном уровне (см., например, статьи 3, 5 и 6 ТЗЭП⁴), они также подлежат применению на трансграничном уровне в результате закрепления внутренних правовых основ, позволяющих принимающей юрисдикционной системе предоставлять и подтверждать правовой статус иностранных систем УИД и удостоверительных услуг.

23. Важность принципа технологической нейтральности для УИД полностью признана. Что касается развивающихся стран, то было указано, что его применение позволит не допустить принятия технических требований, которые могут

⁴ Типовой закон ЮНСИТРАЛ об электронных подписях (издание Организации Объединенных Наций, в продаже под № R.02.V.8).

оказаться для торговцев слишком дорогостоящими или сложными ([A/CN.9/965](#), пункт 38). Применение принципа технологической нейтральности в контексте УИД может означать установление минимальных системных требований для систем УИД, касающихся свойств системы, а не конкретных технологий ([A/CN.9/936](#), пункт 69).

24. Одним из основополагающих принципов коммерческого права является автономия сторон. Однако на его применение распространяются ограничения, установленные в законодательстве, подлежащем обязательному применению ([A/CN.9/936](#), пункт 72). Такие ограничения особенно важны, поскольку законодательные требования, предъявляемые к использованию систем УИД и удостоверительных услуг, часто являются обязательными. По мере продвижения работы **Рабочая группа, возможно, пожелает определить основные правила, которые стороны не могут изменять или от которых они не могут отступать, с тем чтобы повысить определенность и предсказуемость трансграничного признания УИД и удостоверительных услуг** ([A/CN.9/965](#), пункт 109). По этой причине проект положения об автономии сторон (основанный, например, на статье 5 ТЗЭП) не был сформулирован. Тем не менее элементы принципа автономии сторон отражены в проекте статьи 3.

25. Цель принципа автономии сторон состоит также в поддержке обеспечения выполнения договорных соглашений, таких как системные правила для УИД, и системные правила и правовые основы удостоверительных услуг. Системные правила могут быть особенно актуальны в контексте федераций систем УИД (см. [A/CN.9/WG.IV/WP.154](#), пункт 39).

С. Глава III — УИД (проекты статей 8–13)

1. Юридическое признание УИД на основе функциональной эквивалентности (проект статьи 8)

26. Принцип функциональной эквивалентности требует определения требований, которым должны соответствовать электронная запись, метод или процесс, чтобы выполнять те же функции, что и в бумажной среде. Было отмечено, что положение о функциональной эквивалентности будет применяться только в том случае, если значение имеет УИД на бумажной основе ([A/CN.9/965](#), пункт 69), и что в этом положении, возможно, потребуется обеспечить определенную связь с процессами УИД в режиме онлайн ([A/CN.9/965](#), пункт 66).

27. На своей пятьдесят седьмой сессии Рабочая группа выделила некоторые элементы для положения о функциональной эквивалентности, придающего юридическую силу УИД: ссылка на элемент физической идентификации, используемый в режиме онлайн (будь то документ, реестр или другой авторитетный источник); ссылка на все этапы процесса УИД (т.е. идентификация и аутентификация); и ссылка на уровни обеспечения доверия или другой стандарт для оценки уверенности в правильности идентификации ([A/CN.9/965](#), пункты 70–78).

28. В Рабочей группе были высказаны различные мнения относительно предмета юридического признания ([A/CN.9/965](#), пункт 25), который, в свою очередь, определяет направленность положения о функциональной эквивалентности. В контексте УИД предметом юридического признания может быть: а) система УИД; b) идентификационные учетные данные, выданные системой УИД; или c) результат процесса идентификации с использованием системы УИД (т.е. операция с идентификационными данными) ([A/CN.9/965](#), пункт 24).

29. Преобладающее мнение заключается в том, что Рабочей группе следует сосредоточиться на признании процессов (т.е. систем), а также на признании результатов в отношении как УИД, так и удостоверительных услуг ([A/CN.9/965](#), пункты 94–99). В этой связи было также разъяснено, что юридическое признание систем УИД, учетных данных и результатов процесса идентификации

является взаимодополняющим ([A/CN.9/965](#), пункт 26). Таким образом, если системы УИД признаются, то, следовательно, признаются и учетные данные, используемые для идентификации, а также результаты процесса идентификации. Такой подход отражают оба варианта проекта статьи 8, которые обсуждались на пятьдесят седьмой сессии Рабочей группы.

30. В некоторых случаях идентификация осуществляется исключительно в режиме онлайн, и принцип функциональной эквивалентности может оказаться неприменимым ([A/CN.9/965](#), пункт 62). Для учета всех случаев Рабочей группе было предложено обсудить параметры приемлемого метода идентификации вместо того, чтобы пытаться разработать положения о функциональной эквивалентности ([A/CN.9/965](#), пункт 69).

2. Стандарты надежности (проект статьи 9)

31. Элементы, имеющие отношение к определению надежности метода в положении о функциональной эквивалентности, включают: а) договорные соглашения, если это разрешено применимым законодательством; б) сертификация и надзор; и с) уровни обеспечения доверия.

а) Сертификация

32. Сертификация систем УИД и поставщиков удостоверительных услуг может в значительной степени содействовать обеспечению доверия к таким поставщикам и их услугам. Варианты сертификации включают: самосертификацию; сертификацию независимой третьей стороной; сертификацию аккредитованной независимой третьей стороной; и сертификацию государственным органом. Выбор наиболее подходящей формы сертификации зависит от типа услуги, стоимости и желаемого уровня доверия. В контексте отношений между коммерческими предприятиями целесообразно предлагать все варианты сертификации, включая отсутствие сертификации, поскольку деловые партнеры должны иметь возможность выбирать наиболее подходящий для своих нужд вариант, признавая, что каждый вариант будет приводить к различным юридическим последствиям ([A/CN.9/965](#), пункт 112).

33. Тем не менее было высказано мнение, что любое решение, предполагающее создание центрального органа по сертификации, аккредитации или надзору, может оказаться неприемлемым в ситуациях, когда используется технология распределенных баз данных, в частности, из-за проблем, связанных с выявлением органа, который может запросить сертификацию, и органа для проведения оценки и с принятием корректировочных и принудительных мер ([A/CN.9/965](#), пункты 114 и 129).

34. В существующих механизмах юридического признания (см. [A/CN.9/WG.IV/WP.153](#), пункты 61–73 и 76–79), которые основаны на подходе *ex ante* (см. пункты 47–49 ниже), сертификация (включая самосертификацию) является необходимым элементом для оценки систем УИД с использованием стандартов, основанных на результатах.

35. Сертификация также может иметь значение для юридического признания *ex post* (см. пункты 44–45 ниже). Например, пункты (е) и (f) статьи 10 ТЗЭП ссылаются на наличие аккредитации, аудита и самосертификации в качестве факторов при оценке надежности систем, используемых поставщиком сертификационных услуг, но не предписывают это в качестве обязательного условия.

36. Были высказаны различные мнения относительно желательности привлечения к процессу сертификации публичных органов. С одной стороны, было указано, что добровольная сертификация не обязательно будет предусматривать участие публичных субъектов, но может основываться на независимой сертификации ([A/CN.9/965](#), пункт 112).

37. С другой стороны, указывалось, что государственный надзор за деятельностью сертификационных органов частного сектора имеет важное значение для

предупреждения рисков конкуренции и злоупотреблений, в частности в отношении мелких участников рынка ([A/CN.9/965](#), пункты 115 и 128). Кроме того, было отмечено, что аккредитация сертифицирующих органов в государственных учреждениях направлена на обеспечение независимости, беспристрастности и справедливости в деятельности этих органов. В ответ было высказано мнение о том, что независимые органы могут в большей степени содействовать достижению этих целей ([A/CN.9/965](#), пункт 115).

38. Подход, использованный в статье 10 ТЗЭП, является продуктом нейтральности модели. Включение обязательных положений о надзоре может быть понято как стремление воспрепятствовать принятию рыночной модели, основанной на саморегулировании удостоверительных услуг.

б) Контроль

39. Надзор за системами УИД является распространенным явлением, поскольку его наличие считается полезным или даже необходимым для обеспечения доверия к поставщикам услуг и к услугам, которые они предоставляют. Однако создание специального органа влечет за собой административные и финансовые последствия. Использование альтернативных или дополнительных механизмов, например сертификации третьей стороной, может способствовать достижению целей, преследуемых надзором, при одновременном снижении сопутствующих расходов.

40. Было отмечено, что роль государственных учреждений растет не только в области надзора, но и в деле разработки и внедрения систем УИД, а также в предоставлении УИД и удостоверительных услуг, что потребует разделения надзорных функций и других функций, выполняемых публичными органами ([A/CN.9/965](#), пункт 128).

с) Уровни обеспечения доверия и сопоставление

41. Уровень обеспечения доверия является мерой степени доверия к процессам идентификации и аутентификации и поэтому является ключом к установлению надежности системы УИД ([A/CN.9/965](#), пункт 61). Были высказаны различные мнения о желательности ссылки на уровни обеспечения доверия (см. [A/CN.9/965](#), пункты 63–68).

42. Уровни обеспечения доверия могут быть упомянуты в положении о функциональной эквивалентности (т.е. в проекте статьи 8) или в положении, которое устанавливает стандарты надежности системы УИД (т.е. в проекте статьи 9). **Рабочая группа, возможно, пожелает рассмотреть вопрос о том, будет ли достаточно общей ссылки на уровни обеспечения доверия, если будет включена ссылка на уровни обеспечения доверия, или же необходима ссылка на разные уровни обеспечения доверия, а в последнем случае — будет ли каждый уровень обеспечения доверия увязан с различными правовыми последствиями** (см. [A/CN.9/965](#), пункты 59–60).

43. На своей пятьдесят седьмой сессии Рабочая группа обсудила «сопоставление» как метод проверки соответствия системы УИД общему описанию уровня обеспечения доверия (см. [A/CN.9/965](#), пункты 43–48 и 54). Практический пример того, как может работать сопоставление, приводится в документе [A/CN.9/WG.IV/WP.153](#), пункт 80.

3. Определение надежности ex post (проект статьи 9)

44. Проект статьи 9 направлен на реализацию подхода ex post для определения надежности систем УИД. Подход ex post предполагает оценку системы УИД только в случае фактического спора, хотя и на основе предварительно определенных условий. В отношении удостоверительных услуг тексты ЮНСИТРАЛ следовали именно этому подходу (см., например, статья 9(3) КЭС).

45. Дополнительная информация о подходе *ex post* приводится в документах [A/CN.9/965](#) (пункты 40–45) и [A/CN.9/WG.IV/WP.153](#) (пункты 74–75).

4. Презумпция надежности (проект статьи 10)

46. Проект статьи 10 основан на статье 6(3) ТЗЭП, которая предусматривает презумпцию надежности электронных подписей, отвечающих определенным требованиям. Проект статьи 10 может применяться как *ex post*, так и *ex ante*. *Ex post* он поддерживает осуществление проекта статьи 9, указывая объективные технические критерии, которые позволяют легче определить надежность. Тем не менее те же критерии могут быть оценены назначенным органом заранее. В последнем случае проект статьи 10 действует в сочетании с проектом статьи 11.

5. Определение надежности *ex ante* (проект статьи 11)

47. Проект статьи 11 направлен на применение подхода *ex ante* для определения надежности систем УИД.

48. Такой подход предполагает предварительное определение условий, которым должна удовлетворять система УИД для включения в «белый» список признанных систем УИД. Было высказано мнение, что подход *ex ante* предпочтителен, когда используются более высокие уровни обеспечения доверия ([A/CN.9/965](#), пункт 47).

49. При обсуждении этого подхода в Рабочей группе было поднято два вопроса: 1) необходимость централизованного институционального механизма для оценки систем УИД; и 2) привлечение публичных органов. Дополнительная информация об институциональных механизмах для применения подхода *ex ante* приводится в документах [A/CN.9/965](#) (пункты 40–45) и [A/CN.9/WG.IV/WP.153](#) (пункты 61–73). Дополнительная информация об участии публичных органов приводится в документе [A/CN.9/965](#) (пункты 49–50).

6. Обязанности операторов системы УИД (проект статьи 12)

50. В проекте статьи 12(1) указаны исходные элементы для определения основных обязательств операторов системы УИД. Он основан на соответствующих положениях Постановления об eIDAS.

а) Обязанность уведомлять о нарушениях безопасности

51. Проект статьи 12(2) устанавливает обязанность уведомлять о нарушениях безопасности. Эта обязанность является одним из аспектов принципа прозрачности ([A/CN.9/936](#), пункт 88).

52. Нарушения безопасности могут затронуть как системы, так и операции. Наличие надлежащего механизма для уведомления о нарушениях безопасности было сочтено важным фактором для улучшения функциональных характеристик и повышения уровня доверия к УИД и удостоверительным услугам ([A/CN.9/965](#), пункт 123).

53. Уведомления о нарушениях безопасности обладают общими элементами с уведомлениями о компрометации данных, однако здесь имеются также и существенные различия. Примеры действующего законодательства, предусматривающего режим раскрытия информации о нарушениях безопасности, приводятся в документе [A/CN.9/WG.IV/WP.154](#) (пункты 43–44).

б) Обязанность раскрывать информацию об условиях предоставления услуг

54. В процессе обсуждения принципа прозрачности Рабочая группа рассмотрела вопрос об обязанности раскрывать информацию об условиях предоставления услуг ([A/CN.9/965](#), пункт 121). Прозрачность условий предоставления услуг важна не только для пользователей (чтобы они могли сделать осознанный

выбор), но и для конкурентов и других заинтересованных органов (например, при мониторинге конкуренции на рынке) ([A/CN.9/965](#), пункт 121). В существующем виде проект статьи 12(1) не устанавливает отдельно обязанность раскрывать информацию об условиях предоставления услуг.

55. Операторы систем УИД, участвующие в федерациях или иным образом получающие сертификацию своих услуг, будут раскрывать значительный объем информации. Для других поставщиков могут быть установлены минимальные обязанности по раскрытию информации. Например, статья 9(1) ТЗЭП содержит перечень информации, которую поставщик сертификационных услуг должен раскрыть полагающейся стороне.

7. Ответственность операторов системы УИД (проект статьи 13)

56. Было указано, что, поскольку работа Рабочей группы касается правил, применимых на национальном уровне, необходимо рассмотреть вопрос о распределении ответственности ([A/CN.9/965](#), пункт 116), поскольку режим ответственности может оказать существенное влияние на содействие использованию УИД и удостоверительных услуг как в коммерческих, так и в некоммерческих целях.

57. В этой связи Рабочая группа определила следующие вопросы, которые необходимо решить: идентификация субъектов, несущих ответственность, с учетом особых режимов ответственности для публичных субъектов; возможность ограничения ответственности сторон, соблюдающих ранее установленные требования; статутные механизмы для ограничения ответственности (например, освобождение от бремени доказывания или перенос такого бремени); и договорные ограничения ответственности ([A/CN.9/936](#), пункт 85). Краткое описание законодательства, касающегося ответственности операторов систем УИД, приводится в документе [A/CN.9/WG.IV/WP.154](#) (пункты 23–30).

58. В проекте статьи 13(1) реализуется общий принцип, согласно которому оператор системы УИД должен нести ответственность за последствия непредоставления услуг в соответствии с соглашением или в соответствии с требованиями законодательства ([A/CN.9/965](#), пункт 117). Тем не менее в некоторых случаях может быть нелегко определить оператора системы УИД (например, при использовании технологии распределенной базы данных).

59. Согласно этому положению в его нынешнем виде ответственность может нести публичный орган, выступающий в качестве поставщика услуг. Различные виды ответственности могут возникать, когда публичный орган выполняет надзорные функции и выдает исходные идентификационные учетные данные.

60. В настоящее время проект статьи 13 распределяет ответственность только между операторами системы УИД. **Рабочая группа, возможно, пожелает рассмотреть вопрос о том, должны ли нормы об ответственности применяться также в отношении других заинтересованных субъектов** (например, пользователей и полагающихся третьих сторон) или же, в качестве альтернативы, в отношении этих субъектов должны применяться общие нормы об ответственности. Рабочая группа, возможно, пожелает также рассмотреть вопрос о том, следует ли в обязательном порядке раскрывать применимый режим ответственности пользователям и другим заинтересованным субъектам в интересах обеспечения прозрачности.

61. В качестве основания для ответственности в проекте статьи 13 упоминаются умышленные действия и небрежность. Стандарты осмотрительности, включая простую и предполагаемую небрежность и абсолютную ответственность, применительно к ответственности операторов инфраструктуры публичных ключей рассматриваются в документе «Содействие укреплению доверия к электронной торговле»⁵.

⁵ Содействие укреплению доверия к электронной торговле: правовые вопросы международного использования электронных методов удостоверения подлинности и

62. **Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли устанавливать дополнительные нормы в отношении бремени доказывания и определения ущерба** или же такие нормы должны содержаться в применимом национальном законодательстве.

63. Проект статьи 13(2) ограничивает ответственность операторов систем УИД за ущерб, возникший в результате использования услуг сверх ограничений, указанных оператором системы УИД. Это положение дополняет обязанность раскрывать информацию об условиях предоставления услуг, что является одним из аспектов принципа прозрачности. Вопрос о возможности для операторов инфраструктуры публичных ключей ограничивать ответственность или отказываться от ответственности по договору рассматривается в документе «Содействие укреплению доверия к электронной торговле»⁶.

64. Проект статьи 13(3) устанавливает механизм, который побуждает операторов систем УИД применять определенные стандарты, требуя использования таких стандартов в качестве основания для освобождения от ответственности. В противном случае это положение может содержать ссылку на использование более высоких уровней обеспечения доверия.

65. Проект статьи 13(3) подлежит применению с учетом проекта статьи 13(4). Стандарт «грубой небрежности или умышленного неправомерного деяния» закреплён в Законе Виргинии об электронной системе УИД (см. [A/CN.9/WG.IV/ WP.154](#), пункт 29).

66. Альтернативные способы решения вопросов ответственности включают создание страхового механизма, в рамках которого ущерб, понесенный в результате использования системы УИД, возмещается страховщиком. Еще один доступный механизм предусматривает при наступлении определенных условий автоматическую компенсацию за счет активов, заранее зарезервированных для этого в ликвидной форме, или наложение фиксированных штрафов.

D. Глава IV — Удостоверительные услуги (проекты статей 14–18)

67. В качестве предварительного вопроса **Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли ей составлять на основе единого определения понятия «удостоверительная услуга» открытый перечень удостоверительных услуг или же разрабатывать общие нормы, применимые ко всем удостоверительным услугам, и конкретные нормы, применимые к каждой из них.** Открытый перечень удостоверительных услуг может включать: электронные подписи; электронные печати; электронные отметки времени; электронную регистрацию доставки; аутентификацию веб-сайтов; электронное архивирование; электронные услуги условного депонирования и электронные системы контроля присутствия.

1. Юридическое признание удостоверительных услуг на основе функциональной эквивалентности (проект статьи 14)

68. Для того чтобы разработать адекватное положение о функциональной эквивалентности для той или иной удостоверительной услуги, необходимо определить конкретные функции, выполняемые при помощи такой удостоверительной услуги. Проект статьи 14 содержит основные положения о функциональной эквивалентности, разработанные для каждой идентифицированной удостоверительной услуги. **Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли в положении о функциональной эквивалентности удостоверительных услуг рассматривать: а) общие или конкретные стандарты**

подписания (издание Организации Объединенных Наций, в продаже под № R.09.V.4), пункты 179–201.

⁶ Там же, пункты 202–210.

надежности; b) презумпцию надежности; c) оценку надежности *ex ante*; и d) защитную оговорку об исключении отказа.

a) Электронные подписи

69. Проект статьи 14(1) посвящен электронным подписям, которые являются распространенной формой удостоверительных услуг. Положения об использовании электронных подписей содержат все тексты ЮНСИТРАЛ, касающиеся электронной торговли.

70. Некоторые виды электронных подписей и других удостоверительных услуг, например электронное архивирование, могут гарантировать целостность сообщения данных. В текстах ЮНСИТРАЛ сохранение целостности сообщения данных является одним из требований для обеспечения функциональной эквивалентности понятию «оригинал» в бумажной среде. **Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли рассматривать гарантирование целостности в качестве отдельной удостоверительной услуги.**

b) Электронные печати

71. Электронные печати используются в Постановлении об eIDAS для подтверждения происхождения и целостности электронного документа, выданного юридическим лицом (Постановление об eIDAS, декларативная часть 59). Кроме того, «электронные печати могут использоваться для аутентификации любого цифрового актива юридического лица, например программного кода или серверов» (Постановление об eIDAS, декларативная часть 65).

72. Тексты ЮНСИТРАЛ об удостоверительных услугах применимы как к физическим, так и к юридическим лицам. Кроме того, было высказано мнение о том, что текущая работа Рабочей группы должна распространяться также на физические и цифровые объекты, охватывая таким образом также программный код или серверы.

73. Статья 8 ТЗЭТ⁷ требует обеспечения целостности для достижения функциональной эквивалентности понятию «оригинал» в бумажной среде. Пункт 3 статьи 6 ТЗЭП содержит ссылку на понятие «целостность» для тех случаев, когда целью юридического требования о наличии подписи является обеспечение уверенности в целостности информации, к которой она относится.

74. В свете вышеизложенного **Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли рассматривать электронные печати в качестве отдельной удостоверительной услуги** или же их можно рассматривать как разновидность электронных подписей.

c) Электронное архивирование

75. Проект статьи 14(3) касается услуг электронного архивирования, которые в свою очередь связаны с сохранением электронных записей. Сохраняемые электронные записи могут быть созданы впервые в электронном виде или же могут представлять информацию, первоначально изложенную на бумаге. Услуги электронного архивирования могут также гарантировать целостность архивных электронных записей, а также точность времени архивирования.

76. Электронное архивирование выполняет функцию обеспечения правовой определенности относительно действительности электронных архивированных записей в случае возникновения спора и для других нужд. Было высказано предположение о том, что механизм юридического признания для электронного архивирования может ограничиваться обеспечением соблюдения юридических требований юрисдикционной системы, в рамках которой необходимо будет использовать архивированные записи ([A/CN.9/965](#), пункт 126). Если Рабочая

⁷ Типовой закон ЮНСИТРАЛ об электронной торговле (издание Организации Объединенных Наций, в продаже под № R.99.V.4).

группа пожелает рассмотреть положение об электронном архивировании, предлагается использовать в качестве основы для такого обсуждения статью 10 ТЗЭТ, касающуюся хранения сообщений данных.

77. Кроме того, законодательство может содержать требование о том, чтобы архивированные электронные записи можно было также переносить таким образом, чтобы доступ был возможен вне зависимости от развития технологий. Такой результат может быть получен путем применения принципа технологической нейтральности и требований о функциональной эквивалентности понятию «целостность», а именно: при необходимости предъявления информации, эта информация может быть продемонстрирована лицу, которому она должна быть предъявлена (статья 8(1)(b) ТЗЭТ).

d) Другие удостоверительные услуги

78. Электронные отметки времени, о которых говорится в проекте статьи 14(2), предназначены для предоставления подтверждения даты и времени, когда такая отметка была увязана с данными. Они могут также свидетельствовать о целостности данных, с которыми увязаны дата и время.

79. Услуги по электронной регистрации доставки, о которых говорится в проекте статьи 14(4), предназначены для предоставления подтверждения отправки электронного сообщения указанным отправителем и его получения указанным адресатом. Они могут также свидетельствовать о целостности данных, которыми обмениваются, а также о времени отправки и получения данных.

80. Проект статьи 14(5) касается аутентификации веб-сайтов. В соответствии с Постановлением об eIDAS «услуги по аутентификации веб-сайтов обеспечивают средство, с помощью которого посетитель веб-сайта может удостовериться в том, что за сайтом стоит подлинная и законная организация» (Постановление об eIDAS, декларативная часть 67). **Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли рассматривать аутентификацию веб-сайтов в качестве отдельной удостоверительной услуги или же ее можно рассматривать как разновидность электронных подписей.**

81. Проект статьи 14(6) касается услуг условного депонирования, которые заключаются в хранении активов и их передаче уполномоченному лицу после выполнения условий, предусмотренных в соглашении об условном депонировании. Услуги условного депонирования используются в отношении выплаты денежных сумм и передачи исходного кода программного обеспечения. Например, оплата цены товара может быть отложена до получения товара покупателем; в то же время продавец получает подтверждение о том, что деньги для уплаты цены имеются и будут выплачены после доставки и принятия товара.

82. Электронные услуги по подтверждению присутствия предназначены для того, чтобы доказать, что субъект находился в определенном месте в определенное время. Эта удостоверительная услуга обсуждалась в связи с электронными завещаниями. Она может быть также актуальна применительно к онлайн-регистрации, например, для получения банковских услуг. **Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли разработать специальное положение об электронных услугах подтверждения присутствия.**

2. Презумпция надежности удостоверительных услуг (проект статьи 15)

83. В ТЗЭП и ряде национальных законов об электронных подписях проводится различие между удостоверительными услугами на основе степени надежности, которую они предлагают. Такие законы, в частности, предусматривают правовые последствия для электронных подписей, которые удовлетворяют определенным требованиям и, следовательно, обеспечивают более высокую степень надежности. Во избежание путаницы рекомендуется, чтобы в рамках работы Рабочей группы при обсуждении удостоверительных услуг использовалось

понятие степени надежности, а термин «уровень обеспечения доверия» использовался только применительно к системам УИД.

84. **Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли применять в отношении признания удостоверительных услуг понятие уровня обеспечения доверия** или же следует применять какое-либо другое понятие для установления надежности конкретной удостоверительной услуги. Уже отмечалось, что идентификационные учетные данные, позволяющие обеспечить высокий уровень доверия, могут использоваться для удостоверительных услуг с разной степенью надежности ([A/CN.9/965](#), пункт 106). Поэтому не существует какой-либо корреляции между уровнями обеспечения доверия к электронной идентификации и степенью надежности удостоверительных услуг.

3. Ответственность поставщиков удостоверительных услуг (проект статьи 18)

85. В качестве общего принципа поставщики удостоверительных услуг должны нести ответственность за последствия непредоставления услуг в соответствии с соглашением или согласно требованиям законодательства ([A/CN.9/965](#), пункт 117). Степень такой ответственности будет определяться с учетом вида предоставляемой удостоверительной услуги.

86. ТЗЭП содержит положения, касающиеся ответственности, возникающей в результате поведения подписавшей стороны (статья 8), поставщика сертификационных услуг (статья 9) и полагающейся стороны (статья 11). Эти положения устанавливают обязательства для каждого субъекта, участвующего в жизненном цикле электронной подписи. Кроме того, ТЗЭП признает возможность для поставщиков сертификационных услуг ограничить объем или степень их ответственности.

87. Краткое описание законодательства, касающегося ответственности поставщиков удостоверительных услуг, приводится в документе [A/CN.9/WG.IV/ WP.154](#) (пункты 33–35).

Е. Глава V — Международные аспекты (проекты статей 19–20)

1. Трансграничное юридическое признание (проект статьи 19)

88. Трансграничное юридическое признание может пониматься по-разному (см. [A/CN.9/WG.IV/ WP.153](#), пункт 55). На пятьдесят седьмой сессии Рабочей группы было указано, что предоставление национального режима должно быть предпочтительным подходом для трансграничного юридического признания ([A/CN.9/965](#), пункт 30). Проект статьи 19 был сформулирован соответствующим образом.

89. При оценке соответствия иностранной системы УИД может иметь значение применимый режим ответственности. Соответственно, было высказано предположение, что для содействия трансграничному признанию УИД необходимо определить законодательство, применимое к режиму ответственности ([A/CN.9/965](#), пункт 116). Это может потребовать разработки специальной нормы международного частного права или ссылки на существующие нормы. **Рабочая группа, возможно, пожелает рассмотреть вопрос о том, повлечет ли трансграничное юридическое признание применение к иностранным системам УИД и удостоверительным услугам внутригосударственного режима ответственности.**

90. В проекте статьи 19 прямо не рассматривается вопрос об ограничении ответственности. Могут применяться дополнительные нормы, в том числе в соответствии с императивным законодательством, которые могут ограничивать действие таких договорных положений.

91. Проект статьи 19(2) устанавливает степень надежности в качестве стандарта для оценки соответствия иностранной системы УИД или

идентификационных данных. В нем представлены две альтернативы: либо зарубежная система УИД обеспечивает такой же уровень надежности, либо она обеспечивает по существу эквивалентный уровень надежности. Понятие «по существу эквивалентный уровень надежности» взято из статьи 12 ТЗЭП. **Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли в отношении признания систем УИД дать дополнительные рекомендации, касающиеся ссылки на понятия уровней обеспечения доверия и использования со- поставления.**

2. Механизмы институционального сотрудничества (проект статьи 20)

92. Достижению взаимного юридического признания и функциональной совместимости систем УИД и удостоверительных услуг могут способствовать механизмы институционального сотрудничества.

93. В проекте статьи 20 говорится об институциональном сотрудничестве в форме сотрудничества между государствами. Сотрудничество может включать обмен информацией, опытом и успешными видами практики, в частности, в отношении технических требований и уровней обеспечения доверия, экспертной оценки систем УИД и изучения соответствующих разработок. Акт об осуществлении Постановления об eIDAS⁸ содержит дополнительную информацию об обмене информацией и экспертной оценке, в том числе указание на то, что государство-член не обязано предоставлять требуемую информацию, если ее раскрытие может поставить под угрозу общественную или национальную безопасность либо нарушить коммерческую, профессиональную или корпоративную тайну.

94. Другая форма сотрудничества может быть обеспечена через федерацию систем УИД. Федерации обычно основаны на договорных соглашениях, хотя способствовать созданию федерации могут также законодательные положения. Дополнительную информацию о федерации систем УИД см. документ [A/CN.9/WG.IV/WP.154](#), пункт 39.

95. Федерации систем УИД работают на основе технической совместимости и общей правовой базы, определяемой набором системных правил. Созданию такой общей правовой базы может способствовать унификация договорных и законодательных норм ([A/CN.9/965](#), пункт 120).

96. Было упомянуто, что применение в отношении юридического признания механизма ex ante также может привести к определенной форме институционального сотрудничества.

⁸ Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification.