Организация Объединенных Наций A/CN.9/WG.IV/WP.154

Генеральная Ассамблея

Distr.: Limited
12 September 2018
Russian
Original: English

Комиссия Организации Объединенных Наций по праву международной торговли
Рабочая группа IV (Электронная торговля)
Пятьдесят седьмая сессия
Вена, 19–23 ноября 2018 года

Правовые вопросы, связанные с управлением идентификационными данными и удостоверительными услугами

Записка Секретариата

Содержание

V.18-05928 (R) 111018 111018

I. Введение

1. В целях содействия дальнейшему обсуждению в настоящей записке освещаются отдельные аспекты некоторых тем, определенных Рабочей группой как имеющие отношение к рассмотрению ею правовых вопросов, связанных с управлением идентификационными данными (УИД) и удостоверительными услугами (A/CN.9/936, пункт 58). В частности, в ней преследуется цель обратить внимание на основные проблемы и предложить возможные пути их решения и не предполагается ограничивать возможность рассмотрения, при необходимости, дополнительных тем или рассмотрения нескольких тем одновременно. В рабочем документе A/CN.9/WG.IV/WP.153 освещаются некоторые аспекты других тем, определенных Рабочей группой как имеющие отношение к рассматриваемым ею правовым вопросам, связанным с УИД и удостоверительными услугами.

2. Справочная информация о деятельности Рабочей группы по правовым вопросам, связанным с УИД и удостоверительными услугами, изложена в пунктах 6–17 рабочего документа A/CN.9/WG.IV/WP.152. Перечень дополнительных документов, имеющих отношение к этой теме, содержится в пункте 18 рабочего документа A/CN.9/WG.IV/WP.152.

II. Актуальные вопросы будущей работы, связанной с правовыми аспектами управления идентификационными данными и удостоверительных услуг

A. Сертификация поставщиков услуг УИД и удостоверительных услуг

3. Сертификация, включая самосертификацию, аккредитацию и независимый аудит, способна значительно облегчить обеспечение доверия к поставщикам услуг УИД и удостоверительных услуг. Выбор подходящей формы сертификации может зависеть от типа необходимых услуг, их искомой стоимости и желаемого уровня обеспечения доверия.

4. Постановлением eIDAS предусмотрена всеобъемлющая система надзора за удостоверительными услугами и их сертификации. Согласно статье 17 этого постановления, каждое из государств-членов назначает орган, ответственный за регулярное выполнение надзорных функций по отношению к квалифицированным поставщикам удостоверительных услуг и эпизодическое осуществление таких функций в отношении других поставщиков удостоверительных услуг. В пункте 4 статьи 17 приводится перечень конкретных функций, возлагаемых на надзорный орган.

5. Следует отметить, что в соответствии с Постановлением eIDAS наличие надзорного органа необходимо для того, чтобы поставщики удостоверительных услуг могли рассматриваться как квалифицированные. В частности, согласно статье 20, квалифицированные поставщики удостоверительных услуг должны не реже одного раза в 24 месяца проверяться органом по оценке соответствия, отчет которого о результатах проведенной оценки представляется в надзорный орган. В случае невыполнения требований, поступивших от надзорного органа, сам поставщик или определенные виды его услуг могут быть лишены квалифицированного статуса.

6. В свою очередь только квалифицированные поставщики удостоверительных услуг имеют согласно Постановлению eIDAS право предоставлять квалифицированные удостоверительные услуги, связанные с определенными правовыми последствиями, такими как презумпции. Например, в соответствии с пунктом 2 статьи 25 этого постановления, квалифицированная электронная подпись по своим правовым последствиям эквивалентна подписи, поставленной собственноручно.

Одним словом, наличие надзорного органа дает возможность предлагать квалифицированные удостоверительные услуги, связанные с правовыми последствиями.

7. Применительно к удостоверительным услугам в пунктах (e) и (f) статьи 10 ТЗЭП аккредитация, аудит и самосертификация упоминаются в качестве элемента, наличие которого потенциально значимо для оценки того, заслуживают ли доверия системы, используемые поставщиком сертификационных услуг. Соответственно, при данном подходе существование надзорного органа и механизмов аккредитации не считается обязательным, а их роль и значение оцениваются произвольно.

8. В рамках моделей взаимного правового признания, в которых используются официальные перечни (см. A/CN.9/WG.IV/WP.153, пункты 61–73 и 76–79), сертификация (включая самосертификацию) является элементом, необходимым для оценки схем УИД исходя из стандартов, ориентированных на конечный результат. Для такой оценки может требоваться набор заранее составленных профилей.

9. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, должно ли наличие сертификации, включая самосертификацию, аккредитацию и независимый аудит, быть связано с правовыми последствиями, и если да, то с какими именно, или же эти элементы следует указывать как потенциально имеющие значение для оценки надежности поставщиков услуг УИД и доверительных услуг, степени доверия к ним или их иных качеств. В ходе обсуждения Рабочая группа, возможно, также пожелает определить, должно ли использование сертификации, включая самосертификацию, аккредитацию и независимый аудит, носить обязательный характер.

B. Уровни обеспечения доверия

1. УИД

10. Уровень обеспечения доверия обозначает степень надежности утверждения об идентичности, зависящую от характера используемых процессов. Существуют различные определения уровней обеспечения доверия, выработанные публичными и частными структурами. Их формулировки регулярно обновляются с учетом развития технологий и рабочих процессов. В свете принятого принципа технологической нейтральности во внимание принимаются только уровни обеспечения доверия, имеющие технологически нейтральные определения.

11. Национальный институт стандартов и технологий (НИСТ) Соединенных Штатов Америки выделяет три уровня обеспечения доверия, связанных с идентификацией: уровень доверия к идентичности (УДИ), уровень доверия к аутентификатору (УДА) и уровень доверия к федерации (УДФ)[1]. УДИ относится к процессу подтверждения идентификационных данных, УДА — к процессу аутентификации, а УДФ — к протоколу утверждения, используемому в федеративной среде для передачи аутентификационных данных и (если это применимо) для атрибуции информации доверяющей стороне.

12. Говоря конкретнее, УДИ означает, что процедура подтверждения идентификационных данных надежна и позволяет достоверно установить личность; УДА означает, что надежны сам процесс аутентификации и связь аутентификатора с тем или иным идентификатором конкретного лица; УДФ означает надежность протокола утверждения, используемого данной федерацией для передачи аутентификационных данных и для атрибуции информации доверяющей стороне, если система идентификации построена по федеративному принципу[2].

13. Каждому уровню обеспечения доверия соответствует та или иная степень надежности, связанная с определенными требованиями. Например УДИ-1 означает, что атрибуты, если они используются, являются самозаявленными или

[1] NIST Special Publication 800-63-3, *Digital Identity Guidelines*, June 2017, section 2. Available at https://doi.org/10.6028/NIST.SP.800-63-3.

[2] NIST, *Digital Identity Guidelines*, cit., section 5.2.

рассматриваются как таковые. УДИ-2 требует заочной или очной проверки идентичности: атрибуты, идентифицирующие данное лицо, должны быть проверены в его присутствии либо дистанционно, с использованием как минимум неких конкретно оговоренных процедур. УДИ-3 предполагает необходимость подтверждения идентичности в присутствии лица с проверкой идентифицирующих его атрибутов уполномоченным представителем поставщика сертификационных услуг путем физического изучения документов в соответствии с установленными процедурами.

14. В статье 8 Постановления eIDAS определены три уровня обеспечения гарантии для целей УИД: низкий, значительный и высокий, а также указаны связанные с ними критерии. Так, «низкому» уровню гарантии соответствует невысокая степень уверенности в принадлежности данному лицу заявляемой или приписываемой им себе идентичности; «значительному» уровню гарантии соответствует значительная степень уверенности в принадлежности данному лицу заявляемой или приписываемой им себе идентичности, а при «высоком» уровне гарантии степень уверенности в принадлежности данному лицу заявляемой или приписываемой им себе идентичности еще выше, чем при «значительном».

15. Актом, принятым во исполнение Постановления eIDAS[3], установлены минимальные технические спецификации и процедуры, предназначенные для определения надежности и качества процессов записи, управления средствами электронной идентификации, аутентификации, а также организации и управления деятельностью трансграничных поставщиков услуг УИД. Эти технические спецификации и процедуры сформулированы с соблюдением технологической нейтральности.

16. В свете вышеизложенного Рабочая группа, возможно, пожелает рассмотреть вопрос о том, целесообразно ли использовать концепцию уровней обеспечения доверия для установления соответствия юридическим требованиям или определения правовых последствий. В случае утвердительного ответа на этот вопрос она, возможно, также пожелает обсудить то, как соотносятся между собой уровни обеспечения доверия, с одной стороны, и требования и механизмы правового признания, с другой. Рабочая группа, возможно, пожелает обсудить и вопрос о том, следует ли ей заниматься рассмотрением характеристик различных уровней обеспечения доверия, и если да, то в каком объеме.

2. Удостоверительные услуги

17. Принципиальный вопрос, касающийся удостоверительных услуг, состоит в том, должна ли и к ним также применяться концепция уровней обеспечения доверия. В целом ряде национальных законов об электронных подписях предусмотрены два уровня признания таких подписей. Первый уровень распространяется на все электронные подписи независимо от их формы. Второй уровень предполагает признание определенных правовых последствий, таких как презумпция происхождения и целостности, за электронными подписями, удовлетворяющими определенным требованиям. Это можно интерпретировать как выделение различных уровней обеспечения доверия применительно к электронным подписям.

18. В том, что касается удостоверительных услуг, пункт 1 статьи 24 Постановления eIDAS может служить примером использования уровней обеспечения доверия в связи с выполнением требования идентификации при выдаче квалифицированного сертификата. А именно, требование о том, чтобы квалифицированный поставщик удостоверительных услуг проверил достоверность идентификационных данных лица, которому он выдает квалифицированный сертификат, согласно Постановлению eIDAS может быть выполнено дистанционно, с использованием средства электронной идентификации, имеющего «значительный» или «высокий» уровень обеспечения доверия.

[3] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means.

19. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли применять концепцию уровней обеспечения доверия к удостоверительным услугам, и если да, то каким образом.

C. Ответственность

20. Успешное внедрение УИД и удостоверительных услуг в коммерческих и некоммерческих сферах деятельности может во многом зависеть от применяемых положений об ответственности. В этой связи следует отметить, что, хотя средства правовой защиты на случай ложной идентификации сторон в коммерческих сделках, как правило, имеются, ответственность за неправомерное присвоение основополагающей идентичности в бумажной документации может не возникать в случае, если национальным законодательством не предусмотрена ответственность публичных субъектов, предоставляющих этот вид услуг.

21. Рабочей группой уже был определен ряд вопросов, которые заслуживают обсуждения в связи с темой ответственности сторон, участвующих в УИД и удостоверительных услугах, а именно: какие субъекты могут быть привлечены к ответственности (эмитенты, поставщики, другие стороны), учитывая особый режим ответственности для публичных субъектов; возможность ограничения ответственности сторон, соблюдающих ранее установленные требования; статутные механизмы ограничения ответственности, например освобождение от бремени доказывания или перенос такого бремени; и договорные ограничения ответственности (A/CN.9/936, пункт 85).

22. В некоторых случаях будет нелегко идентифицировать субъект, на котором лежит ответственность, например, за атрибуты данных, предоставляемые в рамках удостоверительной услуги, когда для фиксации момента времени используется технология распределенных блоков данных (A/CN.9/936, пункт 86). В других случаях при коммерческих сделках может применяться страховой механизм, в рамках которого ущерб от недобросовестного использования схем электронной идентификации или удостоверительных услуг возмещается страховщиком. Еще один возможный механизм предусматривает при наступлении определенных условий автоматическую компенсацию за счет активов, заранее зарезервированных для этого в ликвидной форме, или наложение фиксированных штрафов.

1. УИД

23. Статья 9 Постановления eIDAS предписывает представление в момент уведомления о схеме УИД информации о режиме ответственности, применимом в отношении поставщика средств электронной идентификации, а также в отношении стороны, обеспечивающей процедуру аутентификации.

24. В статье 11 Постановления eIDAS на уведомляющее государство-член возлагается ответственность за ущерб, причиненный вследствие невыполнения им своих обязательств, касающихся обеспечения присвоения личных идентификационных данных, которые однозначно характеризуют то или иное лицо, именно этому лицу, а также обеспечения наличия в сети аутентификационной информации, используемой для подтверждения личных идентификационных данных. Кроме того, эта статья возлагает на сторону, выдающую средства электронной идентификации, ответственность за ущерб, возникающий вследствие неприсвоения средств электронной идентификации лицу, которое однозначно характеризуется личными идентификационными данными. И наконец, она возлагает на сторону, осуществляющую процедуру аутентификации, ответственность за необеспечение надлежащего функционирования системы онлайновой аутентификации, которая используется для подтверждения персональных идентификационных данных.

25. Статья 11 Постановления eIDAS относится только к трансграничным операциям и распространяется лишь на те случаи, когда несоблюдение носит

умышленный характер или совершается по халатности. Она применяется в соответствии с национальным законодательством, касающимся таких вопросов, как определение ущерба и возложение бремени доказывания, без ущерба для дополнительной ответственности, вытекающей из национального законодательства сторон, которые участвуют в сделках, где используются схемы УИД.

26. Подводя итог, можно сказать, что Постановление eIDAS определяет ответственность участников схемы УИД в случае несоблюдения некоторых названных обязательств, если это несоблюдение носит умышленный характер или допущено по халатности, и при условии, что сделка является трансграничной, и не исключает дополнительной ответственности по национальному законодательству.

27. Статья 281 Закона 2017-20 Бенина предусматривает ответственность оператора системы УИД за ущерб, нанесенный пользователям схем УИД, если этот ущерб причинен умышленно или по халатности.

28. Согласно разделу 1-552 Закона Виргинии об электронной системе УИД оператор структур доверия в рамках систем идентификации или поставщик идентификационных данных не несет ответственности, если идентификационные учетные данные выдаются либо если атрибуты идентификационных данных или «знак доверия» присваивается в соответствии со стандартами УИД, утвержденными министром технологии Содружества Виргинии, положениями любого договора и любыми оформленными в виде документа правилами и стратегиями той структуры доверия в рамках системы идентификации, в состав которой входит данный поставщик идентификационных данных. Согласно разделу 1-550 «знак доверия» — это «машиносчитываемая официальная печать, аутентификационная функция, сертификат, лицензия или логотип, которые могут выдаваться оператором структур доверия в рамках системы идентификации сертифицированному поставщику идентификационных данных в рамках его структуры доверия в подтверждение того, что поставщик идентификационных данных соблюдает документально оформленные правила и регламенты данной структуры доверия в рамках системы идентификации».

29. Короче говоря, Закон Виргинии об электронной системе УИД выводит из-под ответственности тех операторов структур доверия в рамках системы идентификации и тех поставщиков идентификационных данных, которые соблюдают стандарты, установленные публичным органом, положения договоров и правила федераций. Факт соблюдения минимальных спецификаций и стандартов, введенных Содружеством Виргинии, устанавливается путем привлечения независимых сертификационных органов, действующих в качестве третьей стороны, которые проводят объективный, непротиворечивый и поддающийся проверке анализ соблюдения с опорой на четко определенные критерии сертификации[4]. Это исключение не применяется, если оператор структур доверия в рамках системы идентификации или поставщик идентификационных данных совершил действие или упущение по грубой халатности или виновен в умышленном нарушении.

30. В разделе 1-555 Закона Виргинии об электронной системе УИД указано, что никакое положение Закона либо охватываемое им действие или упущение, совершенное публичным субъектом в связи с УИД, не должно рассматриваться в качестве добровольного отказа от суверенного иммунитета этого публичного субъекта.

31. Рабочая группа, возможно, пожелает обсудить вопрос о том, на какие структуры и по какому режиму должна возлагаться ответственность, а также о том, следует ли ввести особый режим ответственности для публичных субъектов.

32. При обсуждении режима ответственности Рабочей группе желательно рассмотреть: a) возможность ограничения ответственности сторон, соблюдающих установленные требования, например, путем освобождения от бремени

[4] Commonwealth of Virginia Identity Management Standards Advisory Council, *Guidance Document 5: Certification of Identity Trust Framework Operators* (draft), Section 7: Certification of Identity Trust Framework Operators.

доказывания или переноса такого бремени; b) вопрос о том, следует ли предусмотреть различные уровни обеспечения доверия для различных режимов ответственности; c) возможность договорного ограничения ответственности; а также d) вопрос о том, должно ли требоваться предоставление метаданных с описанием режима ответственности, включая любые возможные ее ограничения.

2. Удостоверительные услуги

33. Согласно статье 13 Положения eIDAS поставщики удостоверительных услуг несут ответственность за ущерб, причиненный умышленно или по халатности любому физическому или юридическому лицу вследствие несоблюдения обязательств, вытекающих из Постановления. Другими словами, поставщики удостоверительных услуг, выполняющие обязательства, предусмотренные Постановлением, освобождаются от ответственности.

34. Кроме того, статья 13 вводит опровержимую презумпцию умысла или халатности в отношении квалифицированного поставщика удостоверительных услуг, тогда как в отношении неквалифицированного поставщика удостоверительных услуг бремя доказывания умысла или халатности возлагается на лицо, требующее возмещения ущерба. Данное положение ставит целью укрепить доверие пользователей к квалифицированным поставщикам, поскольку в случае возникновения ущерба эта презумпция упрощает взыскание возмещения. И наконец, в статье 13 за поставщиками удостоверительных услуг признается возможность ограничения своей ответственности при том условии, что их клиенты заранее проинформированы об этих ограничениях и что эти ограничения признаются третьими сторонами.

35. В ТЗЭП содержатся положения об ответственности, возникающей в результате действий подписавшего лица (ст. 8), поставщика сертификационных услуг (ст. 9) и лица, пользующегося такими услугами (ст. 11). В этих положениях изложены обязательства каждого субъекта, задействованного на любом этапе процедуры использования электронной подписи. В ТЗЭП признается возможность ограничения поставщиками сертификационных услуг сферы или пределов своей ответственности.

D. Институциональные механизмы сотрудничества

36. Институциональные механизмы сотрудничества способны содействовать обеспечению взаимного правового признания и функциональной совместимости систем УИД и удостоверительных услуг. По своему характеру они могут быть частными или публичными.

37. В статье 12 Постановления eIDAS приводится пример институционального механизма сотрудничества; в ней указывается, что государства-члены должны сотрудничать в обеспечении функциональной совместимости и безопасности схем УИД. Сотрудничество может включать обмен информацией, опытом и примерами надлежащей практики, в частности, в отношении технических требований и уровней обеспечения доверия, коллегиальных обзоров схем УИД и рассмотрения соответствующих нововведений.

38. В акте, принятом во исполнение Постановления eIDAS[5], приводятся дополнительные подробности относительно обмена информацией и коллегиального обзора и, в частности, указывается, что государство-член не обязано предоставлять требуемую информацию, если ее раскрытие может поставить под угрозу общественную или национальную безопасность либо коммерческую, профессиональную или корпоративную тайну. В нем также предусматривается создание сети сотрудничества для облегчения взаимодействия. Следует отметить, что, хотя проведение коллегиального обзора подлежащей уведомлению схемы УИД носит

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

добровольный характер, на практике его результаты могут помочь глубже разобраться в вопросе о соответствии данной схемы требуемым стандартам, вследствие чего такой обзор служит важным звеном механизма уведомления, который занимает центральное место в институциональной структуре, предусмотренной Постановлением eIDAS.

39. Еще одной формой взаимодействия между системами УИД может стать их федерация. В рамках этой модели идентификационные данные, прошедшие проверку в одной системе УИД, предоставляются в согласованном и регламентированном порядке различным сторонам, входящим в другую систему УИД, которая нуждается в таких идентификационных данных для иных целей (см. также A/CN.9/WG.IV/WP.153, пункт 47). Федерация систем УИД обеспечивает для их участников функциональную совместимость благодаря использованию единой технической и правовой платформы, регулируемой комплексом системных правил. Таким образом, создание федерации может способствовать увеличению числа участвующих пользователей и обращений, а также снижению связанных с УИД расходов. Хотя федерации функционируют на договорной основе, наличие законодательных положений может служить фактором, благоприятствующим их деятельности (см., например, положения о применении «знаков доверия» в Законе Виргинии об УИД, пункт 28 выше).

E. Транспарентность

40. Рабочая группа обозначила принцип транспарентности как имеющий прямое отношение к будущим дискуссиям по вопросам УИД и удостоверительных услуг (A/CN.9/936, пункт 8). При этом она подчеркнула две вытекающих из этого принципа обязанности — обнародовать информацию о характере и качестве предлагаемых услуг УИД и удостоверительных услуг, а также уведомлять о нарушениях безопасности.

41. В отношении характера и качества предлагаемых услуг следует отметить, что поставщики идентификационных данных и удостоверительных услуг, входящие в состав федераций или проходящие иную сертификацию своей деятельности, будут раскрывать значительный объем информации. Для других поставщиков могут быть введены минимальные требования по раскрытию информации. Так, например, в пункте 1 статьи 9 ТЗЭП приводится перечень сведений, которые поставщик сертификационных услуг должен раскрыть пользующейся его услугами стороне.

42. Что касается обязанности уведомлять о нарушениях безопасности, то было отмечено, что уведомления о нарушении безопасности обладают общими элементами с уведомлениями о компрометации данных, однако здесь имеются также и существенные различия. Было добавлено, что имеются полезные примеры механизмов, выходящих за рамки простого уведомления в случае нарушения безопасности (A/CN.9/936, пункт 89). Дополнительные соображения могут касаться возможного использования оперативных данных о киберугрозах для снижения рисков.

43. В статье 10 Постановления eIDAS предусмотрена обязанность государств-членов уведомлять о случаях нарушения или компрометации, которые ослабляют надежность трансграничной схемы аутентификации. Соответствующее государство-член должно также незамедлительно приостановить действие скомпрометированных аутентификационных данных или их скомпрометированной части либо аннулировать их.

44. В пункте 2 статьи 19 Постановления eIDAS сформулировано аналогичное положение, обязывающее поставщиков удостоверительных услуг уведомлять надзорный орган и любые другие соответствующие органы, например орган по защите данных, о любом случае нарушения безопасности или утраты целостности, который оказывает значительное воздействие на предоставляемую удостоверительную услугу или на используемую при этом личную информацию. Уведомление

должно направляться без неоправданной задержки, но в любом случае в течение 24 часов после выявления такого нарушения или утраты.

45. В пункте 1 (b) статьи 8 ТЗЭП указан факультативный механизм уведомления, который может быть использован подписавшим лицом в случае компрометации данных о создании подписи или при наличии высокой вероятности того, что они были скомпрометированы.

46. Положение, обязывающее раскрывать информацию о нарушениях безопасности, можно было бы сформулировать следующим образом:

> Поставщики идентификационных данных и удостоверительных услуг незамедлительно [но в любом случае в … -дневный срок после выявления этого факта] уведомляют [надзорный орган] [затронутых этим клиентов и пользующихся их услугами лиц] о любом случае нарушения безопасности или утраты целостности, который оказывает [серьезное] воздействие на предоставляемые услуги, присвоенные идентификационные учетные данные или проведенные аутентификационные процедуры либо на содержащуюся в них личную информацию.
>
> В случае серьезного нарушения безопасности или утраты целостности поставщики идентификационных услуг и удостоверительных услуг приостанавливают оказание затронутых этим услуг [до тех пор, пока…].
>
> Пользователи идентификационных и удостоверительных услуг уведомляют поставщика услуг в случае компрометации сведений, касающихся идентификационных учетных данных, процедур аутентификации или удостоверительных услуг, либо в том случае, если известные пользователю обстоятельства с большой долей вероятности указывают на то, что сведения, связанные с идентификационными учетными данными, процедурами аутентификации или удостоверительными услугами, были скомпрометированы.

47. Проект данного положения содержит факультативные формулировки, позволяющие указать срок направления уведомления и кому оно должно быть направлено, а также определить ту степень воздействия на услуги, идентификационные учетные данные или личную информацию, при которой возникает обязанность предоставлять уведомление. Можно также предусмотреть обязанность приостанавливать функционирование системы УИД и оказание удостоверительных услуг до прекращения нарушения или утечки данных либо, в качестве альтернативы, до завершения новых процедур сертификации или аналогичных процедур.

F. Сохранение данных

48. Рабочая группа уже подчеркивала важность унификации и совместимости режимов сохранения данных для трансграничной торговли (A/CN.9/936, пункт 91). При этом она выделяла по меньшей мере две темы, которые могут представлять интерес. Первая касается защиты данных, вторая — их хранения и архивирования.

49. Защита данных — это область, где могут возникать особенно сложные вопросы. Рабочая группа, возможно, пожелает подтвердить, что в соответствии с общим принципом, согласно которому в текстах ЮНСИТРАЛ, призванных содействовать электронной торговле, не затрагиваются нормы материального права (см. A/CN.9/WG.IV/WP.153, пункт 48), положения законодательства по вопросам защиты данных и связанным с ними вопросам, таким как конфиденциальность, должны оставаться применимыми в полном объеме, и рассмотреть целесообразность каких-либо дополнительных уточнений или пояснений.

50. Хранение и архивирование документов представляет собой функцию, которая может выполняться с использованием электронных средств, о чем уже говорится в статье 10 ТЭЭТ, устанавливающей требования функциональной эквивалентности между сообщениями данных и бумажными документами с точки зрения их сохранения. Обязательства по сохранению документов вытекают из

материального права и связаны со временем, необходимым для вынесения предписаний о различных действиях.

51. Функции хранения и архивирования данных могут быть предметом специальных доверительных услуг (см. ниже, пункты 64–65). В контексте функциональной совместимости доверительных услуг Рабочая группа, возможно, пожелает обсудить вопросы, касающиеся переноса электронных архивов.

G. Надзор за работой поставщиков услуг

52. Если Рабочая группа придет к выводу о целесообразности рассмотрения механизмов УИД и систем удостоверительных услуг, а не связанных с ними операций (см. A/CN.9/WG.IV/WP.153, пункты 57–59), может оказаться полезным или даже необходимым создать надзорный орган для обеспечения доверия к поставщикам услуг и предоставляемым услугам. Однако создание такого органа сопряжено с рядом административных и финансовых последствий. В достижении целей, которые преследует надзор за работой поставщиков услуг, при одновременном сокращении связанных с этой деятельностью издержек, могут помочь такие альтернативные или дополнительные механизмы, как сертификация третьей стороной.

53. Законодательство штатов Вермонт и Вирджиния наделяет полномочиями по надзору за работой поставщиков идентификационных услуг государственные органы. Аналогичным образом, согласно статье 97 Закона 2017-07 Того функции надзора за работой поставщиков удостоверительных услуг возлагаются на национальный сертификационный орган. В соответствии со статьей 283 Закона 2017-20 Бенина поставщики идентификационных услуг назначаются государственным органом. Механизм надзора за управлением идентификационными услугами и их предоставлением также косвенно заложен в системе уведомлений, предусмотренной Постановлением eIDAS.

54. В том что касается поставщиков удостоверительных услуг, законодательство ряда стран наделяет надзорный орган полномочиями по предоставлению квалифицированного статуса или по надзору за предоставлением такого статуса третьими сторонами. Положение eIDAS требует назначения в государствах-членах национального надзорного органа для поставщиков удостоверительных услуг.

55. В МЗЭП упоминание о наличии надзорных органов носит факультативный характер в свете принятого в нем принципа нейтральности моделей, поскольку включение обязательных положений о существования таких органов может быть понято как препятствующее принятию рыночной модели, основанной на саморегулировании удостоверительных услуг.

H. Вопросы, непосредственно связанные с удостоверительными услугами

56. Работа над правовыми вопросами, касающимися удостоверительных услуг, тесно связана с работой над УИД. Соответственно, замечания в отношении удостоверительных услуг в контексте принципа функциональной эквивалентности (A/CN.9/WG.IV/WP.153, пункты 36–37), правового признания (A/CN.9/WG.IV/WP.153, пункты 93–98), уровней обеспечения доверия (пункты 17–19 выше) и ответственности (пункты 33–35 выше) приводятся с учетом рассмотрения тех же вопросов применительно к УИД.

57. Однако в связи с правовым режимом удостоверительных услуг могут также возникать специфические трудности. Одной из основных проблем является то, что каждая удостоверительная услуга имеет свои особенности, что требует рассмотрения отдельного ряда вопросов. Еще один вопрос касается того, должен ли правовой режим удостоверительных услуг включать открытый перечень таких услуг, составленный исходя из общего определения «удостоверительной услуги», или же

следует предусмотреть как общие нормы, относящиеся ко всем удостоверительным услугам, так и конкретные правила, применимые к каждой из них.

58. Помимо этого, для описания функций, которые будут выполняться при использовании каждой удостоверительной услуги, можно сослаться на положения о функциональной эквивалентности, подобные положениям ЮНСИТРАЛ об электронных подписях и сохранении документов (см. A/CN.9/WG.IV/WP.153, пункт 36). При рассмотрении этого предложения могут помочь большой массив существующих законодательных текстов на тему электронных подписей[6] и накопленный опыт их применения.

59. Положение eIDAS является примером всеобъемлющего законодательства об удостоверительных услугах. В нем содержатся, в частности, общие положения об ответственности и бремени доказывания (статья 13; см. пункты 23–26 выше), надзоре (статья 17; см. пункт 53 выше,) и требованиях к безопасности (статья 19; см. пункт 44 выше, касающийся обязанности уведомлять о нарушениях безопасности или утрате данных).

60. Положение eIDAS содержит специальный раздел, применимый ко всем квалифицированным удостоверительным услугам. Квалифицированные удостоверительные услуги распознаваемы благодаря их включению в официальный перечень, который ведут государства — члены Европейского союза. В этой связи Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли проводить различие между удостоверительными услугами в зависимости от уровня обеспечения доверия, присущего той или иной удостоверительной услуге, и, если такое решение будет принято, о том, какой институциональный механизм следует использовать для проведения различия между удостоверительными услугами.

61. Положение eIDAS также содержит конкретные положения в отношении следующих удостоверительных услуг: электронных подписей; электронных печатей; проставления электронной отметки времени; услуг по электронной регистрации доставки и подтверждению подлинности веб-сайтов[7]. Каждая удостоверительная услуга может оказываться в квалифицированной форме. Электронные подписи и электронные печати могут также иметь усиленную форму.

62. В Законе 045-2009/AN Буркина-Фасо имеется статья, содержащая положения, применимые ко всем поставщикам удостоверительных услуг, а также положения о процедуре получения аккредитации, которая имеет отношение к получению статуса квалифицированного поставщика удостоверительных услуг. В этом законе содержатся конкретные положения о квалифицированных электронных сертификатах, электронном архивировании, проставлении электронных отметок времени и услугах по электронной регистрации доставки. В нем также имеется отдельная глава, посвященная электронным подписям.

63. Закон 2017-20 Бенина содержит общую часть, применимую ко всем поставщикам удостоверительных услуг, и конкретные положения о следующих удостоверительных услугах: электронных подписях, электронных печатях, проставлении электронных отметок времени и электронном архивировании.

64. В статье 301 этого закона указано, что «электронное архивирование гарантирует подлинность и целостность хранящихся таким образом документов, данных и информации». В ней также содержится положение о функциональной эквивалентности, аналогичное статье 10 ТЭЭТ.

65. В статье 302 Закона 2017-20 Бенина указано, что цель электронного архивирования заключается в сохранении документов, данных и информации для

[6] Согласно данным системы ЮНКТАД по глобальному отслеживанию законов об информационных технологиях, 145 государств, или 78 процентов их общего числа, приняли законы об электронных операциях, обычно включающие положения об электронных подписях.

[7] Определение этих удостоверительных услуг приводится в документе A/CN.9/WG.IV/WP.150.

последующего использования и что соответствующие данные должны быть структурированы, проиндексированы и храниться таким образом, чтобы обеспечивалась их сохранность и возможность их миграции (см. также пункт 51 выше). Доступ должен обеспечиваться вне зависимости от развития технологий. Данное положение применимо как к документам, изначально изготовленным в электронной форме, так и к документам, изначально изготовленным на бумаге и впоследствии оцифрованным.

66. В Законе 2017-07 Того также содержится статья, положения которой применимы ко всем поставщикам удостоверительных услуг и касаются в том числе процедуры получения статуса квалифицированного поставщика удостоверительных услуг. В этом законе имеются конкретные положения в отношении электронных сертификатов, электронного архивирования, проставления электронных отметок времени и услуг по электронной регистрации доставки. В нем также есть отдельная глава, посвященная электронным подписям.

67. Закон 2017-07 Того дополняется Указом № 2018-062/PR, в котором дополнительно установлены обязательства, общие для всех поставщиков удостоверительных услуг. Эти обязательства касаются безопасности и конфиденциальности данных, ответственности, финансовых ресурсов, доступности, защиты данных, прозрачности и управления риском. Кроме того, в Указе содержатся положения, касающиеся каждой из удостоверительных услуг, перечисленных в Законе 2017-07.

68. К дополнительным видам удостоверительных услуг, которые уже определены, но пока отдельно не регулируются законодательством, относятся электронные счета условного депонирования и электронные системы контроля присутствия. Последняя удостоверительная услуга обсуждается в связи с электронными завещаниями[8].

69. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли использовать в рамках правового режима УИД и удостоверительных услуг одни и те же или различные механизмы. Кроме того, она, возможно, пожелает обсудить, следует ли в правовом режиме удостоверительных услуг использовать открытый перечень таких услуг на основе общего определения «удостоверительной услуги» или предусмотреть общие нормы, относящиеся ко всем удостоверительным услугам, и конкретные правила, применимые к каждой из них. В частности, Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли сформулировать для каждой удостоверительной услуги правила функциональной эквивалентности и является ли ссылка на уровни обеспечения доверия уместной также в контексте удостоверительных услуг.

[8] См., например, статью 8 законопроекта об электронных завещаниях, разрабатываемого Национальной конференцией уполномоченных по унификации законодательства штатов.