



Генеральная Ассамблея

Distr.: Limited
10 September 2021
Russian
Original: English

**Комиссия Организации Объединенных Наций
по праву международной торговли
Рабочая группа IV (Электронная торговля)
Шестьдесят вторая сессия
Вена, 22–26 ноября 2021 года**

**Пояснительная записка к проекту положений
об использовании и трансграничном признании
управления идентификационными данными
и достоверительных услуг**

Записка Секретариата

Содержание

	<i>Стр.</i>
I. Введение	2
Приложение	
Пояснительная записка к проекту положений об использовании и трансграничном признании управления идентификационными данными и достоверительных услуг .	3
I. Введение	3
A. Цель настоящей пояснительной записки	3
B. Задачи	3
C. Сфера охвата	4
D. Структура	4
E. Справочная информация	5
F. Основные понятия и принципы	6
II. Постатейные комментарии	10
A. Глава I. Общие положения (статьи 1–4)	10
B. Глава II. Управление идентификационными данными (статьи 5–12)	15
C. Глава III. Достоверительные услуги (статьи 13–24)	23
D. Глава IV. Международные аспекты (статьи 25 и 26)	30



I. Введение

1. На шестьдесят первой сессии Рабочая группа просила секретариат представить ей проект пояснительных материалов вместе с пересмотренными проектами положений для рассмотрения на ее шестьдесят второй сессии. Эти материалы изложены в пояснительной записке, содержащейся в приложении.
2. Пояснительная записка была подготовлена секретариатом для получения замечаний Рабочей группы и, по возможности, ее принятия. В ней содержатся отчет о результатах обсуждений в Рабочей группе, который был представлен в докладе Комиссии, а также дополнительная контекстуальная информация, касающаяся мандата Рабочей группы. В записке идет речь о проекте положений, который изложен в документе [A/CN.9/WG.IV/WP.170](#), и она будет пересматриваться с учетом любых поправок к этим положениям и любых замечаний, которые будут согласованы Рабочей группой на ее шестьдесят второй сессии. Также пояснительная записка может помочь Рабочей группе в деле доработки этого проекта положений.

Приложение

Пояснительная записка к проекту положений об использовании и трансграничном признании управления идентификационными данными и удостоверительных услуг

I. Введение

A. Цель настоящей пояснительной записки

1. [будет дополнено]

B. Задачи

2. В течение последних двадцати лет наблюдается экспоненциальный рост стоимостного объема коммерческой деятельности в режиме онлайн (т. е. электронных операций между предприятиями, между предприятиями и потребителями, а также между предприятиями и правительствами). Мировой объем электронной торговли увеличился с 64 млрд долл. США в 1999 году до 29 трлн долл. США в 2017 году¹. Такой рост совпал с расширением доступа частных лиц и предприятий к интернету. Например, доля домохозяйств, имеющих доступ к интернету, выросла с 35 процентов в 2002 году до 83,6 процента в 2017 году.² Соответственно возросла доступность услуг электронного правительства (включая услуги, связанные с торговлей), электронных банковских услуг и электронных платежей.

3. Такой рост основывается на доверии и 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. В результате были разработаны различные системы, методы, технологии и устройства для создания цифровых учетных данных физических и юридических лиц и управления ими. Рассмотрение правовых аспектов управления идентификационными данными (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 ряд препятствий на пути расширения использования УИД и удостоверительных услуг. Препятствия юридического характера включают: 1) отсутствие законодательства, придающего юридическую силу УИД и удостоверительным услугам; 2) различия в правовых 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 услуг³.

5. Основная цель [проекта документа] заключается в устранении этих препятствий путем разработки единообразных правовых норм. Такие нормы служат

¹ UNCTAD, E-Commerce and Development Report 2001, UN Doc UNCTAD/SDTE/ECB/1, p. 44; UNCTAD, Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries, UN Doc UNCTAD/DER/2019, p. 15.

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

³ A/CN.9/965, п. 52.

нескольким целям: повысить эффективность; снизить операционные издержки; повысить безопасность и правовую определенность электронных сделок, обеспечив тем самым доверие; и способствовать преодолению отставания в сфере цифровых технологий с помощью согласованных решений.

6. Таким образом, [проект документа] 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 контексте цифровой экономики это означает 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.

C. Сфера охвата

7. [будет дополнено]

D. Структура

8. [Проект документа] состоит из четырех глав, посвященных соответственно общим положениям, УИД, удостоверительным услугам и международным аспектам. Главы I и IV относятся к УИД, и к удостоверительным услугам. Более того, главы II и III во многом сходны по структуре и содержанию. Таким образом, разъяснения, касающиеся того или иного положения главы II, могут также относиться к соответствующему положению главы III в той мере, в какой эти положения совпадают. Это может относиться, в частности, к статьям 13, 14, 15, 22, 23 и 24 в отношении статей 5, 6 и 7, 8, 10, 11 и 12, соответственно.

9. Глава I содержит определения некоторых терминов, встречающихся в [проекте документа]; определение сферы применения; положения о добровольном использовании УИД и удостоверительных услуг, в том числе конкретных услуг; положения о взаимосвязи между [проектом документа] и другими законами, включая требования, обязывающие осуществлять идентификацию или использовать определенные удостоверительные услуги; и положения об автономном толковании, в том числе для целей восполнения пробелов, [проекта документа] с учетом его единообразного характера и международного происхождения.

10. В главе II определяются основные элементы правового режима, применимого к УИД, перечисляются некоторые основные обязанности поставщиков услуг УИД и абонентов, а также изложены положения об ответственности поставщиков услуг УИД. В статье 5 устанавливается принцип юридического признания электронной идентификации и недискриминации УИД. В статье 6 перечислены основные обязанности поставщиков услуг УИД; при этом в ней определяются основные этапы жизненного цикла УИД. В статье 7 рассматриваются обязанности поставщика услуг УИД в случае нарушения безопасности данных, и ее дополняет статья 8 об обязанностях абонентов в случае, если идентификационные учетные данные были скомпрометированы. Статья 9 содержит положение о функциональной эквивалентности офлайновой и электронной идентификации, для которой требуется использование надежного метода. Надежность метода оценивается путем определения ex post на основании обстоятельств, перечисленных в статье 10, или путем назначения ex ante в соответствии со статьей 11. Более того, если метод действительно выполнил свою функцию, то не требуется определять его надежность. Наконец, в статье 12 рассматривается ответственность поставщиков услуг УИД.

11. В главе III определяются основные элементы правового режима, применимого к использованию удостоверительных услуг. Статья 13 содержит общее положение о недискриминации юридических последствий использования удостоверительных услуг. В статье 14 устанавливаются обязанности поставщиков удостоверительных услуг, а в статье 15 рассматриваются обязанности абонентов удостоверительных услуг в случае, если удостоверительная услуга была скомпрометирована. В статьях 16–21 описаны функции конкретных названных услуг (электронные подписи; электронные печати; электронные отметки времени; электронное архивирование; услуги электронной регистрации доставки; аутентификация веб-сайта) и соответствующие требования, включая использование надежного метода. Положения о конкретно названных удостоверительных услугах сформулированы в основном как правила функциональной эквивалентности. Однако, поскольку у той или иной удостоверительной услуги может не существовать бумажного эквивалента, в ее отношении необязательно требуется правило функциональной эквивалентности. В статье 22 содержатся руководящие указания по *ex post* определению надежности метода, использованного для оказания удостоверительной услуги, а в статье 23 — по его назначению *ex ante*. Наконец, в статье 24 изложены положения об ответственности поставщиков удостоверительных услуг.

12. Глава IV содержит положения, призванные обеспечить возможность трансграничного признания УИД и удостоверительных услуг, что является одной из основных целей [проекта документа]. В [проекте документа] не рассматривается вопрос о создании специального органа для юридического признания УИД и удостоверительных услуг, но предусматривается несколько механизмов на основе децентрализованного подхода. Помимо статей 25 и 26, непосредственное отношение к этому имеют соответствующие положения статей 10(3), 11(4), 22(3) и 23(4), касающиеся недопустимости дискриминации по географическому признаку при определении надежности системы УИД и удостоверительных услуг и при назначении надежных систем УИД и удостоверительных услуг. Для обеспечения возможности трансграничного использования системы УИД и удостоверительных услуг также могут иметь значение договорные соглашения.

Е. Справочная информация

1. История разработки проекта документа

13. [См. пункты 4–20 документа [A/CN.9/WG.IV/WP.169](#)].

14. [будет дополнено]

2. Взаимосвязь с принятыми ранее текстами ЮНСИТРАЛ

15. Принятые ранее тексты ЮНСИТРАЛ не содержат положений об удостоверительных услугах. Однако в них содержатся правила функциональной эквивалентности, которые могут иметь значение для определенных удостоверительных услуг. В частности, в статье 7 ТЗЭТ, статье 6 ТЗЭП, статье 9(3) КЭС и статье 9 ТЗЭПЗ устанавливаются требования, которым должны соответствовать электронные подписи, чтобы считаться функционально эквивалентными подписям, проставленным на бумаге. В основу статьи 16 [проекта документа] положена статья 9 ТЗЭПЗ. Аналогичным образом, в статье 10 ТЗЭТ устанавливаются требования функциональной эквивалентности применительно к сохранению информации. Статья 19 [проекта документа] основана на статье 10(1) ТЗЭТ.

16. Статьи 16–21 [проекта документа] относятся к удостоверительным услугам, которые призваны обеспечить уверенность в определенных качествах сообщения данных. При этом не все удостоверительные услуги, охватываемые этими положениями, имеют эквиваленты в бумажной среде. Более того, для обеспечения выполнения положений о функциональной эквивалентности, содержащихся в этих ранее принятых текстах ЮНСИТРАЛ, возможно, не нужно будет использовать ту

или иную конкретно названную в [проекте документа] удостоверительную услугу.

Е. Основные понятия и принципы

17. В данном разделе разъясняются несколько основных понятий и принципов, лежащих в основе [проекта документа]. Дальнейшее разъяснение терминов, которые определены и используются в [проекте документа], изложено в комментарии к статье 1 ниже, а более широкий перечень терминов и понятий, относящихся к УИД и удостоверительным услугам, составленный на основе определений, содержащихся в согласованных на международном уровне юридических и технических текстах, приводится в документе [A/CN.9/WG.IV/WP.150](#). Как указано в этом документе, в упомянутых текстах для одного и того же понятия могут использоваться разные термины, имеющие определения, или один и тот же термин может определяться по-разному.

1. Основополагающие принципы

18. Как и ранее принятые тексты ЮНСИТРАЛ, [проект документа] основан на принципах автономии сторон, технологической нейтральности, функциональной эквивалентности и недискриминации в отношении использования электронных средств, с учетом корректировок⁴. Хотя в [проекте документа] эти общие принципы прямо не указаны, они составляют основу ключевых положений текста. Например, принцип недискриминации, применительно к УИД и удостоверительным услугам, воплощен в статьях 5 и 13, соответственно, а принцип функциональной эквивалентности лег в основу статей 9 и 16–21.

19. Подход, основанный на функциональной эквивалентности, предполагает существование юридических требований, которые прямо или косвенно предписывают некоторые физические действия или действия с бумажными документами, такие как использование бумажного удостоверения для идентификации лица или бумажного сообщения для аутентификации того или иного факта или объекта. Затем в нем анализируются цели и функции этих требований с целью определить, как эти цели или функции могут быть достигнуты или выполнены с помощью электронных средств. Вместе с тем, как и цифровые технологии, упростившие целый ряд видов деятельности, не имеющих бумажных эквивалентов, так и некоторые услуги УИД и удостоверительные услуги, охватываемые [проектом документа], могут не иметь бумажного эквивалента.

2. Управление идентификационными данными (УИД)

20. Идентификация — это процесс распознавания того или иного лица на основе имеющейся информации, относящейся к этому лицу (т. е. атрибутов). Эта информация может быть собрана или накоплена в результате наблюдений. Идентификация имеет особенно важное значение для укрепления доверия к электронным сделкам в режиме онлайн. По сути, идентификация заключается в проверке соответствия собранных или накопленных в ходе наблюдений атрибутов ранее установленным для идентифицируемого лица «идентификационным данным». В этом смысле идентификация часто проводится в ответ на конкретное идентификационное утверждение и предъявление атрибутов для проверки.

21. Соответственно, согласно [проекту документа] УИД включает в себя два отдельных этапа (или две фазы) — во-первых, выдачу идентификационных учетных данных, т. е. данных, которые могут быть представлены для целей электронной идентификации; во-вторых, предъявление и проверку этих учетных данных с помощью электронных средств:

а) первый этап УИД предусматривает сбор атрибутов, которые могут составлять «базовые идентификационные данные» лица (т. е. атрибутов, которые

⁴ См. [A/CN.9/902](#), пп. 52 и 63.

регистрируются государственными органами в системах регистрации актов гражданского состояния и статистического учета естественного движения населения для физических лиц и в реестрах компаний и предприятий для юридических лиц). Эти атрибуты могут быть представлены в виде выданных правительством документов, содержащих учетные данные (например, свидетельство о регистрации), которые заверяются выдающим ведомством. Этот процесс может осуществляться в режиме «офлайн» на основе физических учетных данных, предъявляемых лично, и приводит к выдаче лицу документа, содержащего учетные данные;

б) второй этап УИД предусматривает предъявление этих учетных данных с помощью электронных средств и проверку с помощью электронных средств того, что лицо, предъявившее учетные данные, является лицом, которому эти учетные данные были выданы на первом этапе.

22. Системы УИД используются для управления процессами идентификации, связанными с каждым из этих этапов, а также для управления собранными атрибутами, выданными учетными данными и средствами, используемыми для проверки. Системы УИД могут состоять из одной организации, выполняющей все процессы, относящиеся к каждому этапу УИД, или нескольких организаций, выполняющих эти процессы. Более того, некоторые системы УИД могут предлагать разные «услуги» УИД в зависимости от потребностей сторон (т. е. стороны, желающей идентифицировать, и стороны, желающей быть идентифицированной).

23. Системы УИД используются для предоставления услуг УИД. Системы УИД могут эксплуатироваться публичными или частными субъектами и могут предлагать несколько услуг УИД. На практике публичные системы УИД, как правило, предусматривают оказание одной услуги УИД, тогда как частные системы УИД могут предоставлять несколько услуг УИД, имеющих разные уровни надежности. В другой классификации системы УИД делятся на централизованные или распределенные. [Проект документа] основан на принципах технологической и модельной нейтральности и поэтому может применяться ко всем типам систем и услуг УИД.

24. Поставщики услуг УИД, абоненты, полагающиеся стороны и другие заинтересованные субъекты могут договориться действовать в соответствии с совместимыми принципами, стандартами и технологиями, указанными в правилах системы, чтобы учетные данные, предоставляемые каждым участвующим поставщиком услуг УИД, могли быть понятны всем участвующим полагающимся сторонам и вызвали у них доверие. Такой подход можно назвать «федеративным управлением идентификационными данными», а правила системы, имеющие договорной характер, — «рамочной основой системы доверия». Федеративное управление идентификационными данными может способствовать увеличению числа пользователей и количества приложений, для которых предоставляются одни и те же услуги УИД, что, в свою очередь, позволит ограничить рост расходов и обеспечить долгосрочную устойчивость.

3. Удостоверительные услуги

25. Удостоверительные услуги также имеют решающее значение для укрепления доверия к электронным операциям. По своей сути удостоверительные услуги призваны обеспечить уверенность в определенных качествах сообщений данных, таких как источник, целостность и время осуществления определенного действия в отношении данных. Хотя в [проекте документа] указаны некоторые часто используемые удостоверительные услуги, в нем признается, что могут существовать или могут быть разработаны в будущем и другие удостоверительные услуги.

26. Понятие удостоверительной услуги в [проекте документа] охватывает не только саму услугу, но и предоставление услуги. Например, оно охватывает услуги, поддерживающие способы создания электронной подписи и управления ею, а не только непосредственно электронную подпись.

4. Определение ответственности

27. В соответствии с ранее принятыми текстами ЮНСИТРАЛ, в ряде положений [проекта документа] говорится об использовании надежного метода. В [проекте документа] предусмотрены два механизма оценки надежности метода: в статьях 10 и 22 приводится примерный перечень обстоятельств, которые должны учитываться при определении надежности; статьи 11 и 23 предусматривают механизм назначения надежных методов. Этот подход основывается на статьях 6 и 7 ТЗЭП.

28. При сочетании определения и назначения в [проекте документа] не отдается предпочтения какому-либо одному из упомянутых механизмов, но преследуется цель объединить преимущества обоих механизмов, сведя к минимуму их недостатки, и в конечном итоге предоставить сторонам возможность выбора предпочтительного решения.

29. Не все тексты ЮНСИТРАЛ, касающиеся удостоверительных услуг, содержат положения, позволяющие применять оба подхода, — *ex ante* и *ex post*. Однако подходы *ex ante* и *ex post* обычно считаются совместимыми и взаимодополняемыми.

а) Ретроспективное определение надежности (*ex post*)

30. Вопрос об определении надежности возникает только в случае спора, следовательно, уже после того, как метод был использован (т. е. *ex post*). Таким образом, [проект документа] в целом позволяет осуществлять операции в сфере УИД и ограничивает необходимость определения надежности используемого метода случаями, когда возникает спор о действительности операции из-за отсутствия или недостаточной идентификации одной или нескольких сторон.

31. Преимуществом подхода *ex post* является предоставление сторонам максимально гибких возможностей в выборе технологий и методов. Более того, управление таким подходом может осуществляться на децентрализованной основе и не требует создания какого-либо институционального механизма, что позволяет избежать сопутствующих расходов.

32. С другой стороны, недостатком подхода *ex post* является то, что он не способствует заблаговременному обеспечению правовой определенности и, следовательно, не обеспечивает для пользователей предсказуемость в отношении действительности используемого метода, тем самым потенциально подвергая их дополнительным рискам в случае, если использованный метод будет признан ненадежным. Более того, при таком подходе надежность метода определяется третьей стороной, и это может занять много времени и привести к непоследовательным решениям.

б) Заблаговременное назначение надежных удостоверительных услуг (*ex ante*)

33. Надежные услуги назначаются до использования метода (*ex ante*) на основе перечня заранее определенных условий и в общем плане, а не применительно к конкретной сделке. Уточнение условий, перечисленных в [проекте документа], не должно приводить к установлению требований, связанных с использованием конкретной технологии.

34. Назначение относится не к общим типам услуг УИД и удостоверительных услуг или ко всем услугам УИД и удостоверительных услуг, предлагаемым поставщиком услуг УИД или поставщиком удостоверительных услуг, а к конкретной услуге, предоставляемой конкретным поставщиком услуг.

35. Подход *ex ante* позволяет обеспечить более высокий, по сравнению с подходом *ex post*, уровень ясности и предсказуемости в отношении юридических последствий УИД и удостоверительных услуг, в том числе в контексте трансграничного использования. При этом управление им должно предусматривать возможность быстрой адаптации к развитию технологий, с тем чтобы не

препятствовать инновациям. В ином случае при таком подходе дискриминации могут подвергнуться те услуги УИД и удостоверительные услуги, которые, хотя и будут доступными и основанными на надежных методах, не будут являться назначенными.

36. Принимающая [проект документа] юрисдикционная система должна указать учреждение, отвечающее за назначение, которое может быть как частным, так и публичным органом. Назначающие учреждения могут быть аккредитованы в соответствии с техническими стандартами, применимыми к органам по сертификации продукции, процессов и услуг. Сертификация (в том числе самосертификация) также является полезной для оценки услуг, в рамках которых используются стандарты, основанные на конечных результатах, и поэтому она может иметь значение при их назначении.

37. Необходимый для применения подхода *ex ante* институциональный механизм требует специального механизма назначения, который зачастую управляется централизованно. Такой механизм должен включать в себя разные элементы, в частности критерии оценки услуг, подробное описание процесса оценки принятия решений и источники финансирования. В зависимости от ряда факторов, в том числе наличия институциональных механизмов, управление этой системой лицензирования может быть сложным и дорогостоящим. Именно поэтому процедуру назначения лучше применять к услугам, которые обеспечивают более высокий уровень доверия и надежности и, следовательно, используются для сделок более высокого стоимостного объема. Для принимающих [проект документа] юрисдикционных систем, желающих применять подход *ex ante*, в [проекте документа] предполагается наличие необходимого для этого институционального механизма и не предусматривается его создание или управление им.

5. Международные аспекты

38. Одна из основных целей [проекта документа] является разработка правовой основы, обеспечивающей возможность трансграничного использования УИД и удостоверительных услуг. Для ее достижения применяются принципы технологической нейтральности и недискриминации по географическому признаку. Эти принципы положены в основу статей 10(3), 11(4), 22(3) и 23(4) [проекта документа]. Более того, вопросы трансграничного признания рассматриваются в главе IV (статьи 25 и 26).

39. В [проекте документа] не требуется создания официального институционального механизма для трансграничного юридического признания. Однако примеры таких механизмов имеются на региональном и двустороннем уровне. Принимающие [проект документа] юрисдикционные системы, возможно, пожелают использовать [проект документа] в качестве образца для создания институционального механизма с международными партнерами, в том числе в рамках специального соглашения.

40. [Проект документа] может также способствовать осуществлению положений о взаимном юридическом признании, содержащихся в соглашениях о свободной торговле или в специальных соглашениях о цифровой экономике.

II. Постатейные комментарии

A. Глава I. Общие положения (статьи 1–4)

1. Статья 1. Определения

41. Статья 1 содержит определения терминов, используемых в [проекте документа]⁵.

«Атрибут»

42. «Атрибут» — означает единицу информации или данных, связанную с лицом. Примерами атрибутов физического лица являются, например, имя, адрес, возраст и электронный адрес, а также такие данные, как присутствие в сети и используемое электронное устройство. Примерами атрибутов юридического лица являются, например, официальное наименование, адрес головного офиса, регистрационное наименование, юрисдикционная система регистрации. Понятие атрибута используется в определении идентификационных данных.

43. Атрибуты могут содержать персональные данные, обработка которых является объектом закона о конфиденциальности и защите данных. В [проекте документа] не рассматриваются вопросы конфиденциальности и защиты данных и прямо предусматривается применение этого закона.

Ссылки

[A/CN.9/WG.IV/WP.150](#), п. 13.

«Сообщение данных»

44. Определение термина «сообщение данных» можно найти во всех существующих текстах ЮНСИТРАЛ об электронной торговле. Именно от этого термина следует отталкиваться при определении требований к удостоверительным услугам, поскольку результатом применения удостоверительной услуги является гарантия определенных качеств сообщения данных.

Ссылки

[A/CN.9/1045](#), п. 40.

«Электронная идентификация» [«аутентификация»]

45. Термин «электронная идентификация» означает проверку связи между предполагаемой идентичностью и предъявленными учетными данными и является вторым этапом УИД. Термин «электронная идентификация» используется вместо термина «аутентификация» с целью устранить обеспокоенность по поводу множественности значений термина «аутентификация». В техническом смысле термин «аутентификация» означает подтверждение идентификационных данных.

46. В статье 9 термин «идентификация» используется в нетехническом смысле.

Ссылки

[A/CN.9/1005](#), пп. 13, 84–86, 92; [A/CN.9/1045](#), пп. 134 и 136; [A/CN.9/1051](#), п. 67.

⁵ В поддержку работы над [проектом документа] был подготовлен перечень терминов и понятий, имеющих отношение к УИД и удостоверительным услугам, составленный на основе определений, содержащихся в согласованных на международном уровне правовых и технических текстах, который приводится в документе [A/CN.9/WG.IV/WP.150](#).

«Идентификационные данные»

47. Определение «идентификационных данных» лежит в основе понятия УИД и относится к способности уникальным образом отличить физическое или юридическое лицо в определенном контексте. Таким образом, это понятие связано с контекстом. Это определение основано на определении этого термина, содержащемся в положении 6.40 Рекомендации МСЭ МСЭ-Т X.1252.

Ссылки

[A/CN.9/WG.IV/WP.150](#), п. 31; [A/CN.9/1005](#), п. 108.

«Идентификационные учетные данные»

48. «Идентификационные учетные данные» — это данные или физический объект, содержащий данные, предъявляемые для проверки идентификационных данных. Цифровыми учетными данными могут являться, например, имена пользователей, смарт-карты, мобильные идентификационные и цифровые сертификаты, биометрические паспорта и электронные удостоверения личности. Идентификационные учетные данные в электронной форме могут использоваться в режиме онлайн или офлайн в зависимости от особенностей системы УИД. Термин «идентификационные учетные данные» в широком смысле является синонимом термина «электронные средства идентификации», используемого в региональном и национальном законодательстве (например, в статье 3(2) Регламента об eIDAS).

Ссылки

[A/CN.9/1005](#), п. 110; [A/CN.9/1045](#), п. 137.

«Услуги УИД»

49. Определение термина «услуги УИД» отражает понимание, что УИД состоит из двух стадий (или этапов): «проверка идентификационных данных» и «электронная идентификация». В определении услуг УИД говорится об услугах, которые относятся к одному или обоим этапам, поскольку слово «или», используемое в этом определении, не имеет разделительного значения. В статье 6(а), посвященной основным обязанностям поставщика услуг УИД, перечислены разные этапы и шаги, которые входят в предоставление услуг УИД.

Ссылки

См. [A/CN.9/1005](#), пп. 84 и 109.

«Поставщик услуг УИД»

50. Поставщик услуг УИД — это физическое или юридическое лицо, предоставляющее услуги УИД путем выполнения, напрямую или через субподрядчиков, функций, перечисленных в статье 6. При этом не все функции, перечисленные в этой статье, имеют отношение ко всем системам УИД и, следовательно, поставщик услуг УИД необязательно должен выполнять все перечисленные функции.

Ссылки

[A/CN.9/971](#), п. 97; [A/CN.9/1005](#), п. 111; [A/CN.9/1045](#), п. 88.

«Система УИД»

51. В определении понятия «система УИД» описывается система, используемая для осуществления УИД путем проверки идентификационных данных и осуществления электронной идентификации. В нем говорится о «функциях и возможностях» в соответствии с используемой МСЭ терминологией, а именно Рекомендацией МСЭ-Т X.1252 (положение 6.43). В отличие от определения

понятия «услуги УИД», определение понятия «система УИД» обязательно охватывает оба этапа, даже если на каждом этапе задействованы разные поставщики услуг.

Ссылки

[A/CN.9/1005](#), п. 112.

«Проверка идентификационных данных»

52. Термин «проверка идентификационных данных» относится к первому этапу УИД и предусматривает, в частности, подключение, представляющее собой процесс, используемый поставщиками услуг УИД для проверки заявлений субъекта об идентификационных данных перед выдачей ему учетных данных. Он используется вместо термина «идентификация», чтобы снять обеспокоенность по поводу множественности значений термина «идентификация».

Ссылки

[A/CN.9/1005](#), п. 84.

«Абонент»

53. Термин «абонент» означает лицо, которому предоставляются услуги, и не включает в себя полагающихся сторон. Он предполагает наличие договора между поставщиком услуг и абонентом. Например, под определение «абонент» подпадает лицо, имеющее право электронной подписи.

Ссылки

[A/CN.9/1005](#), пп. 43 и 96. [A/CN.9/1045](#), пп. 18 и 22.

«Удостоверительные услуги»

54. Определение «удостоверительная услуга» сочетает в себе абстрактное описание функции, выполняемой с помощью удостоверительных услуг, которая заключается главным образом в обеспечении уверенности в таких качествах данных, как достоверность и подлинность, и неисчерпывающий перечень удостоверительных услуг, которые конкретно названы в [проекте документа]. Благодаря принятию неисчерпывающих перечней общие положения об удостоверительных услугах можно будет применять к видам удостоверительных услуг, которые появятся в будущем.

55. Ссылка на «методы создания и управления» позволяет пояснить, что понятие «удостоверительная услуга» относится к предоставляемым услугам, а не к результату использования этих услуг. Удостоверительная услуга — это, например, не сама электронная подпись (т. е. данные, идентифицирующие подписавшее лицо и указывающие на его намерения в отношении информации, содержащейся в основном сообщении данных), а скорее услуга, поддерживающая электронную подпись (т. е. услуга, предоставляющая подписавшему лицу методы создания электронной подписи и гарантию выполнения требуемых от электронной подписи функций).

Ссылки

[A/CN.9/965](#), пп. 101–106; [A/CN.9/971](#), пп. 110–111; [A/CN.9/1005](#), пп. 14–18; [A/CN.9/1051](#), пп. 35–40.

«Поставщик удостоверительных услуг»

56. Поставщик удостоверительных услуг — это физическое или юридическое лицо, предоставляющее удостоверительные услуги. Например, поставщиком удостоверительных услуг в отношении электронных подписей в контексте ТЗЭТ

является поставщик сертификационных услуг. В отличие от положений о поставщиках услуг УИД (статья 6), в [проекте документа] не определены функции, которые надлежит выполнять поставщикам удостоверительных услуг.

57. В [проекте документа] не требуется участия третьей стороны, предоставляющей удостоверительные услуги, в качестве условия для юридического признания. Если третья сторона, предоставляющая удостоверительные услуги, не задействуется, то одна и та же организация может выполнять как роль поставщика удостоверительных услуг, так и роль абонента.

Ссылки

[будет дополнено]

2. Статья 2. Сфера применения

58. Статья 2 ограничивает сферу применения [проекта документа] использованием и трансграничным признанием систем УИД и удостоверительных услуг в контексте коммерческой деятельности и услуг, связанных с торговлей. Термин «услуги, связанные с торговлей» призван охватить операции, тесно связанные с торговлей, но не являющиеся коммерческими по своему характеру. В таких операциях могут участвовать государственные учреждения, например таможенные органы, работающие по принципу «единого окна» для оформления импортируемых и экспортируемых товаров.

59. Поскольку использование системы УИД и удостоверительных услуг влечет за собой последствия, выходящие за рамки коммерческих сделок, принимающие [проект документа] юрисдикционные системы могут расширить [его] сферу применения, включив в нее все виды сделок.

60. В соответствии с общим принципом, лежащим в основе текстов ЮНСИТРАЛ об электронной торговле и заключающимся в том, чтобы не вносить в действующие материально-правовые нормы изменения или свести такие изменения к минимуму, в пункте 2(а) разъясняется, что [в проекте документа] не устанавливается никаких новых обязанностей по идентификации.

61. В пункте 2(b) и (с), в котором говорится о том, что [проект документа] не требует использования какой-либо конкретной услуги УИД или удостоверительной услуги, осуществляются принципы технологической нейтральности, в том числе в отношении нейтральности моделей и систем.

62. В пункте 3 сохранены правовые требования, которые обязывают использовать определенную процедуру идентификации или конкретную удостоверительную услугу. Такие обычно нормативные требования предусматривают, например, предъявление конкретного удостоверения личности (например, паспорта) или удостоверения личности, имеющего определенные характеристики, соотносящиеся с соответствующими атрибутами (например, удостоверение личности с фотографией и датой рождения владельца). Требования в отношении идентификации могут также предполагать осуществление идентификации тем или иным определенным лицом с конкретными функциями. Если допускается электронная идентификация, то соответствующие регулирующие органы часто требуют использования определенной процедуры УИД или удостоверительной услуги, например, идентификационных учетных данных, выданных тем или иным государственным ведомством.

63. [Проект документа], благодаря своему характеру документа, создающего благоприятные условия, как и существующие типовые законы ЮНСИТРАЛ, не влияет на применение к УИД и удостоверительным услугам другого законодательства, которое может регулировать предусматриваемую ими деятельность или некоторые существенные аспекты операций, осуществляемых с использованием идентификационных и удостоверительных услуг. Положения пункта 4 уточняют этот принцип в отношении закона о конфиденциальности и защите данных, о

котором конкретно упоминается ввиду его значимости. Это положение не относится к вопросам конфиденциальности в другом контексте.

Ссылки

[A/74/17](#), п. 172; [A/CN.9/936](#), п. 52; [A/CN.9/965](#), п. 125; [A/CN.9/971](#), п. 23; [A/CN.9/1005](#), п. 115; [A/CN.9/1045](#), пп. 76–78.

3. Статья 3. Добровольное использование услуг УИД и удостоверительных услуг

64. В статье 3 указывается, что [проект документа] не навязывает использование УИД или удостоверительных услуг лицу, которое не соглашалось на их использование. Между тем вывод о таком согласии может быть сделан на основании поведения стороны, например, если она выбирает для использования в целях электронной торговли конкретное программное обеспечение или систему электронных сообщений, которые функционируют при поддержке УИД и удостоверительных услуг.

65. Принцип добровольного использования УИД и удостоверительных услуг связан с принципом автономии сторон, поскольку оба эти принципа основаны на волеизъявлении. Согласие на использование УИД и удостоверительных услуг может не совпадать с согласием на обработку личной информации в соответствии с законодательством о конфиденциальности и защите данных.

66. Статья 3, основанная на статье 8(2) КЭС, препятствует установлению каких-либо новых обязанностей по использованию УИД и удостоверительных услуг для абонента, поставщика услуг и полагающейся стороны. Это согласуется с общим правилом, согласно которому внесение изменений в материально-правовые нормы не предполагается.

67. Обязанность использовать УИД и удостоверительные услуги может быть предусмотрена другими законами. Такая обязанность может быть установлена для сделок с публичными учреждениями или сделок, связанных с соблюдением обязательств, установленных регулируемыми органами.

Ссылки

[A/CN.9/965](#), пп. 22 и 110; [A/CN.9/1005](#), п. 116; [A/CN.9/1045](#), п. 79.

4. Статья 4. Толкование

68. Статья 4 основана на положениях, содержащихся в ранее разработанных ЮНСИТРАЛ международных договорах и типовых законах, в том числе об электронной торговле (ст. 3 ТЗЭТ; ст. 4 ТЗЭП; ст. 5 КЭС; ст. 3 ТЗЭПЗ).

69. Пункт 1 призван содействовать единообразному толкованию во всех принимающих [проект документа] юрисдикционных системах. Для этого в нем обращается внимание судей и других органов, выносящих решения, на то, что внутренние законодательные акты, вводящие в действие положения [проекта документа], следует толковать с учетом их международного происхождения и необходимости единообразного применения. Поэтому лицам, выносящим решения, рекомендуется при рассмотрении дел учитывать решения, вынесенные в иностранных юрисдикционных системах, с тем чтобы способствовать упрочению транснациональных тенденций к единообразному толкованию.

70. Пункт 2 призван обеспечивать единообразие в толковании и применении законодательных актов, принимаемых на основе [проекта документа], и с этой целью в нем требуется решать все вопросы, которые напрямую в нем не разрешены, не в соответствии с принципами внутреннего права, а в соответствии с общими принципами, лежащими в основе [проекта документа].

71. Как и в других законодательных текстах ЮНСИТРАЛ об электронной торговле, в [проекте документа] напрямую не указываются общие принципы,

лежащие в его основе. Законодательные тексты ЮНСИТРАЛ об электронной торговле основаны, как правило, на принципах недопустимости дискриминации в отношении использования электронных средств, технологической нейтральности, функциональной эквивалентности и автономии сторон, которые также указаны как важные принципы для рассматриваемого [проекта документа] с некоторыми оговорками. Например, автономия сторон является одним из основополагающих принципов коммерческого права, однако он применяется в пределах, установленных императивными нормами права, в том числе положениями [проекта документа], от которых стороны не могут отступать. Кроме того, как отмечено выше (п. 20), принцип функциональной эквивалентности может оказаться неприменимым, если не предусмотрены требования для режима офлайн.

Ссылки

[A/CN.9/936](#), пп. 67 и 72; См. [A/CN.9/1005](#), пп. 117–118; [A/CN.9/1051](#), пп. 53–56.

В. Глава II. Управление идентификационными данными (статьи 5–12)

1. Статья 5. Юридическое признание УИД

72. Статья 5 обеспечивает юридическое признание УИД, поскольку в ней указано, что электронная форма проверки идентификационных данных и электронная идентификация сама по себе не лишает их юридической силы, действительности, исковой силы или приемлемости в качестве доказательств. Таким образом, в пункте 1 применяется общий принцип недискриминации в отношении использования электронных средств в сфере УИД. Этот принцип применяется независимо от существования офлайнового эквивалента.

73. Статья 5 запрещает дискриминацию в отношении электронной идентификации как результата процесса УИД. В ее названии упоминается не «дискриминация», а «юридическое признание», чтобы сохранить единообразие с названием соответствующих положений в существующих текстах ЮНСИТРАЛ.

74. В пункте (b) указано, что тот факт, что услуга УИД не является назначенной услугой, не препятствует ее юридическому признанию. Другими словами, пункт (b) в равной мере обеспечивает юридическое признание назначенных и неназначенных услуг УИД, обеспечивая тем самым нейтральность подхода, выбранного для оценки надежности. Вместе с тем пункт (b) не означает, что для любой услуги УИД используются надежные методы предоставления и, следовательно, она обеспечивает достаточный уровень доверия в контексте электронной идентификации: для достижения такого результата надежность используемого метода должна оцениваться в соответствии со статьями 10 и 11, в зависимости от обстоятельств.

75. Ссылкой на пункт 3 статьи 2 во вступительной части статьи 5 подчеркивается, что статья 5 не затрагивает любое юридическое требование, согласно которому лицо должно быть идентифицировано в соответствии с процедурой, определенной или предписанной законом. Пункт 3 статьи 2 содержит оговорку, применимую не только к статье 5, но и ко всем остальным положениям [проекта документа].

Ссылки

[A/CN.9/965](#), пп. 107–108; [A/CN.9/1005](#), пп. 79–86; [A/CN.9/1045](#), пп. 17 и 82–84.

2. Статья 6. Обязанности поставщиков услуг УИД

76. В статье 6 перечислены основные обязанности поставщиков услуг УИД. Перечисленные обязанности являются основными обязанностями поставщика услуг УИД и могут быть дополнены другими обязанностями, предусмотренными

законодательством или договором. Невыполнение этих обязанностей может привести к привлечению ответственности в соответствии со статьями 12 и отрицательно сказаться на надежности услуги УИД, даже если она является назначенной услугой.

77. Более того, статья 6 призвана обеспечить, чтобы поставщик услуг УИД нес ответственность за полный комплекс услуг УИД, предоставляемых абоненту, даже если некоторые функции могут выполняться другими субъектами, например подрядчиками или отдельными поставщиками услуг УИД в рамках многосторонней системы УИД в частном секторе. Статья 6 не запрещает поставщику услуг УИД передавать какую-либо функцию на подряд или распределять риски среди своих подрядчиков или других деловых партнеров.

78. Системы УИД могут существенно отличаться по своему назначению и устройству, а также по предлагаемым услугам. В свою очередь, устройство системы УИД может также зависеть от выбранной модели. Соответственно, перечисленные в статье 6 обязанности могут относиться не ко всем поставщикам услуг УИД: скорее, обязанности конкретного поставщика услуг УИД будут определяться устройством системы УИД и типом предоставляемых услуг УИД. Эта гибкость подхода к разработке систем УИД отражена в формулировке «соответствующие назначению и устройству».

79. Обязанности изложены в технически нейтральных формулировках, поскольку принцип технологической нейтральности в контексте УИД соблюдается при минимальных требованиях к системе УИД, которые относятся, скорее, к свойствам системы, а не к конкретным технологиям.

80. В деловой практике функции, перечисленные в статье 6, обычно регулируются договорными правилами функционирования, особенно в том случае, если привлекаются поставщики услуг УИД из частного сектора. Как руководство по выполнению операций эти правила разрабатываются на основе их принципов, применяются на практике и отражаются в договорных соглашениях. Существование такой деловой практики признается установленной обязанностью «иметь операционные правила, принципы и практику». Поскольку они имеют важное юридическое и практическое значение, положения пункта (d) требуют обеспечивать доступ к информации об операционных правилах, принципах и практике для абонентов и третьих сторон.

81. Принцип, согласно которому поставщик услуг должен действовать в соответствии со своими заверениями и обязательствами, был закреплен в статье 9(a) ТЗЭП, в которой устанавливается обязанность поставщика сертификационных услуг «действовать в соответствии с заверениями, которые он дает в отношении принципов и практики своей деятельности».

Ссылки

[A/CN.9/936](#), п. 69; [A/CN.9/1045](#), пп. 85–95.

3. Статья 7. Обязанности поставщиков услуг УИД в случае нарушения безопасности данных

82. В статье 7 установлены основные обязанности поставщиков услуг УИД в случае нарушения безопасности данных, которое оказывает серьезное воздействие на систему УИД. Обязанности, предусмотренные статьей 7, должны выполняться независимо от назначения и устройства системы УИД и не могут быть изменены по договору, в том числе в операционных правилах. Нарушения безопасности могут наносить ущерб как системам УИД, так и услугам УИД, а также могут оказывать воздействие на атрибуты, которыми управляет система УИД.

83. Понятие «нарушение безопасности данных» означает нарушение безопасности, приводящее к случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию передаваемых, хранимых или иным образом обрабатываемых данных или получению доступа к ним. Определение

этого понятия может содержаться в законе о конфиденциальности и защите данных.

84. Понятие «серьезное воздействие» используется в региональных⁶ и национальных законах. При оценке воздействия может учитываться целый ряд факторов. Оценить серьезность воздействия помогает использование бланков уведомления о нарушении безопасности, в которых требуется указать продолжительность нарушения, вид данных, безопасность которых была нарушена, процентную долю пострадавших абонентов и другую необходимую информацию. Также можно получить технические инструкции по информированию об инцидентах, а также ежегодные отчеты об инцидентах в сфере безопасности.

85. С учетом того что целесообразными могут быть иные меры, помимо полного приостановления работы, статья 7 требует от поставщика услуг УИД «принять все разумные меры» для устранения и ограничения распространения последствий нарушения безопасности.

86. В пункте 1(с) устанавливается обязанность уведомлять о нарушениях безопасности, которая является одной из составляющих принципа прозрачности. Наличие надлежащего механизма для уведомления о нарушениях безопасности играет важную роль в деле улучшения функциональных характеристик и повышения уровня доверия к УИД и удостоверятельным услугам.

87. Некоторые составляющие обязанностей, предусмотренных в статье 7, такие как идентификация сторон, которые должны быть уведомлены о нарушении, сроки и содержание уведомления, а также раскрытие информации о нарушении и его технических подробностях, могут быть указаны в национальном законодательстве, в договорных соглашениях и в операционных правилах, принципах и практике поставщика услуг УИД.

88. Установленные в статье 7 обязанности могут совпадать с обязанностями, предусмотренными законодательством о конфиденциальности и защите данных. В этом случае все перечисленные действия, а не только уведомление, должны выполняться в соответствии с действующим законом о конфиденциальности и защите данных.

89. Статья 7 применяется одновременно с законом о конфиденциальности и защите данных, а также любым другим законом, применимым к данному событию. Например, уведомления о компрометации данных в некоторых аспектах схожи с уведомлениями о нарушении безопасности, но при этом также существенно от них отличаются.

Ссылки

[A/CN.9/971](#), пп. 84–87; [A/CN.9/1005](#), пп. 32–36 и 94; [A/CN.9/1045](#), пп. 96–101.

4. Статья 8. Обязанности абонентов

90. В статье 8 устанавливаются обязанности абонентов по уведомлению о скомпрометированных идентификационных учетных данных или о наличии риска того, что могли быть скомпрометированы. Эти обязанности дополняют обязанности поставщика услуг УИД по предоставлению средств уведомления о нарушениях безопасности (статья 6(е)) и реагированию на нарушения безопасности или утрату целостности (статья 7).

91. Соответствующая обязанность появляется у абонента в случае компрометации данных, когда были скомпрометированы идентификационные учетные данные или существуют обстоятельства, создающие риск того, что они могли быть скомпрометированы. Тем самым это событие отличается от события, при котором

⁶ Статья 19(2) Регламента (ЕС) № 910/2014 Европейского парламента и Совета от 23 июля 2014 года об электронной идентификации и удостоверятельных услугах в отношении электронных операций на внутреннем рынке, отменяющего Директиву 1999/93/ЕС («Регламент eIDAS»).

у поставщика услуг УИД появляются определенные обязанности в случае компрометации данных, которым является нарушение безопасности или утрата целостности и которое оказывает серьезное воздействие на услугу УИД.

92. О вероятности того, что идентификационные данные могли быть скомпрометированы, говорится для того, чтобы не предъявлять к абонентам необоснованно высокие требования в отношении наличия технических знаний. Обязанность направлять уведомление должна появляться только при обстоятельствах, дающих основание для возникновения обоснованных сомнений в том, что идентификационные учетные данные функционируют надлежащим образом.

93. Договор между абонентом и поставщиком услуг УИД может предусматривать дополнительные обязанности для абонента. Этот договор может также содержать дополнительную информацию о том, как может быть выполнена обязанность по уведомлению, установленная в статье 8.

94. Ссылка на «с помощью любых других разумных средств» указывает на то, что абонент не ограничен в выборе каналов связи использованием тех, которые предоставляет поставщик услуг УИД.

95. Понятие «скомпрометированные идентификационные данные» относится к случаям несанкционированного доступа к идентификационным учетным данным.

96. Пункт (b) призван учесть те случаи, когда абонент не обладает фактической информацией о том, что данные были скомпрометированы, но имеет основания полагать, что это могло произойти. В его основу положена статья 8(1)(b)(ii) ТЗЭП, в которой предусмотрены аналогичные обязанности для подписавшего.

Ссылки

[A/CN.9/936](#), п. 68; [A/CN.9/971](#), пп. 88–96; [A/CN.9/1005](#), пп. 37–43 и 95–96; [A/CN.9/1045](#), пп. 102–105.

5. Статья 9. Идентификация лица с помощью систем УИД

97. В текстах ЮНСИТРАЛ по электронной торговле правилами функциональной эквивалентности устанавливаются требования, которым должны соответствовать электронные записи, методы или процесс, чтобы соответствовать юридическому требованию, действующему в бумажной среде. В статье 9 предусматривается правило функциональной эквивалентности для тех случаев, когда закон требует идентификации или стороны договариваются об идентификации друг друга. Поскольку целью данного положения является установление условий эквивалентности идентификации в онлайн-овом и офлайн-овом режимах, статья 9 применяется только в том случае, если существует эквивалент идентификации в офлайн-овом режиме. Тем не менее статья 9 является одним из основных положений для установления правового режима УИД.

98. В соответствии с установленными принципами в текстах ЮНСИТРАЛ это правило функциональной эквивалентности дополняет правило юридического признания, изложенное в статье 5. При этом статья 5 применяется ко всем формам электронной идентификации, независимо от существования офлайн-ового эквивалента идентификации, тогда как предметом рассмотрения статьи 9 является электронная идентификация как функциональный эквивалент офлайн-овой идентификации, и поэтому статья 9 может применяться только при наличии бумажного эквивалента.

99. В статье говорится об использовании услуг УИД с целью указать, что требования эквивалентности выполняются при использовании идентификационных учетных данных, а не систем УИД или непосредственно идентификационных данных.

100. Статья 9 не затрагивает требований использовать для идентификации конкретный метод или процедуру, как это предусмотрено в статье 2(3). Эти

требования могут быть связаны с соблюдением нормативных положений, например, банковского законодательства и нормативно-правовых актов по борьбе с отмыванием денег (см. п. 62 выше).

101. Электронная идентификация может использоваться для выполнения требования относительно проверки конкретных идентификационных атрибутов лица, таких как возраст или место жительства, как это требуется при физической идентификации. В этой связи, поскольку понятие «идентификационные данные» определяется со ссылкой на «контекст», которым, в свою очередь, определяются необходимые для идентификации атрибуты, успешная идентификация лица на основании статьи 9 включает в себя проверку необходимых атрибутов. Необходимость проверки соответствующих атрибутов отражена также в формулировке «для этой цели». Проверка конкретных атрибутов не рассматривается в положениях о надежности, содержащихся в статье 10, поскольку эти положения касаются процессов управления идентификационными учетными данными, а не атрибутов, содержащихся в идентификационных учетных данных.

102. Статьи 9 и 16–21 [проекта документа] относятся к случаям, когда закон требует совершения того или иного действия или предусматривает последствия за его несовершение. Эта формулировка, используемая в статье 9 КЭС, была разработана с целью учесть правила функциональной эквивалентности в случаях, когда закон не требует, но предусматривает правовые последствия в отношении определенных действий, а также охватывает случаи, когда закон допускает определенные действия (см. статью 9 ТЗЭПЗ).

Ссылки

[A/CN.9/965](#), пп. 62–85; [A/CN.9/971](#), пп. 24–49; [A/CN.9/1005](#), пп. 97–100; [A/CN.9/1045](#), пп. 106–117; [A/CN.9/1051](#), пп. 42–44.

6. Статья 10. Требования к надежности услуг УИД

103. Статья 10 содержит руководящие указания по определению надежности метода, используемого для идентификации в соответствии со статьей 9, после того как этот метод был использован (подход *ex post*).

104. В пункте 1(a) применяется подход *ex post*, поскольку в нем говорится об использовании метода, который является «надежным для цели, для которой используется услуга УИД». В этом положении отражается понимание того, что надежность — понятие относительное. Тем не менее, в отличие от некоторых удостоверительных услуг, которые могут выполнять несколько функций, электронная идентификация имеет только одну функцию, а именно надежную идентификацию с помощью электронных средств. Эта функция может служить различным целям, каждая из которых связана с разным уровнем надежности.

105. Пункт 1(b) содержит положение, призванное не допустить отказа от услуги УИД, если она фактически выполнила свою функцию. От нее отказываются, когда субъект заявляет о невыполненном ею действии. Для того чтобы предусмотренный в пункте 1(b) механизм действовал, метод, независимо от того, надежный он или нет, должен фактически выполнить функцию идентификации, т. е. связать требующее идентификации лицо с идентификационными учетными данными. Это положение основано на статье 9(3)(b)(ii) КЭС.

106. Пункт 2 содержит перечень обстоятельств, изложенных с использованием технически нейтральных терминов, которые могут иметь значение при определении надежности для лица, выносящего решение. Поскольку данный перечень является не исчерпывающим, а примерным, то значение могут иметь также и другие обстоятельства. Более того, не во всех случаях, когда требуется определить надежность, будут иметь значение все перечисленные обстоятельства. В частности, степень значимости соглашения сторон может существенно различаться в зависимости от уровня признания принципа автономии сторон в области идентификации в соответствующей юрисдикционной системе. Кроме того,

договорные соглашения могут не затрагивать третьих сторон, и поэтому данное обстоятельство не будет иметь значения, когда речь будет идти об участии третьих сторон.

107. В пункте 3 указано, что место предоставления услуги УИД и местонахождение коммерческого предприятия поставщика услуг УИД сами по себе не имеют значения для определения надежности. Это положение призвано упростить трансграничное признание услуг УИД и основано на статье 12(1) ТЗЭП, в которой устанавливается общее правило недискриминации при определении юридической силы сертификата или электронной подписи. См. обсуждение взаимодействия между статьями 12(1) и 12(2) ТЗЭП в документе [A/CN.9/483](#), пп. 28–36.

108. В соответствии с пунктом 4 назначение надежной услуги УИД в соответствии со статьей 11 обеспечивает презумпцию надежности методов, используемых для предоставления назначенной услуги УИД. Это единственное различие между назначенными и неназначенными услугами УИД. Более того, согласно пункту 5(b) презумпция надежности, связанная с назначением, может быть опровергнута.

109. В пункте 5 разъясняется взаимосвязь между статьями 10 и 11, а именно уточняется, что наличие механизма назначения не исключает применения механизма *ex post* определения надежности метода. Это положение основано на статье 6(4) ТЗЭП.

а) Система уровней доверия

110. В статьях 10 и 11 используется понятие «уровень доверия» или говорится об аналогичных системах, названных иначе. Уровень доверия служит для полагающихся сторон руководством в отношении того, насколько они могут доверять процессам проверки идентификационных данных и электронной идентификации, а также в отношении того, являются ли они подходящими для конкретных целей. В [проекте документа] уровни доверия не определяются и не содержатся требования, обязывающего их определять или использовать.

111. Система уровней доверия предусматривает различные уровни доверия, которые связаны с разными требованиями. Другими словами, системы уровней доверия представляют собой системы требований, которым должны соответствовать системы и услуги УИД для того, чтобы обеспечивать определенный уровень уверенности в их надежности. Описание уровней доверия должно быть сформулировано с использованием общих терминов в целях сохранения технологической нейтральности.

112. В свою очередь, требование обеспечить определенный уровень доверия к надежности используемых идентификационных данных может быть выражено как ссылка на уровни системы уровней доверия. Затем конкретные системы и услуги УИД могут быть сопоставлены с требованиями необходимого уровня доверия. В случае соответствия услуги УИД требованиям, относящимся к этому уровню доверия, эта услуга УИД может быть использована для соответствующего конкретного вида операции.

б) Сертификация и надзор

113. В статье 10 в числе возможных значимых обстоятельств упоминается «осуществление надзора или проведение сертификации в отношении услуги УИД», если таковые предусматриваются. Сертификация и надзор могут существенно способствовать формированию доверия к поставщикам услуг УИД и их услугам, в том числе для целей определения надежности используемого метода, поскольку они, как представляется, обеспечивают определенный уровень объективности при оценке надежности используемого метода. Это уже отмечалось в статье 12(a)(vi) ТЗЭПЗ и в статье 10(f) ТЗЭП.

114. 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 деловые партнеры должны иметь возможность выбирать наиболее подходящий для своих нужд вариант с учетом того, что каждый вариант будет приводить к различным последствиям.

115. Наличие надзорного механизма для систем и услуг УИД может быть сочтено полезным или даже необходимым для формирования доверия к УИД. Однако при этом создание надзорного органа влечет за собой административные и финансовые последствия, которые могут оказаться затратными. Согласно [проекту документа] создание надзорного режима не требуется и не упрощается.

116. Существуют разные подходы к участию государственных органов в сертификации и надзоре, и выбор того или иного подхода является политическим решением принимающей [проект документа] юрисдикционной системы. Используемый в [проекте документа] подход основан на принципе нейтральности модели, а ссылки на сертификацию и надзор не исключают применение режимов само-сертификации. Когда государственные учреждения одновременно осуществляют сертификацию и надзор и являются поставщиками услуг УИД, сертификационные и надзорные функции могут быть отделены от предоставления услуг УИД.

117. В некоторых случаях, когда используются определенные виды технологии распределенных баз данных, любое решение, предполагающее создание центрального органа по сертификации, аккредитации или надзору, может оказаться неприемлемым из-за проблем, связанных с выявлением органа, который может, в частности, запрашивать сертификацию, проведение оценки и отвечать за принятие корректировочных и принудительных мер.

Ссылки

[A/CN.9/965](#), пп. 40–55 и 112–115; [A/CN.9/971](#), пп. 50–61; [A/CN.9/1005](#), п. 101; [A/CN.9/1045](#), пп. 118–124; [A/CN.9/1051](#), пп. 47–49; [A/CN.9/WG.IV/WP.153](#), пп. 74–75.

7. Статья 11. Назначение надежных систем и [услуг] УИД

118. Статья 11 дополняет статью 10, предлагая возможность назначения систем [и услуг] УИД. Точнее, в ней перечислены условия, которым должна соответствовать система [или услуга] УИД, чтобы ее можно было включить в список назначенных систем [и услуг] УИД.

119. Назначение систем [и услуг] УИД, для оказания которых используются надежные методы, осуществляется с учетом всех соответствующих обстоятельств, включая перечисленные в статье 10 обстоятельства, имеющие значение для определения надежности метода. Ссылка на перечисленные в статье 10 обстоятельства обеспечивает определенную степень согласованности между методами, назначенными надежными *ex ante*, и методами, признанными надежными *ex post*. Кроме того, назначение «должно соответствовать признанным международным стандартам и процедурам, применимым к процессу назначения», чтобы способствовать трансграничному юридическому признанию и операционной совместимости.

120. Информация о назначенных системах [и услугах] УИД имеет важнейшее значение, поскольку потенциальные подписчики должны знать об их существовании. Назначающий орган обязан публиковать перечень назначенных систем [и услуг] УИД, включая сведения о поставщике услуг УИД, например, на своем веб-сайте, или иным образом информировать общественность о назначении. Важность перечней для обеспечения прозрачности назначения услуг УИД, в том числе в трансграничном контексте, признается также в широко используемых технических стандартах.

121. В пункте 2(а) говорится о стандартах и процедурах, имеющих значение для определения надежности, и его цель заключается в обеспечении определенного единообразия результатов оценок надежности, проводившихся по принципу *ex ante* и *ex post*. С другой стороны, в пункте 3 прямо указывается на стандарты и процедуры, связанные с назначением, такие как оценки соответствия и проверки, которые характерны для подхода *ex ante*.

122. Как и в статье 10(3), в пункте 4 указано, что место предоставления системы [или услуги] УИД и местонахождение коммерческого предприятия поставщика услуг УИД сами по себе не имеют значения для назначения надежной услуги. Следовательно пункт 4 также основывается на статье 12(1) ТЗЭП, которой устанавливается общее правило недискриминации при определении юридической силы сертификата или электронной подписи. На практике это положение позволяет иностранному поставщику услуг УИД просить компетентный орган в принимающей [проект документа] юрисдикционной системе о назначении системы [или услуги] УИД, как указано также в статье 25(3).

Ссылки

[A/CN.9/965](#), пп. 40–55; [A/CN.9/971](#), пп. 68–76; см. [A/CN.9/1005](#), пп. 102 и 105; [A/CN.9/1045](#), пп. 125–129.

8. Статья 12. Ответственность поставщиков услуг УИД

123. Режим ответственности может оказать существенное влияние на содействие использованию УИД и удостоверительных услуг и является одним из основных элементов [проекта документа]. В статье 12 устанавливается единый режим ответственности поставщиков услуг УИД перед абонентами, основанный на принципе, согласно которому поставщик услуг УИД должен нести ответственность за последствия непредоставления услуг в соответствии с требованиями закона и договором.

124. Статья 12 основана на трех элементах: а) она не влияет на применение императивных норм права, в том числе на прямые обязанности поставщика услуг УИД, от которых нельзя отказаться в соответствии с [проектом документа]; б) в ней устанавливается ответственность поставщика услуг УИД за нарушение своих прямых обязанностей, независимо от того, имеют ли они договорную основу; и с) в ней признается возможность ограничения ответственности при определенных условиях.

125. Согласно статье 12 эта ответственность установлена законом и, как таковая, отличается от ответственности в соответствии с договорным правом. Цель статьи заключается в том, чтобы признать, что поставщик услуг может нести ответственность за невыполнение своих обязанностей согласно [проекту документа] независимо от того, имеют ли эти обязанности при этом также договорную основу. Это положение применяется независимо от того, является ли поставщик услуг УИД государственным или частным субъектом.

126. Ответственность поставщиков услуг УИД может возникать в связи с использованием как назначенных, так и неназначенных услуг УИД. Однако эта ответственность не является безоговорочной. Например, поставщик услуг УИД может не нести ответственности перед абонентом, если причиной убытков послужило использование скомпрометированных на тот момент учетных данных, о чем абонент знал или должен был знать.

127. Вопросы, касающиеся ответственности и не рассматриваемые в статье 12, оставлены на урегулирование на основе применимого законодательства, не связанного с проектами положений. Эти вопросы касаются, в частности, стандартного принципа осмотрительности и степени вины, бремени доказывания, определения размера ущерба и компенсации и т. д.

128. В статье 12 признается возможность ограничения ответственности при определенных условиях, а именно, если существуют ограничения в отношении

цели или стоимости операции, для которой используется услуга УИД, и если абонент уведомлен об этом ограничении.

129. Ограничения ответственности могут быть необходимы, в том числе, для ограничения размера стоимости страхования. Ограничения ответственности оговариваются в договоре между поставщиком услуг и абонентом. На деле они, как правило, отражаются в операционных правилах, принципах и практике поставщика услуг.

130. Вопрос о том, в какой мере поставщик услуг УИД может ограничить свою ответственность, регулируется применимым законодательством. [Проект документа] не затрагивает применения любого закона, который сужает право поставщика услуг на ограничение ответственности или установление условий для таких ограничений.

131. В пункте 3(b) не преследуется цель установить новую обязанность информировать, но указывается на то, что это положение не отменяет более жесткие требования в отношении уведомлений, предусмотренные применимым законодательством. Этим законодательством будут определяться любые применимые требования в отношении информирования, включая уведомление или явное одобрение.

132. В статье 12 рассматривается только ответственность поставщиков услуг УИД перед абонентами. Если в результате использования услуг УИД убытки понесла третья сторона, то она может добиваться возмещения ущерба в соответствии с действующими правилами ответственности либо от поставщика услуг, либо от абонента. В последнем случае абонент может затем предъявить требование к поставщику услуг УИД.

133. Статья 12 не затрагивает право поставщика услуг на ограничение ответственности перед третьими сторонами в соответствии с другим законодательством. Согласно статье 6(d) поставщик услуг обязан предоставить третьим сторонам свободный доступ к информации о своих операционных правилах, принципах и практике. Вместе с тем [проект документа] не содержит конкретного требования, согласно которому поставщик услуг должен информировать полагающиеся третьи стороны об ограничениях ответственности, поскольку идентифицировать такие третьи стороны заранее, возможно, будет трудно.

134. Статья 12 применяется к поставщикам услуг УИД независимо от того, являются ли они государственными или частными субъектами. В принимающей [проект документа] юрисдикционной системе может потребоваться адаптировать это положение к любому специальному положению об ответственности государственных учреждений. Статья 12 не применяется к государственным учреждениям, выполняющим надзорные функции и ведущим записи актов гражданского состояния и статистики естественного движения населения, которые могут предоставлять исходные идентификационные учетные данные.

Ссылки

[A/CN.9/936](#), пп. 83–86; [A/CN.9/965](#), пп. 116–118; [A/CN.9/971](#), пп. 98–107; [A/CN.9/1005](#), п. 76; [A/CN.9/1045](#), пп. 130–131; [A/CN.9/1051](#), пп. 13–29.

С. Глава III. Удостоверительные услуги (статьи 13–24)

1. Статья 13. Юридическое признание удостоверительных услуг

135. В статье 13 устанавливается общее правило недискриминации в отношении результата использования удостоверительной услуги, а именно утверждения об определенных качествах сообщения данных. Ссылка на результат использования удостоверительной услуги согласуется с подходом, принятым в статье 5,

обеспечивающей юридическое признание электронной идентификации как результата использования УИД.

136. Статья 13 применяется к удостоверительным услугам независимо от того, перечислены ли они в [проекте документа], и действует независимо от наличия правила функциональной эквивалентности.

Ссылки

[A/CN.9/971](#), пп. 112–115; [A/CN.9/1005](#), пп. 19–26; [A/CN.9/1045](#), пп. 16–17.

2. Статья 14. Обязанности поставщиков удостоверительных услуг

137. В статье 14 устанавливаются основные обязанности поставщиков удостоверительных услуг независимо от того, указано ли в документе название удостоверительной услуги или нет. Основные обязанности могут быть уточнены и дополнены в договорных соглашениях, но отступление от них при этом не допускается. Этот подход аналогичен подходу, используемому в статьях 6 и 7 об обязанностях поставщиков услуг УИД.

138. Ссылка на операционные правила, принципы и практику, «соответствующие назначению и устройству удостоверительной услуги», указывает на то, что обязанности поставщиков удостоверительных услуг различаются в зависимости от устройства и функции каждой удостоверительной услуги.

139. Обязанность предоставлять доступ к информации о политике и практике также третьим сторонам отражает существующую практику, свидетельствующую о том, что такая информация имеет значение для полагающихся сторон при рассмотрении вопроса о принятии результата использования удостоверительной услуги в соответствии с принципом добровольного использования удостоверительных услуг (статьи 2(2)(с) и 3(1)).

140. Ограничения в отношении цели или стоимости операции, для которой может использоваться удостоверительная услуга, обычно указываются в операционных правилах, регулирующих предоставление удостоверительной услуги, которые также включают в себя политику и практику поставщика удостоверительных услуг. Поэтому пункт 1(с) нацелен также на выполнение обязанности обеспечения прозрачности по отношению к третьим сторонам в том, что касается применимых договорных ограничений. Аналогичное положение содержится в статье 9(1)(d)(ii) ТЗЭП.

Ссылки

[A/CN.9/971](#), пп. 152–153; [A/CN.9/1005](#), пп. 28–36 и 73; [A/CN.9/1045](#), пп. 18–21, 57.

3. Статья 15. Обязанности абонентов

141. В статье 15 устанавливаются обязанности абонентов в том случае, если удостоверительная услуга была скомпрометирована. В [проекте документа] не указываются дополнительные обязанности абонентов в отношении использования удостоверительной услуги. Пример таких обязанностей можно найти в статье 8(1)(а) и (с) ТЗЭП.

142. В статье 15 устанавливаются обязанности абонентов в случае компрометации удостоверительных услуг, тогда как в статье 14(2) закреплены обязанности поставщиков удостоверительных услуг в случае нарушения безопасности данных. Понятие «скомпрометированная удостоверительная услуга» относится к случаям несанкционированного доступа к удостоверительной услуге. Соответственно, статья 15 предполагает наступление события, подрывающего надежность удостоверительной услуги, а статья 14 предполагает нарушение безопасности или утрату целостности, которые оказывают существенное влияние на удостоверительную услугу.

143. Подробная информация о том, как выполнять обязанности, перечисленные в статье 15, обычно содержится в договоре, заключаемом между поставщиком удостоверительных услуг и абонентом. Такие договорные соглашения обычно отсылают к принципам и практике поставщика удостоверительных услуг.

144. В [проекте документа] не содержится положений об ответственности абонентов. Поэтому ответственность абонента будет определяться договорными положениями, в которых могут быть указаны дополнительные обязанности абонентов, и общими положениями об ответственности.

145. В отличие от некоторых положений, содержащихся в ранее принятых текстах ЮНСИТРАЛ (см. статью 11 ТЗЭП), в статье 15 не устанавливаются обязанности для третьих сторон, которые могут нести ответственность в соответствии с другим законодательством.

Ссылки

[A/CN.9/1005](#), пп. 37–43; [A/CN.9/1045](#), пп. 22–26.

4. Статья 16. Электронные подписи

146. В статье 16 рассматриваются электронные подписи. Все законодательные тексты ЮНСИТРАЛ об электронной торговле содержат положения об использовании электронных подписей, которые могут проставлять как физические, так и юридические лица. В основу статьи 16 положена формулировка статьи 9 ТЗЭПЗ, в которой, в свою очередь, учтена формулировка статьи 9(3) КЭС.

147. Требование наличия подписи на бумажном документе выполняется, если используется метод идентификации подписавшего сообщение данных и указания намерения подписавшего в отношении подписанного сообщения данных. Ссылка на использование метода «в отношении информации, содержащейся в сообщении данных» относится как к идентификации лица, так и к указанию намерения этого лица.

148. Электронные подписи могут использоваться для достижения разных целей, таких как идентификация отправителя сообщения и установление связи с его содержанием. Существует несколько технологий и методов, которые могут удовлетворять требованиям, предъявляемым к электронной подписи. В условиях торговли стороны могут определить наиболее подходящую технологию и метод электронной подписи с учетом затрат, требуемого уровня безопасности, распределения рисков и других соображений. В принятых ранее текстах ЮНСИТРАЛ подробно обсуждались цели и методы электронных подписей (Руководство по принятию ТЗЭП, пп. 29–62; «Содействие укреплению доверия», пп. 24–66).

Ссылки

[A/CN.9/971](#), пп. 116–119; [A/CN.9/1005](#), пп. 44–51; [A/CN.9/1045](#), п. 34; [A/CN.9/1051](#), п. 50.

5. Статья 17. Электронные печати

149. Электронные печати обеспечивают уверенность в происхождении и целостности сообщения данных, исходящего от юридического лица. На практике они сочетают в себе функции общей электронной подписи, подтверждающей происхождение, и определенных видов подписи, для которых, как правило, используются криптографические ключи, гарантирующие целостность данных. Существование таких электронных подписей отражено в статье 6(3)(d) ТЗЭП. Соответственно, статья 6(3)(d) ТЗЭП положена в основу формулировки требования в отношении целостности данных в статье 17.

150. При разработке статьи 17 учитывались положения регионального законодательства, согласно которому «наряду с удостоверением подлинности документа, выданного юридическим лицом, для аутентификации любого цифрового актива

юридического лица, например программного кода или серверов, могут использоваться электронные печати» (Регламент eIDAS, п. 65).

151. Обеспечить уверенность в происхождении сообщения данных можно путем установления его происхождения, для чего, в свою очередь, необходимо идентифицировать юридическое лицо, создавшее сообщение данных. Для идентификации юридического лица, проставляющего печать, используется тот же метод, который используется для идентификации подписавшего лица, а положения ЮНСИТРАЛ об электронных подписях обычно принимаются как применимые как к физическим, так и к юридическим лицам.

152. Более того, содержащиеся в текстах ЮНСИТРАЛ положения требуют обеспечения целостности для достижения функциональной эквивалентности понятию «оригинал» в бумажной среде. Так, статья 6(3)(d) ТЗЭП содержит ссылку на понятие «целостность» для тех случаев, когда целью юридического требования относительно наличия подписи является обеспечение уверенности в целостности информации, к которой она относится.

153. С учетом вышесказанного, вполне возможно, что юрисдикционные системы, в которых уже приняты положения ЮНСИТРАЛ об электронных подписях, обеспечивающих гарантии целостности, могут не проводить различия между функциями, выполняемыми с использованием электронной подписи, и функциями, выполняемыми с использованием электронной печати. Это может объясняться также тем, что в обычной деловой практике используются гибридные методы, сочетающие электронные подписи и электронные печати.

Целостность

154. Целостность является одним из важнейших компонентов электронных печатей и электронного архивирования, тогда как для других удостоверительных услуг она может являться факультативным компонентом. В ранее принятых текстах ЮНСИТРАЛ обеспечение целостности требуется для достижения функциональной эквивалентности понятию «оригинал» в бумажной среде (статья 8 ТЗЭТ). На положениях статьи 8(3) ТЗЭТ основаны требования относительно обеспечения целостности, содержащиеся в статьях 17 и 19.

Ссылки

[A/CN.9/971](#), пп. 124–128; [A/CN.9/1005](#), пп. 52–54 и 58; [A/CN.9/1045](#), пп. 35–36 и 56–58.

6. Статья 18. Электронные отметки времени

155. Электронные отметки времени подтверждают дату и время, когда такая отметка была связана с данными. Как правило, предусматриваемые в законе последствия увязываются с тем фактом, что дата и время наступления определенного события не могут быть доказаны с достаточной степенью уверенности. Например, может потребоваться доказать дату заключения договора для опровержения утверждений третьих сторон.

156. Отметки времени обычно проставляются в связи с определенными действиями, такими как создание электронной записи в ее окончательной форме, подписание, отправление и получение электронного сообщения и т. д. Требование указать часовой пояс может, но не обязательно, выполняться с помощью ссылки на Единое координированное время (UTC).

157. В статье 18 помимо «документов, записей, информации» упоминаются также «данные». Здесь преследуется цель охватить случаи, когда отметки времени связаны с данными, которые не содержатся в документе или записи и которые не представлены в организованном виде как информация.

Ссылки

[A/CN.9/971](#), пп. 129–134; [A/CN.9/1005](#), п. 55.

7. Статья 19. Электронное архивирование

158. В статье 19 рассматриваются услуги электронного архивирования, которые обеспечивают правовую определенность в отношении действительности сохраненных электронных записей. Используемый для предоставления услуги электронного архивирования метод должен гарантировать целостность архивных электронных записей, а также дату и время архивирования. Более того, архивная информация должна быть доступной согласно требованию обеспечения функциональной эквивалентности понятию «письменная форма» в бумажной среде (статья 6(1) ТЗЭТ).

159. При разработке статьи 19 учитывались, в частности, положения статьи 10 ТЗЭТ, посвященной сохранению сообщений данных. Однако в статье 10 ТЗЭТ говорится о «сохранении» сообщений данных в контексте удовлетворения юридического требования хранить документы в бумажном виде, в то время как в статье 19 говорится об «архивировании», поскольку имеется в виду удостоверительная услуга, предоставляемая для удовлетворения этого требования (т. е. электронного архивирования).

160. Архивные сообщения данных необязательно должны быть отправлены или получены, они могут храниться у их составителя.

161. При передаче и хранении сообщений данных по техническим причинам может потребоваться внесение в сообщение данных дополнений и изменений, не нарушающих его целостности. Такие дополнения и изменения допускаются в той мере, в которой содержание сообщения данных остается полным и неизменным. В частности, в пункте (a)(ii) учитываются перенос файлов и изменение формата, которые являются частью обычной практики хранения данных. Его формулировка основана на статье 8(3)(a) ТЗЭТ.

162. В статье 19 не рассматривается вопрос о том, следует ли обеспечивать возможность переноса архивных электронных записей, чтобы несмотря на устаревание технологий предоставить возможность доступа к ним. Такой результат достигается при применении принципа технологической нейтральности и требований обеспечения функциональной эквивалентности понятию «целостность», чтобы при необходимости предъявления информации, эта информация могла быть продемонстрирована лицу, которому она должна быть предъявлена (статья 8(1)(b) ТЗЭТ).

Ссылки

[A/CN.9/971](#), пп. 135–138; [A/CN.9/1005](#), пп. 56–61; [A/CN.9/1045](#), пп. 37–41.

8. Статья 20. Услуги электронной регистрации доставки

163. Статья 20 обеспечивает уверенность в отправке электронного сообщения отправителем и его получении адресатом, времени отправки и получения, целостности данных, которыми обмениваются, и в том, кто является отправителем и кто получателем.

164. Услуги электронной заказной доставки являются эквивалентом услуг заказных почтовых отправлений, поскольку оба вида услуг используются для подтверждения передачи сообщений. Для обеспечения безопасности и конфиденциальности обменов электронными сообщениями получатель должен быть идентифицирован прежде, чем ему будет предоставлен доступ к электронному сообщению.

165. В статье 20 не упоминаются понятия, используемые в принятых ранее текстах ЮНСИТРАЛ, такие как «отправка» и «получение» (см. статью 10 КЭС), поскольку при ее разработке основное внимание уделялось функциональной

эквивалентности услуг заказных почтовых отправлений и электронной регистрации доставки, а не лежащим в их основе понятиям.

Ссылки

[A/CN.9/971](#), пп. 139–141; [A/CN.9/1005](#), пп. 62–64; [A/CN.9/1045](#), пп. 42–44.

9. Статья 21. Аутентификация веб-сайта

166. В статье 21 рассматривается аутентификация веб-сайта, основная функция которой заключается в установлении связи между веб-сайтом и лицом, которому было передано право или выдана лицензия на использование доменного имени, с целью подтвердить надежность веб-сайта. Таким образом, аутентификация веб-сайта включает в себя два элемента: идентификацию держателя доменного имени веб-сайта и установление связи между этим лицом и веб-сайтом. Идентификация веб-сайта не является целью аутентификации веб-сайта.

167. Статья 21 не является правилом функциональной эквивалентности, поскольку веб-сайт существует только в электронной форме и, следовательно, аутентификация веб-сайта не имеет офлайн-эквивалента.

168. Термин «держатель доменного имени» используется для обозначения лиц, которым регистратор доменных имен передал право или выдал лицензию на использование доменного имени. Это лицо необязательно должно быть «владельцем» сайта, поставщиком информации или оператором.

169. Дополнительные гарантии могут потребоваться в случаях, когда доменное имя используется для платформы, на которой размещаются веб-страницы, созданные и управляемые разными лицами. Например, оператору платформы, возможно, будет необходимо идентифицировать лиц в соответствии с определенной процедурой с целью не нарушить аутентификацию веб-сайта.

Ссылки

[A/CN.9/971](#), пп. 142–144; [A/CN.9/1005](#), пп. 65–66; [A/CN.9/1045](#), пп. 47–48.

10. Статья 22. Требования к надежности удостоверительных услуг

170. В статье 22 содержится исчерпывающий перечень обстоятельств, которые могут иметь значение при определении надежности использованного метода на основе подхода *ex post*. Этот перечень составлен на основе перечней, содержащихся в статье 10 ТЗЭП и в статье 12 ТЗЭПЗ.

171. Подобно понятию надежного метода, используемого для услуг УИД (см. пункт 104 выше), понятие надежного метода, используемого для предоставления удостоверительных услуг, является относительным и зависит от преследуемой цели. Относительность понятия надежности отражена в пункте 1(а), а именно в формулировке «надежным для цели», которая, согласно устоявшемуся обычаю ЮНСИТРАЛ, призвана точнее указать на различные цели использования удостоверительных услуг, а также в указании на «цель, для которой используется удостоверительная услуга».

Уровни надежности

172. В ТЗЭП и ряде национальных законов об электронных подписях проводится различие между удостоверительными услугами исходя из степени надежности, которую они обеспечивают. Такие законы, в частности, придают большую юридическую силу электронным подписям, удовлетворяющим определенным требованиям, и, следовательно, они считаются обеспечивающими более высокую степень надежности. Более того, некоторые законы могут требовать назначения только тех электронных подписей, которые обеспечивают более высокий уровень надежности. Этот подход в [проекте документа] не используется, и

удостоверительные услуги могут быть назначены независимо от того, какой уровень надежности они обеспечивают.

173. Поскольку идентификационные данные, обеспечивающие высокий уровень надежности, могут использоваться для целей удостоверительных услуг, обеспечивающих разные уровни надежности, прямой зависимости между уровнем доверия к услуге УИД и уровнем надежности удостоверительной услуги не существует.

Ссылки

[A/CN.9/965](#), п. 106; [A/CN.9/971](#), пп. 120–121; [A/CN.9/1005](#), пп. 67–68 и 73; [A/CN.9/1045](#), пп. 18–21, 27–29, 52–57, 61; [A/CN.9/1051](#), пп. 45–46.

11. Статья 23. Назначение надежных удостоверительных услуг

174. Статья 23 дополняет статью 22, позволяя назначать удостоверительные услуги на основе подхода *ex ante*. Точнее, в ней перечислены условия, которым должна удовлетворять услуга УИД, чтобы ее можно было включить в список назначенных услуг УИД, считающихся надежными для целей статей 16–21.

175. В статье 23 речь идет главным образом о назначении удостоверительных услуг при том понимании, что процесс назначения удостоверительных услуг неизбежно сопряжен с оценкой таких методов. Аналогично назначению услуг УИД, когда речь идет о назначении удостоверительных услуг, в отношении которых считается, что для их предоставления используются надежные методы, то имеется в виду не общая категория удостоверительных услуг или все удостоверительные услуги, предлагаемые тем или иным поставщиком, а конкретная удостоверительная услуга, предоставляемая идентифицированным поставщиком услуг.

176. Поскольку единственным юридическим последствием назначения является презумпция надежности используемого метода, использование удостоверительных услуг, которые были назначены, но назначение было аннулировано, не позволяет заинтересованной стороне руководствоваться этой презумпцией, но при этом не влияет на определение надежности метода.

177. Согласно статье 23 назначающий орган обязан публиковать список назначенных удостоверительных услуг, включая подробную информацию о поставщиках удостоверительных услуг. Цель этой обязанности заключается в содействии обеспечению прозрачности и информировании потенциальных абонентов о соответствующей удостоверительной услуге. Принимающие [проект положений] юрисдикционные системы, возможно, пожелают рассмотреть способы агрегирования этих списков, чтобы содержащаяся в них информация могла быть найдена в централизованном наднациональном хранилище наподобие тех, которые существуют на региональном уровне.

Ссылки

[A/CN.9/971](#), пп. 150–152; [A/CN.9/1005](#), пп. 69–73; [A/CN.9/1045](#), пп. 30–33, 58–61.

12. Статья 24. Ответственность поставщиков удостоверительных услуг

178. В качестве общего принципа поставщики удостоверительных услуг должны нести ответственность за последствия непредоставления услуг в соответствии с соглашением или согласно требованиям законодательства. Степень такой ответственности будет определяться с учетом нескольких факторов и в том числе вида предоставляемой удостоверительной услуги. Что касается других положений [проекта документа], то статья 24 не затрагивает ответственность за несоблюдение обязанностей, возникающих из правовых норм, не связанных с [проектом документа].

179. В некоторых случаях идентификация поставщика удостоверительных услуг может быть затруднена или невозможна (например, в случае услуг по проставлению отметки времени, используемых в сочетании с технологией распределенного реестра), и, следовательно, может оказаться так, что будет невозможно определить, кто несет ответственность. В таких случаях система может предусматривать другие способы для формирования доверия к использованию удостоверительных услуг.

180. Если обратиться к ранее принятым текстам ЮНСИТРАЛ, то ТЗЭП содержит положения о юридических последствиях поведения подписавшей стороны (ст. 8), поставщика сертификационных услуг (ст. 9) и полагающейся стороны (ст. 11). Этими положениями устанавливаются обязанности каждого субъекта, участвующего в жизненном цикле электронной подписи. Кроме того, в ТЗЭП признается возможность ограничения поставщиками сертификационных услуг объема или степени их ответственности.

Ссылки

[A/CN.9/1005](#), пп. 74–76; [A/CN.9/1045](#), пп. 62–66.

D. Глава V. Международные аспекты (статьи 25 и 26)

1. Статья 25. Трансграничное юридическое признание

181. В статье 25 устанавливается система трансграничного юридического признания УИД и удостоверительных услуг, основанная на предоставлении одинакового правового режима местным и иностранным системам УИД, идентификационным учетным данным, услугам УИД и удостоверительным услугам. В ее основе лежит принцип недискриминации по географическому признаку.

182. Одна из целей статьи 25 заключается в частичном снятии необходимости подачи поставщиками услуг заявок на получение статуса назначенных в нескольких юрисдикционных системах в соответствии со статьей 23. Это может быть особенно полезным в тех юрисдикционных системах, которые руководствуются национальными техническими стандартами, которые, как таковые, могут не совпадать с иностранными техническими стандартами. Осуществлению этого положения могло бы во многом способствовать взаимное признание сертификации, где это возможно.

183. Ссылка на «уровень надежности» в статье 25 охватывает как понятие уровня доверия, являющееся профессиональным термином, используемым для оценки услуг УИД, так и понятие уровня надежности, являющееся профессиональным термином, используемым для оценки удостоверительных услуг. В свою очередь, эти понятия могут иметь значение для определения надежности той или иной услуги или для назначения надежной услуги в соответствии с положениями глав II и III.

184. Из-за трудностей согласования определений на международном уровне в [проекте документа] не устанавливается общая система уровней доверия для систем УИД и уровней надежности для удостоверительных услуг. Более того, в разных юрисдикционных системах существуют разные законы и деловая практика в отношении выработки этих определений, в частности, в том, что касается роли центральных органов власти по сравнению с ролью договорных соглашений.

185. С другой стороны, определение уровня доверия в отношении той или иной услуги УИД и уровня надежности удостоверительной услуги отнимает много времени и ресурсов, и не все юрисдикционные системы могут располагать достаточными ресурсами. Поэтому возможность признания иностранных услуг УИД и удостоверительных услуг исходя из иностранных определений и информации о назначении могла бы иметь особое значение для таких юрисдикционных систем.

186. Ссылка на «систему УИД, услугу УИД или идентификационные учетные данные, в зависимости от обстоятельств» призвана охватить все возможные аспекты, имеющие значение для трансграничного признания. На практике, возможно, будет сочтено предпочтительным сосредоточивать внимание на каждой конкретной услуге УИД, чтобы избежать признания всех услуг УИД, поддерживаемых системой УИД, одинаково надежными, даже если одна или несколько из них могут обеспечивать более низкий уровень надежности. Кроме того, признание идентификационных учетных данных не должно распространяться на учетные данные в системе УИД, которые хотя и остались неизменными, но были выданы с помощью услуги УИД, которая была скомпрометирована.

187. Для признания иностранных систем УИД и удостоверительных услуг поставщику услуг может потребоваться изменить свои условия предоставления услуг. Например, применимое законодательство в признающей юрисдикционной системе может сузить право поставщика услуг на ограничение ответственности.

188. В пункте 1 представлены два альтернативных варианта положения об эквивалентности требуемого уровня надежности. Первый вариант требует по меньшей мере такого же уровня надежности; второй — по существу эквивалентный уровень надежности. Формулировка «по меньшей мере эквивалентный уровень надежности» охватывает также более высокие, чем требуемый, уровни надежности.

189. Понятие «по существу эквивалентный уровень надежности» призвано охватить случаи, когда определения уровня надежности в разных юрисдикционных системах в точности не совпадают, и такие случаи будут, скорее всего, возникать, поскольку общепринятых определений конкретных уровней надежности не существует. Еще одна проблема, которая может быть решена с помощью этого понятия, связана с возможными препятствиями в торговле, возникающими вследствие необходимости соблюдать строгие технические требования.

190. Если системы, услуги или учетные данные обеспечивают по существу эквивалентный уровень надежности, их надежность, определяемая с учетом обстоятельств, указанных в статьях 10 и 22, будет также эквивалентной. «По существу эквивалентный уровень надежности» включает в себя уровни надежности выше требуемого. Понятие «по существу эквивалентный уровень надежности» взято из статьи 12(2) ТЗЭП.

191. В пункте 3 дополнительно разъясняется, каким образом назначающие органы могут назначать иностранные системы УИД и удостоверительные услуги. В нем более подробно рассматриваются механизмы, предусмотренные в статьях 11(4) и 23(4), которые призваны не допустить дискриминацию по географическому признаку в процессе назначения, путем предоставления назначающему органу принимающей [проект документа] юрисдикционной системы возможности полагаться на назначенные иностранным назначающим органом систему УИД и удостоверительные услуги.

192. При принятии нормативных актов для обеспечения применения [проекта документа] принимающая юрисдикционная система может решить, будет ли пункт 3 обеспечивать автоматическое признание (например, услуги УИД и удостоверительные услуги, назначенные иностранным органом, автоматически получают такой же правовой статус, который они получили бы как назначенные в принимающей юрисдикционной системе) или же он будет действовать как презумпция (например, услуги УИД и удостоверительные услуги, назначенные иностранным органом, будут считаться надежными в принимающей юрисдикционной системе, но не будут иметь правового статуса, который они имели бы как назначенные в этой юрисдикционной системе, без дальнейших действий со стороны назначающего органа).

193. Механизмы, основанные на статье 25(3), могут заменить механизмы, основанные на заключении специальных соглашений о взаимном признании между надзорными органами.

Ссылки

[A/CN.9/936](#), пп. 75–77; [A/CN.9/1005](#), п. 120; [A/CN.9/1045](#), пп. 67–74; [A/CN.9/1051](#), пп. 57–66.

2. Статья 26. Сотрудничество

194. Достижению взаимного юридического признания и технической совместимости систем УИД и удостоверительных услуг могут в значительной мере способствовать механизмы институционального сотрудничества. Такие механизмы существуют в различных формах и могут иметь частный или публичный характер. Сотрудничество может включать в себя обмен информацией, опытом и успешными видами практики, в частности, в отношении технических требований, включая уровни доверия и уровни надежности.

195. Более того, статья 26 может способствовать выработке общих определений технических стандартов, включая уровни доверия и уровни надежности, которые поддерживают определение эквивалентности.

Ссылки

[A/CN.9/965](#), пп. 119–120; [A/CN.9/1005](#), п. 122; [A/CN.9/1045](#), п. 75; [A/CN.9/WG.IV/WP.153](#), пп. 95–98.
