



Генеральная Ассамблея

Distr.: General
21 February 2022
Russian
Original: English

Комиссия Организации Объединенных Наций

по праву международной торговли

Пятьдесят пятая сессия

Нью-Йорк, 27 июня — 15 июля 2022 года

Проект типового закона об использовании и трансграничном признании управления идентификационными данными и удостоверительных услуг

Записка Секретариата

1. На своей шестьдесят второй сессии (Вена, 22–26 ноября 2021 года) Рабочая группа IV (Электронная торговля) завершила рассмотрение в третьем чтении проекта положений об использовании и трансграничном признании управления идентификационными данными и удостоверительных услуг и пояснительной записки к ним.
2. На этой сессии Рабочая группа просила секретариат пересмотреть проект положений и пояснительную записку и учесть в нем состоявшееся обсуждение и принятые решения и представить пересмотренный текст в форме типового закона Комиссии для рассмотрения на ее пятьдесят пятой сессии в 2022 году. Секретариату также было поручено препроводить пересмотренный текст всем правительствам и соответствующим международным организациям для того, чтобы они могли представить свои замечания и подготовить затем подборку полученных замечаний для рассмотрения Комиссией ([A/CN.9/1087](#), п. 11).
3. Пересмотренный проект типового закона изложен в Приложении I к настоящему документу, а пересмотренная пояснительная записка — в Приложении II к настоящему документу. В пересмотренных текстах учтены результаты обсуждений Рабочей группы на ее шестьдесят второй сессии, которые изложены в документе [A/CN.9/1087](#).



Приложение I

Проект типового закона об использовании и трансграничном признании управления идентификационными данными и удостоверительных услуг

Глава I. Общие положения

Статья 1. Определения

Для целей настоящего Закона:

- a) «атрибут» означает единицу информации или данных, связанную с лицом;
- b) «сообщение данных» означает информацию, подготовленную, отправленную, полученную или хранимую с помощью электронных, магнитных, оптических или аналогичных средств;
- c) «электронная идентификация» [«аутентификация»] в контексте услуг по управлению идентификационными данными означает процесс, используемый для достижения достаточной уверенности в наличии связи между лицом и идентификационными данными;
- d) «идентификационные данные» означают определенный набор атрибутов, который позволяет уникальным образом отличить лицо в определенном контексте;
- e) «идентификационные учетные данные» означают данные или физический объект, на котором могут находиться данные, которые лицо может представить для электронной идентификации;
- f) «услуги по управлению идентификационными данными» означают услуги, состоящие в управлении проверкой идентификационных данных или электронной идентификацией лиц;
- g) «поставщик услуг по управлению идентификационными данными» означает лицо, которое заключает с абонентом соглашение о предоставлении услуг по управлению идентификационными данными;
- h) «система управления идентификационными данными» означает набор функций и возможностей для управления проверкой идентификационных данных и электронной идентификацией лиц;
- i) «проверка идентификационных данных» означает процесс сбора, проверки и установления действительности атрибутов, достаточных для определения и подтверждения идентификационных данных лица в определенном контексте;
- j) «полагающаяся сторона» означает лицо, которое действует на основании результатов услуг по управлению идентификационными данными или удостоверительных услуг;
- k) «абонент» означает лицо, которое заключает соглашение о предоставлении услуг по управлению идентификационными данными или удостоверительных услуг с поставщиком услуг УИД или поставщиком удостоверительных услуг;
- l) «удостоверительная услуга» означает электронную услугу, которая обеспечивает уверенность в определенных качествах сообщения данных и включает методы создания электронных подписей, электронных печатей, электронных отметок времени, аутентификации веб-сайта, электронного архивирования и электронной регистрации доставки и управления ими;

m) «поставщик удостоверительных услуг» означает лицо, которое заключает с абонентом соглашение о предоставлении одной или нескольких удостоверительных услуг.

Статья 2. Сфера применения

1. Настоящий Закон применяется к использованию и трансграничному признанию услуг по управлению идентификационными данными и удостоверительных услуг в контексте коммерческой деятельности и услуг, связанных с торговлей.
2. Ничто в настоящем Законе не требует идентифицировать лицо.
3. Ничто в настоящем Законе не затрагивает юридическое требование идентифицировать лицо или использовать ту или иную удостоверительную услугу в соответствии с какой-либо определенной или предписанной законом процедурой.
4. За исключением случаев, предусмотренных в настоящем Законе, ничто в настоящем Законе не влияет на применение к услугам по управлению идентификационными данными или удостоверительным услугам любых законодательных норм, применимых в отношении защиты и конфиденциальности данных.

Статья 3. Добровольное использование услуг по управлению идентификационными данными и удостоверительных услуг

1. Ничто в настоящем Законе не требует от какого-либо лица использовать услугу по управлению идентификационными данными или удостоверительную услугу или использовать какую-либо определенную услугу УИД или удостоверительную услугу без согласия этого лица.
2. Для целей пункта 1 вывод о согласии может быть сделан на основании поведения лица.

Статья 4. Толкование

1. При толковании настоящего Закона надлежит учитывать его международное происхождение и необходимость содействовать достижению единообразия в его применении, а также соблюдению добросовестности в международной торговле.
2. Вопросы, относящиеся к предмету регулирования настоящего Закона, которые прямо в нем не разрешены, подлежат разрешению в соответствии с общими принципами, на которых он основан.

Глава II. Управление идентификационными данными

Статья 5. Юридическое признание управления идентификационными данными

С учетом пункта 3 статьи 2 электронная идентификация не может быть лишена юридической силы, действительности, исковой силы или приемлемости в качестве доказательства лишь на том основании, что:

- a) проверка идентификационных данных и электронная идентификация осуществляются в электронной форме либо
- b) система управления идентификационными данными не является назначенной системой согласно статье 11.

*Статья 6. Обязанности поставщиков услуг
по управлению идентификационными данными*

Поставщик услуг по управлению идентификационными данными, как минимум:

- a) имеет операционные правила, принципы и практику, соответствующие назначению и устройству системы управления идентификационными данными, для выполнения как минимум следующих требований:
 - i) подключения лиц к системе, в том числе путем:
 - a. регистрации и сбора атрибутов;
 - b. проверки и верификации идентификационных данных; и
 - c. присвоения идентификационных учетных данных лицу;
 - ii) обновления атрибутов;
 - iii) управления идентификационными учетными данными, в том числе путем:
 - a. выдачи, доставки и активации учетных данных;
 - b. приостановления действия, отзыва и реактивации учетных данных; и
 - c. обновления и замены учетных данных;
 - iv) управления электронной идентификацией лиц, в том числе путем:
 - a. управления факторами электронной идентификации и
 - b. управления механизмами электронной идентификации;
- b) осуществляет деятельность в соответствии с операционными правилами, принципами и практикой и любыми заявлениями, сделанными им в их отношении;
- c) обеспечивает доступность в онлайн-режиме и исправную работу системы управления идентификационными данными;
- d) предоставляет абонентам и третьим сторонам свободный доступ к информации об операционных правилах, принципах и практике;
- e) предоставляет легко доступные средства, позволяющие полагающейся стороне в надлежащих случаях удостовериться в существовании:
 - i) любых ограничений в отношении целей или стоимостного объема операций, для которых может использоваться услуга по управлению идентификационными данными; и
 - ii) любых ограничений в отношении масштаба или объема ответственности, установленных поставщиком услуг по управлению идентификационными данными; и
- f) предоставляет средства, с помощью которых абонент может уведомить поставщика услуг по управлению идентификационными данными о нарушении безопасности в соответствии со статьей 8, и обеспечивает публичную доступность этих средств.

*Статья 7. Обязанности поставщиков услуг по управлению
идентификационными данными в случае нарушения безопасности данных*

1. В случае нарушения безопасности или целостности данных, которое оказывает серьезное воздействие на систему управления идентификационными данными, включая используемые в ней атрибуты, поставщик услуг по управлению идентификационными данными в соответствии с законодательством:

a) принимает все разумные меры для ограничения последствий такого нарушения безопасности или целостности, в том числе, если это уместно, приостанавливает предоставление затронутой услуги или лишает действительности затронутые идентификационные учетные данные;

b) устраняет такое нарушение безопасности или целостности; и

c) уведомляет о таком нарушении безопасности или целостности.

2. Если поставщик услуг по управлению идентификационными данными получает уведомление о нарушении безопасности или целостности от какого-либо лица, поставщик услуг по управлению идентификационными данными:

a) проводит проверку возможного нарушения безопасности или целостности; и

b) принимает любые другие надлежащие меры в соответствии с пунктом 1.

Статья 8. Обязанности абонентов

Абонент направляет уведомление поставщику услуг по управлению идентификационными данными с помощью средств, предоставленных в его распоряжение поставщиком услуг по управлению идентификационными данными согласно статье 6, либо с помощью любых других разумных средств, если:

a) абоненту известно, что его идентификационные учетные данные были скомпрометированы, либо

b) абоненту известно об обстоятельствах, создающих значительный риск того, что его идентификационные учетные данные могли быть скомпрометированы.

Статья 9. Идентификация лица с помощью систем управления идентификационными данными

С учетом пункта 3 статьи 2, в тех случаях, когда закон требует идентифицировать лицо для конкретной цели или предусматривает последствия за отсутствие идентификации, в контексте услуг по управлению идентификационными данными это требование выполняется, если с этой целью для электронной идентификации лица используется какой-либо метод.

Статья 10. Требования к надежности услуг по управлению идентификационными данными

1. Для целей статьи 9 упомянутый в ней метод:

a) должен быть надежным для цели, для которой используется услуга по управлению данными; или

b) должен быть проверенным на практике в части способности выполнять функцию, о которой говорится в статье 9.

2. При определении надежности метода учитываются все соответствующие обстоятельства, которые могут включать:

a) выполнение поставщиком услуг по управлению идентификационными данными обязанностей, перечисленных в статье 6;

b) соответствие операционных правил, принципов и практики поставщика услуг по управлению идентификационными данными, в частности правил, регулирующих нижеперечисленные аспекты, любым применимым признанным международным стандартам и процедурам, имеющим отношение к предоставлению услуг по управлению идентификационными данными, включая системы уровней доверия:

- i) управление;
 - ii) опубликование уведомлений и информации для пользователей;
 - iii) управление информационной безопасностью;
 - iv) ведение учета;
 - v) материальную базу и персонал;
 - vi) технический контроль;
 - vii) надзор и ревизию;
 - c) любой общий контроль или сертификацию в отношении услуги по управлению идентификационными данными;
 - d) любой надлежащий уровень надежности используемого метода;
 - e) цель, для которой используется идентификация;
 - f) любую соответствующую договоренность между сторонами, включая любое ограничение целей или стоимостного объема операций, для которых может использоваться услуга по управлению идентификационными данными.
3. При определении надежности метода не учитываются:
- a) географическое место предоставления услуги по управлению идентификационными данными;
 - b) географическое местонахождение коммерческого предприятия поставщика услуг по управлению идентификационными данными.
4. Метод, используемый для предоставления услуги по управлению идентификационными данными, назначенной в соответствии со статьей 11, считается надежным.
5. Пункт 4 не ограничивает возможности любого лица в отношении:
- a) установления надежности какого-либо метода любым другим способом; или
 - b) представления доказательств ненадежности какого-либо метода, используемого для предоставления услуги по управлению идентификационными данными, назначенной в соответствии со статьей 11.

*Статья 11. Назначение надежных услуг
по управлению идентификационными данными*

1. [Лицо, орган или ведомство, будь то публичное или частное, указанное принимающей юрисдикционной системой в качестве компетентного,] может назначить услуги по управлению идентификационными данными, считающиеся надежными.
2. Это [лицо, орган или ведомство, будь то публичное или частное, указанное принимающей юрисдикционной системой в качестве компетентного]:
 - a) принимает во внимание при назначении услуги по управлению идентификационными данными все соответствующие обстоятельства, включая факторы, перечисленные в статье 10, и
 - b) публикует перечень назначенных услуг по управлению идентификационными данными, включая сведения о поставщике услуг по управлению идентификационными данными.
3. Любое решение о назначении, принятое в соответствии с пунктом 1, должно соответствовать признанным международным стандартам и процедурам, применимым к осуществлению процесса назначения, включая системы уровней доверия.

4. При назначении услуги по управлению идентификационными данными не учитываются:

- a) географическое место предоставления услуги по управлению идентификационными данными;
- b) географическое местонахождение коммерческого предприятия поставщика услуг по управлению идентификационными данными.

*Статья 12. Ответственность поставщиков услуг
по управлению идентификационными данными*

1. Поставщик услуг по управлению идентификационными данными несет ответственность за убытки, причиненные абоненту или полагающейся стороне из-за несоблюдения своих обязанностей, предусмотренных статьями 6 и 7.

2. Пункт 1 применяется в соответствии с нормами об ответственности, содержащимися в законодательстве, и без ущерба для:

- a) любого другого основания для возникновения ответственности, предусмотренного законодательством, включая ответственность за невыполнение обязанностей договорного характера;
- b) любых других правовых последствий невыполнения поставщиком услуг по управлению идентификационными данными своих обязанностей, предусмотренных настоящим Законом.

3. Невзирая на положения пункта 1, поставщик услуг по управлению идентификационными данными не несет ответственности перед абонентом за убытки, понесенные в результате использования услуги по управлению идентификационными данными, в том случае, если:

- a) такое использование выходит за рамки ограничений в отношении цели или стоимости операции, для которой используется услуга по управлению идентификационными данными; и
- b) эти ограничения указаны в соглашении между поставщиком услуг по управлению идентификационными данными и абонентом.

4. Невзирая на положения пункта 1, поставщик услуг по управлению идентификационными данными не несет ответственности перед полагающейся стороной за убытки, понесенные в результате использования услуг по управлению идентификационными данными, в том случае, если:

- a) такое использование выходит за рамки ограничений в отношении целей или стоимости операций, для которых может использоваться услуга по управлению идентификационными данными; и
- b) поставщик услуг по управлению идентификационными данными выполнил обязанности, предусмотренные подпунктом (е) статьи 6, в отношении этой операции.

Глава III. Удостоверительные услуги

Статья 13. Юридическое признание удостоверительных услуг

Результаты, связанные с использованием удостоверительной услуги, не могут быть лишены юридической силы, действительности, исковой силы или приемлемости в качестве доказательства лишь на том основании, что:

- a) они представлены в электронной форме; или
- b) удостоверительная услуга не является назначенной согласно статье 23.

Статья 14. Обязанности поставщиков удостоверительных услуг

1. Поставщик удостоверительных услуг, как минимум:
 - a) имеет операционные правила, принципы и практику, включая план обеспечения непрерывности оказания услуг в случае прекращения им своей деятельности, соответствующие назначению и структуре удостоверительной услуги;
 - b) действует в соответствии со своими операционными правилами, принципами и практикой и любыми заверениями, которые он дает в их отношении;
 - c) предоставляет абонентам и третьим сторонам свободный доступ к информации о своих операционных правилах, принципах и практике;
 - d) предоставляет средства, с помощью которых абонент может в соответствии со статьей 15 уведомить поставщика удостоверительных услуг о нарушении безопасности, и обеспечивает их публичную доступность; и
 - e) предоставляет свободно доступные средства, позволяющие полагающейся стороне в надлежащих случаях удостовериться в существовании:
 - i) любых ограничений в отношении целей или стоимостного объема, в связи с которыми может использоваться удостоверительная услуга; и
 - ii) любых ограничений в отношении объема или степени ответственности, установленных поставщиком удостоверительных услуг.
2. В случае нарушения безопасности или целостности данных, которое оказывает серьезное воздействие на предоставление удостоверительной услуги, поставщик удостоверительных услуг в соответствии с законодательством:
 - a) принимает все разумные меры для ограничения последствий такого нарушения безопасности или целостности, в том числе, если это уместно, приостанавливает предоставление соответствующей услуги или отменяет ее;
 - b) устраняет такое нарушение безопасности или целостности; и
 - c) уведомляет о таком нарушении безопасности или целостности.

Статья 15. Обязанности абонентов

Абонент направляет уведомление поставщику удостоверительных услуг с помощью средств, предоставленных поставщиком удостоверительных услуг в соответствии с пунктом 1 статьи 14, или иным способом с помощью разумных средств, если:

- a) абоненту становится известно, что данные или средства, которыми он пользовался для получения доступа к удостоверительной услуге или для того, чтобы ею воспользоваться, были скомпрометированы; или
- b) абоненту известно об обстоятельствах, создающих значительный риск того, что удостоверительная услуга могла быть скомпрометирована.

Статья 16. Электронные подписи

В тех случаях, когда законодательство требует наличия подписи какого-либо лица или предусматривает последствия в случае отсутствия подписи, это требование выполняется в отношении сообщения данных, если используется какой-либо метод:

- a) для идентификации этого лица и
- b) для указания намерения этого лица в отношении информации, содержащейся в сообщении данных.

Статья 17. Электронные печати

В тех случаях, когда законодательство требует от юридического лица предоставления печати или предусматривает последствия в случае отсутствия печати, это требование выполняется в отношении сообщения данных, если используется какой-либо метод:

- a) для обеспечения надежной уверенности в происхождении сообщения данных и
- b) для обнаружения любых изменений, внесенных в сообщение данных после времени и даты проставления печати, за исключением добавления любых индоссаментов и любых изменений, происходящих в обычном процессе передачи, хранения и демонстрации.

Статья 18. Электронные отметки времени

В тех случаях, когда законодательство требует, чтобы те или иные документы, записи, информация или данные были связаны со временем и датой, или предусматривает последствия в случае отсутствия отметки времени и даты, это требование выполняется в отношении электронного сообщения, если используется какой-либо метод:

- a) для указания времени и даты с уточнением часового пояса и
- b) для привязки времени и даты к сообщению данных.

Статья 19. Электронное архивирование

В тех случаях, когда законодательство требует, чтобы те или иные документы, записи или информация были сохранены, или предусматривает последствия в случае, если они не были сохранены, это требование выполняется в отношении сообщения данных, если используется какой-либо метод:

- a) для обеспечения доступности информации, содержащейся в таком сообщении данных, для последующего использования;
- b) для указания времени и даты архивирования и связывания этого времени и даты с сообщением данных;
- c) для сохранения сообщения данных в том формате, в котором оно было создано, отправлено или получено, или в другом формате, который может подходить для обнаружения любых изменений, внесенных в сообщение данных после этого времени и даты, за исключением добавления любых индоссаментов и любых изменений, происходящих в обычном процессе передачи, хранения и демонстрации; и
- d) для сохранения такой информации, если таковая существует, которая позволяет установить происхождение и место назначения сообщения данных, а также время и дату его отправления или получения.

Статья 20. Услуги электронной регистрации доставки

В тех случаях, когда законодательство требует доставки документа, записи или информации с помощью заказного почтового отправления или аналогичной услуги или предусматривает последствия в случае недоставки, это требование выполняется в отношении сообщения данных, если используется какой-либо метод:

- a) для указания времени и даты получения сообщения данных для доставки; и времени и даты доставки сообщения данных;

- б) для обнаружения любых изменений, внесенных в сообщение данных с момента времени и даты получения сообщения данных для доставки до момента времени и даты его доставки, без учета добавления любых индоссаментов или информации, требуемой настоящей статьёй, и любых изменений, происходящих в обычном процессе передачи, хранения и демонстрации; и
- с) для идентификации отправителя и получателя.

Статья 21. Аутентификация веб-сайтов

В тех случаях, когда законодательство требует аутентификации веб-сайта или предусматривает последствия в отсутствие аутентификации веб-сайта, это требование выполняется, если используется какой-либо метод:

- а) для идентификации лица, которое является держателем доменного имени веб-сайта; и
- б) для установления связи этого лица с этим веб-сайтом.

Статья 22. Требования к надежности удостоверительных услуг

1. Для целей статей 16–21 упомянутый в них метод:

- а) должен быть надежным для цели, для которой используется удостоверительная услуга; или
- б) должен быть проверенным на практике в части способности выполнять функции, о которых говорится в соответствующей статье.

2. При определении надежности этого метода принимаются во внимание все соответствующие обстоятельства, которые могут включать:

- а) выполнение поставщиком удостоверительных услуг обязанностей, перечисленных в статье 14;
- б) соответствие операционных правил, принципов и практики поставщика удостоверительных услуг любым применимым и признанным международным стандартам и процедурам, имеющим отношение к предоставлению удостоверительных услуг;
- с) любой соответствующий уровень надежности используемого метода;
- д) любой применимый отраслевой стандарт;
- е) безопасность аппаратного и программного обеспечения;
- ф) финансовые и людские ресурсы, в том числе наличие активов;
- г) регулярность и объем ревизии, проводимой независимым органом;
- h) наличие заявления, сделанного надзорным органом, аккредитующим органом или на основе добровольной схемы в отношении надежности этого метода;
- і) цель, для которой используется удостоверительная услуга; и
- j) любые соответствующие договоренности между сторонами, включая любое ограничение целей или стоимостного объема операций, для которых может использоваться удостоверительная услуга.

3. При определении надежности метода не учитывается:

- а) географическое место предоставления удостоверительной услуги;
- б) географическое местонахождение коммерческого предприятия поставщика удостоверительных услуг.

4. Метод, используемый для оказания удостоверительной услуги, назначенной в соответствии со статьёй 23, считается надежным.

5. Пункт 4 не ограничивает возможности любого лица в отношении:
- a) установления надежности какого-либо метода любым другим способом; или
 - b) представления доказательств ненадежности какого-либо метода, используемого для оказания удостоверительной услуги, назначенной в соответствии со статьей 23.

Статья 23. Назначение надежных удостоверительных услуг

1. [Лицо, орган или ведомство, будь то публичное или частное, назначенное принимающей юрисдикционной системой в качестве компетентного,] может назначить удостоверительные услуги, которые считаются надежными.
2. [Лицо, орган или ведомство, будь то публичное или частное, назначенное принимающей юрисдикционной системой в качестве компетентного]:
 - a) принимает во внимание при назначении удостоверительной услуги все соответствующие обстоятельства, включая факторы, перечисленные в статье 22; и
 - b) публикует перечень назначенных удостоверительных услуг, включая информацию о поставщике удостоверительных услуг.
3. Любое решение о назначении, принятое в соответствии с пунктом 1, должно соответствовать признанным международным стандартам и процедурам, применимым к осуществлению процесса назначения.
4. При назначении надежной удостоверительной услуги не учитываются:
 - a) географическое место предоставления удостоверительной услуги;
 - b) географическое местонахождение коммерческого предприятия поставщика удостоверительных услуг.

Статья 24. Ответственность поставщиков удостоверительных услуг

1. Поставщик удостоверительных услуг несет ответственность за убытки, причиненные абоненту или полагающейся стороне в результате невыполнения им своих обязанностей, предусмотренных статьей 14.
2. Пункт 1 применяется в соответствии с нормами об ответственности, содержащимися в законодательстве, и без ущерба для:
 - a) любого другого основания для возникновения ответственности, предусмотренного законодательством, включая ответственность за невыполнение обязанностей договорного характера; или
 - b) любых других правовых последствий невыполнения поставщиком удостоверительных услуг обязанностей, предусмотренных настоящим Законом.
3. Невзирая на положения пункта 1, поставщик удостоверительных услуг не несет ответственности перед абонентом за убытки, понесенные в результате использования удостоверительной услуги, в том случае, если:
 - a) такое использование выходит за рамки ограничений в отношении целей или стоимости операции, для которой используется удостоверительная услуга; и
 - b) эти ограничения закреплены в соглашении между поставщиком удостоверительных услуг и абонентом.
4. Невзирая на положения пункта 1, поставщик удостоверительных услуг не несет ответственности перед полагающейся стороной за убытки, понесенные в результате использования удостоверительной услуги, в том случае, если:

- а) такое использование выходит за рамки ограничений в отношении целей или стоимости операций, для которых используется удостоверительная услуга; и
- б) поставщик удостоверительных услуг выполнил свои обязанности, предусмотренные подпунктом 1(е) статьи 14, в отношении этой операции.

Глава IV. Международные аспекты

Статья 25. Трансграничное признание электронной идентификации

1. Электронная идентификация, предоставляемая за пределами [*принимающей юрисдикционной системы*], имеет ту же юридическую силу в [*принимающей юрисдикционной системе*], что и электронная идентификация, предоставляемая в [*принимающей юрисдикционной системе*], если метод, используемый системой управления идентификационными данными, услуга по управлению идентификационными данными или идентификационные учетные данные, в зависимости от обстоятельств, обеспечивают по меньшей мере эквивалентный уровень надежности.
2. При определении того, обеспечивают ли система управления идентификационными данными, услуга по управлению идентификационными данными или идентификационные учетные данные, в зависимости от обстоятельств, по меньшей мере эквивалентный уровень надежности, следует учитывать признанные международные стандарты.
3. Для целей пункта 1 система управления идентификационными данными, услуга по управлению идентификационными данными или идентификационные учетные данные считаются обеспечивающими по меньшей мере эквивалентный уровень надежности, если [*лицо, орган или ведомство, указанные принимающей юрисдикционной системой в соответствии со статьей 11*] определили такую эквивалентность с учетом пункта 2 статьи 10.

Статья 26. Трансграничное признание результата использования удостоверительных услуг

1. Результат использования удостоверительной услуги, предоставляемой за пределами [*принимающей юрисдикционной системы*], имеет ту же юридическую силу в [*принимающей юрисдикционной системе*], что и результат использования удостоверительной услуги, предоставляемой в [*принимающей юрисдикционной системе*], если метод, использованный для предоставления этой удостоверительной услуги, обеспечивает, по меньшей мере, эквивалентный уровень надежности.
2. При определении того, обеспечивает ли удостоверительная услуга по меньшей мере эквивалентный уровень надежности, следует учитывать признанные международные стандарты.
3. Для целей пункта 1 удостоверительная услуга считается обеспечивающей по меньшей мере эквивалентный уровень надежности, если [*лицо, орган или ведомство, указанное принимающей юрисдикционной системой в соответствии со статьей 23*] определило такую эквивалентность с учетом пункта 2 статьи 22.

Статья 27. Сотрудничество

[*Лицо, орган или ведомство, указанное принимающей юрисдикционной системой в качестве компетентного*] может сотрудничать с иностранными организациями путем обмена информацией, опытом и успешными видами практики в области управления идентификационными данными и удостоверительных услуг, в частности в отношении:

- a) признания правовых последствий использования иностранных систем управления идентификационными данными и удостоверительных услуг, предоставляемых в одностороннем порядке или по взаимной договоренности;
- b) назначения систем управления идентификационными данными и удостоверительных услуг; и
- c) определения уровней обеспечения доверия для систем управления идентификационными данными и уровней надежности удостоверительных услуг.

Приложение II

Пояснительная записка к проекту типового закона об использовании и трансграничном признании управления идентификационными данными и достоверительных услуг

I. Введение

A. Цель настоящей пояснительной записки

1. В ходе подготовки и принятия Типового закона ЮНСИТРАЛ об использовании и трансграничном признании управления идентификационными данными и достоверительными услугами (далее «Типовой закон») Комиссия Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ) сочла, что Типовой закон будет в большей мере способствовать согласованию и модернизации законодательства, если его сопроводить справочной и разъяснительной информацией.

2. Настоящая пояснительная записка, составленная во многом на основе подготовительных материалов, относящихся к Типовому закону, призвана помочь тем, кто заинтересован в принятии, использовании и единообразном толковании Типового закона, в частности лицам, ответственным за разработку политики, законодательства, ученых, специалистам-практикам, судьям и арбитрам, коммерческим операторам и пользователям услуг по управлению идентификационными данными и достоверительных услуг. Например, в момент принятия Типового закона такая информация может помочь юрисдикционным системам адаптировать Типовой закон с учетом своих потребностей в том, что касается взаимодействия положений Типового закона и режима регулирования управления идентификационными данными и достоверительных услуг.

B. Задачи

3. 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). Такой рост еще более ускорился в связи с потребностью смягчить последствия пандемии COVID-19¹, сопровождается таким же увеличением количества операций с данными и требует наличия надлежащей правовой и технической базы.

4. Такой рост коммерческой деятельности в режиме онлайн основывается на доверии и должен подкрепляться чувством доверия к электронной среде на постоянной основе. Одним из важных компонентов такого доверия является способность надежно идентифицировать каждую сторону, особенно в отсутствие какого-либо предварительного личного взаимодействия. 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 том числе в электронной форме. В контексте цифровой экономики это означает право на наличие идентификационных данных в цифровой форме.

5. В течение ряда лет предлагались различные решения для проблем, связанных с необходимостью идентификации в режиме онлайн. В результате были разработаны системы, методы, технологии и устройства для создания цифровых

¹ ЮНКТАД, «Доклад о цифровой экономике. Международные потоки данных и развитие: кому служат потоки данных», документ ООН UNCTAD/DER/2021, с. 16–17.

учетных данных физических и юридических лиц и управления ими. Рассмотрение правовых аспектов управления идентификационными данными (далее «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.

6. Еще одним важным компонентом доверия к онлайн-пространству является способность с достаточной уверенностью полагаться на качество данных, которая служит основой для обмена данными. В качестве способов решения проблемы обеспечения такой уверенности были созданы удостоверительные услуги, предоставляющие гарантии таких характеристик сообщения данных, как его происхождение, его целостность и время осуществления определенного связанного с ним действия.

7. На пути расширения использования УИД и удостоверительных услуг могут встречаться различные препятствия. Например, доступ к УИД и удостоверительным услугам может быть ограничен из-за стоимости, недостаточной осведомленности и ограничений технического характера. 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 услуг².

8. Основная цель Типового закона заключается в устранении этих препятствий путем разработки единообразных правовых норм, служащих нескольким целям. Единообразные нормы могут повысить эффективность путем содействия принятию результатов применения УИД и удостоверительных услуг в разных системах; снизить операционные издержки путем упрощения задачи соблюдения нормативных требований; повысить правовую предсказуемость и определенность электронных сделок на основе единого подхода к рассмотрению вопросов, в том числе с помощью механизмов трансграничного признания; и способствовать преодолению отставания в сфере цифровых технологий за счет повышения доступности общих решений.

9. В частности, правовая основа для УИД и удостоверительных услуг будет способствовать безопасному внедрению идентификационных данных в цифровой форме и обеспечению безопасности операций с данными. 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.

С. Сфера охвата

10. Типовой закон применяется к использованию и трансграничному признанию услуг УИД и удостоверительных услуг в контексте коммерческой деятельности и услуг, связанных с торговлей. Принимающие Типовой закон юрисдикционные системы могут принять решение расширить сферу применения Типового закона, включив в нее некоммерческую деятельность.

11. В отношении обмена данными может действовать множество разных законодательных актов. Типовой закон не преследует цели повлиять на эти действующие законы, а именно законодательство, применимое к конфиденциальности и защите данных. В нем также не предусматриваются новые обязательства по использованию УИД и удостоверительных услуг или любой конкретной

² A/CN.9/965, п. 52.

услуги УИД или удостоверительной услуги, и не затрагивается никакое такое действующее требование (см. пп. 102–104 ниже).

12. Положения Типового закона, касающиеся УИД, применяются к идентификации физических и юридических лиц. Положения об удостоверительных услугах применяются к любой информации, имеющей форму сообщения данных. Оба набора положений применяются независимо от того, каким лицом — физическим или юридическим — является поставщик услуг, абонент или полагающаяся сторона.

D. Структура

13. Типовой закон состоит из четырех глав, посвященных соответственно общим положениям, УИД, удостоверительным услугам и международным аспектам. Главы I и IV относятся и к УИД, и к удостоверительным услугам. Кроме того, главы II и III имеют значительные сходства по структуре и содержанию. Таким образом, разъяснения, касающиеся того или иного положения главы II, могут 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.

14. Глава I содержит определения некоторых терминов, встречающихся в Типовом законе; определение сферы применения; положения о добровольном использовании УИД и удостоверительных услуг, в том числе конкретных услуг; положения о взаимосвязи между Типовым законом и другими законами, включая требования, обязывающие осуществлять идентификацию или использовать определенные удостоверительные услуги; и положения об автономном толковании Типового закона, в том числе для целей восполнения пробелов, с учетом его единообразного характера и международного происхождения.

15. 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 УИД и недискриминации в отношении электронной идентификации. В статье 6 перечислены основные обязанности поставщиков услуг УИД; при этом основные обязанности поставщиков услуг УИД соотнесены с базовыми компонентами систем УИД и основными процессами 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 офлайн и электронной идентификации, для которой требуется использование надежного метода. Надежность метода оценивается путем определения *ex post* исходя из 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.

16. 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 некоторых удостоверительных услуг может не существовать бумажного эквивалента, в их отношении необязательно будет требоваться соблюдение правила функциональной эквивалентности. В статье 22 содержатся руководящие указания по *ex post* определению надежности метода, использованного для оказания удостоверительной услуги, а в статье 23 — по *ex ante* назначению. Наконец, в статье 24 изложены положения об ответственности поставщиков удостоверительных услуг.

17. В главе IV содержатся положения, призванные обеспечить возможность трансграничного признания УИД и удостоверительных услуг, что является одной из основных целей Типового закона. В Типовом законе не рассматривается вопрос о создании специального органа для юридического признания УИД и удостоверительных услуг, но предусматривается несколько механизмов на основе децентрализованного подхода. Наряду со статьями 25, 26 и 27, отношение к этой теме 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. Также для обеспечения возможности трансграничного использования систем УИД и удостоверительных услуг могут использоваться договорные соглашения.

Е. Справочная информация

1. История разработки

18. Типовой закон разработан во исполнение просьбы, высказанной Комиссией на ее сорок восьмой сессии в 2015 году. На той сессии Комиссия просила секретариат провести подготовительную работу по правовым вопросам, связанным с УИД и удостоверительными услугами, в том числе путем организации коллоквиумов и совещаний групп экспертов для дальнейшего обсуждения этих вопросов на уровне Рабочей группы³, и предоставить результаты этой подготовительной работы Рабочей группе IV с целью получить от нее рекомендации относительно точной сферы полномочий, возможной методике и приоритетов для рассмотрения Комиссией⁴.

19. В ответ на эту просьбу Комиссии на ее сорок девятой сессии в 2016 году была представлена записка секретариата о правовых вопросах, связанных с УИД и удостоверительными услугами (A/CN.9/891), содержащая резюме обсуждений, состоявшихся на коллоквиуме ЮНСИТРАЛ по правовым вопросам, связанным с управлением идентификационными данными и удостоверительными услугами, который был проведен 21–22 апреля 2016 года в Вене⁵. Комиссия решила, что тему УИД и удостоверительных услуг следует сохранить в программе работы Рабочей группы⁶.

20. Получив мандат от Комиссии, Рабочая группа предварительно обсудила эту тему на своей пятьдесят четвертой сессии (Вена, 31 октября — 4 ноября 2016 года). Рабочая группа согласилась с тем, что ее будущую работу в области УИД и удостоверительных услуг следует ограничить вопросами использования систем УИД для коммерческих целей и что в ходе этой работы следует рассматривать и частных и публичных поставщиков услуг УИД. Рабочая группа согласилась также с тем, что сначала можно было бы провести работу по УИД, а затем приступить к рассмотрению удостоверительных услуг, однако, поскольку эти две тематики тесно связаны между собой, работу по выявлению и определению терминов, имеющих отношение и к УИД, и к удостоверительным услугам,

³ *Официальные отчеты Генеральной Ассамблеи, семидесятая сессия, Дополнение № 17 (A/70/17)*, пп. 354–355 и 358.

⁴ Там же, п. 358.

⁵ Там же, *семьдесят первая сессия, Дополнение № 17 (A/71/17)*, п. 228.

⁶ Там же, пп. 235–236.

следует проводить одновременно по обеим темам. Она также согласилась с тем, что особое внимание следует уделить многосторонним системам УИД и идентификации физических и юридических лиц и что ей следует продолжить свою работу посредством дальнейшего разъяснения целей проекта, уточнения сферы его охвата, выявления применимых общих принципов и разработки необходимых определений (A/CN.9/897, пп. 118–120 и 122).

21. В соответствии с решениями, принятыми ею ранее, на своей пятьдесят пятой сессии (Нью-Йорк, 24–28 апреля 2017 года) Рабочая группа обсудила, среди прочего, цели, общие принципы и сферу охвата своей работы по УИД и удостоверительным услугам (A/CN.9/902, пп. 29–85).

22. Комиссия подтвердила мандат, предоставленный Рабочей группе (см. п. 19 выше) на ее пятидесятой сессии в 2017 году, и обратилась к секретариату с просьбой рассмотреть возможность созыва совещаний групп экспертов. Государствам и международным организациям было предложено поделиться имеющимся опытом⁷. Соответственно, секретариат созвал совещание группы экспертов по правовым вопросам, связанным с УИД и удостоверительными услугами, в Вене 23–24 ноября 2017 года.

23. С учетом также результатов совещания группы экспертов на своей пятьдесят шестой сессии (Нью-Йорк, 16–20 апреля 2018 года) Рабочая группа определила следующие вопросы как имеющие отношение к обсуждению правовых вопросов, связанных с УИД и удостоверительными услугами: сфера охвата работы; общие принципы; определения; требования и механизмы взаимного признания; сертификация УИД и удостоверительных услуг; уровни обеспечения гарантий для УИД и удостоверительных услуг; ответственность; институциональные механизмы сотрудничества; прозрачность; обязательство идентифицировать; сохранение данных; и надзор за работой поставщиков услуг (A/CN.9/936, пп. 61–94).

24. На своей пятьдесят первой сессии в 2018 году по рекомендации Рабочей группы (A/CN.9/936, п. 95) Комиссия просила Рабочую группу провести работу в целях подготовки текста, направленного на содействие трансграничному признанию УИД и удостоверительных услуг, на основе принципов и вопросов, определенных Рабочей группой (см. выше п. 23)⁸.

25. Соответственно, Рабочая группа продолжила рассмотрение определенных ею вопросов (A/CN.9/965, пп. 10–129) на своей пятьдесят седьмой сессии (Вена, 19–23 ноября 2018 года).

26. Первый свод проектов положений о трансграничном признании УИД и удостоверительных услуг (A/CN.9/WG.IV/WP.157) вместе с пояснительными замечаниями (A/CN.9/WG.IV/WP.158) был представлен на рассмотрение Рабочей группы на ее пятьдесят восьмой сессии (Нью-Йорк, 8–12 апреля 2019 года). Рабочая группа рассмотрела проекты положений о сфере применения, признании и надежности систем УИД и удостоверительных услуг, видах удостоверительных услуг, которые должны быть охвачены, и обязанностях и ответственности поставщиков услуг УИД и удостоверительных услуг (см. A/CN.9/971, пп. 13–153).

27. На той сессии Рабочая группы просила секретариат при участии соответствующих экспертов подготовить конкретные предложения по вопросам, касающимся надежности систем УИД (A/CN.9/971, п. 67). В ответ на эту просьбу секретариат созвал в Вене 22–23 июля 2019 года совещание группы экспертов для обсуждения стандартов и процедур для юридического признания системы УИД, а также других вопросов, охватываемых в проектах положений, в частности

⁷ *Официальные отчеты Генеральной Ассамблеи, семьдесят вторая сессия, Дополнение № 17 (A/72/17)*, п. 127.

⁸ Там же, *семьдесят третья сессия, Дополнение № 17 (A/73/17)*, п. 159.

надежности систем УИД и обязанностей и ответственности поставщиков услуг УИД.

28. На своей пятьдесят второй сессии в 2019 году Комиссия выразила удовлетворение прогрессом, достигнутым Рабочей группой⁹. Она отметила, что Рабочей группе следует работать над подготовкой такого документа, который мог бы применяться к использованию УИД и удостоверительных услуг как на внутренней, так и на трансграничной основе, и что результаты этой работы будут иметь значение также для решения вопросов, выходящих за рамки коммерческих сделок¹⁰.

29. На своей пятьдесят девятой сессии (Вена, 25–29 ноября 2019 года) Рабочая группа рассмотрела пересмотренный набор проектов положений (A/CN.9/WG.IV/ WP.160), в котором были учтены результаты консультаций секретариата с экспертами (см. выше п. 27). Рабочая группа тщательно изучила текст проектов положений, обратив особое внимание на положения, касающиеся удостоверительных услуг (A/CN.9/1005, пп. 10–122). Она также предварительно обсудила форму документа, и явное предпочтение при этом было выражено тому, чтобы документ был разработан как типовой закон, а не конвенция (там же, п. 123).

30. На своей пятьдесят третьей сессии в 2020 году Комиссия вновь выразила удовлетворение работой, проделанной этими рабочими группами¹¹.

31. Рабочей группе на ее шестидесятой сессии (Вена, 19–23 октября 2020 года) был представлен второй пересмотренный набор проектов положений (A/CN.9/WG.IV/ WP.162), который она полностью рассмотрела на этой сессии (A/CN.9/1045, пп. 16–138). Она также выразила согласие с возможным проведением неофициальных консультаций для обсуждения нерассмотренных тем.

32. Неофициальные консультации с делегатами и наблюдателями были проведены в период с 15 по 17 марта 2021 года в дистанционном режиме для обсуждения вопросов ответственности, связи проектов положений с существующими текстами ЮНСИТРАЛ и трансграничного признания, а также определений и других терминологических вопросов.

33. Рабочая группа на ее шестьдесят первой сессии (Нью-Йорк, 6–9 апреля 2021 года) была проинформирована об итогах состоявшихся неофициальных консультаций. С учетом ограничений, обусловленных смешанным форматом проведения сессии (в том числе сокращенной продолжительности заседаний), при рассмотрении третьего пересмотренного набора проектов положений (A/CN.9/WG.IV/ WP.167) Рабочая группа сосредоточила внимание на вопросах, обсуждавшихся в ходе этих консультаций (A/CN.9/1051, пп. 13–67).

34. На своей пятьдесят четвертой сессии в 2021 году Комиссия заслушала информацию о том, что, несмотря на сокращенную продолжительность заседаний, Рабочая группа добилась значительного прогресса на пути к завершению работы над документом. Комиссия выразила удовлетворение достигнутым прогрессом и призвала Рабочую группу завершить свою работу и представить ее итоги на рассмотрение Комиссии на пятьдесят пятой сессии в 2022 году¹².

35. На своей шестьдесят второй сессии (Вена, 22–26 ноября 2021 года) Рабочая группа провела очередное чтение проектов положений (A/CN.9/1087, пп. 12–114) на основе пересмотренного набора проектов положений (A/CN.9/WG.IV/ WP.170) в сопровождении пояснительной записки (A/CN.9/WG.IV/ WP.171). Рабочая группа просила секретариат пересмотреть проект положений и пояснительную записку и учесть в них состоявшееся обсуждение и принятые решения и препроводить пересмотренный текст в форме

⁹ *Официальные отчеты Генеральной Ассамблеи, семьдесят четвертая сессия, Дополнение № 17 (A/74/17)*, п. 175.

¹⁰ Там же, п. 172.

¹¹ Там же, *семьдесят пятая сессия, Дополнение № 17 (A/75/17)*, часть вторая, пп. 41 и 51(d).

¹² Там же, *семьдесят шестая сессия, Дополнение № 17 (A/76/17)*, гл. IX.

типового закона Комиссии для рассмотрения на ее пятьдесят пятой сессии. Секретариату было поручено препроводить пересмотренный текст всем правительствам и соответствующим международным организациям для того, чтобы они могли представить свои замечания, и подготовить затем подборку полученных замечаний для рассмотрения Комиссией ([A/CN.9/1087](#), п. 11).

36. [будет дополнено]

2. Взаимосвязь с ранее принятыми текстами ЮНСИТРАЛ

37. В принятых ранее текстах ЮНСИТРАЛ нет положений об удостоверительных услугах. Однако в этих текстах предусмотрены правила функциональной эквивалентности, которые могут быть применимы к определенным удостоверительным услугам. В статье 7 Типового закона ЮНСИТРАЛ об электронной торговле (ТЗЭТ)¹³, статье 6 Типового закона ЮНСИТРАЛ об электронных подписях (ТЗЭП)¹⁴, статье 9(3) Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах (КЭС)¹⁵ и статье 9 Типового закона об электронных передаваемых записях (ТЗЭПЗ)¹⁶ устанавливаются требования, которым должны соответствовать электронные подписи, чтобы считаться функционально эквивалентными подписям, проставленным на бумаге. Эти положения требуют идентификации подписывающего лица, что может предполагать использование электронной идентификации и в целом УИД. Статья 9 ТЗЭПЗ положена в основу статьи 16 Типового закона.

38. Аналогичным образом, в статье 10 ТЗЭТ устанавливаются требования функциональной эквивалентности применительно к сохранению информации, и статья 10(1) ТЗЭТ положена в основу статьи 19 Типового закона. Другие положения текстов ЮНСИТРАЛ, которые использовались в качестве основы для разработки статей Типового закона, указываются в сносках к соответствующим статьям. Вместе с тем для обеспечения выполнения положений о функциональной эквивалентности, содержащихся в ранее принятых текстах ЮНСИТРАЛ, возможно, не потребуется использовать ту или иную конкретно указанную в Типовом законе удостоверительную услугу.

39. Ряд вопросов, имеющих отношение к Типовому закону, в частности об оценке надежности, ответственности и механизмах трансграничного признания, подробно рассматриваются в пособии по международному использованию электронных подписей¹⁷.

Г. Основные понятия и принципы

40. В настоящем разделе разъясняются несколько основных понятий и принципов, лежащих в основе Типового закона. Более подробные разъяснения терминов, которым даны определения и которые используются в Типовом законе, приводятся в комментарии к статье 1 ниже, тогда как в документе [A/CN.9/WG.IV/WR.150](#) представлен более широкий перечень терминов и понятий, относящихся к УИД и удостоверительным услугам, составленный на основе определений, содержащихся в согласованных на международном уровне юридических

¹³ ЮНСИТРАЛ, *Типовой закон ЮНСИТРАЛ об электронной торговле и Руководство по принятию 1996 года с дополнительной статьей 5-бис, принятой в 1998 году* (1999 год), издание Организации Объединенных Наций в продаже под № R.99.V.4.

¹⁴ ЮНСИТРАЛ, *Типовой закон об электронных подписях с руководством по принятию* (2002 год), издание Организации Объединенных Наций, в продаже под № R.02.V.8.

¹⁵ United Nations, *Treaty Series*, vol. 2898, p. 3.

¹⁶ ЮНСИТРАЛ, *Типовой закон об электронных передаваемых записях* (2018 год), издание Организации Объединенных Наций, в продаже под № R.17.V.5.

¹⁷ Секретариат ЮНСИТРАЛ, «Содействие укреплению доверия к электронной торговле: правовые вопросы международного использования электронных методов удостоверения подлинности и подписания» (2007 год), издание Организации Объединенных Наций, в продаже под № R.09.V.4.

и технических текстах. 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

41. Как и ранее принятые тексты ЮНСИТРАЛ, Типовой закон основан на принципах автономии сторон, технологической нейтральности, функциональной эквивалентности и недискриминации в отношении использования электронных средств с учетом возможных корректировок¹⁸.

42. Принцип автономии сторон позволяет сторонам договора выбирать применимые правила в пределах, установленных императивными нормами права. Он основан на признании того факта, что именно стороны договора могут наилучшим образом определить наиболее подходящие правила для конкретной сделки.

43. Принцип недискриминации, впервые сформулированный в статье 5 ТЗЭТ и известный также как принцип юридического признания, гарантирует, что информация не может быть лишена юридической силы, действительности или исковой силы на том лишь основании, что она составлена в электронной форме.

44. Принцип технологической нейтральности гарантирует, что в законодательстве не будет содержаться предписаний и не будут выражаться предпочтения в отношении использования каких-либо конкретных технологий или методов, благодаря чему соответствующие законы позволяют учесть развитие технологий в будущем. Технологическая нейтральность необходима для достижения совместимости систем, обеспечивающей на практике условия для обмена потоками данных. Юридическим обоснованием данного принципа является широкое определение понятия «сообщение данных», впервые встречающееся в статье 2(е) ТЗЭТ, которое призвано охватить все существующие и будущие технологии.

45. Принцип функциональной эквивалентности устанавливает критерии, при соблюдении которых электронные сделки считаются удовлетворяющими требованиям в отношении формы, применимым к бумажным документам, в частности в том, что документ должен быть составлен в письменной форме, быть подлинным или что он должен быть подписан. Этот принцип 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. 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.

46. Хотя в Типовом законе эти общие принципы прямо не указаны, они составляют основу ключевых положений текста. Принцип автономии сторон закреплен в статье 3, а принцип недискриминации, как он применяется к УИД и удостоверительным услугам, предусмотрен положениями статей 5 и 13, соответственно. Более того, принцип функциональной эквивалентности лег в основу статьи 9 об электронной идентификации и статей 16–21 о конкретных удостоверительных услугах. Вместе с тем некоторые удостоверительные услуги, охватываемые Типовым законом, могут не иметь бумажного эквивалента, и, следовательно, принцип функциональной эквивалентности не будет к ним применяться.

2. Управление идентификационными данными (УИД)

47. Идентификация — это процесс распознавания того или иного лица как отличающегося от других лиц на основе имеющейся информации, относящейся к этому лицу (т. е. атрибутов). Эта информация может быть собрана или накоплена в результате наблюдений. Идентификация заключается, в частности, в проверке

¹⁸ См. [A/CN.9/902](#), пп. 52 и 63.

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 того или иного лица и предъявление атрибутов для его проверки.

48. Соответственно, согласно Типовому закону 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 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, чьи учетные данные были предъявлены, является лицом, которому эти учетные данные были выданы на первом этапе.

49. Системы УИД используются для управления процессами идентификации, связанными с каждым из этих двух 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, та или иная система УИД может предлагать разные «услуги» УИД. Стороны (т. е. сторона, желающая идентифицировать, и сторона, желающая быть идентифицированной) могут выбрать подходящую услугу УИД в соответствии со своими потребностями.

50. Системы УИД могут эксплуатироваться публичными или частными субъектами. 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. При применении принципа технологической нейтральности (см. выше п. 44) Типовой закон не предполагает заранее использования какой-либо технологии или модели и поэтому может применяться ко всем типам систем и услуг УИД.

51. 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 вызывали 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, может сократить расходы и тем самым обеспечить долгосрочную устойчивость.

3. Удостоверительные услуги

52. Удостоверительные услуги — это онлайн-услуги, которые обеспечивают уверенность в определенных качествах сообщений данных, таких как источник, целостность и время осуществления какого-либо определенного действия в отношении данных. Гарантия качества данных имеет важнейшее значение для установления доверия при обмене данными, на котором строится цифровая торговля. В Типовом законе указаны некоторые часто используемые удостоверительные услуги и признается, что могут существовать или могут быть разработаны в будущем и другие удостоверительные услуги.

53. Понятие удостоверительной услуги в Типовом законе охватывает не только саму услугу, но и предоставление услуги. Например, электронная подпись может быть проставлена с помощью той или иной услуги, для которой используются способы создания электронной подписи и управления ею. Во избежание сомнений в положениях Типового закона уточняется, относятся ли они к способам предоставления услуги электронной подписи или к электронной подписи, являющейся результатом этой услуги.

4. Оценка надежности

54. В соответствии с ранее принятыми текстами ЮНСИТРАЛ, в ряде положений Типового закона говорится об использовании надежного метода для оказания услуг по управлению идентификационными данными и удостоверительных услуг. В Типовом законе 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.

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

55. Один из возможных подходов к оценке надежности метода предполагает проведение такой оценки до использования этого метода (*ex ante*) на основе перечня заранее определенных условий и в общем контексте, а не применительно к конкретной сделке. В Типовом законе такой подход характеризуется как назначение надежных услуг, и в статье 11 (применимой к услугам УИД), и в статье 23 (применимой к удостоверительным услугам) перечисляются требования для такого назначения, которые включают в себя те же обстоятельства, которые должны учитываться при определении надежности.

56. Объектом назначения являются не общие типы услуг УИД и удостоверительных услуг или все услуги УИД и удостоверительные услуги, предлагаемые поставщиком услуг УИД или поставщиком удостоверительных услуг, а конкретная услуга, предоставляемая конкретным поставщиком услуг.

57. Подход *ex ante* позволяет обеспечить более высокий уровень ясности и предсказуемости в отношении юридических последствий УИД и удостоверительных услуг, в том числе в контексте трансграничного использования. При этом управление им предполагает наличие институционального механизма, т. е. учреждения, компетентного управлять процедурой назначения.

58. Принимающая Типовой закон юрисдикционная система, желающая применять подход *ex ante*, 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) является полезной для проведения оценки услуг с использованием стандартов, основанных на конечных результатах, и поэтому она может иметь значение при их назначении.

59. Типовой закон предполагает наличие институционального механизма, необходимого для применения подхода *ex ante*, но не содержит положений о его создании или управлении им. 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.

60. Механизм назначения должен быстро адаптироваться к развитию технологий, с тем чтобы не препятствовать инновациям. В ином случае могут подвергнуться дискриминации те услуги УИД и удостоверительные услуги, которые не были назначены, хотя являются доступными и основанными на надежных методах. Более того, дальнейшее уточнение условий назначения не должно приводить к установлению требований, навязывающих конкретные технологии.

b) Ретроспективное определение надежности (ex post)

61. Другой возможный подход к оценке надежности метода откладывает проведение такой оценки до того момента, когда возникает спор о надежности. Следовательно, оценка проводится только после того, как метод был использован («ex-post»). В Типовом законе такой подход характеризуется как определение надежности, и в статье 11 (применимой к услугам УИД) и в статье 23 (применимой к удостоверительным услугам) перечисляются требования для такого определения, включая неисчерпывающий перечень подлежащих учету обстоятельств.

62. Подход ex post в целом позволяет осуществлять операции по УИД без проведения предварительной оценки надежности и ограничивает необходимость оценки надежности случаями фактического возникновения спора. Он также обеспечивает максимальную гибкость для сторон 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.

63. С другой стороны, подход ex post может не обеспечивать более высокий уровень предсказуемости относительно действительности используемого метода до его практического использования и тем самым подвергает стороны риску того, что этот метод может быть признан ненадежным. Более того, определение надежности метода поручается третьей стороне, и сама эта процедура может занять много времени и привести к непоследовательным решениям.

c) Комбинированный подход

64. В Типовом законе сочетаются определение и назначение, благодаря чему обеспечивается возможность признания любой услуги УИД и удостоверительной услуги, но также содержатся руководящие указания относительно того, какие услуги УИД и удостоверительные услуги предлагают более высокий уровень доверия к их надежности («двухуровневый» подход). При этом в Типовом законе 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.

65. Не все тексты ЮНСИТРАЛ содержат положения, позволяющие применять оба подхода, — ex ante и ex post. Однако подходы ex ante и ex post обычно считаются совместимыми и взаимодополняющими. Комбинированный подход, применяемый в Типовом законе, строится на положениях статей 6 и 7 ТЗЭТ.

5. Вопросы ответственности

66. Режим ответственности может оказать существенное влияние на содействии более широкому использованию УИД и удостоверительных услуг и является одним из основных элементов Типового закона. В разное время

законодатели применяли разные решения — от отказа от специального режима ответственности до принятия положений, касающихся стандартов поведения и правил ответственности, применимых только к поставщикам услуг, или же ко всем соответствующим сторонам (поставщикам услуг, абонентам и полагающимся сторонам)¹⁹. Последний подход закреплен в ТЗЭТ²⁰.

67. Распределение ответственности в отношении УИД и удостоверительных услуг в основном осуществляется на основе договорных соглашений или на основании закона. Последний подход может быть предпочтительным для того, чтобы исключить возможность отказа от некоторых положений по договоренности. Более того, законодательные нормы могут применяться и в отсутствие договорного соглашения, т. е. в отношении полагающихся сторон.

68. В статьях 12 и 24 устанавливается единообразный режим ответственности поставщиков услуг перед абонентами и полагающимися сторонами, основанный на принципе, согласно которому поставщик услуг должен нести ответственность за последствия непредоставления своих услуг в соответствии с требованиями закона. Соответственно, статьи 12 и 24 устанавливают законодательную основу ответственности, которая действует наряду с договорной и внедоговорной ответственностью. Более того, Типовой закон позволяет поставщикам услуг ограничивать свою ответственность как перед абонентами, так и перед полагающимися сторонами.

69. В Типовом законе не рассматривается ни степень вины, необходимая для наступления ответственности, ни вид и размер возместимого ущерба²¹. Следовательно, в том случае, если на момент включения Типового закона в законодательство, никакие специальные правила в отношении поставщиков услуг УИД и удостоверительных услуг не принимаются, к таким вопросам будут применяться обычные правила принимающей Типовой закон юрисдикционной системы.

5. Международные аспекты

70. Международный охват имеет важнейшее значение для использования УИД и удостоверительных услуг и в целом для электронных сделок. Однако, два вида препятствий могут помешать их использованию на международном уровне: техническая несовместимость, ведущая к операционной несовместимости, и юридические препятствия для трансграничного признания²².

71. Юридические препятствия могут возникнуть из-за противоречивых национальных подходов, особенно когда в законодательстве предписывается использование определенных технологии, метода или продукта или для них предусматриваются благоприятные условия. В этом случае внутренние правовые требования могут затруднить признание несоответствующих видов услуг УИД или удостоверительных услуг. Более того, национальные технические стандарты, которые могут появиться также при применении «двухуровневого» подхода, в том случае, если они связаны с юридическими презумпциями, могут привести к возникновению разрозненных требований, которые также могут препятствовать трансграничному использованию.

72. Одной из основных целей Типового закона является разработка правовой основы, обеспечивающей возможность трансграничного использования УИД и удостоверительных услуг. Для ее достижения применяются принципы

¹⁹ «Содействие укреплению доверия к электронной торговле», п. 175.

²⁰ См. подробнее в пояснительной записке к ТЗЭТ, пп. 77–81.

²¹ См. по этим вопросам «Содействие укреплению доверия к электронной торговле», пп. 177–193 (основания ответственности в рамках инфраструктуры публичных ключей) и пп. 194–201 (стороны, имеющие право требовать возмещения ущерба, и объем возместимого ущерба).

²² «Содействие укреплению доверия к электронной торговле», пп. 137–152.

технологической нейтральности и недискриминации по географическому признаку²³, которые положены в основу статей 10(3), 11(4), 22(3) и 23(4) Типового закона. Более того, вопросы трансграничного признания непосредственно рассматриваются в главе IV. Как следствие, Типовой закон не только не поощряет принятие законодательства, ориентированного на конкретные технологии, но и способствует разработке совместимых технических стандартов, в том числе в рамках сотрудничества.

73. В соответствии с подходом, который применялся в отношении ранее принятых текстов ЮНСИТРАЛ, для юридического признания иностранных услуг УИД и удостоверительных услуг согласно Типовому закону необходимо учитывать не только географическое место предоставления услуг. Если говорить точнее, то Типовой закон требует определения надежности иностранных услуг УИД и удостоверительных услуг по принципу *ex post* с учетом тех же обстоятельств, которые имели бы значение для аналогичных внутренних услуг УИД и удостоверительных услуг. В нем также предусматриваются механизмы назначения надежных услуг в отношении иностранных услуг УИД и удостоверительных услуг с учетом тех же обстоятельств, которые имели бы значение для аналогичных внутренних услуг УИД и удостоверительных услуг. Если коротко, то определяющее значение для решения вопроса о юридическом признании должно иметь не географическое место предоставления услуг, а их техническая надежность.

74. В Типовом законе не требуется создания официального институционального механизма для трансграничного юридического признания. Однако примеры таких механизмов имеются на региональном и двустороннем уровне. Принимающие Типовой закон юрисдикционные системы, возможно, пожелают использовать Типовой закон в качестве образца для создания институционального механизма с международными партнерами, в том числе в рамках специального соглашения.

75. Главы соглашений о свободной торговле, посвященные электронной торговле, обычно содержат положения об электронных подписях или других формах электронной идентификации, которые зачастую именуется «методами аутентификации», и все чаще предусматривают требование относительно взаимного признания методов электронной идентификации. Более того, соглашения о цифровой экономике предусматривают модуль, специально разработанный для цифровых идентификационных данных и призванный создать условия для обеспечения трансграничной операционной совместимости. Принятие Типового закона может способствовать выполнению этих положений соглашений о свободной торговле и цифровой экономике.

II. Постатейные комментарии

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

1. Статья 1. Определения

76. Статья 1 содержит определения терминов, используемых в Типовом законе.

«Атрибут»

77. «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

²³ Нейтральность с точки зрения технологий и недискриминационный подход к иностранным подписям и услугам уже признаны основополагающими принципами формирующегося консенсуса относительно правовых механизмов трансграничного признания электронных подписей в документе «Содействие укреплению доверия к электронной торговле», п. 149.

являются, например, официальное наименование, адрес головного офиса, регистрационное наименование, юрисдикционная система регистрации. Понятие атрибута используется в определении идентификационных данных.

78. Атрибуты могут содержать персональные данные, обработка которых является объектом закона о конфиденциальности и защите данных. В Типовом законе 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»

79. Определение термина «сообщение данных» можно найти во всех существующих текстах ЮНСИТРАЛ об электронной торговле, где он используется для осуществления принципа технологической нейтральности (см. выше п. 44). 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»]

80. Термин «электронная идентификация» означает проверку связи между предполагаемой идентичностью физического или юридического лица 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.

81. Раскрытия имени физического лица или наименования юридического лица для выполнения требований к электронной идентификации может не потребоваться, если достаточно проверки других атрибутов. Такой подход согласуется с подходом, применявшимся в ранее принятых текстах ЮНСИТРАЛ, а именно в ТЗЭП, согласно которому «для целей определения «электронной подписи» в соответствии с Типовым законом, термин «идентификация» может толковаться более широко, чем простая идентификация подписавшего по его имени»²⁴.

82. 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.

«Идентификационные данные»

83. В основе понятия УИД лежит определение «идентификационных данных», в котором говорится о способности уникальным образом отличить физическое или юридическое лицо в определенном контексте. Таким образом, это понятие имеет контекстуальную привязку. Это определение основано на определении этого термина, содержащемся в положении 6.40 Рекомендации МСЭ-Т X.1252.

Ссылки

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

²⁴ Пояснительная записка к ТЗЭП, п. 117.

«Идентификационные учетные данные»

84. «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 eIDAS)²⁵.

Ссылки

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

«Услуги УИД»

85. 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

[A/CN.9/1005](#), пп. 84 и 109; [A/CN.9/1087](#), п. 19.

«Поставщик услуг УИД»

86. 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, могут иметь отношение ко всем системам УИД, и, следовательно, поставщик услуг УИД необязательно должен выполнять все перечисленные функции. Упоминание о существовании договоренности с абонентом напоминает о том, что поставщик услуг УИД несет ответственность за полный набор предоставляемых услуг, независимо от того, выполняются ли связанные с этим функции напрямую или через посредников.

Ссылки

[A/CN.9/971](#), п. 97; [A/CN.9/1005](#), п. 111; [A/CN.9/1045](#), п. 88, [A/CN.9/1087](#), п. 22.

«Система УИД»

87. 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 Х.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.

²⁵ Регламент (ЕС) № 910/2014 Европейского парламента и Совета от 23 июля 2014 года об электронной идентификации и удостоверительных услугах в отношении электронных операций на внутреннем рынке, отменяющий Директиву 1999/93/ЕС («Регламент eIDAS»).

Ссылки

[A/CN.9/1005](#), п. 112, [A/CN.9/1087](#), п. 19.

«Проверка идентификационных данных»

88. 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. Субъектом может являться физическое или юридическое лицо. Термин «проверка идентификационных данных» используется вместо термина «идентификация», чтобы снять обеспокоенность по поводу множественности значений термина «идентификация».

Ссылки

[A/CN.9/1005](#), п. 84.

«Полагающаяся сторона»

89. Термин «полагающаяся сторона» означает физическое или юридическое лицо, которое действует на основании результатов услуг УИД или удостоверительных услуг. Например, полагающаяся сторона является лицом, действующим на основании электронной подписи, а не на основании удостоверительной услуги, с помощью которой была создана электронная подпись. Это определение базируется на определении, содержащемся в статье 2(f) ТЗЭП.

Ссылки

[A/CN.9/1087](#), пп. 55 и 72.

«Абонент»

90. Термин «абонент» означает лицо, которому предоставляются услуги, и не включает в себя полагающихся сторон. Он предполагает наличие между поставщиком услуг и абонентом взаимоотношений, которые могут иметь договорной или иной характер (например, могут быть предписаны законом). 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; [A/CN.9/1087](#), п. 23.

«Удостоверительные услуги»

91. 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 Типовом законе. Благодаря принятию неисчерпывающих перечней общие положения об удостоверительных услугах можно будет применять к видам удостоверительных услуг, которые появятся в будущем.

92. 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»

93. 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 Типовом законе не определены функции, которые надлежит выполнять поставщикам удостоверительных услуг. Ссылка на наличие договоренности с абонентом напоминает о том, что поставщик удостоверительных услуг несет ответственность за весь комплекс предоставляемых услуг, независимо от того, выполняются ли связанные с ними функции напрямую или через посредство третьих сторон.

94. В Типовом законе 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

[A/CN.9/1087](#), п. 22.

2. Статья 2. Сфера применения

95. Положения статьи 2 ограничивают сферу применения Типового закона использованием и трансграничным признанием 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.

96. Поскольку использование системы УИД и удостоверительных услуг влечет за собой последствия, выходящие за рамки коммерческих сделок, принимающие Типовой закон юрисдикционные системы могут расширить его сферу применения, включив в нее все виды электронных сделок с участием бизнеса, правительства и потребителей.

97. 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 Типовом законе не устанавливаются никаких новых обязанностей по идентификации.

98. 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 регулирующие органы часто требуют использования определенной процедуры УИД или удостоверительной услуги, например идентификационных учетных данных, выданных тем или иным государственным ведомством.

99. Благодаря своему характеру документа, создающего благоприятные условия, Типовой закон, как и существующие законодательные тексты ЮНСИТРАЛ по электронной торговле, не влияет на применение к УИД и удостоверительным услугам другого законодательства, которое может регулировать такую 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 упоминается конкретно в силу 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; [A/CN.9/1087](#), п. 27.

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

100. В статье 3 указывается, что Типовой закон не навязывает использование УИД или удостоверительных услуг лицу, которое не давало согласие 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.

101. 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 не во всех случаях может совпадать с согласием на обработку личной информации в соответствии с законодательством о конфиденциальности и защите данных.

102. 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.

103. Более того, в статье 3 указывается, что Типовой закон не требует использования какой-либо конкретной услуги УИД или удостоверительной услуги, и тем самым осуществляется принцип технологической нейтральности, в том числе в отношении нейтральности моделей и систем.

104. Обязанность использовать УИД и удостоверительные услуги или конкретную услугу УИД или удостоверительную услугу может быть предусмотрена другими законами. Такая обязанность может быть установлена, например, для сделок с публичными учреждениями или сделок, связанных с соблюдением обязательств, установленных регулирующими органами.

Ссылки

[A/CN.9/965](#), пп. 22 и 110; [A/CN.9/1005](#), п. 116; [A/CN.9/1045](#), п. 79; [A/CN.9/1087](#), п. 28.

4. Статья 4. Толкование

105. 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).

106. Пункт 1 призван содействовать единообразному толкованию во всех принимающих Типовой закон юрисдикционных системах, и для этого в нем обращается внимание судей и других органов, выносящих решения, на то, что внутренние законодательные акты, вводящие в действие положения Типового закона, следует толковать с учетом их международного происхождения и необходимости единообразного применения. Поэтому лицам, выносящим решения (адьюдикаторам), рекомендуется при рассмотрении дел учитывать решения, вынесенные в иностранных юрисдикционных системах, с тем чтобы способствовать упрочению транснациональных тенденций к единообразному толкованию.

107. Пункт 2 призван обеспечивать единообразие в толковании и применении законодательных актов, принимаемых на основе Типового закона, и с этой целью в нем требуется решать все вопросы, которые напрямую в нем не разрешены, не в соответствии с принципами внутреннего права, а согласно общим принципам, лежащим в основе Типового закона.

108. Как и в других законодательных текстах ЮНСИТРАЛ об электронной торговле, в Типовом законе напрямую не указываются лежащие в его основе общие принципы. Законодательные тексты ЮНСИТРАЛ об электронной торговле основаны, как правило, на принципах недопустимости дискриминации в отношении использования электронных средств, а также технологической нейтральности, функциональной эквивалентности и автономии сторон, которые также указаны как важные принципы для Типового закона с некоторыми оговорками (см. выше пп. 41–45). Например, автономия сторон является одним из основополагающих принципов коммерческого права, однако он применяется в пределах, установленных императивными нормами права, в том числе положениями Типового закона, от которых стороны не могут отступать. Кроме того, как было отмечено (п. 46 выше), принцип функциональной эквивалентности может оказаться неприменимым, если не предусмотрены требования в отношении офлайн-эквивалента.

Ссылки

[A/CN.9/936](#), пп. 67 и 72; [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

109. 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 ней применяется общий принцип недискриминации в отношении использования электронных средств в сфере УИД. Этот принцип применяется независимо от существования офлайн-эквивалента.

110. Статья 5 запрещает дискриминацию в отношении электронной идентификации как результата процесса УИД. В ее названии говорится не о «дискриминации», а о «юридическом признании», чтобы сохранить единообразие с названием соответствующих положений в существующих текстах ЮНСИТРАЛ.

111. 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.

112. 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 Типового закона.

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

113. 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. Слова «как минимум» во вступительной формулировке в статье 6 указывают на то, что поставщик услуг УИД не может отступать от выполнения этих основных обязанностей и что он по-прежнему несет ответственность перед абонентами и полагающимися сторонами также в том случае, если он пользуется услугами подрядчиков для предоставления своих услуг. Невыполнение этих обязанностей может привести к привлечению к ответственности в соответствии со статьей 12 и отрицательно сказаться на надежности услуги УИД, даже если она является назначенной услугой.

114. Обязанности, перечисленные в статье 6, 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.

115. 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. Соответственно, слова «как минимум» в подпункте (a) указывают на то, что поставщик услуг УИД обязан иметь разработанные правила, принципы и практику в отношении требований к выполнению перечисленных функций. Статья 6 не запрещает поставщику услуг УИД передавать какую-либо функцию на подряд или распределять риски среди своих подрядчиков или других деловых партнеров.

116. Принцип, согласно которому поставщик услуг должен действовать в соответствии со своими заверениями и обязательствами, уже 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».

117. 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 исходя из устройства системы УИД и типа предоставляемых услуг

УИД. Эта гибкость подхода к устройству системы УИД отражена в формулировке «соответствующие назначению и устройству».

118. 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. Эти правила, служащие руководством по выполнению операций, разрабатываются на основе принципов, применяющихся 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 предоставлять абонентам и третьим сторонам доступ к информации об операционных правилах, принципах и практике. Положение о свободном доступе, содержащееся также в пункте (e), призвано упростить доступ к информации для таких сторон, как микро- или малые предприятия, которые могут быть в меньшей степени знакомы с техническими аспектами.

119. В пункте (e) перечислены обязанности, которые поставщики услуг УИД должны выполнять, чтобы ограничить свою ответственность перед полагающимися сторонами, и он тем самым дополняет положения статьи 12. Такой механизм призван предотвратить возникновение трудностей, связанных с требованием проведения предварительной идентификации всех возможных полагающихся сторон.

120. Аналогичным образом, пункт (f) дополняет положения статьи 8, поскольку в нем устанавливаются обязанности поставщика услуг УИД в отношении уведомления о нарушениях безопасности абонентом.

Ссылки

[A/CN.9/936](#), п. 69; [A/CN.9/1045](#), пп. 85–95; [A/CN.9/1087](#), пп. 30–33, 55 и 61.

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

121. 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.

122. 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 также содержаться в законе о конфиденциальности и защите данных.

123. Понятие «серьезное воздействие» используется в региональных²⁶ и национальных законах. При оценке воздействия может учитываться целый ряд факторов. Оценить серьезность воздействия можно с помощью 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 органы, ответственные за конфиденциальность и защиту данных, могут предоставлять технические инструкции по информированию об инцидентах, а также ежегодные отчеты об инцидентах в сфере безопасности.

²⁶ Статья 19(2) Регламента eIDAS.

124. 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.

125. 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 удостоверяемым услугам.

126. 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.

127. 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 других законах, а именно в законе о конфиденциальности и защите данных, в договорных соглашениях и в операционных правилах, принципах и практике поставщика услуг УИД. В этом случае все перечисленные действия, а не только уведомление, должны выполняться в соответствии с действующим законом о конфиденциальности и защите данных.

Ссылки

[A/CN.9/971](#), пп. 84–87; [A/CN.9/1005](#), пп. 32–36 и 94; [A/CN.9/1045](#), пп. 96–101; [A/CN.9/1087](#), п. 35.

4. Статья 8. Обязанности абонентов

128. 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(f)) и реагированию на нарушения безопасности или утрату целостности (статья 7).

129. 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 у поставщика услуг УИД появляются определенные обязанности в случае компрометации данных, которым является нарушение безопасности или целостности данных и которое оказывает серьезное воздействие на услугу УИД. Невыполнение абонентом своих обязанностей согласно статье 8 необязательно освобождает поставщика услуг УИД от ответственности.

130. 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.

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

132. 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 и которая призвана обеспечить, что к абонентам не будут предъявляться 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.

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; [A/CN.9/1087](#), пп. 36–37.

5. Статья 9. Идентификация лица с помощью систем УИД

133. В текстах ЮНСИТРАЛ по электронной торговле правилами функциональной эквивалентности устанавливаются требования, которым должны соответствовать электронные записи, методы или процесс, чтобы удовлетворять тому или иному юридическому требованию, действующему отношении бумажных документов. 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 определение условий для признания эквивалентности идентификации в онлайн-ом и офлайн-ом режимах, статья 9 применяется только в том случае, если существует эквивалент офлайн-ой идентификации. Тем не менее статья 9 является одним из основных положений, устанавливающих правовой режим УИД.

134. Метод, используемый для выполнения правила, установленного в статье 9, должен соответствовать положениям пункта 1 статьи 10, т. е. быть надежным для цели, для которой используется услуга УИД, или проверенным на практике в части способности выполнять функцию, для которой он используется.

135. В соответствии с установленными в текстах ЮНСИТРАЛ принципами 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-ого эквивалента идентификации, тогда как предметом рассмотрения статьи 9 является электронная идентификация как функциональный эквивалент офлайн-ой идентификации, и поэтому статья 9 может применяться только при наличии бумажного эквивалента.

136. В статье 9 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.

137. 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. 98 выше).

138. 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.

139. Статьи 9 и 16–21 Типового закона 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 допускает определенные действия и предусматривает правовые последствия в их отношении.

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; [A/CN.9/1087](#), п. 38.

6. Статья 10. Требования к надежности услуг УИД

140. 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*). В ней говорится о методе, используемом для предоставления услуги УИД, а не о методе, используемом для целей системы УИД, поскольку одна система УИД может поддерживать предоставление нескольких услуг УИД, для которых используются методы с разными уровнями доверия.

141. 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.

142. 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.

143. Типовой закон в целом требует избрания надежных методов, и пункт 1(b) не преследует цели способствовать использованию ненадежных методов или признавать законным их использование. Скорее, в нем признается, что с технической точки зрения функция (в случае статьи 9 — идентификация) и надежность являются двумя независимыми атрибутами, и поясняется, что согласно Типовому закону идентификация может быть осуществлена фактически или с помощью надежного метода. Другими словами, достижение цели идентификации на практике снимает необходимость подтверждения надежности использованного метода.

144. 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.

145. 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 подписи²⁷.

146. В соответствии с пунктом 4 назначение надежной услуги УИД на основании статьи 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.

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

а) Система уровней доверия

148. В статьях 10 и 11 используется понятие «уровень доверия» или говорится об аналогичных системах, названных иначе. Система уровней 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 Типовом законе уровни доверия не определяются и не содержатся требования, обязывающего их определять или использовать.

149. 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.

150. Системы уровней доверия могут быть использованы для удовлетворения потребностей рынка в руководящих принципах в отношении степени надежности предлагаемой услуги УИД. Поставщик услуг УИД, не включающий в свои операционные правила, принципы и практику ссылку на уровни доверия, скорее всего, будет рассматриваться как предлагающий услуги с самым низким уровнем доверия. Вместе с тем общепринятое на глобальном уровне определение системы уровней доверия пока не согласовано, и возможно придется использовать разные национальные или региональные определения.

151. 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 к необходимому уровню доверия. В случае, если услуга УИД отвечает требованиям, относящимся к этому уровню доверия, эта услуга УИД может быть использована для соответствующего конкретного вида операции.

²⁷ Обсуждение взаимосвязи между статьями 12(1) и 12(2) ТЗЭП см. в документе [A/CN.9/483](#), пп. 28–36.

b) Сертификация и надзор

152. 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.

153. 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.

154. 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.

155. Существуют разные подходы к участию государственных органов в сертификации и надзоре, и выбор того или иного подхода является политическим решением принимающей Типовой закон юрисдикционной системы. Когда государственные учреждения одновременно осуществляют сертификацию и надзор и являются поставщиками услуг УИД, сертификационные и надзорные функции могут быть отделены от предоставления услуг УИД.

156. Согласно Типовому закону создание надзорного режима не требуется и не упрощается. Используемый в Типовом законе подход основан на принципе нейтральности модели, а ссылки на сертификацию и надзор не исключают применение режимов самосертификации.

157. 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, органа для проведения оценки и органа, отвечающего 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.9/1087](#), пп. 42–46 и 105–106; [A/CN.9/WG.IV/WP.153](#), пп. 74–75.

7. Статья 11. Назначение надежных услуг УИД

158. Статья 11 дополняет статью 10, предлагая возможность назначения услуг УИД. Точнее, в ней перечислены условия, которым должна соответствовать услуга УИД, чтобы ее можно было включить в список назначенных услуг УИД. Аналогично статье 10 в статье 11 говорится о методе, используемом для предоставления той или иной услуги УИД, а не о методе, используемом для целей системы УИД, поскольку одна система УИД может поддерживать предоставление нескольких услуг УИД с разными уровнями надежности и, следовательно, может быть или может не быть назначенной.

159. Назначение систем 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.

160. Распространение информации о назначенных услугах УИД имеет важнейшее значение, поскольку потенциальные подписчики должны знать об их существовании. Назначающий орган обязан публиковать перечень назначенных услуг УИД, включая сведения о поставщике услуг УИД, например, на своем веб-сайте. Важность перечней для обеспечения прозрачности назначения услуг УИД, в том числе в трансграничном контексте, признается также в широко используемых технических стандартах. Для информирования общественности о назначенных услугах УИД могут быть использованы и другие методы, однако эти методы должны дополнять, а не заменять публикацию перечня.

161. 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*.

162. Как и в статье 10(3), в пункте 4 указано, что место предоставления услуги УИД и местонахождение коммерческого предприятия поставщика услуг УИД сами по себе не имеют значения для назначения надежной услуги. Пункт 4 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 Типовой закон юрисдикционной системе о назначении услуги УИД.

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; [A/CN.9/1087](#), пп. 47–49.

8. Статья 12. Ответственность поставщиков услуг УИД

163. Как уже отмечалось (см. п. 68 выше), в статье 12 устанавливается единый режим ответственности поставщиков услуг УИД, основанный на принципе, согласно которому поставщик услуг УИД должен нести ответственность за последствия непредоставления услуг абонентам и полагающимся сторонам. Цель статьи заключается в том, чтобы признать, что поставщик услуг может нести ответственность за невыполнение своих обязанностей согласно Типовому закону 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.

164. 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 Типовым законом; 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.

165. Согласно статье 12 эта ответственность установлена законом и как таковая существует наряду с договорной и внедоговорной ответственностью. Соответственно, статья 12, как указано в пункте 2(а), не затрагивает действие положений о договорной и внедоговорной ответственности, относящихся к поставщикам услуг ИДМ и содержащихся во внутреннем законодательстве.

166. 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.

167. 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.

168. В статье 12 признается возможность ограничения ответственности при определенных условиях. Ограничения ответственности могут быть необходимы в том числе для ограничения размера стоимости страхования и, как правило, отражаются в операционных правилах, принципах и практике поставщика услуг. В статье 12 также признается практика ограничения поставщиками услуг УИД своей ответственности по-разному, в зависимости от стороны (т. е. абонента или полагающейся стороны) и вида услуги (например, высокой или низкой стоимости сделки). Она не затрагивает право поставщика УИД руководствоваться другими законами для придания силы ограничению ответственности, если это не противоречит его обязательствам в соответствии с Типовым законом, включая обязательства, имеющие отношение к ограничению ответственности.

169. Пункт 3 допускает ограничение ответственности поставщика услуг УИД в отношении абонента при двух условиях. Во-первых, если использование услуги УИД выходит за ограничение в отношении цели или стоимости операции и объема ответственности, применимое к операции, для которой используется услуга УИД. Во-вторых, если ограничения оговорены в соглашении между поставщиком услуг УИД и абонентом. Согласно определению «абонента» ссылка на «соглашение» призвана охватить все виды отношений между поставщиком услуг УИД и абонентом, будь то договорного или иного характера.

170. Аналогичным образом, пункт 4 позволяет поставщику услуг УИД ограничить ответственность перед полагающейся стороной при двух условиях. Во-первых, если использование услуги УИД выходит за ограничение в отношении цели или стоимости операции или объема ответственности, применимое к операции, в отношении которой используется услуга УИД. Во-вторых, если поставщик услуг УИД выполнил свои обязанности, предусмотренные статьей 6(е), в отношении предоставления полагающимся сторонам легко доступных средств для получения информации об ограничениях в отношении конкретной операции.

171. В статье 12 рассматривается только ответственность поставщиков услуг УИД перед абонентами и полагающимися сторонами. Если в результате использования услуг УИД убытки понесла другая 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.

172. Статья 12 применяется к поставщикам услуг УИД независимо от того, являются ли они государственными или частными субъектами. В принимающей Типовой закон 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; [A.CN.9/1087](#), пп. 52–73.

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

1. Статья 13. Юридическое признание удостоверительных услуг

173. 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.

174. Статья 13 применяется к удостоверительным услугам независимо от того, перечислены ли они в Типовом законе, 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

175. 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. Аналогично статье 7(1) все обязанности, перечисленные в статье 14(2), должны выполняться в соответствии с применимым законодательством, если таковое существует.

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

177. 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 (статья 3(1)).

178. В подпункте 1(e) устанавливается механизм информирования полагающихся сторон об ограничениях в отношении цели или стоимости, для которой может использоваться удостоверительная услуга, а также об ограничениях в отношении охвата и объема ответственности, аналогичный механизму, предусмотряемому в статье 6(e) и дополняющему статью 24.

179. В пункте 2 устанавливаются обязанности поставщиков удостоверительных услуг в случае компрометации данных. Предварительным условием в нем является нарушение безопасности или целостности данных, которое оказывает серьезное воздействие на услугу УИД.

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; [A/CN.9/1087](#), пп. 74–76.

3. Статья 15. Обязанности абонентов

180. В статье 15 устанавливаются обязанности абонентов в том случае, если удостоверительная услуга была скомпрометирована. Понятие «скомпрометированная удостоверительная услуга», лежащее в основе этой статьи, относится к случаям несанкционированного доступа к удостоверительной услуге и предполагает наступление события, подрывающего надежность удостоверительной услуги.

181. В статье 15 признается, что абонент вряд ли сразу будет знать о проблемах, создающих угрозу для удостоверительной услуги в целом, но ему может быть известно, что видимая информация была скомпрометирована, а также ему может быть известно о рисках, связанных с информацией, которую абонент непосредственно не видит, например, с закрытым ключом. Именно поэтому в пунктах (а) и (b) рассматриваются два разных объекта.

182. 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 операционным правилам, принципам и практике поставщика удостоверительных услуг.

183. В Типовом законе не указываются дополнительные обязанности абонентов в отношении использования удостоверительной услуги. Пример таких обязанностей можно найти в статье 8(1)(а) и (с) ТЗЭП.

184. В Типовом законе 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.

185. В отличие от статьи 11 ТЗЭП, в статье 15 не устанавливаются обязанности для полагающихся 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; [A/CN.9/1087](#), пп. 77–78.

4. Статья 16. Электронные подписи

186. 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 лица²⁸. В основу статьи 16 положена формулировка статьи 9 ТЗЭПЗ, в которой, в свою очередь, учтена формулировка статьи 9(3) КЭС и устанавливаются требования в отношении функциональной эквивалентности между рукописными и электронными подписями. Следовательно, термин «идентификация» в статье 16 следует толковать в соответствии с устоявшимся значением этого термина в аналогичных положениях ЮНСИТРАЛ и в обеспечивающих их принятие законодательных актах.

187. Требование наличия подписи на бумажном документе выполняется, если используется метод идентификации подписавшего сообщения данных и указания намерения подписавшего в отношении подписанного сообщения данных. Ссылка на использование метода «в отношении информации, содержащейся в

²⁸ См. также в целом документ «Содействие укреплению доверия к электронной торговле».

сообщении данных» относится как к идентификации лица, так и к указанию намерения этого лица.

188. 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. Цели и методы электронных подписей подробно обсуждались в принятых ранее текстах ЮНСИТРАЛ²⁹.

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; [A/CN.9/1087](#), пп. 82–84.

5. Статья 17. Электронные печати

189. 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, для обеспечения целостности 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.

190. 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).

191. 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.

192. 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.

193. 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.

²⁹ ТЗЭП, *Руководство по принятию*, пп. 29–62; «Содействие укреплению доверия», пп. 24–66.

Целостность

194. 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; [A/CN.9/1087](#), пп. 85–86.

6. Статья 18. Электронные отметки времени

195. 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.

196. 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).

197. 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

198. В статье 19 рассматриваются услуги электронного архивирования, обеспечивающие 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).

199. При разработке статьи 19 учитывались, в частности, положения статьи 10 ТЗЭТ, посвященной сохранению сообщений данных. При этом в статье 10 ТЗЭТ говорится о «сохранении» сообщений данных, поскольку речь идет о выполнении юридического требования хранить документы в бумажном виде, а в статье 19 говорится об «архивировании», поскольку имеется в виду удостоверительная услуга, предоставляемая для удовлетворения этого требования (т. е. электронного архивирования).

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

201. 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 пункте (с) учитываются перенос файлов и изменение формата, которые являются частью обычной практики хранения данных. Его формулировка основана на статье 8(3)(а) ТЗЭТ.

202. 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

203. 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.

204. 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.

205. 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

206. 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.

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

208. Термин «держатель доменного имени» означает лиц, которым регистратор доменных имен передал право или выдал лицензию на использование доменного имени. Такое лицо необязательно должно быть «владельцем» сайта, поставщиком информации или оператором.

209. 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

210. В статье 22 содержится неисчерпывающий 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.

211. Подобно понятию надежного метода, используемого для услуг УИД (см. выше п. 141), 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

212. В ТЗЭП и ряде региональных и национальных законов об электронных подписях проводятся различия между удостоверительными услугами исходя из степени надежности, которую они обеспечивают. Такие законы, в частности, придают более весомую 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 Типовом законе не используется, и удостоверительные услуги могут быть назначены независимо от того, какой уровень надежности они обеспечивают.

213. Поскольку идентификационные учетные 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; [A/CN.9/1087](#), пп. 87 и 105–106.

11. Статья 23. Назначение надежных удостоверительных услуг

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

215. В статье 23 рассматривается главным образом назначение удостоверительных услуг при том понимании, что процесс назначения удостоверительных услуг неизбежно сопряжен с оценкой таких методов. Аналогично назначению услуг УИД, если речь идет о назначении удостоверительных услуг, для предоставления которых, как считается, используются надежные методы, то имеется в виду не общая категория удостоверительных услуг и не все удостоверительные услуги,

предлагаемые тем или иным конкретным поставщиком, а конкретная удостоверительная услуга, предоставляемая идентифицированным поставщиком услуг.

216. 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 *ex post*.

217. 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 Типовой закон юрисдикционные системы, возможно, пожелают рассмотреть способы агрегирования данных этих списков, чтобы эта 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

218. В качестве общего принципа поставщики удостоверительных услуг должны нести ответственность за последствия непредоставления услуг в соответствии с соглашением или согласно другим требованиям законодательства. Степень такой ответственности будет определяться с учетом нескольких факторов и в том числе вида предоставляемой удостоверительной услуги.

219. Положения статьи 24 составлены по аналогии с положениями статьи 12 об ответственности поставщиков услуг УИД, и следовательно, соображения, имеющие отношение к статье 12, могут также относиться и к статье 24. В частности, в статье 24, как и в статье 12, закрепляется законодательная основа ответственности, которая действует наряду с договорной и внедоговорной ответственностью, и действие положений внутреннего права о договорной и внедоговорной ответственности, относящихся к поставщикам удостоверительных услуг, не затрагивается положениями статьи 24, как указано в пункте 2(а).

220. В некоторых случаях идентификация поставщика удостоверительных услуг может быть затруднена или невозможна (например, в случае использования услуг по проставлению отметки времени 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.

221. Если обращаться 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 ответственности³⁰.

³⁰ См. рассмотрение конкретных примеров наступления ответственности в рамках инфраструктуры публичных ключей в документе «Содействие укреплению доверия к электронной торговле», пп. 211–232.

Ссылки

[A/CN.9/1005](#), пп. 74–76; [A/CN.9/1045](#), пп. 62–66; [A/CN.9/1087](#), п. 89.

D. Глава IV. Международные аспекты (статьи 25–27)**1. Статья 25. Трансграничное признание электронной идентификации**

222. В статье 25 устанавливается механизм трансграничного юридического признания электронной идентификации, призванная предоставить одинаковый правовой режим местным и иностранным системам УИД, услугам УИД и идентификационным учетным данным. В ее основе лежит принцип недискриминации по географическому признаку, и основное внимание в ней сосредоточено на электронной идентификации как результате использования систем УИД, услуг УИД и идентификационных учетных данных.

223. Одна из целей статьи 25 заключается в том, чтобы частично снять необходимость подачи поставщиками услуг заявок на получение статуса назначенных в соответствии со статьей 23 в нескольких юрисдикционных системах. 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.

224. Определения уровней надежности в разных юрисдикционных системах могут не совпадать в точности. В отсутствие общепринятых определений конкретных уровней надежности случаи такого несовпадения вполне могут возникать. С целью устранить трудности, связанные с трансграничным признанием и обусловленные таким несовпадением, в статье 25 используется формулировка «по меньшей мере эквивалентный уровень надежности», под которой подразумеваются такие же или более высокие уровни надежности по сравнению с требуемым уровнем. Эту формулировку не следует толковать как требующую соблюдения строгих технических требований, что может привести к возникновению препятствий на пути взаимного признания и, в конечном итоге, затруднить торговлю.

225. Ссылка на «систему УИД, услугу УИД или идентификационные учетные данные, в зависимости от обстоятельств» призвана охватить все возможные аспекты, имеющие значение для трансграничного признания электронной идентификации. На практике, возможно, будет сочтено предпочтительным сосредоточивать внимание на конкретной услуге УИД, чтобы избежать признания всех услуг УИД, поддерживаемых одной 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, которые хотя и остались неизменными, но были выданы с помощью услуги УИД, которая была скомпрометирована.

226. Для признания иностранных систем, услуг УИД и идентификационных учетных данных поставщику услуг может потребоваться изменить свои условия предоставления услуг. Например, применимое законодательство в признающей юрисдикционной системе может ограничивать право поставщика услуг на ограничение своей ответственности.

227. В пункте 3 дополнительно разъясняется, каким образом назначающие органы могут назначать иностранные системы УИД и удостоверительные услуги. В нем более подробно рассматривается механизм, предусмотренный в статье 11(4), в которой предусматривается недопущение дискриминации по географическому признаку в процессе назначения за счет предоставления назначающему органу принимающей Типовой закон юрисдикционной системы возможности полагаться на назначение, сделанное иностранным назначающим

органом, и включения в нее систем УИД и учетных данных в качестве возможных объектов назначения. Следовательно, в пункте 3 применяется подход *ex ante*.

228. При определении эквивалентности компетентному органу следует принимать во внимание перечень обстоятельств, имеющих значение для определения надежности методов, используемых для предоставления услуг УИД, приведенный в статье 10(2) с целью обеспечить согласованность процедур определения надежности.

229. Определение надежности услуги УИД, системы УИД или идентификационных учетных данных отнимает много времени и ресурсов, и не все юрисдикционные системы могут располагать достаточными для этого ресурсами. Поэтому возможность признания иностранных услуг УИД и идентификационных учетных данных исходя из иностранных определений и информации о назначении могла бы иметь особое значение для таких юрисдикционных систем, которые располагают незначительными ресурсами. Положения пункта 3 позволяют создавать механизмы, способные также заменить договоренности, основанные на заключенных надзорными органами специальных соглашениях о взаимном признании.

230. При принятии нормативных актов для обеспечения применения Типового закона принимающая юрисдикционная система может решить, будет ли пункт 3 обеспечивать автоматическое признание (например, услуги УИД, 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, 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).

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; [A/CN.9/1087](#), пп. 90–101.

2. Статья 26. Трансграничное признание результата использования удостоверительных услуг

231. В статье 26 предусматривается механизм трансграничного признания результата использования удостоверительных услуг аналогичный механизму, установленному в статье 25 для электронной идентификации. Соответственно, соображения в отношении статьи 25 могут иметь отношение и к статье 26.

232. Статья 26 в целом совместима с использованием существующих механизмов трансграничного признания результата использования удостоверительных услуг, такими как перекрестное признание и перекрестная сертификация в инфраструктурах публичных ключей³¹.

Ссылки

[A/CN.9/1087](#), пп. 90–101.

3. Статья 27. Сотрудничество

233. Достижению взаимного юридического признания и технической совместимости систем УИД и удостоверительных услуг в значительной мере могут 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

³¹ Более подробно о перекрестном признании и перекрестной сертификации см. «Содействие укреплению доверия к электронной торговле», пп. 163–172.

успешными видами практики, в частности, в отношении технических требований, включая уровни доверия и уровни надежности.

234. Более того, статья 27 может способствовать согласованию общих определений технических стандартов, включая уровни доверия и уровни надежности, которые поддерживают определение эквивалентности. В деловой практике понятия уровня доверия и уровня надежности используются как своего рода термины для оценки УИД и удостоверительных услуг, соответственно. Из-за трудностей согласования общепринятых на глобальном уровне определений в Типовом законе не устанавливается общая система уровней доверия для систем УИД или 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.

235. Сотрудничество должно осуществляться на добровольной основе и в соответствии с применимыми национальными законами и нормативными положениями. Ссылка на «иностранная организации» призвана охватить все организации, независимо от их юридического статуса, которые могут способствовать достижению поставленных целей.

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/WR.153](#), пп. 95–98; [A/CN.9/1087](#), пп. 108–109.