Организация Объединенных Наций A/CN.9/WG.IV/WP.141

Генеральная Ассамблея

Distr.: Limited
30 January 2017

Original: Russian

Комиссия Организации Объединенных Наций по праву международной торговли
Рабочая группа IV (Электронная торговля)
Пятьдесят пятая сессия
Нью-Йорк, 24-28 апреля 2017 года

Правовые вопросы, связанные с управлением идентификационными данными и удостоверительными услугами

Записка Секретариата

Российская Федерация представила Секретариату документ для рассмотрения на пятьдесят пятой сессии Рабочей группы. Текст, полученный Секретариатом, воспроизводится в качестве приложения к настоящей записке.

V.17-00122 (R) 080217 090217

Приложение

Предложение Российской Федерации

Совершенствование системы управления идентификационными данными при использовании трансграничного пространства доверия и общей инфраструктуры доверия применительно к трансграничным электронным коммерческим сделкам

Введение

Двадцать четвертого мая 2016 года в ходе семьдесят второй сессии Экономической и социальной комиссии для Азии и Тихого океана (ЭСКАТО) было принято Рамочное соглашение об упрощении процедур трансграничной торговли в АТР.

Целью данного Рамочного соглашения является «… содействие развитию безбумажной трансграничной торговли посредством создания условий для взаимного признания документов и данных о торговле в электронной форме и обмена ими, а также посредством содействия повышению операционной совместимости национальных и субрегиональных систем «единого окна» и/или других систем безбумажной торговли в целях повышения эффективности и транспарентности международных торговых сделок и обеспечения более строгого соблюдения нормативных требований».

Статья 5 вышеназванного Рамочного соглашения одним из принципов обозначает «совершенствование трансграничного пространства доверия» (пункт 1 (g)).

Представляемый документ ставит перед собой цель продолжить работу по совершенствованию трансграничного пространства доверия в области электронной торговли, что является важным пунктом повестки дня для ЭСКАТО и Комиссии Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ).

Данный документ (A/CN.9/WG.III/WP.136) уже был представлен на рассмотрение Рабочей группы III ЮНСИТРАЛ по урегулированию споров в режиме онлайн на тридцать второй сессии, проходившей в Вене 30 ноября – 4 декабря 2015 года. По рекомендации участников Рабочей группы, документ был передан на рассмотрение IV Рабочей группы по электронной торговле в связи с его соответствием повестке для данной Рабочей группы. Основное внимание уделяется техническому, организационному и правовому механизмам укрепления трансграничного пространства доверия при ведении электронной торговли в регионе АТР. В ходе собрания пятьдесят третьей сессии Рабочей группы IV ЮНСИТРАЛ по электронной торговле делегация Российской Федерации заявила о намерении представить на рассмотрение Рабочей группы на следующей сессии предложение по теме управления идентификационными данными при условии, что Комиссия подтвердит включение этой темы в повестку дня следующей сессии Рабочей группы. Делегациям было предложено представить информационные материалы по вопросам управления идентификационными данными для содействия рассмотрению этой темы.

Проблема обеспечения безопасности трансграничного обмена электронными документами является весьма актуальной и отмечается в глобальных и региональных заявлениях, а именно:

- содействие исследованиям и сотрудничеству, делающим возможным эффективное и безопасное использование данных и программного обеспечения, в частности электронных документов и операций, включая электронные средства удостоверения подлинности, и совершенствование методов обеспечения безопасности (разработанная ВВУИО+10 концепция ВВУИО на период после 2015 года. С5. Укрепление доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ), пункт (f));

- содействие укреплению уверенности и доверия в электронной среде в глобальном масштабе путем поощрения использования защищенных трансграничных потоков информации, включая электронные документы, и усилиям по расширению и укреплению Азиатско-тихоокеанской информационной инфраструктуры и укреплению доверия и безопасности при использовании ИКТ (Декларация лидеров участниц АТЭС 2012 года, Владивостокская декларация: Интеграция – чтобы расти, инновации – чтобы процветать).

В настоящее время в мире существует несколько успешных методов решения такой задачи:

- в Европейской комиссии – на основании Постановления Европейского парламента и Совета ЕС об оказании электронных услуг по идентификации и обеспечению надежности электронных операций на внутреннем рынке (проект – eIDAS[1]);

- в Евразийском экономическом союзе – на основании Договора о Евразийском экономическом союзе и Концепции использования услуг и юридически значимых электронных документов при межгосударственном информационном взаимодействии[2];

- в Азиатско-Тихоокеанском регионе – на основе Паназиатского альянса за развитие электронной торговли (ПАА)[3].

Потребности, связанные с развитием глобальной экономики, особенно в кризисные периоды, требуют активизации интеграционных процессов в различных экономических и социальных областях, в том числе путем использования современных ИКТ-технологий, основанных на инновациях.

Одной из главных проблем, встающих при рассмотрении вопросов трансграничной торговли, является безопасность и конфиденциальность передаваемой посредством сети Интернет информации. Для решения данной проблемы используется система управления идентификационными данными (Identity Management – IdM). IdM – это набор функций и возможностей (например, администрирование, управление и техническое обслуживание, обнаружение, обмен сообщениями, сопоставление и увязка, обеспечение реализации политики, аутентификация и утверждение), используемых для:

• гарантирования информации, подтверждающей идентичность (например, идентификаторов, регистрационных данных, атрибутов);

[1] http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond.

[2] www.eurasiancommission.org/docs/Download.aspx?IsDlg=0&print=1&ID=5713.

[3] www.paa.net/.

- гарантирования идентичности объекта (например, пользователей/абонентов, групп, устройств пользователей, организаций, поставщиков доступа к сети и поставщиков услуг, сетевых элементов и объектов, а также виртуальных объектов);
- обеспечения коммерческих приложений и приложений безопасности[4].

Целями IdM являются:

- управление доступом (технические средства должны быть доступны только зарегистрированным пользователям и для целей, которые определяются владельцами);
- конфиденциальность доступа;
- целостность системы IdM.
- для достижения данных целей перед системой IdM ставятся следующие задачи:
- обеспечение необходимой производительности системы с заложенными показателями отказоустойчивости;
- обеспечение функционала управления идентификационными данными (создание, изменение, заморозка, архивация или удаление идентификационной информации);
- обеспечение защиты идентификационных данных;
- обеспечение использования безопасных механизмов идентификации и аутентификации (электронная подпись, двухуровневая парольная защита, биометрическая аутентификация и пр.);
- обеспечение операционной совместимости используемых решений обеспечения безопасности;
- обеспечение целостности системы IdM и идентификационной информации.

Выделяют две модели систем IdM: ориентированную на приложения, и ориентированную на пользователя[5].

В крупномасштабных системах IdM ориентированная на приложения система IdM означает, что услуги и стратегии определения идентичности предназначены для удовлетворения потребностей поставщиков идентификационных данных и оптимизированы в отношении требований со стороны приложений, например предоставления учетной информации пользователей. В системе IdM, ориентированной на приложения, имеются оператор идентификационных данных и пользовательская сторона. При предоставлении пользователю услуги идентификации между этими двумя объектами, как правило, происходит обмен информацией об идентичности. Под идентичностью следует понимать представление какого-либо объекта в виде одного или нескольких атрибутов, которые позволяют однозначно распознать объект или объекты в каком-либо контексте в той мере, в какой это необходимо. В целях управления определением идентичности (IdM) термин «идентичность» толкуется как контекстуальная идентичность (подмножество атрибутов), т.е. разнообразие атрибутов ограничивается рамками с определенными граничными условиями (контекстом), в которых объект существует и взаимодействует. Исторически сложилось так,

[4] https://www.itu.int/rec/T-REC-X.1252-201004-I/en.
[5] https://www.itu.int/rec/T-REC-X.1253-201109-I/en.

что технологии идентификации и управления доступом к идентификационной информации были ориентированы главным образом на аутентификацию конечных пользователей для обеспечения федеративного доступа к приложениям и услугам (под федеративным доступом понимается использование такой модели доступа, при которой существует множество провайдеров данных идентичности, которые могут быть доверенными для пользователя и при необходимости управлять частичной информацией об идентичности пользователей. Информация об идентичности пользователей каждого провайдера данных идентичности может использоваться на коллективной основе). Поэтому требование обеспечения безопасности ограничивается рамками домена конкретного приложения.

Основное внимание в ориентированной на пользователя системе IdM направлено главным образом на конечных пользователей, и система оптимизирована с учетом их потребностей. Это означает, что основной целью системы IdM является обеспечение предоставления пользователям удобных и комплексных услуг определения идентичности. Главная особенность системы заключается в предоставлении пользователю полного контроля над его идентификационными данными. Идентификационная информация пользователя, в случае ее распространения, должна проходить через пользователя, с тем чтобы дать ему возможность применения при необходимости определенной персональной политики, например выбора персональных предпочтений в отношении конфиденциальности или персональной авторизации. В системе IdM, ориентированной на пользователя, в вычислительную среду пользователя должна быть включена клиентская программа, взаимодействующая с сервером IdM для поиска информации об идентичности. Вследствие этого необходимы простые и всеобъемлющие руководящие указания по обеспечению безопасности, которые помогут пользователю безопасно установить и развернуть любое соответствующее программное средство. Программное обеспечение должно контролировать определенную информацию пользователя, связанную с безопасностью. Модель, в центре которой находится пользователь, отличается от других моделей IdM акцентом на то, что конкретный пользователь, а не какой-либо орган сохраняет контроль над тем, каким образом создаются, распространяются, обновляются и прекращают действие атрибуты идентичности пользователя. Это означает, что пользователь обладает всеми полномочиями в течение жизненного цикла своей идентификационной информации. Уровень контроля может определяться требованиями к обеспечению конфиденциальности пользователя.

В рамках Международного союза электросвязи (МСЭ) и его Сектора стандартизации электросвязи (МСЭ-Т) вопросы IdM начали рассматриваться в 2006 году, в котором была создана Фокусная группа (ФГ) по IdM при Исследовательской комиссии (ИК) 17 МСЭ-Т, которая занимается вопросами безопасности в области электросвязи/ИКТ. Задачей данной ФГ являлось рассмотрение вопросов и общих принципов IdM в области электросвязи/ИКТ. Позже активность данной ФГ переросла в глобальную инициативу МСЭ по IdM, реализация которой проходила в 2008 году. В данной инициативе принимали участие ИК 2, 9, 11, 13, 16 и 17 МСЭ-Т. Кроме того, с 2009 года по настоящее время при ИК 17 действует объединенная координирующая группа по IdM (JCA-IdM). В рамках данной группы была разработана дорожная карта стандартов в области IdM, которая включает в себя наработки в данной области следующих организаций: ATIS, ETSI, IETF, ISO/IEC, ITU, NIST, OASIS, Kantara Initiative и 3GPP (описание деятельности и выпущенных стандартов МСЭ и указанных организаций в области IdM представлено на сайте МСЭ: http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/ict-part06.aspx).

Создание «трансграничного пространства доверия в области электронной торговли» (далее – ПД-Т при ведении электронной торговли) будет способствовать упрощению процедур и развитию международной торговли. Кроме того, создание ПД-Т в области электронной торговли позволит упростить процесс идентификации и IdM для стран-участников ПД-Т. Данное утверждение связано со значением термина «доверие» в контексте безопасности, который может трактоваться как твердая уверенность в надежности и истинности информации или в возможности и расположенности объекта действовать надлежащим образом в конкретном контексте. Таким образом, создание доверительного пространства между государствами поможет унифицировать использование механизмов обеспечения безопасности (например, все страны будут использовать единый подход к выбору таких механизмов, как электронная подпись, двухуровневая парольная защита и т.д.), а также позволит повысить уровень доверия (постоянная, поддающаяся измерению мера уверенности в репутации, способностях, силе или истинности кого-то или чего-то) между участниками электронной коммерческой деятельности.

Под ПД-Т при ведении электронной торговли предлагается понимать сочетание правовых, организационных и технологических условий, рекомендуемых соответствующими специализированными учреждениями (департаментами) Организации Объединенных Наций и международными организациями с целью обеспечения доверия при международном обмене электронными документами и данными между сторонами (субъектами), взаимодействующими в электронной форме при ведении электронной торговли. Его основная цель заключается в предоставлении при помощи системы IdM доверенных услуг различного уровня (базового, среднего, высокого) пользователям в процессе их электронного взаимодействия. Это позволит придавать юридическую значимость электронному взаимодействию по усмотрению пользователей независимо от их местоположения и юрисдикции. Одним из важнейших направлений исследований в данной сфере будет анализ возможных механизмов IdM.

Под «сторонами (субъектами), взаимодействующими в электронной форме» при ведении электронной торговли предлагается понимать всю совокупность органов публичной власти, физических и юридических лиц, взаимодействующих в рамках отношений, возникающих в результате создания, отправки, передачи, получения, хранения и использования электронных документов и данных в ходе ведения электронной торговли.

Эти предложения преследуют цель определить подходы и вопросы, которые будут обсуждаться в контексте разработки свода рекомендаций по формированию и функционированию трансграничного пространства доверия (рекомендации по ПД-Т при ведении электронной торговли) в соответствующих организациях системы Организации Объединенных Наций. Они призваны облегчить создание технологической, институциональной и правовой инфраструктуры для практического использования рекомендаций по ПД-Т при ведении электронной торговли, в частности упростить систему IdM для обеспечения безопасности электронных коммерческих сделок.

Концептуальные подходы

1. Рекомендации по ПД-Т при ведении электронной торговли предлагается сориентировать на обеспечение гарантии прав и законных интересов граждан и организаций, находящихся под юрисдикцией государств – членов Организации Объединенных Наций, при осуществлении юридически значимых информационных операций при ведении торговли в электронной форме с использованием Интернета и других открытых систем ИКТ массового использования.

2. Упомянутые институциональные гарантии предлагается обеспечивать в рамках коммерческой деятельности специализированных операторов, которые:

- предоставляют пользователям набор доверенных услуг ИКТ для осуществления IdM;
- работают в рамках авторитетных правовых режимов, которые включают – но не ограничиваются этим – ограничения, введенные в связи с обработкой персональных данных.

3. Предлагается дать описание различных возможных правовых режимов:

- основанные на международных соглашениях (конвенциях) и/или на прямо применяемых международных нормах;
- основанные на коммерческих соглашениях и/или общей торговой практике;
- без специального международного регулирования.

Правовые режимы могут получать дополнительную поддержку со стороны традиционных институтов (правительственные органы, урегулирование в судебном порядке, страхование рисков, нотариат и другие) благодаря взаимному признанию электронных документов, подкрепляемых доверенными услугами в области ИКТ.

Авторитетные правовые режимы могут также предусматривать введение особых требований в отношении материальной и финансовой поддержки коммерческой деятельности специализированных операторов в случае причинения ими ущерба своим пользователям, включая случаи компрометации персональных данных.

Вопросы институциональных гарантий и правовых режимов, связанных с формированием и функционированием региональных и глобальных кластеров ПД-Т в области электронной торговли, а также с функциональными услугами, предоставляемыми в рамках этих кластеров, предлагается рассмотреть в отдельной рекомендации ЮНСИТРАЛ.

4. Предлагается дать описание возможных наборов доверенных инфраструктурных услуг в области ИКТ с учетом степени важности функциональных прикладных применений. Одним из важнейших направлений исследований в данной сфере будет анализ возможных механизмов управления IdM. Услуги в области ИКТ и нынешний уровень доверия к ним могут определяться функциональными операторами информационных систем (операторы, организующие и/или осуществляющие хранение и обработку данных идентичности в информационной системе, а также определяющие цели и действия (операции), совершаемые с данными идентичности в информационной системе) с учетом угроз, рисков, правовых режимов и потребностей пользователей. Для того чтобы обеспечить необходимый уровень доверия, операторы IdM могли бы работать в нейтральных международных условиях, определяемых конкретными правовыми режимами. Предлагается дать описание организационных структур, необходимых для создания и поддержания нейтральных международных условий.

Общие положения, касающиеся формирования и функционирования региональных и глобальных кластеров ПД-Т в области электронной торговли, функциональных услуг, предоставляемых в рамках этих кластеров, а также наборов доверенных инфраструктурных услуг в области ИКТ можно рассмотреть в рамках разработанной СЕФАКТ/ЕЭК/ООН «Рекомендации по обеспече-

нию юридически значимого доверительного трансграничного электронного взаимодействия».

Осуществление IdM, а также описание отдельных доверенных услуг в области ИКТ может стать предметом технических стандартов и рекомендаций МСЭ, ОТК 1, ЕТСИ и других структур.

5. Набор отличительных признаков для целей IdM должен определяться правовыми режимами, регулирующими коммерческую деятельность операторов, специализирующихся на выполнении задач идентификации, и функциональных операторов, и может подкрепляться соответствующими доверенными услугами в области ИКТ. Деятельность операторов может регулироваться специальными организационными и техническими требованиями, направленными, помимо прочего, на защиту персональных данных.

Наборы отличительных признаков для целей IdM и сами процедуры идентификации могут служить основой для определения уровней доверия в системах идентификации. Такие уровни доверия могут иметь важнейшее значение для регулирования взаимодействия между различными кластерами доверия (см. пункт 9).

6. Предлагается дать описание механизмов взаимодействия отдельных государств и их международных объединений с другими международными структурами в рамках формирования общего ПД-Т в области электронной торговли:

6.1. На основе присоединения к существующему правовому режиму, который обеспечивает институциональные гарантии субъектам электронного взаимодействия:

- полное присоединение государства к существующему правовому режиму на основе международных договоров и/или прямо применяемых международных норм, в которых уже поставлена или решена задача по формированию регионального ПД-Т в области электронной торговли, включая функциональные услуги, предоставляемые в рамках этого ПД-Т в области электронной торговли;

- частичное присоединение государства к существующему правовому режиму на основе международных договоров и/или прямо применяемых международных норм в части положений, касающихся формирования регионального и/или функционального ПД-Т в области электронной торговли;

6.2. На основе взаимодействия между различными международными объединениями:

- на первом этапе группа государств создает изолированный региональный кластер ПД-Т в области электронной торговли, включая функциональные услуги ПД-Т в области электронной торговли, предоставляемые в рамках этого ПД-Т в области электронной торговли, предоставляя институциональные гарантии субъектам электронного взаимодействия в рамках правового режима, определяемого этими государствами, а также обеспечивая безопасность электронных коммерческих сделок;

- на втором этапе определяются протоколы и механизмы доверительного взаимодействия с другими международными объединениями в связи с взаимным признанием различных правовых режимов. Такое взаимное признание должно учитывать институциональные гарантии и требования информационной безопасности, относящиеся к каждой из международных структур, возможно, на основе шлюзов информационной безопасно-

сти (ШИБ), функционирующих в рамках специальных правовых режимов и отвечающих за IdM;

6.3. На основе взаимодействия государства с другими государствами или международными объединениями:

- на первом этапе государство создает изолированный национальный кластер ПД-Т в области электронной торговли, функционирующий в рамках национального правового режима, определяемого этим государством;

- на втором этапе определяются протоколы доверительного взаимодействия с другими государствами и/или международными объединениями в связи с взаимным признанием различных правовых режимов. Такое взаимное признание должно учитывать институциональные гарантии и требования информационной безопасности, относящиеся к этим государствам и международным структурам, возможно, на основе шлюзов ШИБ, функционирующих в рамках специальных правовых режимов и отвечающих за IdM.

7. Предлагается дать описание механизмов создания кластеров по аналогии с пунктом 6 для правовых режимов, основанных на коммерческих соглашениях и/или общей торговой практике.

8. Предлагается дать описание механизмов формирования глобального ПД-Т в области электронной торговли на основе объединения различных кластеров в одну матрицу, построенную в соответствии со следующими параметрическими входными данными:

- виды функциональных услуг и региональная сфера охвата;

- виды правовых режимов и их разновидности.

9. Предлагается дать описание подходов к созданию нескольких видов ШИБ как ключевых элементов построения глобальной матрицы ПД-Т в области электронной торговли для обеспечения безопасности электронных коммерческих сделок.

Целью создания таких шлюзов (ШИБ) может быть обеспечение условий и безопасности для взаимодействия между различными кластерами глобального ПД-Т в области электронной торговли. При создании шлюзов (ШИБ) можно рассмотреть все необходимые аспекты: технологические, организационные и правовые.

Подходы к созданию типичных ШИБ могут учитывать наличие различных возможных уровней взаимодействия между различными кластерами ПД-Т в области электронной торговли. В частности, создание шлюзов (ШИБ), осуществляющих IdM, может осуществляться только на правовом и организационном уровнях и на комплексном уровне: правовом, организационном и технологическом.

Подходы к созданию типичных шлюзов информационной безопасности (ШИБ) могут учитывать использование профилей перехода, описывающих и определяющих переход из одного кластера в другой. В этих профилях перехода можно учитывать уровни доверия в системах идентификации, используемых внутри взаимодействующих кластеров, см. пункт 5.

Описание нескольких типов ШИБ может быть предметом технических стандартов и рекомендаций МСЭ и ОТК 1.

Создание ПД-Т при ведении электронной торговли при помощи объединенной инфраструктуры доверия

Как было сказано выше, основной целью создания ПД-Т при ведении электронной торговли является предоставление при помощи системы IdM доверенных услуг различного уровня (базового, среднего, высокого) пользователям в процессе их электронного взаимодействия.

ПД-Т при ведении электронной торговли представляет собой фундаментальную, легко масштабируемую платформу, обеспечивающую унифицированный и безопасный доступ к доверенным электронным услугам при помощи IdM. При этом учитываются существующие электронные системы и механизмы IdM, так что требования к их обновлению для включения в ПД-Т при ведении электронной торговли, как ожидается, будут минимальными.

В процессе работы над системой ПД-Т при ведении электронной торговли была предложена архитектура общей инфраструктуры доверия (ОИД), описаны взаимосвязи между ее различными компонентами и их взаимодействие с пользователями, причем работа одновременно велась по трем направлениям: технологическому, организационному и правовому. Анализ вариантов практической реализации и сценарии использования ОИД позволили подготовить перечень документов, необходимых для полного технического описания системы. Архитектура ОИД выбрана так, что ее можно легко масштабировать. Она легко расширяется на любом уровне рассмотрения за счет входа в нее новых компонентов, таких как новые правовые системы, новые наднациональные участники, новые операторы услуг доверия и услуг данных идентичности.

Технико-технологический уровень ОИД

Технологических механизмов обеспечения IdM и оказания услуг доверия может быть множество. Главным требованием, предъявляемым к элементам ОИД, является обеспечение операционной совместимости. Регулирование на данном уровне происходит с помощью различных стандартов и инструкций, как предусмотрено документами Координационного совета регуляторов доверенного электронного обмена данными (далее – КСР ДЭОД). Технологическое функционирование служб по предоставлению услуг доверия можно показать на примере использования такого механизма IdM, как электронная подпись (далее в тексте – ЭП) при трансграничном электронном взаимодействии. Для сравнения представлены два варианта реализации ОИД: децентрализованная схема при условно «низком» уровне доверия между участниками информационного взаимодействия (см. рис. 1) и централизованная схема при «среднем» уровне доверия между ними (см. рис. 2).

В таблице 1 отражены особенности построения децентрализованной и централизованной схем ОИД. Процедура использования ЭП как механизма системы IdM для двух вариантов реализации ОИД описана в таблице 2.

Таблица 1

Особенности использования механизма IdM в ОИД для информационного взаимодействия с «низким» и «средним» уровнем доверия

Низкий уровень доверия (рис. 3)	Средний уровень доверия (рис. 4)
1. Услуги апостилирования предоставляют национальные операторы услуг апостилирования (УАп). Эти же операторы могут осуществлять и другие услуги, касающиеся IdM. 2. Международные организации (операторы и регуляторы) отсутствуют. 3. Национальные регуляторы взаимодействуют напрямую, обмениваясь между собой сертификатами безопасности. 4. Национальные регуляторы обеспечивают деятельность национальных операторов услуг доверия, на которых распространяется юрисдикция, в отношении их сертификатов и сертификатов национальных регуляторов, на которых распространяется другая юрисдикция.	1. Услуги апостилирования предоставляются международным оператором УАп. Эти же операторы могут предоставлять и другие услуги, касающиеся IdM. 2. Присутствуют международные организации: международный регулятор ОИД и международные операторы услуг доверия. 3. Национальные регуляторы ОИД взаимодействуют только через наднационального регулятора ОИД. Также и национальные операторы услуг доверия взаимодействуют через соответствующего международного оператора. 4. Международный регулятор ОИД централизованно обеспечивает сертификатами национальных операторов услуг доверия и национальных регуляторов ОИД 5. Национальные регуляторы обеспечивают деятельность национальных операторов услуг доверия, на которых распространяется их юрисдикция в отношении их сертификатов и сертификатов международного регулятора.

Таблица 2

Процедура использования ЭП как механизма системы IdM в схемах с «низким» и «средним» уровнем доверия

Низкий уровень доверия (рис. 3)	Средний уровень доверия (рис. 4)
1. Физическое/юридическое лицо 1 отправляет документы, подписанные ЭП в рамках юрисдикции J, выбирая при этом необходимый уровень квалификации используемых услуг доверия, предоставляемых ОИД (базовый, средний или высокий). 2. Запрос на проверку документов с ЭП в рамках юрисдикции J направляется национальному оператору услуг апостилирования (УАп), на который распространяется юрисдикция Q. 3. Запрос на проверку документов перенаправляется национальному оператору УАп, на которого распространяется юрисдикция J. 4. Осуществляется математическая проверка ЭП в рамках юрисдикции J. 5/6. Отправляется запрос/ответ о статусе сертификата национальному оператору услуг подписи (УП), на которого распространяется юрисдикция J. 7. Национальный оператор УАп, на которого распространяется юрисдикция Q, получает подтверждение корректности ЭП в рамках юрисдикции J. 8. Национальный оператор УАп, на которого распространяется юрисдикция Q, удостоверяет полученный запрос и направляет его физическому/юридическому лицу 2.	1. Физическое/юридическое лицо 1 отправляет документы, подписанные ЭП в рамках юрисдикции J, выбирая при этом необходимый уровень квалификации используемых услуг доверия, предоставляемых ОИД (базовый, средний или высокий). 2. Запрос на проверку документов с ЭП в рамках юрисдикции J направляется международному оператору УАп I-J-Q. 3. Осуществляется математическая проверка ЭП в рамках юрисдикции J. 4/5. Отправляется запрос/ответ о статусе сертификата национальному оператору услуг подписи (УП), на которого распространяется юрисдикция J. 6. Международный оператор УАп I-J-Q удостоверяет полученный запрос и направляет его физическому/юридическому лицу 2.

Рис. 1

Схема проверки ЭП в рамках ПД-Т с «низким» уровнем доверия (децентрализованная схема)

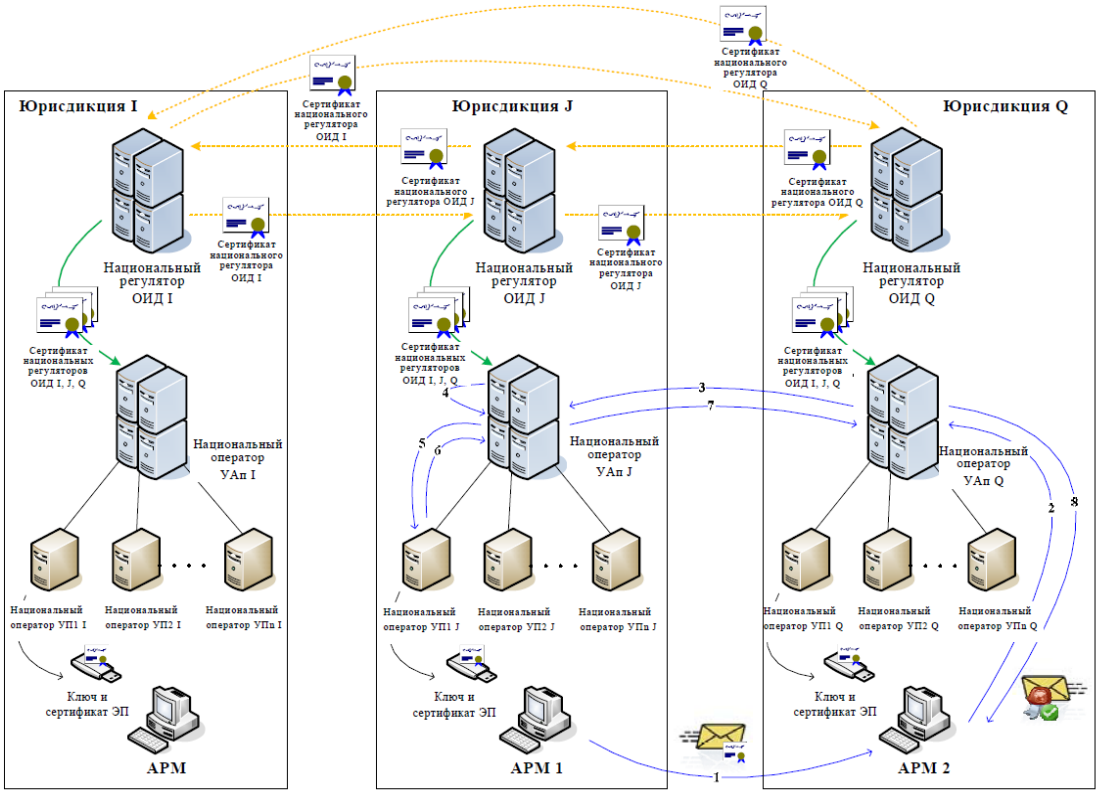
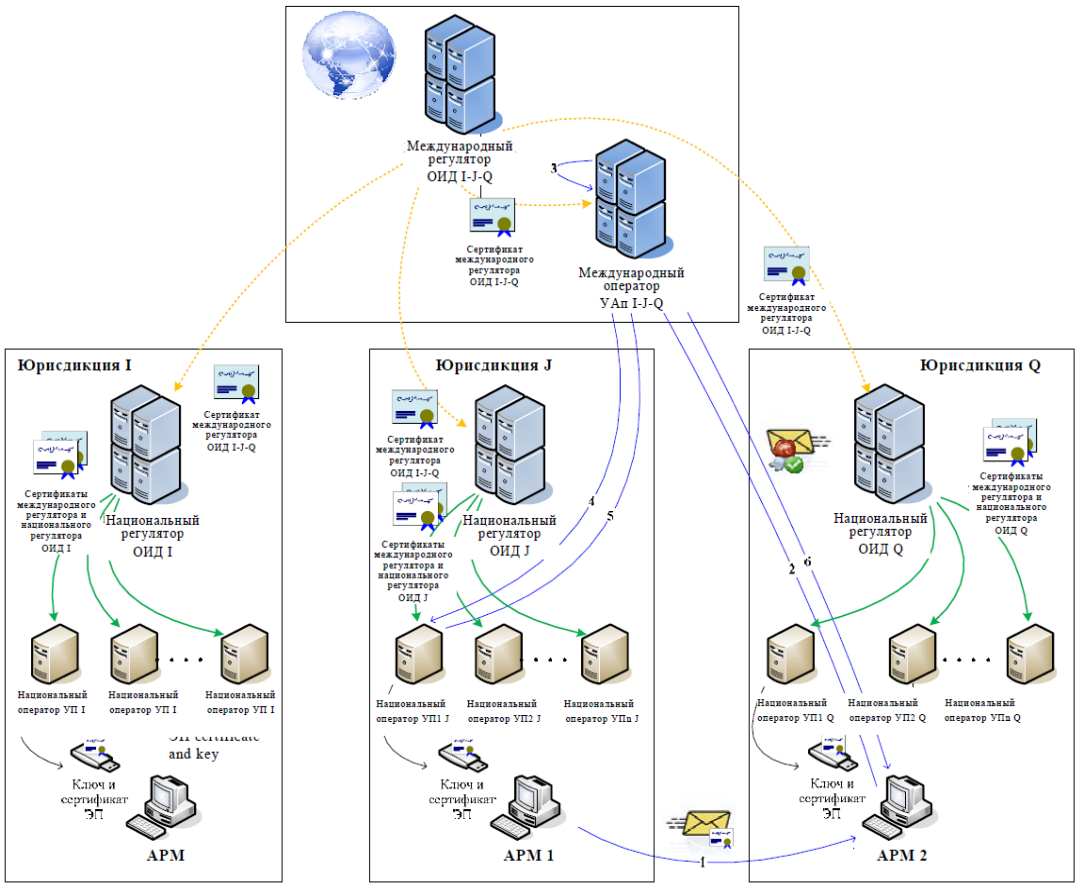


Рис. 2
Схема проверки ЭП в рамках ПД-Т со «средним» уровнем доверия (децентрализованная схема)

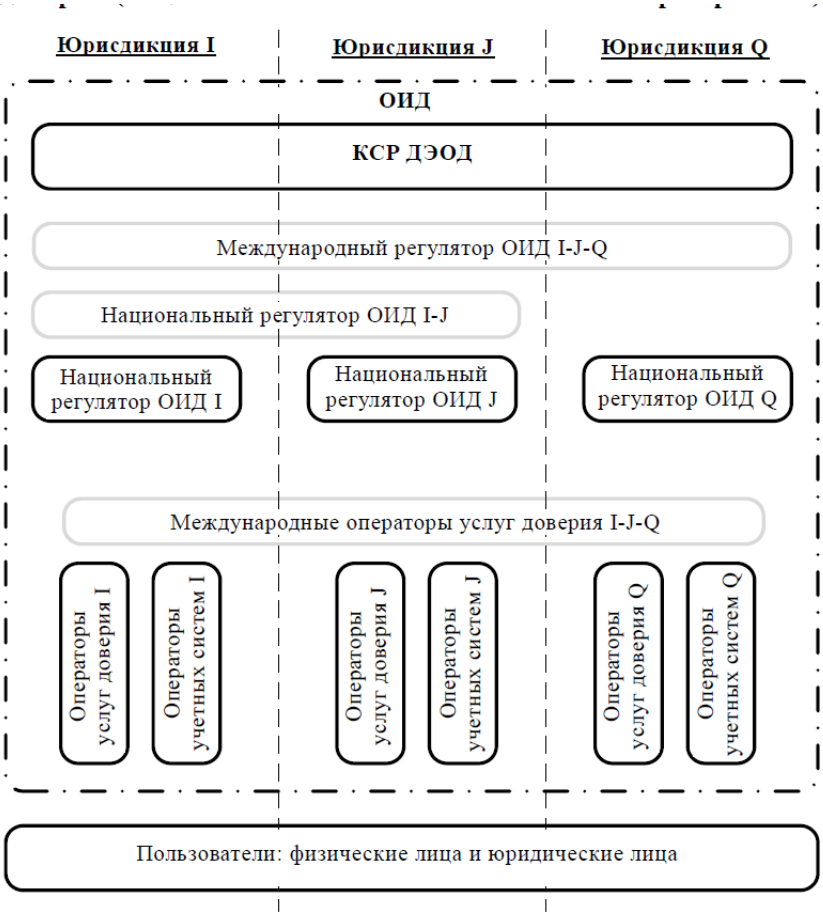


Организационный уровень

Взаимное юридически значимое признание IdM и услуг доверия, предоставляемых в рамках юрисдикций разных государств, достигается путем создания и функционирования КСР ДЭОД. Деятельность данной организации регламентируется уставом КСР ДЭОД, который должны признать и подписать все его уполномоченные члены – т.е. регулирующие органы электронного обмена данными, представленные в первую очередь национальными регуляторами ОИД.

Организационное регулирование можно представить в виде следующей схемы (см. рис. 3):

Рис. 3
Схема организационного регулирования трансграничного пространства доверия
(опциональные элементы обозначены серой рамкой)



КСР ДЭОД издает ряд документов, полномочия на издание которых закреплены в его уставе:

- требования к членам КСР ДЭОД, соответствие которым является необходимым условием полноправного членства в КСР ДЭОД;
- руководящие принципы по проведению предварительного («теневого») надзора для приема в КСР ДЭОД и взаимного периодического аудита для сохранения добровольного членства в КСР ДЭОД;
- критерии соответствия, которым должны удовлетворять операторы услуг ОИД, а также операторы IdM и услуг доверия, и методология применения этих критериев;
- схема оценки/проверки операторов услуг ОИД, а также операторов IdM и услуг доверия на соответствие этим критериям.

В ПД-Т при ведении электронной торговли каждая правовая система представлена национальным регулятором ОИД (см. рис. 3, национальные регуляторы ОИД I, J, Q), который регламентирует работу операторов услуг доверия и операторов IdM в рамках своей юрисдикции.

Для групп государств с большой степенью интеграции (например, ЕврАзЭС или ЕС) существует вероятность образования наднационального регулятора ОИД (см. рис. 3, наднациональный регулятор ОИД I-J). Таким образом, один наднациональный регулятор ОИД I-J заменяет группу национальных регуляторов ОИД I и J.

Естественная масштабируемость ОИД обеспечивается процедурой приема новых членов в КСР ДЭОД (новые правовые системы и наднациональные участники) и схемой проверки операторов услуг ОИД и операторов IdM на соответствие критериям, опубликованным КСР ДЭОД (новые операторы IdM и услуг доверия).

Если члены КСР ДЭОД (см. ниже) достигли условно «среднего» уровня доверия, они могут инициировать создание международного регулятора ОИД и международных операторов IdM и услуг доверия (см. рис. 3, международный наднациональный регулятор ОИД I J Q и международные операторы услуг доверия I J Q). Международный регулятор ОИД будет осуществлять координацию взаимодействия международных операторов услуг доверия, а также национальных регуляторов ОИД (согласно уставу КСР ДЭОД) и/или наднациональных регуляторов ОИД.

Чтобы стать национальным оператором услуг доверия или оператором учетной системы, поставщику соответствующих услуг необходимо пройти аккредитацию у национального регулятора ОИД в том же государстве. Международные операторы услуг доверия обязаны проходить аккредитацию у международного регулятора ОИД. Требования к аккредитации операторов услуг доверия и операторов учетных систем, а также требования к их деятельности регулируются критериями соответствия, опубликованными КСР ДЭОД, и возможными национальными дополнениями, изданными соответствующим регулятором.

Пользователями электронных услуг в рамках ПД-Т при ведении электронной торговли могут выступать как физические, так и юридические лица. Пользователи выбирают по их усмотрению или по договоренности необходимый им уровень квалификации услуг доверия.

Услуги предоставляются соответствующими поставщиками – операторами услуг доверия. В ряде случаев услуги могут предоставлять и операторы учетных систем. Операторы услуг доверия и операторы учетных систем объединены общей инфраструктурой доверия.

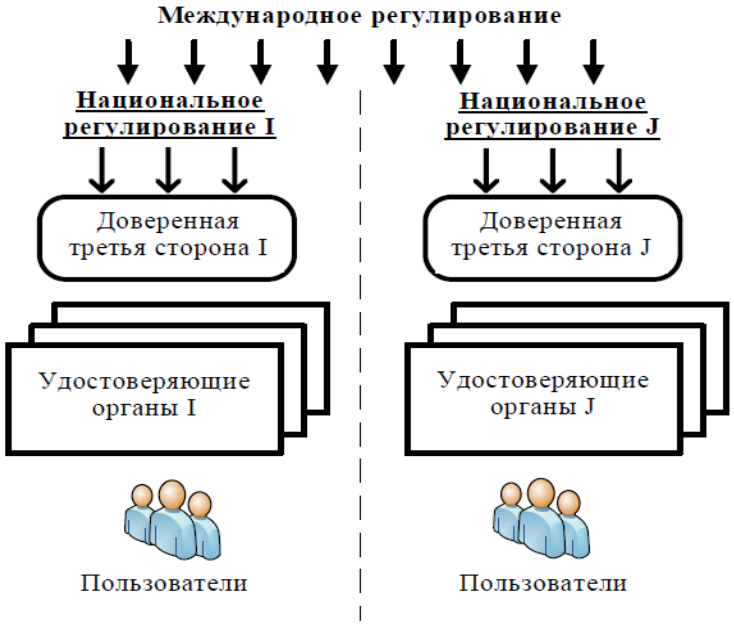
Услуги доверия, являющиеся элементами ПД-Т при ведении электронной торговли, могут иметь различные варианты реализации в зависимости от уровня доверия между участниками информационного взаимодействия. Например, при условно «высоком» и «среднем» уровне взаимного доверия между членами КСР ДЭОД можно эффективно использовать централизованные международные услуги, предоставляемые в соответствии с согласованными стандартами. В случае условно «низкого» уровня доверия предоставление услуг доверия будет организовано по децентрализованному принципу – на основе национальных услуг в каждом государстве.

Правовой уровень

ПД-Т при ведении электронной торговли может строиться на одно- или многодоменной основе. С точки зрения правового и организационного регулирования многодоменная основа является более сложным вариантом. Многодоменность предполагает применение технических средств доверенной третьей

стороны (далее в тексте – ДТС). На рис. 4 представлена общая схема правового регулирования.

Рис. 4
Схема правового регулирования трансграничного пространства доверия



Правовое регулирование трансграничного информационного взаимодействия можно разделить на две части: международную и национальную. Международное правовое регулирование осуществляется на основе следующих видов документов:

- международные договоры/соглашения;
- акты различных международных организаций;
- международные стандарты и регламенты;
- соглашения между участниками трансграничного информационного взаимодействия по конкретным вопросам;
- типовые правовые акты.

В свою очередь национальное правовое регулирование также строится на комплексе нормативных правовых актов, характерных для каждой отдельной правовой системы.

Резюме

Как видно из приведенного выше материала, создание ПД-Т при ведении электронной торговли является оптимальным вариантом совершенствования системы IdM со следующих точек зрения:

- создание национальных, региональных и международных кластеров доверия позволит обеспечить повышение операционной совместимости использования механизмов IdM, например ЭП;

- взаимное юридически значимое признание IdM и услуг доверия, предоставляемых под юрисдикцией разных государств позволит выработать единый подход к стандартизации систем IdM;
- принятие международных договоров и соглашений, а также международных стандартов и регламентов по вопросам использования ПД-Т позволит повысить уровень доверия участников электронной торговли, что позволит упростить осуществление IdM;
- деятельность КСР ДЭОД позволит выработать единые критерии соответствия, которым должны удовлетворять операторы IdM и услуг доверия, а также методологию применения этих критериев.

Совершенствование системы IdM, в свою очередь, позволит создать условия для безопасной трансграничной международной коммерческой деятельности. Для создания ПД-Т при ведении электронной торговли необходимо осуществить ряд системных мероприятий, а именно:

- внедрение технических решений в части обеспечения безопасности и конфиденциальности информации;
- внедрение организационных решений в части создания координирующей структуры;
- внедрение регуляторно-правовых решений в части создания международных договоров об использовании ПД-Т при ведении электронной торговли.

Далее для организации ПД-Т при ведении электронной торговли необходимо провести координацию между организациями, которые занимаются вопросами IdM и трансграничной торговли (ИСО, МСЭ, СЕФАКТ/ЕЭК ООН, ЮНСИТРАЛ, АТЭС и т.д.) с целью выработки единого подхода как к стандартизации использования ПД-Т при ведении электронной торговли как механизма IdM, так и к использованию ПД-Т при ведении электронной торговли для осуществления трансграничного электронного взаимодействия и коммерческой деятельности.

Следующим шагом по продвижению разработки видится обсуждение накопленного опыта и знаний с различными партнерами (экспертами и организациями), заинтересованными в облегчении, упрощении и одновременно придании юридической силы трансграничным электронным услугам.

Такими заинтересованными партнерами могут быть в первую очередь как политические, так и экономические структуры[6]. К политическим структурам, уже частично вовлеченным в работу по этому направлению, можно отнести как наднациональные организации (например, СНГ, АТЭС, ЕС, ШОС), так и структуры, созданные в рамках двусторонних отношений между некоторыми государствами. К экономическим структурам, заинтересованным в достижении этой цели, относятся, например, соответствующие подразделения Организации Объединенных Наций, такие как СЕФАКТ/ООН/ЕЭК, ЮНСИТРАЛ (Рабочие группы III и IV), а также ЕЭК ООН, ЕЭП, ЕврАзЭС и другие. Можно предположить, что существующие естественные особенности (исторические, культурные, политические, экономические, технические и т.д.) различных регионов

[6] В этом продукте могут быть заинтересованы также и другие гуманитарные структуры, например, в области права, Гаагская конференция по международному частному праву, а также структуры в области медицины и образования; однако, на наш взгляд, такие организации будут скорее пользоваться уже созданным ПД-Т, чем поддерживать его разработку нового продукта.

мира приведут к тому, что различные международные или региональные организации стран создадут «свои собственные» координационные структуры (КСР ДЭОД) и архитектуры ОИД в зависимости от степени доверия внутри каждого формата и упомянутых естественных особенностей.

Поэтому мы исходим из того, что на первых этапах реализации этого проекта будет существовать не единый «домен доверия» для всей планеты (например, на уровне какой-либо из структур Организации Объединенных Наций), а несколько «доменов доверия» на уровне регионов или даже отдельных стран[7]. Несмотря на это, даже создание отдельных «доменов доверия» позволит усовершенствовать систему IdM в силу необходимости обеспечения операционной совместимости внутри такого «домена доверия».

После того как будет определена архитектура ОИД (в соответствующем «домене доверия»), можно будет приступить к написанию дальнейшего пакета документов организационного, нормативного и технологического характера, согласованного в рамках КСР ДЭОД. Таким образом, будет обеспечена операционная совместимость в рамках соответствующего «домена доверия».

Принятие этого пакета документов членами КСР ДЭОД (в соответствующем «домене доверия») позволит перейти к заключительному этапу практического внедрения систем трансграничного юридически значимого электронного взаимодействия.

Комментарий для сведения экспертов Рабочей группы IV ЮНСИТРАЛ «Электронная торговля»

Проблема обеспечения безопасности и идентификации объектов и субъектов в ходе ведения электронной торговли может быть решена в контексте предложенной выше модели (модель формирования и функционирования ПД-Т в области электронной торговли в виде матрицы, построенной на основе региональных и глобальных кластеров, связанных между собой и включающих функциональные услуги, предоставляемые в рамках этого ПД-Т в области электронной торговли) следующим образом:

- создается функциональный кластер ПД-Т при ведении электронной торговли, специализирующийся на создании зоны доверия для осуществления IdM применительно к трансграничным электронным коммерческим сделкам;
- в географическом плане в этот кластер могут входить все государства – члены Организации Объединенных Наций;
- функционирование этого кластера обеспечивается с помощью коммерческой деятельности специализированного оператора или группы связанных между собой операторов;
- предметом коммерческой деятельности специализированных операторов может быть предоставление пакетов доверенных услуг по IdM, основанных на наборе идентификационных схем, принятых в рамках платформ для электронной торговли;
- правовой режим коммерческой деятельности специализированных операторов устанавливается в рамках соглашений с электронными торговыми площадками.

[7] Информационно-правовое пространство, в котором используется одна и та же ОИД.