Согласовано Итоговым совещанием ПРГ КИ 17-19 ноября 2015 г.

ОТЧЕТ
О РЕЗУЛЬТАТАХ АНАЛИЗА ПО ТЕМЕ:

«РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО СОЗДАНИЮ И МОДИФИКАЦИИ ТЕХНОЛОГИЙ ТРАНСГРАНИЧНОГО ЮРИДИЧЕСКИ ЗНАЧИМОГО ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ С УЧЕТОМ СОВРЕМЕННОГО МЕЖДУНАРОДНОГО ОПЫТА (В ТОМ ЧИСЛЕ СТРАН АТР) ПО СОЗДАНИЮ ТРАНСГРАНИЧНОГО ПРОСТРАНСТВА ДОВЕРИЯ»

АННОТАЦИЯ

Настоящий документ содержит рекомендации по учету в деятельности администраций железных дорог стран членов ОСЖД требований ЕС и стран азиатско-тихоокеанского региона в области юридически значимого трансграничного электронного документооборота и построения трансграничного пространства доверия, а также рекомендации по возможной доработке программно-технических средств администраций железных дорог стран членов ОСЖД, участвующих в организации юридически значимого трансграничного электронного документооборота.

ОГЛАВЛЕНИЕ

1. Введение

В последнее время лидерами ряда ведущих стран мира, поставлены масштабные задачи в области экономической интеграции, которые должны быть поддержаны со стороны информационных технологий.

В числе таких задач создание единого экономического пространства от Атлантики до Тихого океана и развитие региональной экономической интеграции на основе согласованных интересов с партнёрами по Евразийскому экономическому союзу (ЕАЭС).

Удешевление и повышение надежности движения товаров по всей логистической цепочке от производителя до потребителя является одним из ключевых факторов содействия международной торговле. Имеется в виду выстраивание экономически оправданных и безопасных цепочек поставок товаров, организация эффективного взаимодействия различных видов транспорта, оснащение транспортных узлов и коридоров современными информационно-техническими средствами.

Одним из ведущих интеграционных факторов является использование информационно-коммуникационных технологий (ИКТ), в том числе построение и внедрение механизмов доверия в электронной среде на глобальном уровне посредством содействия трансграничному юридически значимому обороту информации, включая электронные документы.

Об этом, в частности, говорится в Декларации лидеров Азиатско-Тихоокеанского экономического сотрудничества (АТЭС), принятой на 20-й встрече лидеров экономик АТЭС в рамках форума АТЭС 2012:

«Мы признаем важность информационно-коммуникационных технологий (ИКТ) в качестве важнейшего фактора для дальнейшей интеграции в регионе АТЭС. Мы считаем возможным и необходимым быть более активными в продвижении уверенности и доверия в электронной среде на глобальном уровне путем поощрения безопасных трансграничных потоков информации, включая электронные документы. Мы вновь подтверждаем необходимость продолжать усилия для расширения Азиатско-Тихоокеанской информационной инфраструктуры и укреплению доверия и безопасности при использовании ИКТ»[1].

В настоящем отчете содержится анализ современных мировых подходов к созданию электронного трансграничного пространства доверия и, в частности, организации трансграничного юридически значимого электронного документооборота. На основе проведенного анализа предлагаются рекомендации по использованию ведущих мировых практик по построению трансграничного электронного взаимодействия в деятельности администраций железных дорог стран членов ОСЖД.

[1] http://apec.org/Meeting-Papers/Leaders-Declarations/2012/2012_aelm.aspx

2. Анализ применения технологий электронной подписи и юридически значимого трансграничного электронного документооборота в деятельности межгосударственных организаций, ЕС и стран азиатско-тихоокеанского региона

2.1. Анализ применения Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах

Конвенция ООН об использовании электронных сообщений в международных договорах (далее – Конвенция) принята 23.11.2005 г. резолюцией 60/21 на 53-ем пленарном заседании 60-ой сессии генеральной ассамблеи ООН и была подписана Минэкономразвития от имени РФ в Нью-Йорке 25 апреля 2007 года. Конвенция регламентирует электронное трансграничное взаимодействие применительно к коммерческим договорам. Цель Конвенции заключается в том, чтобы способствовать международной торговле за счет устранения потенциальных юридических препятствий или неопределенности в отношении использования электронных сообщений при заключении или исполнении договоров между сторонами (коммерческими партнерами), находящимися в разных странах.

Конвенция регулирует вопросы юридической силы сообщений, сделанных в электронной форме, в частности электронную форму договоров. Конвенция допускает заключение договоров в электронной форме и признает юридическую силу иных сообщений, переданных по электронной почте, факсу, телексу и с помощью иных электронных, магнитных, оптических или аналогичных средства.

Основные положения Конвенции:

- Конвенция применяется в случае, если коммерческие предприятия сторон расположены в разных государствах. По общему правилу, не имеет значения, являются ли эти государства участниками Конвенции. Иными словами, обязательства по Конвенции связывают государство, которое решает вопрос о признании электронной формы договора;
- Договор не может быть лишен силы лишь на том основании, что он составлен в электронной форме;
- Если законодательство страны требует соблюдения письменной формы сделки, то электронное сообщение, информация в котором доступна для последующего использования, приравнивается к письменной форме договора;
- Если по законодательству страны требуется подписание договора, то электронная форма договора имеет юридическую силу, если она позволяет достоверно определить сторону и ее намерение в отношении информации, переданной в электронной форме. Другими словами, с учетом всех обстоятельств дела оценивается надежность метода передачи информации и возможность установить, что сообщение исходило от определенного лица[2];

[2] Статья 9, пункт 3: «В случаях, когда законодательство требует, чтобы сообщение или договор были подписаны стороной, или предусматривает наступление определенных последствий в случае отсутствия подписи, это требование считается выполненным в отношении электронного сообщения, если:
a) использован какой-либо способ для идентификации этой стороны и указания намерения этой стороны в отношении информации, содержащейся в электронном сообщении; и
b) этот способ:

- Конвенция содержит нормы, посвященные времени отправления и получения электронных документов, исправлению ошибок в электронном документе.

Конвенция принята в Российской Федерации в соответствии с постановлением Правительства Российской Федерации от 24 октября 2013 года № 940. Российская Федерация приняла Конвенцию с рядом заявлений. В частности, в соответствии с пунктом 2 статьи 19 Конвенции, Российская Федерация не будет применять Конвенцию к сделкам, в отношении которых законодательством Российской Федерации установлена нотариальная форма или требование о государственной регистрации, а также к сделкам купли-продажи товаров, в отношении которых установлены запреты либо ограничения к перемещению через таможенную границу Таможенного союза. Кроме того, в Российской Федерации Конвенция применяется только в том случае, когда стороны договора договорились о ее применении. Это означает, что по умолчанию Конвенция к договорам не применяется и, соответственно, электронная форма договоров и юридических сообщений не признается. Такое заявление сделано в соответствии с действующим Гражданским кодексом РФ, который признает юридическую силу сделок в электронной форме, если только стороны сами договорились об этом.

2.2. Анализ документов межгосударственных организаций (Евразийский экономический союз – ЕАЭС, Координационный Совет по транссибирским перевозкам) по вопросам использования имеющих юридическую силу электронных документов

Для реализации поставленных задач организации трансграничного электронного взаимодействия на практике в рамках ЕАЭС (ранее – Таможенный союз) уже принят (а перечисленные ниже Соглашения утверждены на государственном уровне) начальный пакет нормативно-правовых документов, в том числе следующие:

- Соглашение о создании, функционировании и развитии Интегрированной информационной системы внешней и взаимной торговли таможенного союза (ИИСВВТ);
- Соглашение о применении информационных технологий при обмене электронными документами во внешней и взаимной торговле на единой таможенной территории Таможенного союза;
- «Модель и Методология формирования в сети Интернет трансграничного пространства доверия» (далее Модель/Методология)

В этих документах определены цели, функции и порядок создания международной информационной системы, в том числе для обеспечения процедур таможенного и других видов контроля, а также электронных аукционов.

---

i) либо является настолько надежным, насколько это соответствует цели, для которой электронное сообщение было подготовлено или передано, с учетом всех обстоятельств, включая любые соответствующие договоренности;

ii) либо, как это фактически продемонстрировано на основании самого способа или с помощью дополнительных доказательств, позволил выполнить функции, описанные в подпункте, а выше.»

Первоначальная задача состоит в том, чтобы синхронизировать электронные подписи для участия на площадках Евразийского союза, а потом и с другими странами. Создание общего пространства с единой площадкой для торгов отвечает главной цели Евразийского Союза.

Кроме того, впервые в международном праве введено расширенное понятие «электронного документа»[3], а также термины «учетная система»[4], «общая инфраструктура документирования информации»[5] и «доверенная третья сторона – ДТС»[6].

При этом сервис ДТС является ключевым для формирования трансграничного пространства доверия (ПД-Т), которое предназначено для охраны прав и законных интересов граждан и организаций при совершении ими юридически значимых информационных транзакций с использованием сети Интернет. Наряду с сервисом ДТС могут использоваться и другие сервисы доверия, работа по системному описанию которых проводилась в формате РСС-СНГ.

Далее рассматриваются положения перечисленных документов, принятых в рамках ЕАЭС, актуальные для организации трансграничного электронного взаимодействия в интересах администраций железных дорог стран членов ОСЖД.

Наибольший интерес представляет описание набора сервисов общей инфраструктуры доверия. Основное назначение данных сервисов заключается в обеспечении интерактивности реквизитов (атрибутов) документов. При этом основное внимание уделяется правовому содержанию данных реквизитов.

В настоящее время в Российской Федерации установлен перечень таких реквизитов («Правила делопроизводства в федеральных органах исполнительной власти, утвержденных постановлением Правительства Российской Федерации от 15 июня 2009 г. № 477). Данный перечень представляет собой целостную систему неразрывно связанных с документом данных. Эта система предназначена для придания качества юридической силы информационному наполнению официального документа, издаваемого в рамках реализации полномочий органов власти, как при межведомственном взаимодействии, так и при взаимодействии с другими субъектами информационного взаимодействия, прежде всего с гражданами и организациями.

---

[3] Здесь и далее в этом разделе приведены определения из «Соглашения о применении информационных технологий при обмене электронными документами во внешней и взаимной торговле на единой таможенной территории Таможенного союза».

«электронный документ о внешней и взаимной торговле» – формализованная запись информации в электронном виде, заверенная электронной цифровой подписью и отвечающая правилам и требованиям документирования при осуществлении внешней и взаимной торговли на единой таможенной территории Таможенного союза (электронный документ).

[4] «учетная система» – информационная система, содержащая информацию из правоустанавливающих документов субъектов электронного взаимодействия, на основании которой составляются или выдаются юридически значимые электронные документы.

[5] «общая инфраструктура документирования информации в электронном виде» – совокупность информационно-технологических и организационно-правовых мероприятий, правил и решений, реализуемых в целях придания юридической силы электронным документам, используемым при осуществлении внешней и взаимной торговли на единой таможенной территории Таможенного союза.

[6] «доверенная третья сторона» – организация, наделенная правом в соответствии с законодательством государства каждой из Сторон осуществлять деятельность по проверке электронной цифровой подписи в электронных документах в фиксированный момент времени в отношении составителя и (или) адресата электронного документа.

Это качество полноты и системности реквизитов документов должно быть сохранено при формировании перечня сервисов общей инфраструктуры доверия, поскольку они в своей совокупности будут реализовывать интегрированное качество юридической значимости информационного взаимодействия субъектов – юридических и физических лиц.

Реквизиты, которые, согласно существующим стандартам, постановлениям и прочим законодательным актам, регулирующим документооборот, должны присутствовать в бумажном документе, необходимо сохранить при переходе к электронной форме. При этом подтверждение достоверности реквизитов предлагается обеспечить применением сервисов общей инфраструктуры доверия, включающих сервисы документирования, дополнительные сервисы и сервис доступа.

К сервисам документирования относятся:

- сервис подписи;
- сервис времени;
- нотариальный сервис;
- сервис апостилирования;
- сервис местоположения;
- сервис мониторинга правовых статусов;

К дополнительным сервисам относятся:

- сервис обеспечения платежей;
- сервис доверенного хранения данных;
- информационный сервис.

Приведенный набор сервисов не претендует на полноту, при необходимости он может быть дополнен.

Каждый сервис может иметь несколько реализаций, подход к описанию которых может быть основан на понятиях централизации/децентрализации и моно/мульти-юрисдикции. Иными словами, предлагается рассматривать три возможные реализации каждого сервиса.

Light-реализация, которая для большинства сервисов подразумевает выполнение функционала сервиса самой учетной системой. Данная реализация сервисов отражает текущую парадигму электронного документа – документа, атрибуты которого статичны. Интероперабельность учетных систем обеспечивается в основном применением бумажных экземпляров документов.

Medium-реализация, при которой сервис организован централизованно для нескольких юрисдикций. Один оператор сервиса обслуживает субъектов различных юрисдикций.

Heavy-реализация, при которой сервис организован децентрализованно для нескольких юрисдикций. В каждой юрисдикции есть один или несколько операторов, обслуживающих субъектов этой же юрисдикции. Операторы различных юрисдикций взаимодействуют между собой.

Выбор централизованного или децентрализованного варианта зависит от уровня доверия между операторами учетных систем различных юрисдикций. При высоком уровне доверия некоторые сервисы общей инфраструктуры могут быть реализованы централизовано под управлением одного международного оператора. При низком уровне доверия все сервисы

общей инфраструктуры реализуются децентрализовано – в каждой юрисдикции существует как минимум один «национальный» оператор.

Трансграничность обеспечивается путем взаимодействия таких национальных операторов.

Сложившаяся практика трансграничного электронного взаимодействия в интересах администраций железных дорог стран членов ОСЖД отвечает уровню Heavy-реализации: так, например, в ОАО «РЖД» определен оператор - Удостоверяющий центр ОАО «НИИАС», обслуживающий клиентов информационных систем ОАО «РЖД», задействованных в международном информационном обмене (например, АС ЭТРАН), а также взаимодействующий с аналогичными операторами других юрисдикций. В связи с этим далее рассматриваются рекомендации к Heavy-реализации сервисов общей инфраструктуры доверия.

Особое внимание стоит обратить на тот момент, что общая инфраструктура доверия будет построена на основе конкретных технических

решений. Будет определено конечное число унифицированных интерфейсов,

с помощью которых учетные системы смогут взаимодействовать между собой и обращаться к сервисам общей инфраструктуры. Таким образом, любой оператор учетной системы для обеспечения ее интероперабельности должен будет привести интерфейсы УС в соответствие с интерфейсами общей инфраструктуры.

2.2.1. Сервис подписи

Сервис подписи предназначен для подтверждения волеизъявления физических лиц – участников информационного взаимодействия.

Волеизъявление участника подтверждается его электронной подписью. Сертификат ЭП участника (подписанта) выдается УЦ, функционирующим в той же юрисдикции, что и участник (национальным УЦ). Данный национальный УЦ имеет отношения доверия с аналогичными национальными УЦ других юрисдикций. При этом отношения доверия построены по принципу кросс-сертификации национальных УЦ. Каждый национальный УЦ может иметь несколько подчиненных УЦ. Т.е. в пределах одной юрисдикции существует иерархическая структура удостоверяющих центров, во главе которой стоит один национальный УЦ, имеющий отношения доверия с аналогичными национальными УЦ других юрисдикций.

Подобная реализация сервиса подписи подразумевает распределение нагрузки между УЦ (каждый УЦ обслуживает субъектов своей юрисдикции) и повышенную отказоустойчивость сервиса в целом. Еще одним преимуществом этих реализаций является возможность построения структуры удостоверяющих центров на основе существующих операторов – коммерческих и государственных УЦ.

В тоже время ключевым моментом, на который нужно обратить внимание, является то, что данная реализация подразумевает наличие у каждого субъекта информационного взаимодействия средства электронной подписи, реализующего все криптографические алгоритмы, применяемые в данной PKI архитектуре.

Возможен также такой вариант реализации сервиса (Heavy-2-реализация) – волеизъявление участника подтверждается его электронной подписью, которая

заверяется ЭП оператора сервиса апостилирования (возможные реализации сервиса апостилирования описаны ниже). УС и УЦ, выпустивший сертификат ЭП подписанта, могут быть субъектами различных юрисдикций (субъектами разных стран).

Порядок проверки ЭП следующий. УС отправляет в сервис апостилирования запрос на проверку ЭП подписанта. Математическая проверка ЭП (проверка целостности подписанных данных) осуществляется

локально сервисом апостилирования. Проверка статуса сертификата подписанта осуществляется путем обращения сервиса апостилирования к УЦ, выпустившему сертификат подписанта. Подписанная ЭП оператора сервиса апостилирования квитанция, содержащая результаты математической проверки ЭП участника, результаты проверки статуса сертификата участника и время проверки10, отправляется в УС. Данная квитанция хранится в УС и может быть пролонгирована посредством обращения к сервису апостилирования, что позволяет обеспечить подтверждение ЭП участника по истечении срока действия его сертификата.

2.2.2. Сервис времени

Сервис времени предназначен для подтверждения времени совершения

какой-либо операции, к примеру, времени изменения учетной записи, к которой организуется разграниченный on-line доступ, или издания на основании этой записи электронного документа, имеющего статус off-line.

В Heavy-реализации время совершения операции заверяется ЭП оператора сервиса времени. Локальные часы сервиса времени синхронизируются с сигналами точного времени.

2.2.3. Нотариальный сервис

Нотариальный сервис предназначен для безусловного подтверждения волеизъявления физического лица, совершенного с применением электронной подписи. Функцией нотариального сервиса является совершение нотариальных действий и/или действий с электронными документами с использованием электронной подписи нотариуса. Состав квитанций, выдаваемых сервисом апостилирования, может быть скорректирован с учетом потребностей УС.

Примером реализации может служить синхронизация часов УС по протоколу NTP с ntp-серверами Microsoft, ГЭВЧ ВНИИФТРИ и пр. Синхронизация может осуществляться по сигналам спутниковых группировок ГЛОНАСС/GPS или по сигналам атомного эталона времени. Примером реализации может служить протокол TSP (RFC3161).

Функциями нотариального сервиса являются:

- преобразование документов, оформленных на бумажном носителе, в электронную форму без потери юридической силы, присущей бумажному документу в силу имеющихся на нем реквизитов;
- преобразование электронных документов, в форму документов на бумажном носителе без потери юридической силы, присущей электронному документу в силу имеющейся под ним электронной подписи;

- безусловное подтверждение волеизъявления физического лица, совершенного в присутствии нотариуса, путем заверения электронной подписи участника (волеизъявителя) электронной подписью нотариуса;
- нотариальное удостоверение сделок в электронной форме путем проставления дополнительной электронной подписи (ЭП нотариуса) на данных, фиксирующих сделку.

Приведенный набор функций не претендует на полноту, при необходимости он может быть дополнен.

Особенностью нотариального сервиса является условие обязательного участия нотариуса, как субъекта, в процессе выполнения указанных функций. Это означает, что к нотариальному сервису неприменимо понятие централизованного оператора. Поэтому рассматривается единственная реализация сервиса с децентрализованным оператором, под которым подразумеваются нотариусы (нотариаты).

Доверие между институтами нотариата различных юрисдикций может обеспечиваться посредством сервиса апостилирования.

2.2.4. Сервис апостилирования

Сервис апостилирования предназначен для заверения данных (контент, подпись, зашифрованный контент и пр.) для юридически значимого применения в пределах различных юрисдикций. Иными словами, заявитель (УС или иной субъект информационного взаимодействия) и УЦ, выпустивший сертификат подписанта проверяемой ЭП, принадлежат различным юрисдикциям.

Сервис апостилирования по запросам УС и иных участников информационного взаимодействия выдает следующие типы квитанций:

- квитанция о результате проверки ЭП;
- квитанция о результате проверки действительности сертификата подписанта.

Выданные сервисом апостилирования квитанции могут быть пролонгированы, с помощью соответствующего запроса.

Heavy-реализация подразумевает децентрализованную архитектуру. В данной архитектуре национальные сервисы апостилирования различных юрисдикций взаимодействуют непосредственно между собой.

Порядок работы в данном случае следующий. Заявитель направляет запрос на проверку ЭП в национальный сервис апостилирования (принадлежащий той же юрисдикции, что и заявитель). Национальный сервис апостилирования перенаправляет запрос в тот национальный сервис апостилирования, который взаимодействует с УЦ, выпустившим сертификат подписанта. Квитанция о проверке ЭП по той же цепочке в обратном порядке перенаправляется заявителю. В данной реализации заявитель непосредственно взаимодействует только с национальным сервисом апостилирования своей юрисдикции; процедуры взаимодействия национальных сервисов апостилирования между собой для заявителя скрыты.

Взаимодействие национальных сервисов апостилирования между собой осуществляется с применением специализированных сертификатов. Управление

жизненным циклом данных специализированных сертификатов осуществляет один УЦ; оператор данного УЦ имеет статус международной организации.

Такой подход с одной стороны обеспечивает возможность централизованного управления инфраструктурой национальных сервисов апостилирования, а с другой стороны обеспечивает распределение нагрузки между национальными сервисами апостилирования и повышает безотказность инфраструктуры в целом. Однако возникает необходимость в утверждении единого криптографического алгоритма, используемого при взаимодействии национальных сервисов апостилирования.

2.2.5. Сервис местоположения

Сервис местоположения предназначен для заверения места совершения операции (к примеру, места внесения учетной записи или места издания электронного документа).

Heavy-реализация – запись УС содержит атрибут, в котором указываются координаты места совершения операции (например, координаты, полученные от спутниковых группировок ГЛОНАСС/GPS). Координаты заверяются ЭП оператора сервиса местоположения.

2.2.6. Сервис мониторинга правовых статусов

Сервис мониторинга правовых статусов субъектов информационного взаимодействия (далее СМПС) предназначен для регистрации, поддержания в актуальном состоянии и прекращения действия правовых статусов субъектов информационного взаимодействия - юридических лиц, а также

правомочий, полномочий и прав подписи физических лиц.

Heavy-реализация – правовой статус субъекта указывается в его атрибутном сертификате. Атрибутный сертификат может быть однозначно связан с сертификатом ЭП субъекта или с любым другим документом.

Управление жизненным циклом атрибутного сертификата осуществляет оператор СМПС, алгоритм работы которого аналогичен алгоритму работы УЦ, управляющего жизненным циклом сертификатов ЭП.

Сервис имеет децентрализованную архитектуру и так же как реализации сервиса подписи отношения доверия между различными операторами СМПС могут быть построены:

- по принципу кросс-сертификации или иерархии СМПС во главе с СМПС, обладающим статусом международной организации – Heavy-1-реализация сервиса СМПС;
- с применением сервиса апостилирования – Heavy-2-реализация сервиса СМПС.

Преимуществом данной реализации является отсутствие необходимости в перевыпуске сертификата ЭП при изменении правомочий субъекта. Сертификат субъекта выпускается на длительный период и перевыпускается только в случае изменения идентификационных данных субъекта (к примеру, ФИО). В то же время атрибутный сертификат отражает правомочия субъекта в конкретной УС и может перевыпускаться всякий раз, как изменяются правомочия субъекта (к примеру, при

изменении должности субъекта). Субъект может обладать неограниченным числом атрибутных сертификатов, каждый из которых отвечает за тот или иной вид правомочий.

2.2.7. Сервис обеспечения платежей

Сервис обеспечения платежей предназначен для подтверждения фактов оплаты сборов, тарифов, налогов и т.п., связанных с совершением юридически значимых действий.

Heavy-реализация – субъект оплачивает комплекс услуг, включающий возможность использования установленной совокупности учетных систем и сервисов общей инфраструктуры. При этом стоимость указанного комплекса услуг может закладываться в стоимость выпуска и обеспечения жизненного цикла сертификата ЭП субъекту.

2.2.8. Сервис доверенного хранения данных

Сервис доверенного хранении данных предназначен для реализации своеобразной «банковской ячейки» в которой можно хранить, в том числе в зашифрованном виде, юридически значимую информацию в отношении отдельных физических и юридических лиц (по договору с ними), в случае, когда затраты на самостоятельное хранение таких данных представляются для пользователей излишними или небезопасными.

Heavy-реализация – данные хранятся в сервисе доверенного хранения в шифрованном виде с применением асимметричного шифрования. Доступ к данным осуществляется с применением СМПС. Передача данных в сервис хранения осуществляется по защищенному каналу.

2.2.9. Информационный сервис

Информационный сервис выполняет справочно-информационную функцию – предоставляет пользователям возможность ознакомления с теми или иными данными УС.

Heavy-реализация – информационный сервис содержит динамично изменяющиеся материалы. Сервис реализован отдельным оператором (операторами), обеспечивающим повышенные требования к доступности информации.

2.2.10. Сервис доступа

Совершение информационных транзакций в режиме on-line предполагает отсутствие непосредственного контакта УИВ. При этом возникает проблема надежной дистанционной идентификации, которая особенно актуальна в процессе УСО.

В процессе УСО участниками могут выступать: истцы, ответчики, нейтральные стороны, операторы платформ УСО, провайдеры сервисов УСО. Требования идентификации для всех них должны быть унифицированы и четко определены.

Сервис доступа обеспечивает:

1. защищенный доступ для пользователей российских криптографических алгоритмов;
2. гибкие механизмы задания политики разграничения доступа;
3. разграничение доступа на основе любых элементов X.509 сертификатов;
4. настраиваемые механизмы проверки сертификатов, включая поддержку протокола OCSP и самостоятельное построение цепочки сертификации. Поддерживается также использование сетевого справочника (LDAP) и точек распространения списков отозванных сертификатов и обновлений к ним;
5. поддержку кросс-сертификатов и «мостов доверия».

Для выработки требований надежной идентификации на системной основе, необходимо обозначить основные элементы системы, которые обеспечивают идентификацию УИВ при совершении ими информационных транзакций. К таковым компонентам можно отнести:

- набор идентификационных признаков, которыми может быть формализовано описан участник (физическое или юридическое лицо), для целей дистанционной идентификации – идентификаторы;
- средства доступа;
- операторы сервиса доступа.

Для систем идентификации можно выделить типовой процесс доступа к информационным ресурсам, состоящий из следующих этапов:

1) Присвоение адекватного идентификатора участника до начала той или иной информационной транзакции.

2) Регистрация идентификатора в информационной системе оператора сервиса доступа.

3) Предоставление доступа участнику к совершению им информационных транзакций путем соотнесения предъявленного участником идентификатора с зарегистрированными в отношении этого участника прав. Данный этап включает в себя:

- идентификацию – предъявление участником идентификатора в системе;
- аутентификацию – проверка принадлежности участнику предъявленного им идентификатора;
- авторизацию – предоставление участнику определенных прав доступа.

4) Регламентированная фиксация результатов процедуры доступа и предоставление информации о событиях доступа.

Идентификаторы можно разделить на две категории:

- свойства, которыми обладает участник (внешность, отпечаток пальца, голос, ДНК и т.п.);
- информация, которую знает участник (ФИО, пароль, псевдоним, закрытый ключ ЭП и т.п.).

Очевидно, что применение различных типов идентификаторов и вариантов организации операторов сервиса доступа требует различных финансовых затрат. Поэтому для каждой области применения необходимо выработать такие наборы идентификационных признаков, которые с одной стороны, могут обеспечить надежный контроль доступа участников информационного взаимодействия к совершению ими информационных транзакций, а с другой стороны, могут

обеспечить низкую стоимость сервиса доступа. Необходимый уровень контроля доступа может быть определен на основе анализа модели угроз и уязвимостей для различных информационных систем.

Перечисленный набор сервисов может расширяться и дополняться в соответствии международными рекомендациями ITU-T X.842 «Информационная технология – методы безопасности – Руководящие принципы для использования и управления услугами доверенной третьей стороны».

2.3. Описание правил организации электронной идентификации/аутентификации и электронных сервисов доверия для надлежащего функционирования трансграничного пространства доверия электронным подписям в странах ЕС (Положение ЕС об электронной идентификации и услугах доверия eIDAS)

Документ «Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC» (далее – Положение) вступил в силу в Европейском союзе 17.09.2014 г., что является основанием для прекращения действия с 01.07.2016 г. Директивы Европейского парламента и Совета 1999/93/ЕС от 13 декабря 1999 года «О правовых основах Сообщества для электронных подписей» (далее – Директива).

Отметим, что Директива стала одним из первых документов в мире, регулирующим доверенные электронные сервисы, однако только в ограниченной их части (в части электронной подписи). Новое Положение осуществляет переход к комплексному регулированию использования доверенных электронных услуг, к которым отнесены:

- электронная подпись[7] и проверка электронной подписи;
- электронная печать[8] и проверка электронной печати;
- электронный штамп времени[9];
- электронная контролируемая доставка[10];
- аутентификация сайтов;
- долговременная сохранность электронных подписей, печатей и/или сертификатов, связанных с этими услугами.

Следует отметить, что по вопросу электронной идентификации акт затрагивает только те схемы идентификации, о которых страны официально

---

[7] Здесь и далее для данного раздела приведены определения из Положения.
Электронная подпись - данные в электронной форме, присоединенные или логически связанные с другими данными в электронной форме и используемые подписантом для подписания.

[8] электронная печать - данные в электронной форме, присоединенные или логически связанные с другими данными в электронной форме и подтверждающие их происхождение и целостность.

[9] электронный штамп времени - данные в электронной форме, устанавливающие связь других данных в электронной форме с конкретным временем и создающие тем самым доказательство существования указанных данных в этот момент времени.

[10] электронная служба контролируемой доставки (electronic registered delivery service) - сервис, обеспечивающий возможность передачи данных между третьими сторонами с использованием электронных средств и обеспечивающий доказательства, относящиеся к обработке передаваемых данных, в том числе доказательства отправки и получения данных; а также защищающий передаваемые данные от риска утраты, кражи, повреждения или внесения несанкционированных изменений.

известили Евросоюз, и только тех поставщиков услуг, которые работают на уровне Евросоюза. В плане оказания услуг доверия, акт не затрагивает случаи оказания таких услуг в рамках закрытых систем, действующих на основании национального законодательства или соглашений между ограниченным кругом участников.

Основные вопросы, регулируемые Положением:

1. Правила организации электронной идентификации/аутентификации и электронных сервисов доверия для электронных транзакций для обеспечения надлежащего функционирования внутреннего рынка ЕС.
2. Условия, на которых Государства-участники должны признавать и принимать средства электронной идентификации физических и юридических лиц, подпадающие под заявленную схему электронной идентификации другого Государства-участника.
3. Правовая и организационная основа для электронных подписей, электронных печатей, электронных штампов времени, электронных документов, электронных сервисов доставки и аутентификации веб-сайтов.

Технологические требования и требования по безопасности к электронным подписям, печатям и штампам времени практически совпадают с приведенными в Директиве и в Положении содержатся ссылки на соответствующие статьи Директивы.

Различие между подписями и печатями – функционально-правовое. Согласно данным в Положении определениям, в отличие от подписи (т.е. выражения воли подписанта[11]), которая всегда совершается физическим лицом-подписантом, печать предназначена для использования юридическими лицами (п.59 преамбулы) и лишь удостоверяет происхождение и целостность покрываемых ею данных.

Положение применяется:

- к электронной идентификации/аутентификации конечных пользователей/систем, предоставляемой и осуществляемой от имени или под ответственность Государств-участников;
- к операторам сервисов доверия, учрежденным в Евросоюзе и предоставляющим необходимую техническую инфраструктуру,
- к органам надзора за операторами сервисов доверия;
- к предоставляемым операторами сервисов доверия услугам.

Положение не применяется к предоставлению сервисов доверия, основанных на добровольных соглашениях в соответствии с частным правом, а также к аспектам, относящимся к заключению и действительности контрактов или иных правовых обязательств, в случаях, когда существуют специальные требования, предусмотренные национальным правом.

В части терминологии необходимо упомянуть употребление понятий усиленная и квалифицированная электронная подпись (advanced electronic signature и qualified electronic signature*)*. При этом эквивалентной в правовом отношении собственноручной подписи признается только квалифицированная электронная подпись. В Положении подчёркивается, что квалифицированной признается усиленная электронная подпись, созданная на основе квалифицированного сертификата и обязательно с использованием квалифицированного устройства для создания электронных подписей. В результате фактически появился ещё один

[11] подписант - физическое лицо, которое создает электронную подпись.

подвид подписи – усиленная электронная подпись на основе квалифицированного сертификата (но не являющаяся квалифицированной электронной подписью).

Кроме того, в Распоряжении услуги не всегда последовательно поддерживают определенный уровень доверия (например, «квалифицированный уровень»). Наглядным примером такого непоследовательного подхода является описание квалифицированного штампа времени, в требованиях которого указывается применение усиленной, а не квалифицированной подписи. Тем самым понижается уровень доверия к сервису штампов времени. Логично и целесообразно при оказании услуг квалифицированных сервисов применять квалифицированную подпись, чтобы не возникало «разрывов» в предоставляемом уровне доверия на всей цепочке между участниками электронного взаимодействия.

Положение является достаточно четким и структурированным документом, но предмет его рассмотрения относительно узок, а также присутствует ограничение по применяемым технологиям (предполагается применение технологии PKI и TSL–списков).

Положение устанавливает общие для всех сервисов доверия требования в части обеспечения безопасности, доступности, интероперабельности. Операторы сервисов доверия могут быть как неуполномоченными (неквалифицированными), так и уполномоченными (квалифицированными). При этом под квалифицированным оператором сервиса доверия понимается оператор сервиса доверия, который отвечает требованиям, установленным данным Положением. Необходимыми условиями обеспечения качества предоставляемых услуг операторами сервисов доверия в Положении названы журналирование и архивное хранения журналов операций, выполняемых сервисами доверия, также регулярный аудит деятельности уполномоченных (квалифицированных) операторов сервисов доверия.

Необходимо также отметить, что в рамках реализации Положения до 18 сентября 2015 г. должны быть определены:

- процедуры устанавливания и проверки личности физических и юридических лиц, которые обращаются за получением средств электронной идентификации;
- процедуры выдачи средства электронной идентификации;
- механизмы аутентификации доверенной стороны, где физическое или юридическое лицо использует средство электронной идентификации;
- организационные формы единицы, принимающей участие в процессе выдачи средств электронной идентификации;
- технические спецификации и спецификации безопасности выданного средства электронной идентификации;
- технические спецификации и форматы доверенных списков (TSL-списки);
- форматы усовершенствованной электронной подписи или методы ссылок, в случае если использованы альтернативные форматы.

Очевидно, что перечисленные процедуры и спецификации, в случае участия администраций железных дорог стран членов ОСЖД в трансграничном электронном взаимодействии с железнодорожными администрациями стран Евросоюза, должны быть реализованы в структурах администраций железных дорог стран членов ОСЖД, уполномоченных предоставлять доверенные сервисы и услуги идентификации.

2.4. Анализ использования электронных документов и электронной подписи в хозяйственной деятельности стран Азиатско-Тихоокеанского региона

2.4.1. АТЭС

В рамках АТЭС был создан в 2005 году научно-исследовательский центр электронного правительства при Университете Васеда (Waseda University) в Токио, Япония, для выработки решений различных задач электронного правительства. Он также предлагает рекомендации по совершенствованию внедрения электронного правительства. Проект находится на самофинансировании Японии, Сингапура, Таиланда и китайского Тайпея. Основная деятельность центра – мониторинг и оценка проекта электронного АТЭС, поддержание банка данных "электронного правительства" для стран-членов и проведение дистанционных тренингов системы[12].

Одной из проблем по данной тематике является обеспечение безопасной передачи трансграничных электронных документов для защиты прав и законных интересов граждан и организаций, находящихся под юрисдикцией различных стран, в том числе на платформе международной информационной безопасности. Одним из основных препятствий по обеспечению безопасности трансграничной электронной среды является неоднородность видов инфраструктуры ИКТ для электронного обмена документами и отсутствие международных стандартов для совместимости.

Для обсуждения этих вопросов в России в сентябре 2013 г. был организован семинар экспертов АТЭС "Интероперабельные ИКТ: семантический, лингвистический и другие аспекты". В семинаре приняли участие представители 10 экономик АТЭС, представители международных организаций, таких как: ЮНСИТРАЛ, ЕЭК ООН, Паназиатский альянс по электронной торговле, а также Европейского союза (Германия).

Положение на мировой арене в области интероперабельности ИКТ было охарактеризовано участниками семинара следующими утверждениями:

1. Наличие огромного числа информационных систем, действующих в рамках правительственных учреждений и компаний, и которые различаются по используемому оборудованию и программному обеспечению, и большинство из которых не может напрямую обмениваться информацией в режиме «машина-машина».
2. Наличие десятков конкурирующих стандартов, которые только затрудняют информационный обмен несмотря на огромную работу, проводимую многочисленными органами по стандартизации (на национальном, региональном и международном уровнях).
3. Большинство развитых стран не готово отказаться от уже созданных и эффективно функционирующих информационных систем в пользу будущих еще несуществующих систем.
4. Отсутствие единых стандартов в области аналитической деятельности.

[12] http://apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.aspx

Итоги семинара могут быть сгруппированы в двух основных областях: особенности технической совместимости ИКТ и использование организационных, правовых и технологических механизмов для совместимости ИКТ.

В качестве основных особенностей технической совместимости выделены:

1. Технические стандарты и спецификации. Развитие Интернета сделало возможным широкое распространение и добровольное принятие ряда технических стандартов, спецификаций и Интернет-протоколов. Взаимодействие, таким образом, означает способность обеспечить беспрепятственный двунаправленный поток данных через определенные интерфейсы.
2. Децентрализованная и масштабируемая архитектура и администрирование. Интернет состоит из взаимосвязанных сетей, которые работают независимо от централизованной структуры или администрации. Это позволяет легко добавлять новые системы, приспособленные к местным условиям и потребностям пользователей.
3. Технологическая нейтральность. Пользователи и приложения в разных сетях могут взаимодействовать посредством разных технологий, систем и языков. С учетом быстрых темпов технологического прогресса нейтральные нормы направлены на то, чтобы позволить использование любых будущих разработок без принятия дополнительных мер законодательного порядка.
4. Клиентоориентированная архитектура. Обеспечивает взаимосвязь различных систем и сервисов, что обеспечивает инновационное развитие и постоянное совершенствование.
5. Повышение надежности работы объектов инфраструктуры: при взаимодействии отдельные системы могут способствовать повышению общей устойчивости и надежности, отчасти потому, что отказ составных частей, как правило, не угрожает выходом из строя всей сети.

Описанный подход основан на преимущественно либеральной модели, направленной на совместимость ИКТ.

Во второй области считается необходимым использовать в основном нормативно - организационные, правовые и технологические механизмы для обеспечения более высокого уровня взаимного доверия и безопасности. Этот подход основан на применении следующих принципов:

1. Унификация. В ИКТ должна использоваться единая организационная и техническая инфраструктура (единые формы представления информации) для организации трансграничного электронного документооборота.
2. Масштабируемость. Совместимые организационные и технические инфраструктуры должны поддерживать возможность регистрации новых участников, так чтобы они оперативно могли начать использование системы. Эти инфраструктуры должны также позволить пользователям выбирать набор услуг, соответствующие их потребностям.
3. Равная надежность инфраструктуры, в которой применяются общие минимальные единые требования безопасности для всех ее участников.
4. Легализация электронных документов с обеспечением их признания в равной степени в соответствующих юрисдикциях.

5. Клиентоориентированная архитектура, которая включает в себя простые, четкие и удобные пользовательские интерфейсы, и единую систему доступа к сервисам электронного обмена документами.
6. Систематизация, которая включает в себя следующие компоненты:

- согласованность организационных, правовых и технических мер;
- единство структуры доверия и инфраструктурных систем;
- переход от двустороннего взаимодействия к мультивекторной совместимости там, где это уместно;
- согласованные лингвистические алгоритмы и технологии для информационных систем.

Второй подход нашел свое отражение в представленных Россией материалах в документ Международного саммита информационного общества (World Summit on the Information Society, WSIS) "WSIS+10 Vision for WSIS Beyond 2015".

Эксперты АТЭС по итогам семинара высказали предположение, что оба подхода и их сочетание могут быть использованы в строительстве двусторонних или многосторонних международных информационных систем трансграничного электронного документооборота в Азиатско-Тихоокеанском регионе, в зависимости от функциональности и соответствующих требований к обеспечению доверия и безопасности. Для этого необходимо предпринять следующие первоочередные меры:

1. Инициирование на встрече АТЭС диалога о трансграничном обмене нормативными документами и сбор информации о существующей практике в этой области.
2. Разработка правовой базы взаимодействия на уровне АТЭС.
3. Обеспечение признания результатов удостоверения аутентичности, передаваемой в трансграничном режиме информации. Этого можно достигнуть путём создания системы национальных удостоверяющих центров и национальных регуляторов этих центров, заключения международного соглашения о взаимном признании и условиях взаимного признания результатов удостоверения аутентичности, передаваемой в трансграничном режиме информации.
4. Обеспечение трансграничности, транспарентности и безбарьерности. Необходима разработка стандартов для юридически значимого взаимодействия как внутри стран, так и между различными странами.
5. Преодоление лингвистических барьеров. Поиск решения проблемы совместимости существующих стандартов, стандартных классификаций, справочников (национальных, международных, отраслевых и т.д.), используемых экономиками в сети Интернет, и разработка электронных сделок и лингвистических алгоритмов для информационных систем электронной торговли.
6. Преодоление неоднородности в аналитической деятельности различных экономик. Разработка единых стандартов в области аналитической решений.

Следует также отметить, что оба подхода легли в основу основополагающих принципов Комиссии ООН по праву международной торговли, ЮНСИТРАЛ (United Nations Commission on International Trade Law, UNCITRAL) о недискриминации, функциональной эквивалентности и технологической нейтральности в отношении систем электронного документооборота.

2.4.2. Китай

Осуществляя стратегию "один пояс – один путь" (Экономический пояс Шелкового пути и "Морской Шелковый путь 21-го века"), Китай постепенно выявляет потенциал развития трансграничной электронной торговли с Россией и странами Центральной и Западной Азии. Все большее число китайских предприятий, находящихся в приграничных районах, обращают свой взгляд на развитие трансграничной электронной торговли и строительство "Сетевого Шелкового пути".

Продолжительный рост уровня взаимного политического доверия и стратегического взаимодействия между Китаем и Россией, активное участие правительств и деловых кругов двух стран в продвижении торговли, улучшение бизнес-климата, снижение уровня таможенных пошлин и совершенствование финансовой системы в России предоставляют исключительные возможности для развития китайско-российской трансграничной электронной торговли.

В соответствии с распоряжением Правительства Российской Федерации от 10 октября 2011 г. № 1772-р в ходе 16-й регулярной встречи правительств России и Китая в Пекине 11 октября 2011 г. был подписан Меморандум между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области модернизации экономики. Реализация положений Меморандума призвана способствовать созданию благоприятных условий для ведения предпринимательской деятельности, усилению модернизационной составляющей российско-китайского торгово-экономического сотрудничества, содействовать реализации совместных проектов, инвестированию в инновационные технологии, созданию и продвижению на рынок конкурентоспособных продуктов. Договоренности формулируются следующим образом (раздел Информационно-коммуникационные технологии, пункт 3):

«Стороны признают важность организации трансграничного взаимодействия с использованием электронной цифровой подписи и признают необходимость сотрудничества в рамках создания общей инфраструктуры документирования информации в электронном виде с целью придания юридической значимости обмену многопрофильной информацией и обеспечения охраны прав потребителей современных электронных услуг. Стороны признают целесообразность активизации деятельности по подготовке комплексных предложений, направленных на решение задачи обеспечения трансграничного взаимодействия и функционирования информационных систем».

Для стимуляции применения электронного документирования информации и онлайновой торговой индустрии парламент КНР узаконил электронные подписи. Закон дает электронным подписям равноценный статус с собственноручной подписью и позволяет использовать их при совершении онлайновых сделок. Однако закон четко определяет сферы применения электронных подписей (так же, как в Чехии, Франции, Японии, Бельгии, Китае, Индии). Например, финансовые контракты электронной подписью не подписываются.

3. Рекомендации по учету в деятельности администраций железных дорог стран - членов ОСЖД требований ЕС и стран Азиатско-Тихоокеанского региона в области юридически значимого трансграничного электронного документооборота

Формирование трансграничного пространства доверия, обеспечивающего юридическую значимость международного электронного взаимодействия, предполагает создание совокупности сервисов, деятельность которых должна быть гармонизирована на правовом, организационном и технико-технологическом уровне.

При этом следует иметь в виду, что речь идет о гармонизации децентрализованных и не интегрированных национальных систем документооборота, разработанных на различных технологиях, принципах и приоритетах, которые весьма сложно сочетать и интегрировать.

Сегодня в большинстве национальных законодательных актах вопрос международного признания электронной подписи (и связанных с ней ключей и их сертификатов) обеспечивается включением соответствующих положений. В подобных положениях говорится, что электронная подпись, которая может быть проверена ключом проверки электронной подписи (открытым ключом), имеющим иностранный сертификат, признается таковой, если с государством, орган которого выдал сертификат, имеется договор о признании таких электронных подписей.

Трансграничный электронный документооборот в деятельности администраций железных дорог стран членов ОСЖД связан зачастую с государствами ближнего зарубежья, с которыми отсутствуют договора (соглашения) о взаимном признании электронных подписей (например, для ОАО «РЖД» данный момент это – Белоруссия и Украина, в перспективе – Литва, Латвия, Казахстан).

Для функционирования подобного юридически значимого трансграничного электронного документооборота наибольшее значение имеют договоры между службами третьих доверенных сторон государств-участников (или компаний-участников) международного информационного обмена. В Приложении 1 приведен пример содержания подобного договора. В настоящее время такие договоры уже заключены и действуют между некоторыми ДТС администраций железных дорог стран членов ОСЖД и организациями, выполняющими функции ДТС в интересах железных дорог России, Белоруссии, Украины, Литвы, Латвии и Казахстана.

Кроме того, установление доверия между ответственными органами различных стран, операторами соответствующих сервисов и конечными пользователями УС требует дальнейшей разработки нормативной базы в целях применения ответственными органами и операторами сервисов доверия общих согласованных процедур.

Далее рассмотрен примерный перечень нормативно-организационных документов, разработка которых в администрациях железных дорог стран – членов ОСЖД может потребоваться для корректной реализации трансграничного электронного взаимодействия и участия Холдинга в построении единого пространства доверия. Предлагаемый перечень основывается на документе "Концепция разработки и принятия проектов документов для координации и аудита деятельности участников ОИД", разработанном по заказу Минком связи РФ

в рамках работ Регионального содружества в области связи (РСС) по формированию трансграничного пространства доверия (далее ПД-Т) и соответствует самому общему случаю низкого уровня доверия (так называемая Heavy-реализация, см. п. 2.2 настоящего документа) между участниками информационного взаимодействия, что влечет за собой децентрализованную реализацию сервисов доверия.

Кроме того, предполагается наличие национального регулятора ОИД, что обуславливается возложением на Минком связи РФ функции доверенной третьей стороны при обмене электронными документами в случаях, если ее участие в таком обмене предусмотрено международными договорами Российской Федерации (Постановление Правительства Российской Федерации от 24 июля 2014 г. № 698).

3.1. Документы правового блока

3.1.1. Положение об операторе сервиса места (СМ)

- закрепляет за УЛО УС право обращаться к оператору СМ с запросом на заверение места совершения операции и устанавливает обязанность оператора СМ обработать такое обращение;
- устанавливает необходимую и достаточную информацию, содержащуюся в ответе на запрос на заверение места совершения операции;
- устанавливает национального регулятора ОИД, ответственным за аккредитацию операторов СМ;
- устанавливает перечень документов, необходимый и достаточный для аккредитации юридического лица в качестве оператора СМ;
- устанавливает Реестр национальных операторов СМ в качестве основного источника информации об аккредитованных операторах СМ;
- устанавливает национального регулятора ОИД, ответственным за ведение Реестра операторов СМ;
- указывает услуги операторов СМ, которые оказываются возмездно и безвозмездно.

3.1.2. Положение об операторе сервиса доверенного хранения данных (СДХД)

- устанавливает, какие документы проверяются средствами оператора СДХД, и какие документы оператор СДХД проверяет посредством обращения в соответствующие УС;
- закрепляет за клиентом право обращаться к любому оператору СДХД с запросом на внесение изменений/удаление учетной записи и устанавливает обязанность оператора СДХД обработать такое обращение;
- устанавливает для СДХД перечень операций с учетными записями, для выполнения которых необходимо предъявить идентификатор и проверить действительность сертификата клиента;
- закрепляет за клиентом право обращаться к любому оператору СДХД с запросом на предоставление данных по учетной записи и устанавливает обязанность оператора СДХД обработать такое обращение;
- устанавливает для каждой УС перечень операций с учетными записями, для выполнения которых необходимо предъявить идентификатор, проверить действительность сертификата и правовой статус клиента;

- устанавливает национального регулятора ОИД ответственным за аккредитацию операторов СДХД;
- устанавливает перечень документов, необходимый и достаточный для аккредитации юридического лица в качестве оператора СДХД;
- устанавливает Реестр национальных операторов СДХД в качестве основного источника информации об аккредитованных операторах СДХД;
- устанавливает национального регулятора ОИД, ответственным за ведение Реестра операторов СДХД.

3.1.3. Положение об операторе информационного сервиса (ИС)

- закрепляет за УЛО УС право обращаться к оператору ИС с запросом на публикацию данных и устанавливает обязанность оператора ИС обработать такое обращение;
- устанавливает перечень документов, необходимый и достаточный для публикации данных;
- устанавливает, какие документы проверяются средствами оператора ИС, и какие документы оператор ИС проверяет посредством обращения в соответствующие УС;
- закрепляет за клиентом право обращаться к любому оператору ИС с запросом на предоставление данных по учетной записи и устанавливает обязанность оператора ИС обработать такое обращение;
- устанавливает для каждой УС перечень операций с учетными записями, для выполнения которых необходимо предъявить идентификатор, проверить действительность сертификата и правовой статус клиента;
- устанавливает национального регулятора ОИД, ответственным за аккредитацию операторов ИС;
- устанавливает перечень документов, необходимый и достаточный для аккредитации юридического лица в качестве оператора ИС;
- устанавливает Реестр национальных операторов ИС в качестве основного источника информации об аккредитованных операторах ИС;
- устанавливает национального регулятора ОИД, ответственным за ведение Реестра операторов ИС.

3.1.4. Положение об операторе сервиса мониторинга правовых статусов (СМПС)

- закрепляет за клиентом право обращаться к любому национальному оператору СМПС с просьбой выпустить атрибутный сертификат и устанавливает обязанность оператора СМПС обработать такое обращение;
- устанавливает перечень документов, необходимый и достаточный для выпуска атрибутного сертификата клиенту;
- устанавливает какие документы проверяются средствами оператора СМПС, и какие документы оператор СМПС проверяет посредством обращения в соответствующие УС;
- устанавливает типы сертификатов и идентификаторов, необходимую и достаточную информацию, содержащуюся в сертификате;

- закрепляет за клиентом право обращаться к любому оператору СМПС с просьбой проверить атрибутный сертификат и устанавливает обязанность оператора СМПС обработать такое обращение;
- устанавливает перечень необходимых и достаточных условий, выполнение которых является основанием для признания атрибутного сертификата действительным;
- закрепляет за клиентом право обращаться к оператору СМПС, который выпустил ему атрибутный сертификат, с просьбой приостановить/возобновить действие/отзывать атрибутный сертификат и устанавливает обязанность оператора СМПС обработать такое обращение;
- устанавливает структуру списка аннулированных атрибутных сертификатов и необходимую и достаточную информацию, содержащуюся в списке;
- устанавливает типы доступа к списку аннулированных атрибутных сертификатов on-line/off-line;
- устанавливает национального регулятора ОИД, ответственным за аккредитацию операторов СМПС;
- устанавливает перечень документов, необходимый и достаточный для аккредитации юридического лица в качестве оператора СМПС;
- устанавливает Реестр национальных операторов СМПС в качестве основного источника информации об аккредитованных операторах СМПС;
- устанавливает национальную организацию (национального регулятора ОИД), уполномоченную вести Реестр операторов СМПС;
- указывает услуги операторов СМПС, которые оказываются возмездно и безвозмездно.

3.2. Документы организационного блока

3.2.1. Регламент оператора сервиса места (СМ) определяет:

- формат и состав запроса на заверение места совершения операции;
- требования по защите информации.

3.2.2. Регламент оператора сервиса доверенного хранения данных (СДХД) определяет:

- способы обеспечения технической доступности СДХД;
- перечень документов, необходимый и достаточный для добавления/изменения/удаления учетной записи;
- порядок проверки документов средствами оператора СДХД;
- порядок обращения оператора СДХД к другому оператору СДХД для проверки документов;
- требования информационной безопасности;
- требования по защите персональных данных;
- требования по обеспечению архивного хранения;
- требования по протоколированию операций;
- порядок предъявления идентификатора и проверки действительности сертификата Лица;
- требования к применяемым средствам доступа;
- формат и состав запроса на предоставление данных по учетной записи.

3.2.3. Регламент оператора информационного сервиса (ИС) определяет:

- способы обеспечения технической доступности ИС;
- перечень документов, необходимый и достаточный для публикации данных;
- порядок проверки документов средствами оператора ИС;
- порядок обращения оператора ИС к другому оператору ИС для проверки документов;
- требования по обеспечению защиты персональных данных;
- требования по обеспечению архивного хранения;
- требования по протоколированию операций;
- порядок предъявления идентификатора и проверки действительности сертификата Лица;
- требования к применяемым средствам доступа.

3.2.4. Регламент оператора сервиса мониторинга правовых статусов (СМПС) определяет:

- перечень документов, необходимый и достаточный для выпуска атрибутного сертификата клиенту согласно декларируемому правовому статусу последнего;
- порядок проверки документов средствами оператора СМПС;
- порядок обращения оператора СМПС в УС для проверки документов;
- требования по защите персональных данных;
- порядок формирования запроса на проверку действительности атрибутного сертификата;
- способы обеспечения доступности СМПС в части выполнения функций по проверке действительности атрибутных сертификатов;
- содержание квитанции о проверке действительности атрибутного сертификата;
- способы обеспечения доступности оператора СМПС в части приема заявлений на приостановление/возобновление действия/отзыв атрибутных сертификатов;
- порядок предъявления идентификатора и проверки действительности сертификата клиента;
- требования к применяемым средствам доступа;
- требования информационной безопасности;
- максимально допустимое время публикации списка аннулированных атрибутных сертификатов с момента подачи заявления клиентом;
- требования доступности (для on-line и off-line доступа) аутентичности списка аннулированных атрибутных сертификатов;
- порядок сопровождения сертификатов, выпущенных данным оператором.

3.2.5. Сметы услуг операторов СМ, СДХД, ИС, СМПС определяют:

- порядок ценообразования услуг оператора;
- способы оплаты услуг оператора.

3.2.6. Номенклатура и характеристики идентификаторов устанавливают требования:

- для каждого типа идентификатора;
- к порядку утилизации идентификаторов.

3.3. Документы технико-технологического блока

3.3.1. Стандарты, описывающие взаимодействие участников ПД-Т:

- Набор стандартов, описывающих взаимодействие Национального регулятора общей инфраструктуры доверия с оператором УС;
- Набор стандартов, описывающих взаимодействие оператора информационного сервиса с оператором УС;
- Набор стандартов, описывающих взаимодействие оператора сервиса доверенного хранения данных с оператором УС;
- Набор стандартов, описывающих взаимодействие оператора сервиса мониторинга правовых статусов с оператором УС.

3.3.2. Стандарты, описывающие проведение аудита деятельности операторов сервисов доверия Национальным регулятором общей инфраструктуры доверия

- описывают технологию проведения аудита деятельности операторов;
- определяют средства проведения аудита.

3.3.3. Эксплуатационная документация

3.3.4. Инструкции

- описывают технологию проверки документов как в бумажной, так и в электронной формах;
- устанавливают перечень средств для проверки документов.

3.3.5. Формы заявлений

- устанавливают форму заявления клиента при запросе на выпуск сертификата;
- устанавливают форму заявления на проверку действительности сертификата и ЭП;
- устанавливают форму квитанции по результатам проверки действительности сертификата и ЭП.

4. Рекомендации по возможной доработке программно-технических средств администраций железных дорог стран - членов ОСЖД, участвующих в организации юридически значимого трансграничного электронного документооборота

1. Реализация сервисов общей инфраструктуры доверия (сервисов ДТС), описанных в п.2.2 настоящего документа, на уровне Heavy-реализации.
2. Реализация доверенных услуг (в том числе, электронной службы контролируемой доставки) и технических спецификаций, определенных Положением ЕС об электронной идентификации и услугах доверия eIDAS.
3. Реализация технических стандартов и спецификаций интероперабельного взаимодействия.
4. Реализация клиентоориентированной архитектуры, которая включает в себя простые, четкие и удобные пользовательские интерфейсы, и единую систему доступа к сервисам электронного обмена документами.
5. Соблюдение принципов «технологической» нейтральности.

5. Предложения по применению в деятельности администраций железных дорог стран - членов ОСЖД опыта межгосударственных организаций, ЕС и стран Азиатско-Тихоокеанского региона по использованию юридически значимого трансграничного электронного документооборота и построению трансграничного пространства доверия

К настоящему времени технологические решения для организации юридически значимого электронного взаимодействия в грузоперевозочном процессе достаточно глубоко проработаны с железными дорогами России, Белоруссии и Украины. Данные решения базируются на использовании сервисов ДТС – важнейшего элемента построения общей инфраструктуры доверия.

С использованием подобных технологий предполагается в ближайшей перспективе организовать взаимодействие и других администраций железных дорог стран членов ОСЖД с администрациями железных дорог ряда стран Евразии с различным уровнем развития технологий PKI. При этом технологии доверенной третьей стороны позволяют не изменять существующие в странах технологий PKI и упростить их создание, если они еще не развиты.

По сути, отрасль железнодорожного транспорта стран Евразии сейчас стоит на пороге создания ОИД на основе ИОК.

В результате построения ОИД станет возможной проверка информационными системами различных организаций сертификатов ключей проверки электронных подписей, сформированных различными удостоверяющими центрами, входящими в ОИД, а также электронных подписей, сформированных под электронными документами в процессе электронного взаимодействия.

Взаимодействие национальных ИОК и ДТС может быть организовано наиболее эффективным образом при наличии координирующего органа, который выступал бы в роли организатора и координатора ОИД железных дорог Евразии (ОИД ЖД).

Основной функцией такого координирующего органа могла бы стать разработка унифицированного Соглашения между ДТС взаимодействующих железных дорог, содержащего следующие положения:

- права и обязанности служб ДТС;
- юридическая и финансовая ответственность сторон;
- условия обмена информацией между ДТС;
- порядок разрешения споров и конфликтных ситуаций между ДТС.

Кроме того, унифицированное Соглашение могло бы содержать перечень рекомендуемых стандартов и алгоритмов взаимодействия ДТС, из которого взаимодействующие ДТС при заключении двухсторонних соглашений могли бы выбрать устраивающий их вариант с учетом национальных правовых особенностей и ограничений. Также рассматриваемый орган мог бы оказывать необходимое методическое, технологическое и правовое сопровождение процесса взаимодействия ДТС.

Реализация процедур признания в ДТС страны получателя ЭП страны отправителя требует наличия защищенного взаимодействия между ДТС. Это взаимодействие должно осуществляться на сетевом уровне и может быть реализовано как через сеть Интернет, так и через выделенную сеть передачи данных. Таким образом, все ДТС железнодорожных администраций Евразии

должны взаимодействовать через единую систему контролируемой доставки (наличие которой устанавливается Положением ЕС об электронной идентификации и услугах доверия eIDAS), обеспечивающей гарантированную и защищенную передачу документов между этими ДТС.

Система контролируемой доставки должна представлять из себя программно-технический комплекс, к которому подключены по каналам связи все ДТС стран участников. При этом подключение каждой из ДТС осуществляется с использованием защищенных протоколов на базе согласованных криптографических алгоритмов. Взаимодействие ДТС с системой контролируемой доставки строится по схеме квитирования всех получаемых электронных сообщений и документов, что позволяет отправителю контролировать факт передачи в систему сообщений, передачу сообщений получателю, подтверждение получателя о приеме сообщения и т.д. Однако только описанного выше технического решения недостаточно для обеспечения контролируемости доставки. Необходимо обеспечить наличие двусторонних соглашений между оператором системы контролируемой доставки и ДТС участников ОИД. При этом такая система контролируемой доставки должна работать по единым правилам для всех ДТС, входящих в ОИД ЖД. Поэтому в качестве оператора такой системы должен выступать координационный орган ОИД ЖД.

Таким образом, ОИД ЖД строится на базе системы контролируемой доставки, через которую ДТС стран участников взаимодействуют между собой при обеспечении юридической значимости трансграничного электронного документооборота. Координационный орган ОИД ЖД, являющийся оператором системы контролируемой доставки, обеспечивает единый порядок взаимодействия между собой ДТС стран участников с учетом требований национальных законодательств в области использования ЭП. Все участники ОИД ЖД, включая систему контролируемой доставки, должны обладать необходимым набором криптографических алгоритмов для обеспечения юридически значимого взаимодействия между ДТС участников ОИД ЖД через систему контролируемой доставки. Порядок взаимодействия ДТС участников между собой и с системой контролируемой доставки осуществляется на базе двусторонних договоров. Этими же договорами регламентируется обмен участниками криптографическими алгоритмами, сертификатами и ключами подписи. Указанные договорные документы разрабатываются сторонами на базе типовых договорах, определенных координирующим органом ОИД ЖД.

Построение ОИД ЖД должно основываться на следующих основных мероприятиях:

- создание координационного органа ОИД ЖД;
- построение системы контролируемой доставки;
- согласование принципов формирования и обеспечения функционирования ОИД ЖД;
- проработка правовых и организационных вопросов взаимного признания электронной подписи с учетом особенностей национальных законодательств в области ее использования;
- решение комплекса вопросов ввоза-вывоза средств ЭП;
- разработка необходимых типовых документов по заключению соответствующих соглашений с участниками ОИД ЖД;
- формирование ДТС стран участников ОИД ЖД;

- отработка принципов и организационно-технических процедур двустороннего взаимодействия между ДТС участников через систему контролируемой доставки;
- заключение двусторонних договоров между ДТС участников ОИД ЖД.

Учитывая имеющийся опыт и научно-технический задел в решении задач трансграничного электронного взаимодействия ОАО «РЖД» может взять на себя решение следующих задач по построению ОИД ЖД:

- разработка совместно с участниками ОИД ЖД принципов формирования и обеспечения функционирования ОИД железных дорог государств Евразии;
- проработка совместно с участниками ОИД ЖД правовых и организационных вопросов взаимного признания электронной подписи с учетом особенностей национальных законодательств в области ее использования;
- подготовка предложений по техническим и технологическим вопросам построения в ОАО «РЖД» инфраструктуры по проверке и признанию электронных документов с иностранными электронными подписями в рамках ОИД ЖД;
- разработка необходимых типовых документов по заключению соответствующих соглашений с участниками ОИД ЖД;
- проработка вопросов обеспечения финансовых гарантий и ответственности участников трансграничного взаимодействия в рамках информационного обмена с участием страховых и банковских организаций.

6. Список определений и сокращений

АТЭС (APEC)	–	Азиатско-Тихоокеанское экономическое сотрудничество (Asia-Pacific Economic Cooperation)
ДТС	–	Доверенная третья сторона
ИОК	–	Инфраструктура открытых ключей
КЭП	–	Квалифицированная электронная подпись
ОАО «РЖД»	–	Открытое акционерное общество «Российские железные дороги»
ОИД	–	Общая инфраструктура доверия
ПД-Н	–	Национальное пространство доверия
ПД-Т	–	Трансграничное пространство доверия
СКЗИ	–	Средства криптографической защиты информации
УИВ	–	Участник информационного взаимодействия
УЛО	–	Уполномоченное лицо оператора
УС	–	Учетная система
УСО	–	урегулирование споров в режиме on-line (в режиме реального времени)
УЦ	–	Удостоверяющий центр
УЭП	–	Усиленная электронная подпись
ЭД	–	Электронный документ – формализованная запись информации в электронном виде, заверенная электронной подписью и отвечающая правилам и требованиям документирования
ЭДО	–	Электронный документооборот
ЭП	–	Электронная подпись
ЭЦП	–	Электронная цифровая подпись

Приложение 1

Рекомендации по содержанию договора между уполномоченными службами третьей доверенной стороны государства А и государства В

Договор заключается между уполномоченными службами третьей доверенной стороны государства А и государства В, вместе именуемых далее как «стороны», в целях реализации Конвенции о порядке признания юридического значения иностранных электронных документов (сообщений) и/или их электронных подписей в международном информационном обмене, участниками которой являются государство А и государство В, и предназначен для урегулирования порядка взаимодействия сторон в качестве служб третьей доверенной стороны.

Предметом данного договора является:

- порядок взаимодействия сторон договора и условия обмена информацией между сторонами для достижения целей соглашения по признанию юридического значения иностранных электронных документов и/или сообщений и их подписей при международном трансграничном информационном обмене;
- обеспечение гарантий доверия к электронным документам и сообщениям, удостоверенным стороной, в юрисдикции которого находится адресат, и признания правомерности применения электронных подписей в исходящих и/или входящих электронных документах и сообщениях в соответствии с правилами и требованиями национального законодательства страны пребывания службы третьей доверенной стороны.

Стороны должны договориться о том, что они признают юридическую силу электронных документов исходящих от составителей, подпадающих под юрисдикцию противоположной стороны и выполненных по правилам и требованиям ее национального законодательства, если электронный документ или сообщение имеет электронный апостиль, оформленный в соответствии с требованиями Конвенции о порядке признания юридического значения иностранных электронных документов (сообщений) и/или их электронных подписей в международном информационном обмене и выполнен в соответствии с правилами.

Обмен информацией между сторонами, в рамках данного договора осуществляется в виде транзита электронных документов и/или сообщений. Электронный документооборот между сторонами осуществляется в соответствии с правилами, стандартами, техническими протоколами и регламентами электронного документооборота, в рамках которых осуществляется взаимодействие сторон.

Прием, обработка и отправка электронных документов и/или сообщений стороны осуществляют в соответствии с порядком формирования, отправки, приема и обработки транзитных электронных документов, установленным правилами (регламентами, стандартами) обмена электронными документами и/или сообщениями.

Электронные документы или сообщения для прохождения процедуры легализации направляются заинтересованными пользователями стороне договора,

в юрисдикции которой они находятся, с указанием электронного адреса конечного адресата. Легализация сторонами электронных документов и/или сообщений и их подписей при трансграничном информационном обмене осуществляется в порядке, установленном Конвенцией.

Стороны заверяют или удостоверяют форму представления и оборота электронных документов (сообщений), целостность и подлинность их форм представления и оборота (соответственно неприкосновенность и подлинность содержания) и/или соответствие их электронных подписей правилам и требованиям национального законодательства, если иное не установлено межгосударственным соглашением.

Стороны не заверяют или не удостоверяют соответствие содержания (контента) электронных документов и/или сообщений требованиям национального законодательства, если иное не установлено межгосударственным соглашением или национальным законодательством.

Стороны признают, что используемые сторонами средства защиты информации обеспечивают достаточную защиту и целостность форм представления и оборота электронных документов и сообщений и позволяют идентифицировать лиц, от имени которых используется электронные подписи в порядке, установленном правилами и требованиями законодательства каждой стороны.

Стороны должны договориться о том, что вся переписка и обмен документами между сторонами и от имени сторон ведется в электронной форме. Электронные документы или сообщения от имени стороны оформляются в соответствии с порядком и требованиями действующего законодательства стороны, от которой электронный документ или сообщение исходит.

В соответствии с заключенным соглашением стороны должны иметь право:

- осуществлять обмен электронными документами и сообщениями в соответствии с принципами и правилами, установленными в Конвенции;
- передавать информацию, связанную с оказанием услуг третьей доверенной стороны по запросам уполномоченных на то лиц и организаций, имеющих право на их получение в порядке и в соответствии с действующим законодательством стороны;
- приостанавливать информационный обмен на условиях и в порядке, установленном техническими регламентами по проведению регламентных и профилактических работ.

Одновременно стороны, заключившие договор, несут обязанности, в числе которых могут быть названы следующие основные:

- обеспечение в трансграничном обмене взаимных гарантий и доверия к электронным документам и сообщениям;
- обеспечение правомерности применения электронных подписей и способов защиты исходящих и/или входящих электронных документов и сообщений в соответствии с правилами и требованиями национального законодательства страны пребывания стороны договора;
- обеспечение каждой из сторон договора другой стороной (на условиях взаимного обмена) необходимыми регламентами и программными средствами (интерфейсом) для проведения проверок электронных документов (сообщений) и/или их электронных подписей, исходящих от

другой стороны договора и выполненных в соответствии с требованиями ее национального законодательства;

- автоматизированное заверение или удостоверение с формированием электронного апостиля форм представления и оборота входящих транзитных электронных документов и/или сообщений и/или их электронных подписей, исходящих от пользователей, находящихся в юрисдикции (домене) стороны договора на соответствие требованиям национального законодательства и адресованных адресатам, находящимся в юрисдикции (в домене) другой стороны договора;
- легализация стороной договора на основе проведения автоматизированной процедуры проверки всех получаемых от другой стороны транзитных электронных документов и/или сообщений и их апостилей, установленных другой стороной и заверения или удостоверения с формированием собственного апостиля транзитного электронного документа или сообщения, подписанного электронной подписью уполномоченного (должностного) лица легализующей стороны в соответствии с требованиями ее национального законодательства, в которой электронный документ или сообщение должны быть использованы адресатом;
- экспертиза и проверка электронных подписей в электронных документах и сообщениях на подлинность и соответствие требованиям национального законодательства страны с выдачей экспертных заключений в порядке, установленном законодательством страны пребывания стороны;

Каждая сторона договора обязана вести и поддерживать в актуальном и безопасном состоянии электронный реестр (базу данных), в котором должен регистрироваться каждый факт заверения (удостоверения) электронного документа (сообщения) или его электронной подписи и факт формирования электронного апостиля.

Каждая сторона обязана вести автоматизированное документирование всех своих действий и процессов, происходящих в информационной системе стороны и связанных с исполнением услуг третьей доверенной стороны с пошаговой фиксацией даты и времени.

Каждая сторона по запросам другой стороны обязана провести экспертизу электронной подписи в электронных документах и/или сообщениях, сформированных в ее юрисдикции, и предоставить другой стороне экспертное заключение.

Каждая сторона в случае наличия на то указания обязана сформировать и отправить в адрес отправителя уведомление (квитанцию) о исполнении процедур доверия в отношении транзитной корреспонденции с указанием страны реквизитов службы и времени их прохождения.

Каждая сторона обязана обеспечивать другую сторону по ее запросам доказательствами, связанными с действиями стороны по фактам оказания услуг:

- по подтверждению фактов отправки отправителем и или получения адресатом электронных документов и/или сообщений;
- по фактам заверения или удостоверения электронных документов и/или сообщений;
- по фактам удостоверения электронных подписей;
- по экспертизе (проверке) электронных подписей в документах и сообщениях;

- по архивированию и депозитарному хранению контрольных экземпляров электронных документов;
- по исполнению иных действий, связанных с оказанием услуг службы третьей доверенной стороны.

Стороны могут проводить архивирование и депозитарное хранение контрольных экземпляров электронных документов, оказывать заявителям иные дополнительные услуги.

Стороны обязуются в процессах оказания услуг выполнять требования по обеспечению информационной безопасности и конфиденциальности информации, содержащейся в транзитных документах и сообщениях, в соответствии с международными рекомендациями и требованиями действующего законодательства Стороны.

Каждая сторона договора обязана иметь необходимые лицензии, сертификаты или аттестацию на ведение деятельности по оказание услуг третьей доверенной стороны, если в соответствии с требованиями действующего национального законодательства таковые необходимы.

Стороны самостоятельно организуют взаимодействие между своими автоматизированными системами сообщений на основе действующих международных стандартов, рекомендаций и протоколов обмена.

Порядок технического и технологического сопряжения информационных систем сторон и их автоматизированных систем сообщений устанавливается на основе согласованных технических регламентов, стандартов и/или рекомендаций.

За ненадлежащее исполнение своих обязательств стороны несут материальную ответственность в соответствии с требованиями национального законодательства либо положениями международного соглашения об учреждении системы международного юридически значимого документооборота.

При передаче документов и сообщений, полученной от третьих лиц, стороны отвечают за точность и своевременность её обработки, за целостность и соответствие данных полученного и передаваемого сообщения, соблюдение требований обеспечения конфиденциальности информации.

Стороны не несут ответственности за содержание (контент) транзитных электронных документов и/или сообщений, если иное не установлено межгосударственным соглашением или национальным законодательством.

Каждая сторона отвечает за действия, совершаемые лицами, которые уполномочены этой Стороной выполнять от ее имени установленные процедуры и/или услуги третьей доверенной стороны в процессах легализации электронных документов, сообщений и их электронных подписей.

Информация, содержащаяся в транзитных документах и сообщениях, является конфиденциальной и не подлежит разглашению. Стороны обязуются сохранять конфиденциальность этой информации.

Стороны вправе установить для себя претензионный порядок урегулирования споров и разногласий, возникающих из договора. Претензия заявляется в письменной форме и должна быть подписана уполномоченным представителем Стороны. Если по претензии потребуются дополнительные документы, необходимые для ее рассмотрения, они запрашиваются у заявителя претензии. При этом указывается срок, необходимый для их представления. В случае неполучения затребованных документов к указанному сроку, претензия рассматривается на основании имеющихся документов. Ответ на претензию

представляется стороне, заявившей претензию, подписывается уполномоченным представителем Стороны, отвечающей на претензию. Непредставление ответа на претензию рассматривается как отказ в удовлетворении претензии.

Все споры и разногласия, вытекающие из настоящего Договора или в связи с ним, в том числе касающиеся его исполнения, нарушения, прекращения или действительности, которые Стороны не смогли разрешить путем переговоров, подлежат разрешению в соответствии с документами, определяющими ее правовой статус и порядок разрешения споров.

Стороны освобождаются от ответственности за частичное или полное неисполнение своих обязательств, если это неисполнение явилось следствием обстоятельств непреодолимой силы, возникших после заключения договора, или в результате событий чрезвычайного характера, а также сбоев, неисправностей и отказов оборудования; сбоев и ошибок программного обеспечения; сбоев, неисправностей и отказов систем связи, энергоснабжения, кондиционирования и других систем жизнеобеспечения, не позволяющих осуществлять эксплуатацию необходимого для выполнения договора оборудования, которые стороны не могли предвидеть или предотвратить.

Сторона, для которой стало невозможным выполнение своих обязательств в виду действия обстоятельств непреодолимой силы, обязана немедленно сообщить другой стороне о начале, изменении масштаба, характера и прекращении действия обстоятельств, воспрепятствовавших выполнению договорных обязательств.

По прошествии обстоятельств непреодолимой силы стороны обязуются принять все меры для ликвидации последствий и уменьшения причиненного ущерба.

В случае принятия международных или межгосударственных соглашений, или иных нормативных правовых актов по вопросам, регулируемым договором, изменение соответствующих положений договора оформляется дополнительным соглашением.

Каждая из сторон вправе расторгнуть договор, письменно уведомив другую сторону в установленный договором срок.