

# Технологическое и нормативное обеспечение трансграничного электронного юридически-значимого документооборота

## Аналитическая записка

*Материал подготовлен совместно МОО «Ассоциация защиты информации», ООО «Газинформсервис», ООО «Русское Техническое Общество», ООО «Топ Кросс», ООО «УЦ ГИС»*

Целью данной аналитической записки является обоснование наличия достаточных правовых оснований для организации трансграничного защищенного электронного юридически-значимого документооборота при взаимодействии с использованием сервисов доверенной третьей стороны.

Соглашение о государственных (муниципальных) закупках в рамках единого экономического пространства (ЕЭП) (далее – Соглашение) подписано членами Комиссии Таможенного союза в Москве 9 декабря 2010 года.

В соответствии с Соглашением, информационные системы, обеспечивающие процесс проведения закупок в электронном формате стран-членов Таможенного Союза должны дать возможность участия в электронных государственных закупках поставщикам из Белоруссии, Казахстана и Российской Федерации<sup>1</sup>. Под информационными системами для проведения закупок в электронном виде в соглашении понимаются электронные торговые площадки (ЭТП).

Предусмотрена поэтапная реализация Соглашения:

1 этап (для Российской Федерации, Республики Беларусь) - внесение изменений в законодательство каждого из государств Сторон, направленных на приведение в соответствие законодательства каждого из государств Сторон с настоящим Соглашением, внедрение информационных систем, обеспечивающих процесс проведения закупок в электронном формате в соответствии с настоящим Соглашением, и введение национального режима для Российской Федерации и Республики Беларусь - до 1 января 2012 г.;

2 этап (для Республики Казахстан) - внесение изменений в законодательство государства Стороны, направленных на приведение в соответствие законодательства государства Стороны с настоящим Соглашением и внедрение информационных систем, обеспечивающих процесс проведения закупок в электронном формате в соответствии с настоящим Соглашением - до 1 июля 2012 г.;

---

<sup>1</sup> «национальный режим» - режим, предусматривающий, что каждая Страна обеспечивает для целей закупок товаров (работ, услуг), происходящих с территорий государств Сторон, поставщикам и потенциальным поставщикам государств Сторон, предлагающих такие товары, выполняющих работы и оказывающих услуги для целей закупок, режим не менее благоприятный, чем предоставляется национальным товарам (работам, услугам), поставщикам и потенциальным поставщикам своего государства, предлагающим такие товары, а также выполняющим работы и оказывающим услуги. Страна происхождения товара определяется в соответствии с правилами определения страны происхождения товаров, действующими на единой таможенной территории Таможенного союза.

3 этап (для Российской Федерации, Республики Беларусь, Республики Казахстан) введение национального режима для всех государств Сторон - до 1 января 2014 года.

Однако по состоянию на декабрь 2012 года такая возможность в эксплуатационном режиме не предоставляется ни одной из официальных ЭТП стран-членов единого экономического пространства.

Основной (если не единственной) причиной, которая, по мнению законодателей, регуляторов и исполнителей (Совет Федерации, Государственная Дума, Минкомсвязь, Минэкономразвития, ФСБ, ФАС и Евразийская Экономическая Комиссия), препятствует исполнению данного соглашения, является неопределенность в нормативном обеспечении применения аналогов собственноручной подписи - электронной подписи (ЭП), электронной цифровой подписи (ЭЦП), как средства обеспечения юридической силы трансграничного электронного документооборота.

В законодательствах стран Единого экономического пространства (ЕЭП), как и в законодательства большинства современных государств, где есть нормы связанные с электронным документооборотом, обеспечение юридической силы, *как свойства* электронных документов, базируется на гарантиях аутентичности и целостности документов. При этом в основном<sup>2</sup>, для обеспечения свойств аутентичности и целостности электронных документов используются криптографические методы, а правовые основы закладываются в международном и национальном законодательстве. Поэтому для организации защищенного электронного юридически-значимого взаимодействия может потребоваться согласование между странами-участниками отличий правового регулирования (например, требований к условиям применения криптографических средств) и отличий в средствах и способах обеспечения заданных значений защищенности.

Для организации защищенного электронного документооборота в Беларуси, России и Казахстане, в соответствии с рядом национальных нормативно-правовых актов, используются криптографические средства. При этом все указанные страны развивают собственную криптографию, имеют собственные стандарты криптографических алгоритмов, используемых для создания и проверки ЭП (ЭЦП) и собственные реализации данных алгоритмов (средства электронной подписи и их аналоги)<sup>3</sup>. В общем случае, эти решения между собой не совместимы, т.е. электронный документ, подписанный ЭЦП на основе криптографических стандартов Республики

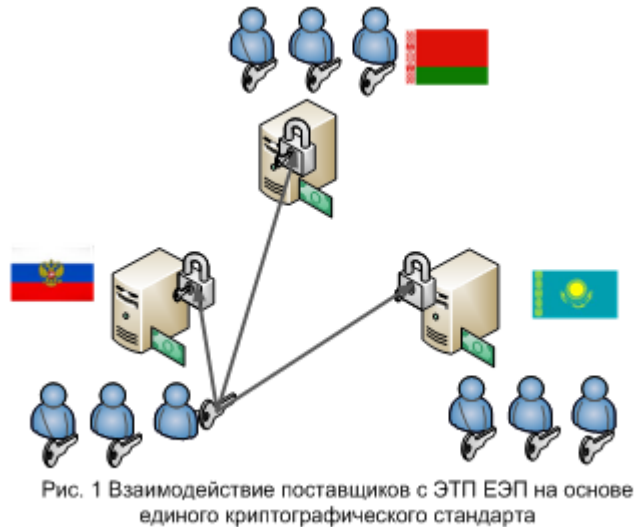
---

<sup>2</sup> Есть исключения, в частности Федеральный закон РФ № 63-ФЗ от 06.04.2011 предусматривает возможность использования некриптографической *простой электронной подписи*, которая в данном материале рассматриваться не будет, как неприменимая для рассматриваемых прикладных задач.

<sup>3</sup> В основе стандартов стран ЕЭП лежат общие подходы, но в настоящее время национальные реализации «навстречу» не совместимы.

Беларусь, не может быть проверен при помощи средств ЭЦП Республики Казахстан и российских средств ЭП. Аналогично и в случае с электронным документом, подписанным на основе Российских и Казахстанских средств криптографической защиты информации (СКЗИ).

Наиболее очевидным решением в этой ситуации, казалось бы, является использование общего, единого для ЕЭП криптографического стандарта для процедур электронной подписи (рис.1).



В пользу этого подхода говорит наличие криптографических стандартов СНГ - ГОСТ 34.310-2002. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования». Но такой подход противоречит национальным законодательствам, которые определяют необходимость использования сертифицированных по национальным стандартам средств электронной подписи, а так же не позволяет гармонизировать правовую основу применения электронной подписи в разных странах (а отличия существенные, начиная с терминов, заканчивая смысловым содержанием аналогов собственноручной подписи). По этим причинам вышеуказанные стандарты СНГ не имеют широкого применения и не могут быть использованы для решения задачи трансграничных госзакупок в Таможенном Союзе.

Другим очевидным решением, казалось бы, должен стать подход на основе импорта/экспорта средств электронной подписи (СКЗИ) партнеров, взаимный обмен ими, для оснащения национальных ЭТП и поставщиков госзаказа (рис. 2).

Но этот вариант имеет большое количество организационных и технических сложностей, и кроме того не разрешает весь перечень проблем. Прежде всего, средства электронной подписи являются шифровальными (криптографическими) средствами, а их экспорт и импорт имеет ряд существенных ограничений, затрудняющих реализацию данного варианта. В соответствии с «Положением о порядке ввоза на таможенную территорию таможенного союза и вывоза с таможенной территории таможенного союза шифровальных (криптографических) средств»:

«Ввоз и вывоз шифровальных средств осуществляется на основании разовых лицензий, выдаваемых уполномоченным органом государства - участника таможенного союза, на территории которого зарегистрирован заявитель».

Кроме того, ряд вопросов, связанных с использованием средств электронной подписи требует их периодического обслуживания провайдерами сертификационных услуг (например, удостоверяющими центрами), которые функционируют в соответствии с требованиями национальных законодательств и получение таких сервисов не в стране присутствия затруднено (например, изготовление квалифицированного сертификата ключа проверки электронной подписи иностранцу). Даже при решении задачи ввоза-вывоза средств электронной подписи для конкретной информационной системы, при масштабировании системы организационные проблемы возникают вновь, так как они требуют поэкземплярного учета этих средств, и каждый случай ввоза или вывоза требует оформления разовой лицензии.

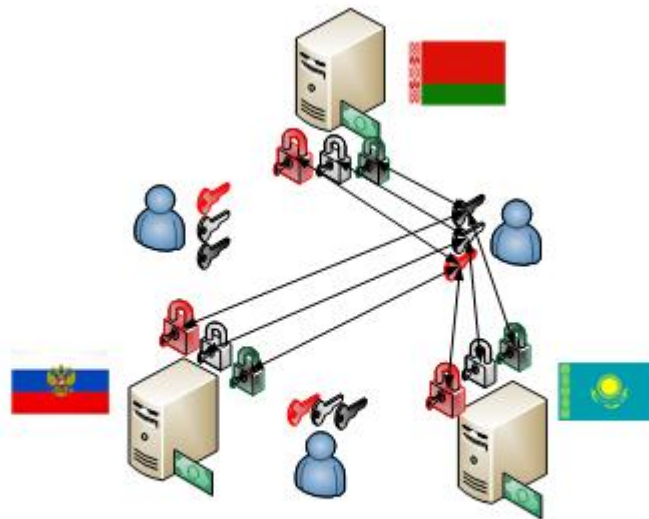


Рис. 2 Взаимодействие поставщиков с ЭТП ЕЭП на основе ввоза-вывоза национальных СКЗИ

К техническим особенностям данного варианта следует отнести, так же, необходимость оснащения всех ЭТП и всех поставщиков полным набором средств электронной подписи, что в настоящее время, кроме организационной затруднений,

осложняется и отсутствием совместимости, при работе на одном средстве вычислительной техники наиболее распространенных в странах Таможенного Союза СКЗИ.

К правовым недостаткам данного варианта следует отнести то, что в этом случае сторонам не предоставляется возможность получения документального подтверждения правомерности применения сертификата ключа проверки подписи для подписания конкретного типа документов в соответствии с законодательством страны происхождения электронного документа. В результате, каждый из контрагентов должен принимать решение о доверии электронному документу, не имея на это достаточных правовых оснований.

**Таким образом, вариант, основанный на вывозе и ввозе СКЗИ, не является технологичным и неприменим для массового использования, для развивающихся информационных систем и для информационных систем предполагающих наличие четких правовых условий применения электронных документов, к которым электронные торговые площадки и процедуры госзаказа относятся в полной мере.**

Для реализации защищенного трансграничного электронного юридически-значимого документооборота на основе криптографических средств целесообразно использовать иные подходы, позволяющие реализовать адекватные (по обеим сторонам границы) уровни криптографической защиты информационных потоков и достаточные правовые основания для признания юридической силы электронных документов, т.е. методы, обеспеченные достаточной нормативной базой.

За годы, прошедшие с момента постановки данного вопроса на повестку дня в Российской Федерации (как правило, здесь приводится 2006 год, когда в рамках ФЦП «Электронная Россия» был создан узел международного взаимодействия Общероссийского государственного информационного центра), данный вопрос был проанализирован экспертами разных стран, объединенными в различных международных форматах – ЕврАзЭС, КТС (ЕврАзЭК), ШОС, РСС, АТЭС и др. В результате этой многолетней работы были выработаны три базовых принципа:

- 1) для создания «пространства доверия» на основе технологий информационной безопасности и в строгом соответствии с нормами международного и национального права, необходимо чтобы каждая из взаимодействующих сторон оставалась в своем национальном правовом поле;

- 2) необходимо чтобы каждая из взаимодействующих сторон использовала собственные национальные криптографические стандарты;
- 3) решение вопросов гармонизации технологий криптографической защиты и юридически-значимого оформления «пространства доверия» должно быть делегировано специализированным операторам, функционирующим по принципу *Доверенной третьей стороны (ДТС)*<sup>4</sup>.

Схема взаимодействия сторон при реализации этих базовых принципов представлена на рис.3.

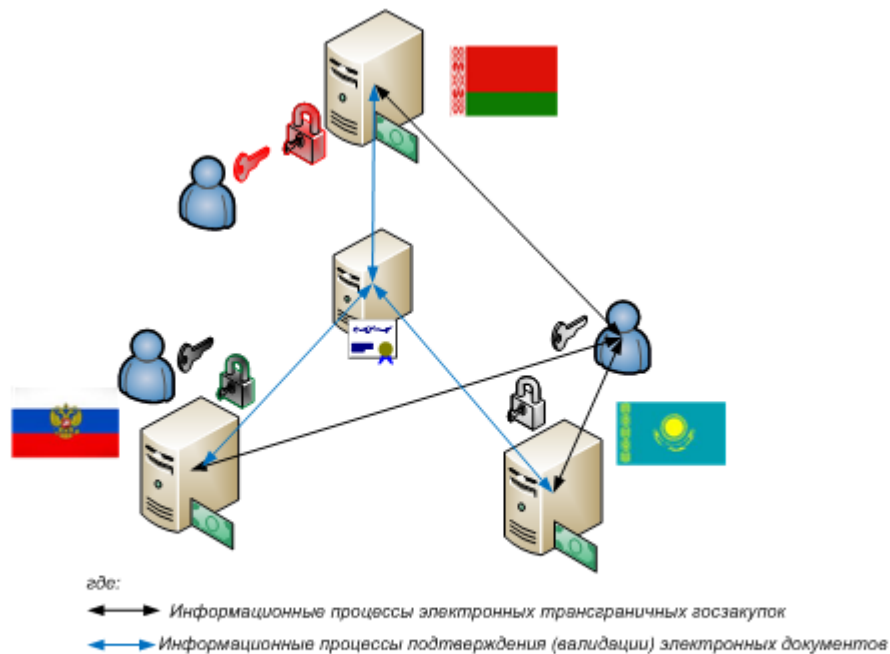


Рис. 3 Взаимодействие поставщиков с ЭТП ЕЭП на основе сервисов валидации электронных документов с помощью ДТС

Данный вариант активно обсуждался в последнее время:

- в международных форматах АТЭС, ЕврАзЭС, ШОС, ЕЭП, РСС и др.;
- на специализированных Форумах (РКИ-Форум Россия, РКИ-Форум Украина, Рускрипто, Европейский Форум по электронной цифровой подписи (EFPE) и др.);
- в рамках рабочих групп (в Минэкономике, Минкомсвязи и др.);

<sup>4</sup> Доверенная третья сторона (ДТС) это организация или представитель организации, который оказывает одну или несколько услуг безопасности, и является доверенным для других субъектов относительно действий, связанных с этими услугами безопасности. (ITU IT Recommendation X.842. Information technology – Security Techniques – Guidelines for the use and management of trusted third party services).

- в рамках экспертных советов (в том числе в Государственной Думе РФ - Экспертного совета по развитию юридически значимого документооборота и применению электронно-цифровой подписи при Комитете Государственной Думы по экономической политике, инновационному развитию и предпринимательству);
- на парламентских слушаниях в Совете Федерации на тему «Об использовании электронной подписи: состояние нормативно-правовой базы и практика её применения», которые состоялись 23.11.2012;
- и т.д.

По результатам, до недавнего времени, однозначно фиксировалось отсутствие достаточного нормативного обеспечения для применения данного подхода к решению задачи. При этом на вопросы экспертов в области сервисов ДТС о том, каких именно нормативных документов не хватает, конкретных ответов со стороны критиков данного подхода не поступает.

Нормативно-правовая модель обеспечения функционирования ДТС разработана в институте государства и права РАН в рамках работ по созданию узла международного взаимодействия в 2006 году. Это совокупность взаимосвязанных нормативных документов, позволяющая оценить достаточность нормативной базы применительно к конкретным задачам двустороннего и многостороннего трансграничного электронного юридически-значимого документооборота (рис. 4).

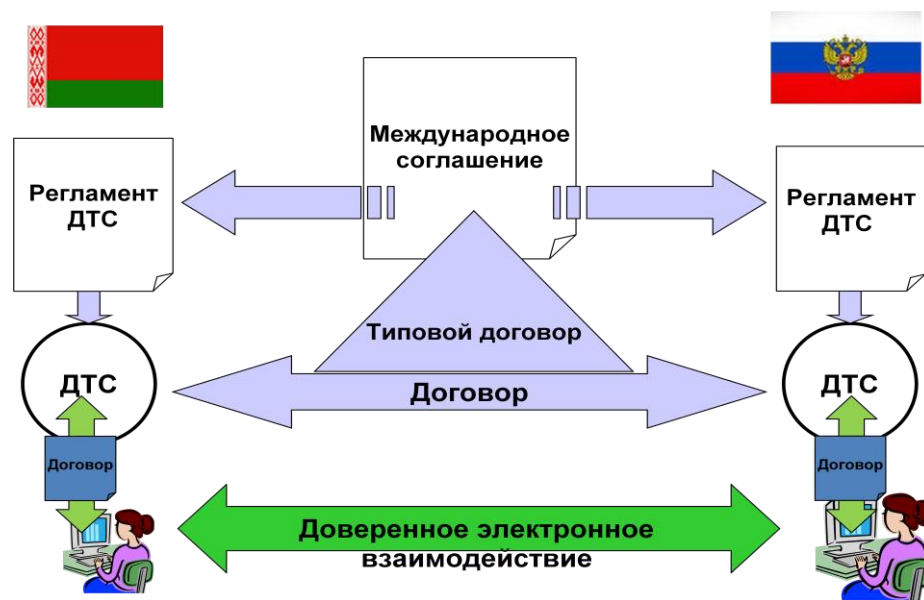


Рис. 4. Нормативно-правовая модель обеспечения функционирования ДТС в интересах доверенного электронного взаимодействия

Основу правовой модели составляет Международное соглашение. В рамках Таможенного Союза таким документом, определяющим ДТС в качестве технологии обеспечения юридической силы трансграничного электронного документооборота, является «Соглашения о применении информационных технологий при обмене электронными документами во внешней и взаимной торговле на единой таможенной территории Таможенного союза», (далее «**Соглашение по ИТ**»), которое подписано членами Таможенного Союза в Москве 21 сентября 2010 года и ратифицировано Федеральным Законом № 101-ФЗ от 10 июля 2012 года.

Следующим основополагающим фактором правовой модели является легитимность деятельности операторов услуг ДТС в каждой из взаимодействующих стран. Это вопрос о правовой основе оказания услуг по проверке электронной подписи в электронных документах, так как именно это и выполняет провайдер услуг ДТС при обращении к нему участника трансграничного электронного документооборота, и именно таким образом, вводится определение ДТС в Соглашении по ИТ:

"доверенная третья сторона" - организация, наделённая 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".

Прежде всего, следует отметить, что данный вопрос должен быть изучен в отношении законодательств каждой из взаимодействующих сторон. Авторы данного материала опираются в данном аспекте на результаты многолетней работы под эгидой Минкомсвязи России, в которой принимали участие эксперты большого количества стран в рамках ряда вышеупомянутых международных объединений. Технология ДТС изначально ориентирована на инвариантность и непротиворечивость в отношении национального законодательства, поэтому она неоднократно одобрялась экспертами из Казахстана, Узбекистана, Китая, Беларуси и других стран и заинтересованные лица могут ознакомиться с результатами международных экспертиз. Теоретической основой исследований стала «Методология формирования и функционирования в сети Интернет трансграничного пространства доверия» (Методология ПД-Т), разработанная Минкомсвязью России и одобренная 5 ноября 2012 года в г. Баку на совместном заседании 47-го Совета глав администраций связи Регионального содружества в области связи (РСС) и 18-го Координационного совета государств-участников СНГ по информатизации при РСС (<http://www.rcc.org.ru>). Там же Комиссии РСС по информатизации и Комиссии РСС по информационной безопасности было поручено подготовить предложения по практической реализации Методологии ПД-Т в интересах стран участников РСС. **В данной аналитической записке мы показываем, что к**



**практической реализации Методологии ПД-Т на примере Госзакупок на пространстве Таможенного Союза всё готово.**

**Итак, еще раз подчеркнем постановку вопроса: имеются ли в России достаточные правовые основания для деятельности провайдеров услуг по проверке электронной подписи в электронном документе, независимо от страны происхождения данного документа и сертификата ключа проверки подписи?**

Начнем рассматривать этот вопрос с основного нормативного акта по этой проблематике – Федерального закона от 06.04.2012 № 63-ФЗ «Об электронной подписи».

**Статья 7. Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами**

*1. Электронные подписи, созданные в соответствии с нормами права иностранного государства и международными стандартами, в Российской Федерации признаются электронными подписями того вида, признакам которого они соответствуют на основании настоящего Федерального закона.*

*2. Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки электронной подписи выдан в соответствии с нормами иностранного права.*

**Ст. 13 Удостоверяющий центр**

1. Удостоверяющий центр ....

...

*осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей.*

Совокупность двух данных норм Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» позволяет сделать вывод, что УЦ может оказывать услуги по проверке электронных подписей, созданных в соответствии с нормами права иностранного государства и международными стандартами.

Для внесения еще большей определенности в вопрос о достаточности правовых основ применения модели ДТС, проанализируем нормативы в отношении средств, которые требуются для реализации данного сервиса и определим, относится ли данная деятельность к лицензируемым видам.

Итак, ранее было установлено, использование модели с участием ДТС при трансграничном документообороте, технологически означает реализацию *доверенного сервиса проверки электронных документов с электронной подписью*. В Федеральном законе от 06.04.2011 № 63-ФЗ (Статья 2) представлено определение понятия «средства электронной подписи»:

*9) средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;*

Таким образом, для реализации указанного вида услуги, УЦ использует средства электронной подписи, которые являются шифровальными (криптографическими) средствами, и, следовательно, сама услуга относится к области шифрования информации.

В соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» (Статья 12), оказание услуг в области шифрования информации подлежит лицензированию.

Далее, Постановление правительства РФ от 16 апреля 2012 г. N 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» вводит перечень выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств. Данный перечень включает п. 25 «Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей».

На основании анализа данных положений Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» и Постановления правительства РФ от 16 апреля 2012 г. N 313, можно сделать вывод, что для оказания услуги по проверке электронного документа с электронной подписью необходимо применять средства электронной подписи, относящиеся к шифровальным (криптографическим) средствам, следовательно, провайдер такой услуги должен иметь лицензию на оказание услуг в области шифрования информации. Таким образом,

любой лицензиат ФСБ, обладающий лицензией на оказание услуг в области шифрования информации, в том числе и УЦ, имеет право оказывать такой вид услуг.

Остальные документы, входящие в правовую модель, представленную на рис.4 – это договоры и регламенты, которые являются локальными актами, разрабатываются операторами и согласуются между взаимодействующими сторонами в соответствии с положениями гражданского законодательства.

Результатом активной работы экспертного сообщества по данному вопросу является то, что совещанием экспертов в Комитете Совета Федерации по экономической политике, в преддверии вышеупомянутых парламентских слушаний, зафиксирована достаточность технологических и правовых основ для реализации трансграничного электронного юридически-значимого документооборота на основе сервисов ДТС, а так же определено, что положения **Соглашения по ИТ** можно рассматривать как работающий регламент обмена электронными юридически-значимыми документами в рамках Таможенного Союза. Кроме того, эксперты рекомендуют модель **Соглашения по ИТ** использовать в отношениях между странами, не входящими в Таможенный Союз. Вот что дословно написано в проекте рекомендаций Совета Федерации по вопросу «Об использовании электронной подписи: состояние нормативно-правовой базы и практика ее применения»:

Ратифицированное Соглашение (*Соглашение по ИТ* – прим. авт.) определило регламент признания иностранной электронной подписи и иностранного сертификата ключа подписи для указанной сферы и указанных государств. Однако не выработаны концептуальные подходы в целях эффективного решения задачи интероперабельности электронной подписи и строгой аутентификации лица, подписавшего электронный документ, для развития отношений России с другими государствами.

В связи с этим, в этом же документе предлагается:

Разработать, с учетом практики реализации Соглашения о применении информационных технологий при обмене электронными документами во внешней и взаимной торговле на единой таможенной территории Таможенного союза, концепцию обеспечения безопасности передачи данных и юридической силы электронных документов при трансграничном взаимодействии в целях заключения Россией соответствующих соглашений России с другими государствами.

**Таким образом:**

- **в формате Таможенного Союза подписано и ратифицировано сторонами международное соглашение, определяющее, что для подтверждения подлинности электронных документов при трансграничном электронном документообороте используется доверенная третья сторона;**

- **законодательством РФ определена возможность оказания услуг проверки электронных документов с электронной подписью, в том числе иностранного происхождения;**
- **существует институт лицензирования данного вида деятельности, а следовательно, и институт контроля и предъявления организационно-технических требований к данному виду услуг;**
- **договорная база и регламенты оказания данного вида услуг определяются операторами и их контрагентами, практика реализации таких договоров и регламентов существует;**
- **правовая модель оказания услуги проверки электронных документов с электронной подписью обладает полнотой, т.е. обеспечивает необходимые и достаточные правовые условия для предоставления данного вида услуг;**
- **на рынке представлены операторы, имеющие соответствующие технологии и обладающие необходимыми лицензиями, готовые к практической работе.**

Однако, как было отмечено выше, по состоянию на декабрь 2012 года, когда пишется данная аналитическая записка, положения Соглашения (по госзакупкам в ЕЭП) на практике не реализуются, т.е. равный технологический и правовой режим (национальный режим) для участия поставщиков в электронных торгах независимо от страны происхождения товара и/или услуги, на сегодня на Едином Экономическом Пространстве не создан. И в качестве причины, по-прежнему указываются проблемы отсутствия нормативной базы по применению электронной подписи. В результате экспертами АЗИ принято решение обратиться с данным материалом в:

- Евразийскую экономическую комиссию;
- Исполнительный комитет Регионального содружества в области связи;
- Управление Президента Российской Федерации по применению информационных технологий и развитию электронной демократии;
- Минкомсвязь России;
- Минэкономразвития России;
- Федеральную службу безопасности;
- Федеральную антимонопольную службу.

Полагаем, что представленная информация позволит разрешить сложившуюся ситуацию и реализовать на практике положения **Соглашения по ИТ** и **Соглашения по госзакупкам** в части касающейся процесса проведения закупок в электронном виде для стран-членов Таможенного Союза, обеспечив возможность участия в электронных государственных закупках на территории ЕЭП поставщикам из Белоруссии, Казахстана и Российской Федерации, а так же позволит использовать полученный опыт в трансграничных информационных системах других стран.

*Председатель комитета по развитию инфраструктуры  
открытых ключей Межрегиональной Общественной  
Организации «Ассоциация защиты информации», к.т.н.*

*Кирюшкин С.А.*

*«14» декабря 2012 г.*