Экспертный центр Электронного государства
D-RUSSIA.RU

GiS
ГАЗИНФОРМСЕРВИС

Электронное взаимодействие

юридически значимые аспекты

Санкт-Петербург
2016

Настоящий сборник представляет собой материалы исследований актуальных вопросов трансграничного электронного взаимодействия, в подготовке которых в период 2014-2016 годов принимали участие следующие соавторы: Домрачев Алексей Александрович, советник Департамента проектов по информатизации Министерства связи Российской Федерации, Дупан Анна Сергеевна, кандидат юридических наук, директор Институт проблем правового регулирования ВШЭ, Евтушенко Сергей Николаевич, Действительный государственный советник Российской Федерации, референт Аппарата Правительства Российской Федерации, Исаков Владимир Борисович, доктор юридических наук, профессор Национального исследовательского университета «Высшая школа экономики», Кирюшкин Сергей Анатольевич, кандидат технических наук, советник Генерального директора ООО «Газинформсервис», эксперт ЭСКАТО ООН, Сазонов Александр Валентинович, эксперт СЕФАКТ ООН, заместитель генерального директора по развитию ЗАО «Национальный удостоверяющий центр», Фургель Игорь Аркадьевич, Dr. rer. nat., руководитель органа подтверждения и сертификации T-Systems International GmbH.

Этот сборник не является официальным, а предназначен для обсуждения в экспертном сообществе, занимающимся вопросами цифровой экономики, электронного правительства, единого окна, защиты информации, трансграничного электронного юридически-значимого документооборота, доверенной третьей стороны.

Сборник издан компанией «Газинформсервис» при поддержке Экспертного центра электронного государства D-Russia.ru.

Оглавление

1 Прикладные задачи региональной и глобальной интеграции на пути к цифровой экономике

Выступая 2 сентября 2016 года на Восточном экономическом форуме во Владивостоке, Президент Российской Федерации Владимир Владимирович Путин выразил уверенность, что Россия и страны Азиатско-тихоокеанского региона могли бы иметь общее пространство «цифровой экономики» международной интеграции, «речь идет о создании правовых и технологических условий для электронного взаимодействия». «Евразийская экономическая комиссия уже ведет создание системы взаимодействия в сфере транспорта, внешней торговли, таможенных, ветеринарных, налоговых и других процессов», – напомнил Президент РФ.

Интегральное понятие «цифровой экономики» предполагает интенсивное применения информационных технологий в отраслях экономики, т.е. промышленности, сельском хозяйстве, городском хозяйстве, бытовых системах, меняющего на основе возможностей обработки больших объёмов информации, средства производства, предметы производства, способы их потребления.

Мировые тренды на экономическую глобализацию и региональную интеграцию предполагают тесную увязку планов по развитию инфраструктуры электронного правительства Российской Федерации с лучшими зарубежными практиками и цифровыми перспективами, существующими и разрабатываемыми в различных международных форматах, прежде всего на постсоветском пространстве, в европейском и азиатско-тихоокеанском регионах, а также в профильных структурах Организации Объединенных Наций.

Такими направлениями являются:

формирование единых региональных цифровых пространств[1] в рамках глобальной экономики;

переход от регулирования разновидностей электронных подписей к формированию системной совокупности доверенных сервисов;

формирование региональных трансграничных пространств доверия[2] на основе совокупности доверенных сервисов;

увязка инфраструктуры доверенных сервисов с функциональным наполнением многообразных информационных систем, применяемых в электронной коммерции, телемедицине, дистанционном образовании и других юридически значимых электронных приложений;

---

[1] **Региональное цифровое пространство** – совокупность ИТ-инфраструктуры, используемой в целях информатизации деловых, экономических, культурных и социальных процессов на уровне региональных интеграционных объединений.

[2] **Трансграничное пространство доверия** - совокупность правовых, организационных и технических условий, рекомендуемых специализированными структурами ООН и профильными международными организациями с целью обеспечения доверия при международном обмене электронными документами и данными между субъектами электронного взаимодействия.

использование преимуществ, предоставляемых современными технологиями, в том числе на основе блокчейн, при одновременном устранении негативных проявлений, выявленных на примере биткоинов.

Общей задачей реализации данных направлений является устранение барьеров на пути развития современных электронных экономических и социальных сервисов, предоставляемых потенциально всему населению планеты, на основе придания качества юридической значимости трансграничному электронному документообороту.

Формируемое в развитых и развивающихся странах мира постиндустриальное или информационное общество представляет собой глобальный тренд современности. Одним из характерных явлений такого информационного общества является сеть Интернет, благодаря которой существенная доля жителей планеты получила качественно новые возможности по доступу к разнообразной информации и взаимным коммуникациям.

В принципе Интернет приблизил физических и юридических лиц, находящихся под юрисдикцией различных государств, к получению современных высококачественных деловых и социальных (телемедицина, дистанционное образование, другие) услуг.

Важным фактором безболезненного прохождения финансового кризиса является экономия денежных средств на всех уровнях, от государств и транснациональных корпораций до рядовых граждан, для которых этот фактор становится достаточно острым.

Налицо противоречие между широкими возможностями сети Интернет и всё возрастающими расходами на становящийся анахронизмом бумажный документооборот, который нарастает лавинообразно. Последний фактор вызван общей тенденцией глобализации экономики и социальной жизни, при которой наблюдается существенный рост денежных, транспортных, людских информационных потоков , в основе обслуживания большинства из них лежит единичная документированная информационная транзакция.

Кроме того, наблюдается также очевидное противоречие между ограниченным количеством в мире высококлассных центров предоставления услуг, прежде всего медицинских и образовательных, и потенциальной востребованностью этих услуг со стороны жителей планеты. Непосредственное получение услуг в таких центрах влечет за собой существенные транспортные расходы и затраты на пребывание, что исключает из числа их пользователей наименее обеспеченные слои населения и во многом средний класс. При этом, поскольку образ таких новейших услуг реально присутствует в сети Интернет, повышается социальная напряженность в обществе. Дистанционное предоставление услуг, как возможное решение, также предполагает первоочередное решение проблем документирования информации в электронном виде, обозначенное выше. Это есть фактор охраны прав пользователей и других участников сопутствующих правовых отношений, наработанный веками в рамках

традиционного бумажного документооборота, яркими примерами которых являются медицинская или зачетная книжки, договор и так далее.

Решение всех этих проблем является одним из глобальных вызовов, перед которым стоит сегодня современная цивилизация.

В последнее время высшим руководством страны, в том числе совместно с лидерами ряда ведущих стран мира, поставлены масштабные задачи в области экономической интеграции, которые должны быть поддержаны со стороны информационных технологий, в том числе:

- Россия предлагает двигаться к созданию от Атлантики до Тихого океана единого экономического и человеческого пространства[3];

- Развитие региональной экономической интеграции - это стратегический выбор России. И мы будем реализовывать его, основываясь на согласованных интересах с партнёрами по Таможенному союзу и Единому экономическому пространству с учётом перспектив формирования Евразийского экономического союза. На Владивостокском саммите мы представляли не только свои, российские интересы и подходы, а опирались на согласованную позицию тройки: Россия, Казахстан и Белоруссия[4];

- Мы признаем важность информационно-коммуникационных технологий (ИКТ) как ключевого фактора, ведущего к интеграции в регионе АТЭС. Мы верим, что возможно и необходимо проявлять большую активность в повышении доверия в электронной среде на глобальном уровне посредством содействия трансграничному юридически значимому обороту информации, включая электронные документы. Мы ещё раз подтверждаем необходимость многостороннего взаимодействия в расширении и усилении Азиатско-Тихоокеанской информационной инфраструктуры для построения доверия и безопасности в использовании ИКТ[5].

Эти глобальные установки отражены в поручении Президента Российской Федерации № Пр-2831 от 23 октября 2012 года о проведении всестороннего анализа итогов председательства Российской Федерации в Форуме «Азиатско-тихоокеанское экономическое сотрудничество» в 2012 году и подготовке комплексного плана дальнейших действий в рамках АТЭС, в котором предписано обратить особое внимание на реализацию инициатив и проектов по приоритетам российского председательства, использованию возможностей экономик АТР, в том числе для налаживания взаимодействия стран и многосторонних объединений Азиатско-тихоокеанского региона с формирующимся Евразийским экономическим союзом.

Такая глобальная география (от Атлантики до Тихого океана) предполагает развитие современных логистических технологий для всех видов транспорта (железнодорожного, авиационного, речного и морского, а также автомобильного и трубопроводного). При этом уникальное

---

[3] Источник http://www.putin-itogi.ru/2012/02/27/statya-v-v-putina-rossiya-i-menyayushhijsya-mir/

[4] Источник: http://rus.apec2012.ru/news/20120909/462965221.html

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

геополитическое положение России в центре этого мирового региона создает хорошие предпосылки для повышения роли страны в глобальной экономике, в том числе на основе инновационных технологий, к которым относятся ИКТ. Наращивание транспортной и информационной связанности в важнейшем регионе мира будет способствовать экономической интеграции региона и предоставлению качественных трансграничных услуг населению и организациям, находящихся в различных юрисдикциях.

С другой стороны, сочетание этих двух важнейших инфраструктур (логистика и ИКТ) может придать дополнительный импульс для развития транспортной отрасли России и стран ближнего зарубежья, радикальному сокращению издержек временного и финансового характера на обслуживание бумажного документооборота, становящегося все большим анахронизмом, и пересечение пунктов пропуска для всех видов транспортных средств. Инновационные решения по обеспечению трансграничного юридически значимого документооборота, отработанные на постсоветском пространстве, в последующем могут быть тиражированы на европейском и азиатско-тихоокеанском направлениях. Это находится в контексте задач, поставленных Президентом Российской Федерации.

2 Исследование и анализ перспектив формирования единых региональных цифровых пространств

Формирование единых региональных цифровых пространств в рамках глобальной экономики (далее – ЕЦП) является актуальным трендом современности и нацелено на обеспечения условий для ускоренного формирования и развития различных региональных интеграционных объединений как эффективной и конкурентоспособной организации в рамках мировой экономики, а также для устойчивого развития экономик отдельных стран в интересах повышения жизненного уровня их населения.

Например, бизнес-сообщество стран Евразийского экономического союза предложило сформировать единое цифровое пространство ЕАЭС. Такая идея была выдвинута на прошедшем в ноябре 2015 года в Минске первом заседании президиума Делового совета ЕАЭС[6].

Аналогичные тенденции отмечаются в европейском (Положение № 910/2014 [7]) и азиатско-тихоокеанском (Паназиатский альянс по электронной коммерции[8]) регионах.

Указанные факты и тенденции будущего развития показывают необходимость и своевременность максимального использования потенциала различных интеграционных проектов и объединения усилий стран в рамках движения к цифровой трансформации своих экономик и построению ЕЦП.

---

[6] http://www.e-cis.info/news.php?id=13561
[7] https://ec.europa.eu/digital-single-market/en/trust-services-and-eid
[8] https://paa.net/

2.1 Общетеоретические подходы

Анализируя актуальную статью по кибер-физическим системам[9], в контексте задачи построения единого цифрового пространства (ЕЦП) ЕАЭС можно предложить дополнить архитектуру цифровой экономики комплементарным набором кибер-социальных систем.

Это обусловлено тем, что во всех государствах-членах ЕАЭС разработаны и реализуются национальные программы построения электронных правительств в соответствии с общепринятыми международными практиками. Кроме того, в соответствии с Договором о ЕАЭС на протяжении ряда лет ведется общая программа по созданию Интегрированной информационной системы Союза (ИИСС). Начаты работы по реализации механизма единого окна. Целью всех этих инициатив является создание благоприятных условий для деятельности физических, юридических и уполномоченных лиц, находящихся в юрисдикции государств-членов ЕАЭС в рамках формируемого ЕЦП. При этом предполагается в условиях глобальной экономики, что ЕЦП по определению не может быть замкнутым, а должно проектироваться открытым по отношению к совершению юридически значимых электронных транзакций с контрагентами в других экономических регионах мира, прежде всего с географически ближними – Европой и Юго-Восточной Азией. Расширение международных форматов ШОС и БРИКС еще более увеличивает количество вероятных контрагентов, число которых может приближаться к миллиарду.

Таким образом, в рамках проектов электронных правительств, механизмов единого окна, ИИСС, взаимодействующих с ключевыми мировыми международными форматами, формируется массовый состав лиц – участников информационных транзакций, которые вступают между собой в разнообразные социальные взаимоотношения, формируя кибер-социальные системы, во многом адекватные по своей архитектуре кибер-физическим системам, а также связанным с ними технологиями промышленного Интернета, Умных городов, Умных транспортных систем и других.

Более того, при реализации на практике этих масштабных проектов целесообразно при проектировании закладывать общую инфраструктуру, например, телекоммуникационную и центров обработки данных для обоих типов кибер-систем, физических и социальных. Для этого хорошо подходит форма государственно-частного партнерства, что особенно эффективно в условиях финансово-экономического кризиса.

В то же время формализованное описание всех категорий лиц конечно будет отличаться от сигналов, поступающих от физических датчиков. Для

---

[9] Кибер-физические системы, как основа цифровой экономики, авторы В.П. Куприяновский, Д.Е. Намиот, С.А.Синягов, опубликовано https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&sqi=2&ved=0ahUKEwjzxJ-jn6LOAhWB3SwKHRkVCyIQFggzMAQ&url=http%3A%2F%2Fcyberleninka.ru%2Farticle%2Fn%2Fkiber-fizicheskie-sistemy-kak-osnova-tsifrovoy-ekonomiki.pdf&usg=AFQjCNGrmAWL2bXExqO-SKNhNqO9rKTGdA&sig2=7RdQ96WtMlrL_grGGWTV0w&bvm=bv.128617741,d.bGg

физических, юридических и уполномоченных лиц могут быть характерны следующие признаки: правомочия, полномочия, волеизъявление, правовой статус, место и время совершения информационной транзакции между ними, апостильное и/или нотариальное заверение, платеж госпошлины, а также контент, обладающий юридической силой в рамках транзакции.

Кроме того, в рамках телемедицины может рассматриваться формализованное описание состояния пациента и история его болезни с рекомендациями уполномоченных лиц клиники. Аналогично для дистанционного образования – формализованный мониторинг знаний студента и результат оценки знаний преподавателем.

Признавая наличие общих инфраструктурных компонент, следует подчеркнуть принципиальное различие между двумя типами кибер-систем, которое заключается в том, что все категории лиц относятся к субъектам права, тогда как физические датчики могут быть отнесены к объектам прав, которые не обладают волеизъявлением. В тоже время, определенная правовая ответственность за возможный ущерб третьим лицам может быть возложена на операторов кибер-физических систем, что должно быть предусмотрено регламентами и договорами, например, в рамках систем автоматического таможенного выпуска товаров.

Другим принципиальным различием между двумя типами кибер-систем состоит в их целеполагании: кибер-физические системы служат принятию детерминистических решений в рамках оптимизации управления и функционирования физических систем, тогда как кибер-социальные системы призваны оптимизировать условия (среду) для принятия адекватных решений их пользователями (субъектам права) в рамках их волеизъявления. Именно поэтому для кибер-социальных систем требуется не только технологическая интероперабельность, которая достаточна для кибер-физических систем, но и институциональная поддержка, включающая и институциональную интероперабельность для достижения качества юридической значимости кибер-социального взаимодействия как в национальных, так и в международных рамках.

Субъектность прав всех категорий лиц предполагает наличие расширенной конфигурации терминалов кибер-систем, вместо датчиков – рабочие места с использованием средств электронной (цифровой) подписи, а также соответствующие инфраструктуры - открытых ключей и доверенной третьей стороны (для трансграничного режима). Эти инфраструктуры призваны поддерживать параметр волеизъявления лиц. Другие возможные параметры, приведенные выше, могут поддерживаться отдельными доверенными электронными сервисами в рамках трансграничного пространства доверия в версии централизованных реестров. Соотношение технологии блокчейн, основанной на децентрализации, и обоих типов кибер-систем требует отдельного рассмотрения.

В настоящее время бумажный документооборот между всеми категориями лиц имеет институциональный характер, который сложился

естественным образом на протяжении веков в результате выполнения различных типовых процессов, носящих функциональных характер. В случае возникновения (или для предотвращения) конфликтной ситуации при ретроспективном рассмотрении граждане могут подать регламентированный набор документов в государственные органы, обратиться в суд или страховые компании, а также получить нотариальную поддержку. Представляется, что массовое сознание носит инертный характер, поэтому в рамках проектов электронных правительств или при трансграничном информационном взаимодействии необходимо обеспечить адекватную институциональную поддержку. Можно сказать, что если для кибер-физических систем требуется преимущественно технологическая стандартизация или интероперабельность, то для кибер-социальных систем требуется дополнительно обеспечить институциональную интероперабельность по указанным выше направлениям для достижения качества юридической значимости электронных документов, признаваемых в национальной или международной юрисдикциях.

В этой связи можно утверждать, что системы электронных правительств являются частным случаем трансграничного информационного взаимодействия. Они различаются уровнями национального или международного регулирования. Других принципиальных различий между ними нет.

Как отмечалось выше, развитие международных форматов приводит к появлению новых контрагентов по разные стороны границы, а так же к увеличению товарооборота между существующими партнерами. С реализацией трансграничных кибер-социальных систем эта тенденция будет только развиваться. При этом ожидается увеличение доли B2C-транзакций, которые будут осуществляться через торговые системы, предлагающие упрощенные и унифицированные процедуры разбора конфликтных ситуаций в режиме on-line, и тем самым повышающие уровень доверия при удаленном взаимодействии. Упрощение торговых процедур и, как следствие, повышение товарооборота приведет к необходимости оптимизации на транспортно-логистическом уровне.

Для формирования трансграничных кибер-социальных систем в России имеется необходимый задел, который описан в других частях международного раздела системного проекта электронного правительства, в том числе в форматах ЮНСИТРАЛ, ЭСКАТО, СЕФАКТ и других. Также в них обоснована постановка задачи по созданию глобального логистического коридора между Европой и Юго-Восточной Азией через территорию стран ЕАЭС.

В контексте настоящих тезисов можно предложить рассмотреть инициативу по организационному созданию Альянса, решающего триединую задачу:

- создание современного транспортного коридора в указанной географии на основе мультимодальных технологий;

- обеспечение поддержки логистических технологий со стороны Умных транспортных кибер-систем или промышленного Интернета;

- обеспечение бесшовного прохождения транспортных грузов и пассажиропотока со стороны кибер-социальных систем на основе комплексного использования электронных правительств, единого окна, ИИСС, во взаимодействии с аналогичными системами в Европе и Юго-Восточной Азией при соответствующей институциональной интероперабельности.

Целесообразно составить дорожную карту для решения указанной задачи.

2.2 Концептуальные подходы

Содержательная схожесть задач по формированию ЕЦП в различных регионах мира и необходимость их последующей интеграции в рамках глобальной экономики актуализируют проблему выработки базовых архитектур цифровой экономики на основе имеющегося опыта, полученного прежде всего в рамках Центра ООН по упрощению процедур торговли и электронным деловым операциям (СЕФАКТ ООН), в том числе по темам формирования и функционирования единого окна и трансграничного пространства доверия, как естественное развитие указанных тем в направлении ЕЦП.

Задача по реализации мероприятий по формированию единого цифрового пространства Евразийского экономического союза уже выдвинута в повестку дня, что также предполагает выработку базовых архитектур.

При формировании архитектуры ЕЦП предлагаются следующие концептуальные подходы.

В рамках архитектуры верхнего уровня при формировании ЕЦП необходимо выделить набор решений *инфраструктурного* и *функционального* характера. Функциональные решения предназначены для непосредственного удовлетворения различных общественных потребностей экономического и социального характера, тогда как инфраструктурные решения предназначены для придания функциональным сервисам определенных свойств/качеств, таких как доверие и безопасность[10].

Таким образом, функциональные и инфраструктурные решения являются дополнительными по отношению друг к другу, и, поэтому, должны рассматриваться и проектироваться всегда в комплексе.

Функциональные решения могут быть такими же разнообразными и многоцелевыми, как и сама жизнь, так как они служат удовлетворению всевозможных общественных и социальных потребностей. К решениям *функционального* характера можно отнести:

концентраторы (хабы) сервисов электронной коммерции[11];

---

[10] безопасность является одним из аспектов доверия.

[11] http://paa.net/

электронные платежные системы;

системы предоставления электронных государственных услуг;

системы телемедицины;

системы дистанционного образования;

системы единого окна[12][13];

различные приложения Internet of Things (IoT)[14], умный дом, смарт город, Internet of Vehicles (IoV)[15] и другие;

различные информационно-аналитические системы в совокупности с системами маркировки товаров, предназначенные, в том числе для мониторинга товарных потоков в целях прослеживаемости до конечного потребителя.

К решениям *инфраструктурного* характера, включающим также аспекты информационной безопасности, необходимо отнести:

региональные и глобальные трансграничные пространства доверия (ТПД)[16];

системы защиты персональных данных[17];

системы защиты коммерческой, врачебной тайны и других видов информации ограниченного доступа;

системы защиты критически важных объектов информатизации;

другие решения, в том числе информационно-безопасные, вносящие вклад в достижение и сохранение необходимого уровня доверия между пользователями соответствующей инфраструктуры [10].

2.3 Архитектурные решения

Важным архитектурно образующим признаком ЕЦП является целесообразность использования трансграничного пространства доверия для поддержки юридически значимого трансграничного информационного взаимодействия, в том числе – трансграничного электронного юридически-значимого документооборота в рамках любых функциональных сервисов, требующих, либо предполагающих определенный уровень доверия между пользователями этих сервисов.

Это в особенности относится к функциональным решениям, которые можно отнести к классу учетных информационных систем, в которых содержится информация из правоустанавливающих документов, которая требует специальных мер поддержки со стороны электронных сервисов *доверия*. К таким функциональным приложениям относятся, например,

---

[12] http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352r.pdf

[13] http://www.unece.org/fileadmin/DAM/trade/ctied7/ece_trade_324e.pdf

[14] https://tools.ietf.org/html/rfc7452

[15] http://mddb.apec.org/Documents/2014/TEL/TEL50-PLEN/14_tel50_plen_020.pdf

[16] http://www1.unece.org/cefact/platform/download/attachments/55378391/Rec+draft+v.0.952+10.03.16.pdf

[17] http://www.cbprs.org/Consumers/ConsumerDetails.aspx

юридически значимые услуги, предоставляемые на основе концентраторов (хабов) электронной коммерции, электронные платежные системы, а также систем предоставления электронных государственных услуг, телемедицины, дистанционного образования и многие другие, построенные, в том числе, с использованием архитектуры «единого окна».

Под трансграничным пространством доверия (ТПД) понимается совокупность правовых, организационных и технических условий, рекомендуемых специализированными структурами ООН и профильными международными организациями с целью обеспечения доверия при международном обмене электронными документами и данными между субъектами электронного взаимодействия.

Под субъектами электронного взаимодействия понимаются органы государственной власти, физические и юридические лица, взаимодействующие в рамках отношений, возникающих при формировании, отправке, передаче, получении, хранении и использовании электронных документов и данных.

Создание и сохранение общих предпосылок для установления и поддержания определенного (требуемого или ожидаемого) уровня доверия между субъектами электронного взаимодействия с целью обеспечения взаимного юридически значимого признания сервисов доверия, предоставляемых под различными юрисдикциями, является *системообразующим фактором* ТПД.

Необходимо подчеркнуть, что «доверие» само по себе является фундаментально общественной функцией. Поэтому построение какого-либо института, обеспечивающего «доверие» и одновременно основанного исключительно на технологиях, а не на общественных отношениях, представляется невозможным.

Эффективным путем обеспечения доверия в рамках ТПД видится сопряжение традиционно существующих институтов, способных адекватно поддержать реализацию системообразующего фактора ТПД, с организационными и технологическими возможностями, предоставляемыми современными ИКТ-сервисами.

Отдельные функциональные приложения, такие, например, как процедуры урегулирования споров в режиме онлайн, могут не использовать весь инструментарий ТПД, а только упрощенные специфические системы идентификации истцов, ответчиков и третьих сторон, адекватных тем, что используются на тех торговых площадках, где возник спор.

Различные функциональные приложения, такие как Internet of Things (IoT), умный дом, смарт город, Internet of Vehicles (IoV) и другие аналоги можно отнести к классу информационно-справочных систем, которые обрабатывают различную информацию, сведения или данные, но не электронные документы. В этой связи использование сложных и дорогостоящих электронных сервисов доверия ТПД может оказаться экономически и организационно нецелесообразным.

Предполагается, что различные информационно-аналитические системы в совокупности с системами маркировки товаров, предназначенные, в том числе, для мониторинга товарных потоков в целях прослеживаемости до конечного потребителя, могут использовать информационные ресурсы из учетных и информационно-справочных систем в соответствии с заранее заданным аналитическим алгоритмом для контрольных целей и пресечения возможных неправомерных действий.

Вопросы обеспечения защиты информации, а также юридической значимости электронных документов, могут основываются на следующих общих архитектурных принципах:

скоординированной организацией, специализированной международной нейтральной сети уполномоченных операторов, по аналогии с Trusted Third Party (TTP) или Accountability Agents (AA);

определением для таких операторов организационных, технологических, правовых и институциональных требований;

определением требований по проведению независимого аудита таких операторов,

проведением независимого комиссионного аудита операторов согласно установленным требованиям;

регламентацией доступа с клиентского уровня к нужным сведениям (коммерческая тайна, персональные данные, другие виды информации ограниченного доступа, электронные документы), за которые несут ответственность уполномоченные операторы.

Для учетных систем целесообразно выделить два уровня: корпоративный и общего пользования. При этом могут использоваться различные транспортные решения:

набор информационных шин, шлюзов, систем межведомственного электронного взаимодействия, а также выделенные каналы связи – для корпоративных систем;

сеть Интернет и аналоги – для систем общего пользования.

Для целей эффективного программного управления формированием ЕЦП целесообразно разграничивать сегменты – интеграционный и национальные – по критерию централизации или децентрализации деятельности уполномоченных функциональных или инфраструктурных операторов.

Необходимым условием доверия к единому цифровому пространству является безопасность и устойчивость последнего. При этом можно выделить три уровня: сетей связи, обработки данных и сервисов.

Эти уровни представляют собой разновидность доверия к функциональной устойчивости / доступности функциональных сервисов. Именно такое доверие - доверие "функционального уровня" или "первого порядка" - зависит от сети связи, обработки данных и устойчивости функциональных сервисов самих по себе.

Доверие "второго порядка" может обеспечиваться специфическими сервисами доверия, которые предоставляются на различном уровне квалификации в зависимости от потребностей пользователей этих сервисов. Доверие "второго порядка" возникает вследствие того, что пользователи сервисов доверия могут рассчитывать на юридическую значимость результатов использования этих сервисов доверия. Таким образом, доверие "второго порядка" - это доверие "юридического уровня". Очевидно, что оно не зависит ни от конкретных видов сетей, ни от конкретной технической обработки данных, ни от конкретных функциональных сервисов.

3 Институциональная основа технологий обеспечения признаков юридически-значимого взаимодействия

Для сторон юридически-значимого взаимодействия характерны следующие признаки:

1) правомочия,
2) полномочия,
3) волеизъявление,
4) правовой статус,
5) место и время совершения действий ,
6) апостильное и/или нотариальное заверение,
7) подтверждение оплаты пошлин, налогов, сборов,
8) контент, обладающий юридической силой.

Технология электронной подписи призвана поддерживать параметр волеизъявления лиц. Другие возможные признаки, приведенные выше, могут обеспечиваться отдельными доверенными электронными сервисами в рамках информационного пространства доверия национального, регионального или международного (трансграничного) уровня.

Традиционный бумажный документооборот имеет институциональный характер, который сложился естественным образом на протяжении веков в результате выполнения различных типовых функциональных процессов. В случае возникновения (или для предотвращения) конфликтной ситуации при ретроспективном рассмотрении участники традиционного бумажного документооборота могут подать регламентированный набор документов в государственные органы, обратиться в суд или страховые компании, а также получить нотариальную поддержку. Всё это – элементы институционального обеспечения традиционного бумажного документооборота.

Массовое сознание носит инертный характер, поэтому и в рамках проектов, включающих электронный юридически-значимый документооборот, в том числе - трансграничный (электронное правительство, электронные госуслуги, электронная торговля, телемедицина, дистанционное образование и т.д.) необходимо обеспечить адекватную институциональную поддержку, в том числе и в случаях, когда такие проекты предполагают

трансграничное информационное взаимодействие. Для электронного документооборота в массовых системах технические решения существенно опережают институциональное обеспечение, и это является существенным барьером, который пока успешно преодолевается только в небольших странах и локальных международных форматах. Крупные страны и межрегиональные объединения испытывают существенные затруднения, что приводит к неэффективным бюджетным затратам преимущественно на технологическое обеспечение [3]. Правовая модель, обеспечивающая электронный юридически-значимый документооборот (в том числе - трансграничный), должна так же обеспечивать возможность в случае возникновения (или для предотвращения) конфликтной ситуации, обратиться в государственные органы, обратиться в суд или страховые компании, а также получить нотариальную поддержку. В настоящее время подобная общая (т.е. не привязанная к конкретным международным форматам и бизнес-процессам) правовая модель, обеспечивающая институциональность такого электронного юридически-значимого взаимодействия в мире отсутствует.

4 Цель обеспечения интероперабельности трансграничного информационного юридически-значимого взаимодействия

Общей целью обеспечения интероперабельности трансграничного информационного юридически-значимого взаимодействия является создание благоприятных условий для деятельности физических, юридических лиц, органов государственной власти и международных организаций при трансграничном взаимодействии в рамках формируемого единого цифрового пространства (ЕЦП). При этом предполагается, в условиях глобальной экономики, что ЕЦП по определению не может быть замкнутым, а должно проектироваться открытым по отношению к совершению юридически значимых электронных транзакций с контрагентами в других экономических регионах мира, прежде всего с географически ближними, т.е. для ЕАЭС – Европой и Юго-Восточной Азией. Расширение международных форматов ШОС и БРИКС еще более увеличивает количество вероятных контрагентов, число которых может приближаться к миллиарду.

Таким образом, в рамках комплекса проектов электронного правительства, электронных государственных услуг, электронной торговли, телемедицины, дистанционного образования, имеющих сервисы единого окна и возможную трансграничность, взаимодействующих с ключевыми мировыми международными форматами, формируется массовый состав лиц – участников информационных транзакций, которые вступают между собой в разнообразные социальные взаимоотношения, формируя сложные гуманитарно-технологические кибер-социальные учетные системы.

Такие отношения могут быть структурированы по уровням регулирования: национальный, международный, или торговых обычаев (наподобие Правил ИНКОТЕРМС Международной торгово-промышленной палаты). А также по категориям лиц, вступающих между собой в отношения: физические, юридические, органы государственной власти.

Следует учитывать, что правовые и социальные отношения являются потенциально конфликтогенными, поэтому правила взаимодействия с властью, регламенты разбора конфликтных ситуаций, система страхования рисков и порядок нотариального обеспечения прав также должны быть адекватными для всех уровней регулирования и категорий лиц. Таким образом, система требований должна представлять собой многомерную матрицу, с уровнями регулирования и категориями участников. В этой матрице должны быть учтены технические, организационные и правовые аспекты требований к доверенным сервисам, реализуемым в рамках пространства доверия, национального или трансграничного. Такая система требований должна стать основной выработки разноуровневых кибер-социальных архитектур, использующих инфраструктуру трансграничного пространства доверия. При этом особо необходимо отметить, что государства и их объединения не должны нести ответственность за все виды возможных рисков, однако международное сообщество и государства обязаны определить требования к бизнесу в вопросах охраны прав и законных интересов граждан и организаций, находящихся в различных юрисдикциях, а также в целях технической, организационной и институциональной интероперабельности, при этом не ограничивая разумной предпринимательской инициативы.

Доверенные сервисы не могут существовать сами по себе, они должны инфраструктурно поддерживать конкретные приложения деловой или социальной направленности, потребность в которых испытывает общество, например, в создании современных транс-евразийских транспортных коридоров, в подтверждении страны происхождения товаров, в подтверждении таможенной стоимости товаров, в обеспечении трансграничного доступа к электронным государственным услугам и др.. Удовлетворение реальных потребностей должно привести к формированию новых рынков доверенных сервисов, в том числе трансграничного характера, прототипом которых является рынок услуг удостоверяющих центров.

5 История развития направления трансграниных кибер-социальных учетных систем

5.1 Становление проблематики в Российской Федерации

Работы по развитию трансграничных кибер-социальных учетных систем в форме трансграничного пространство доверия (далее – ТПД или «проект Трансграничность») развивались в РФ несколькими этапами.

1 этап. Основные концептуальные подходы к реализации проекта

Трансграничность начали формироваться в рамках ФАПСИ при Президенте Российской Федерации, начиная с 2002 года, в контексте организации многостороннего сотрудничества в области информационной безопасности на базе Международного центра по информатике и электронике (ИнтерЭВМ). В этот период поддержка проекту оказывалась со стороны Генерального директора ФАПСИ Матюхина Владимира Георгиевича (разработчик в рамках КГБ СССР электронной цифровой подписи, которая лежит в основе технологий доверенной третьей стороны - ДТС) и Вице-Президента ТПП России Исакова Владимира Борисовича (разработчик фундаментальной теории юридических фактов в праве, которая лежит в основе типового учетно-информационного процесса).

2 этап. Практическую реализацию эти идеи получили в период 2004 – 2008 годов под эгидой Федерального агентства по информационным технологиям, где впервые в мире был создан программно-аппаратный комплекс ДТС, который был апробирован на направлении Европейского союза (Польша, Эстония) с использованием российских и американских криптографических алгоритмов ЭЦП. Однако, на массовый сервис в то время выйти не удалось в связи с отсутствием системно-институциональных оснований для деятельности ДТС. Также в этот период начались контакты и приступили к реализации пилотных проектов в международных форматах СНГ, ШОС, ЕврАзЭС. Разработан мультиформатный проект Конвенции о взаимном признании электронных документов при трансграничном обмене на основе Гаагской конвенции 1961 года об апостилях. Этот проект документа в последующем был положен в основу одного из Соглашений Комиссии таможенного союза и Договора о Евразийском экономическом союзе.

3 этап. Импульс дальнейшему практическому развитию проекта Трансграничность был дан в 2009 году в рамках запуска создания ИИСВВТ. Также важным фактором явилась постановка задачи на 16-м заседании Координационного совета государств-участников СНГ по информатизации (КСИ) при Региональном содружестве в области связи (РСС), состоявшемся 28 сентября 2010 года в Кишиневе по выработке общих подходов к построению ТПД на основе Интернет в рамках СНГ. Этот этап продолжался до конца 2012 года. Детализированные итоги работ в этот период докладывались в Администрацию Президента Российской Федерации, Правительство Российской Федерации, ФСБ России, другие заинтересованные ведомства [11], [12].

4 этап. Включает работы, выполняемые ведомствами Российской Федерации совместно с ЕЭК в настоящее время в различных международных форматах, их результаты кратко отражены ниже.

Платформой для выполнения проекта Трансграничность на текущем этапе являются следующие поручения и установки высокого уровня.

В последнее время высшим руководством страны, в том числе совместно с лидерами ряда ведущих стран мира, поставлены масштабные

задачи в области экономической интеграции, которые должны быть поддержаны со стороны информационных технологий, в том числе:

- Россия предлагает двигаться к созданию от Атлантики до Тихого океана единого экономического и человеческого пространства;
- Развитие региональной экономической интеграции - это стратегический выбор России. И мы будем реализовывать его, основываясь на согласованных интересах с партнёрами по Таможенному союзу и Единому экономическому пространству с учётом перспектив формирования Евразийского экономического союза. На Владивостокском саммите мы представляли не только свои, российские интересы и подходы, а опирались на согласованную позицию тройки: Россия, Казахстан и Белоруссия ;
- Мы признаем важность информационно-коммуникационных технологий (ИКТ) как ключевого фактора, ведущего к интеграции в регионе АТЭС. Мы верим, что возможно и необходимо проявлять большую активность в повышении доверия в электронной среде на глобальном уровне посредством содействия трансграничному юридически значимому обороту информации, включая электронные документы. Мы ещё раз подтверждаем необходимость многостороннего взаимодействия в расширении и усилении Азиатско-Тихоокеанской информационной инфраструктуры для построения доверия и безопасности в использовании ИКТ .

Эти глобальные установки отражены в поручении Президента Российской Федерации № Пр-2831 от 23 октября 2012 года о проведении всестороннего анализа итогов председательства Российской Федерации в Форуме «Азиатско-тихоокеанское экономическое сотрудничество» в 2012 году и подготовке комплексного плана дальнейших действий в рамках АТЭС, в котором предписано обратить особое внимание на реализацию инициатив и проектов по приоритетам российского председательства, использованию возможностей экономик АТР, в том числе для налаживания взаимодействия стран и многосторонних объединений Азиатско-тихоокеанского региона с формирующимся Евразийским экономическим союзом.

Мероприятия по реализации проекта Трансграничность включены в план действий по АТЭС, утвержденный Председателем Правительства Российской Федерации.

5.2 История развития направления в Евразийском Экономическом Союзе

Основными вехами развития проблематики трансграничного пространства доверия в ЕАЭС являются следующие события:

- 29 мая 2014 года в Астане подписан, а, в последствии, ратифицирован странами-членами и вступил в силу Договор о создании ЕАЭС, в котором вопросы построения ТПД отражены в Статье 23 и Приложении 3, а также намечены вектора дальнейшего структурирования

ТПД в рамках единых Требований, Концепции и Стратегии;

- Принята Концепция использования при межгосударственном информационном взаимодействии сервисов и имеющих силу электронных документов, в которой раскрывается институциональный характер ТПД через необходимость разработки Модельного кодекса института международного электронного нотариата на основе сервисов и служб доверенных третьих сторон государств-членов;

- разработана Стратегия развития ТПД, в которой ведется дальнейшее развитие институциональной линии в рамках постановки задачи по обеспечению функционирования института международного электронного нотариата, прежде всего, как социального института, направленного на организацию и закрепление устойчивой формы совместной деятельности людей в электронном виде, в качестве основы при решении спорных вопросов в области электронного взаимодействия и использования в других социальных, государственных и правовых институтах;

- разработана Концепция создания международного частно-государственного партнерства для формирования в сети Интернет ТПД в рамках евразийской экономической интеграции и решения других задач, реализуемых на основе юридически значимого электронного документооборота;

- ведется разработка бизнес-плана для создания государственно-частного партнерства на основе решения КСИ при РСС, принятого в Астане, силами Международного информационно-маркетингового центра СНГ в Республике Беларусь;

- заключено соглашение между РСС и Инновационным центром «Сколково», в котором предусмотрено создание Центра компетенции по Трансграничности;

- в рамках Экспертного совета СНГ принято решение о разработке Модельного закона института электронного нотариата на платформе сервисов и служб ДТС, коррелированного с аналогичной работой, проводимой в ЕАЭС;

- на основе принятых ранее Модели и Методологии разработаны Основные подходы к формированию в сети Интернет трансграничного пространства доверия государств-участников СНГ, гармонизированные с подходами в ЕАЭС;

- принципы, заложенные в Основных подходах, позволили сформулировать универсальные подходы к масштабированию ТПД, которые внесены для обсуждения в ЭСКАТО, ВТО, ОЧЭС, СЕФАКТ, ЮНСИТРАЛ, другие форматы.

Для перевода идей построения кибер-социальных учетных систем трансграничного уровня на Евразийском пространстве в практическую плоскость важно рассмотреть их в увязке с другими проектами информационного обеспечения, которые реализуются в настоящее время в ЕАЭС, и соотнести их с уже реализованными в мире.

В настоящее время в рамках ЕАЭС решается несколько взаимоувязанных задач:

1. Формирование цифровой экономики.

2. Обеспечение прослеживаемости движения товаров до конечного потребителя.

3. Развитие интегрированной информационной системы Союза на платформе ИИСВВТ.

4. Создание, обеспечение функционирования и развития трансграничного пространства доверия.

5. Формирование механизма единого окна, а также ряд других проектов информационной поддержки интеграционных процессов в рамках ЕАЭС и для взаимодействия с основными экономическими регионами мира.

На реализацию совокупности информационных проектов оказывают существенное влияние следующие факторы:

- изначально отсутствовала задача прослеживания товаров до конечного потребителя, чем наносится экономический ущерб, прежде всего России, которая вынужденно находится в режиме взаимных санкций;
- ограниченное бюджетное финансирование в связи с кризисом;
- недостаточная активность бизнеса;
- необходимость противодействия политике отдельных стран по использованию безальтернативных решений в рамках цифровой экономики в различных регионах мира.

Для повышения эффективности работ целесообразно использовать международный опыт, лучшие мировые практики и аналоги, обзор которых представлен в данном разделе.

5.3 Развитие тематики в Форуме Азиатско-тихоокеанского экономического сотрудничества (АТЭС)

За период, начиная с 2012 года в АТЭС и АСЕАН можно выделить следующие основные признаки развития проблематики:

- вопросы реализации проекта Трансграничность отражены в декларациях лидеров АТЭС 2012 и 2014 годов;

- реализован ряд проектов за счет бюджета АТЭС во Владивостоке, Казани, Сан-Франциско, Гонолулу, связанных общей тематикой реализации различных аспектов электронной коммерции на платформе ТПД;

- на 50-м заседании APEC TEL в Брисбене после года блокирования американской стороной удалось выработать общую редакцию принципов интероперабельности ИКТ при трансграничном электронном документообороте, в которой полностью учтены интересы ЕАЭС.

5.4 Развитие направления в форматах ООН (ЮНСИТРАЛ, СЕФАКТ, МСЭ, ЭСКАТО)

В ООН за последние годы можно выделить следующие направления деятельности по тематике кибер-социальных учетных систем трансграничного уровня:

- в рамках итоговых документов Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО + 10) отражена проблематика проекта Трансграничность в качестве одного из принципиально нового явления информационного общества, возникшего в последние годы;
- впервые с 1991 года Россия инициировала и возглавила разработку рекомендации СЕФАКТ по вопросу построения трансграничного пространства доверия, включая механизмы идентификации и аутентификации;
- в рамках рабочей группы III ЮНСИТРАЛ (Урегулирование споров в режиме онлайн - УСО) внесено российской предложение об использовании для УСО подходов, излагаемых в проекте рекомендации СЕФАКТ, предложение принято, будет переведено на все официальные языки ООН и рассмотрено на ближайшем заседании;
- в рамках МСЭ внесен и принят к разработке российский вклад по подготовке международного стандарта на основе пакета принципов интероперабельности ИКТ;
- в рамках ЭСКАТО при подготовке проекта международного соглашения о трансграничном электронном документообороте учтены российские предложения по пакету принципов интероперабельности ИКТ, при этом укрепление ТПД признано в качестве основополагающего принципа ООН.

5.5 Развитие проблематики кибер-социальных учетных систем трансграничного уровня в ЕС

В ЕС за последние годы можно выделить следующие направления деятельности по тематике кибер-социальных учетных систем трансграничного уровня:

- российскими представителями сделан ряд докладов в рамках Диалога Россия – ЕС по информационному обществу по вопросам Web 3.0 (понимаемом, как трансграничное пространство доверия), в результате была достигнута договоренность о продолжении консультаций на экспертном уровне;
- заключен Меморандум о сотрудничестве между компаниями Ростелеком и Дойче Телеком [13] о сотрудничестве в области организации доверенных юридически значимых сервисов;
- прорабатываются вопросы создания пилотного проекта трансграничного юридически-значимого документооборота на базе

функционала международных грузоперевозок с участием компаний Аэрофлот и Люфтганза.

- приняты, реализуются и модернизируются дорожные карты по цифровой экономике на основе «Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (project – eIDAS)» [8] .

5.6 Развитие проблематики кибер-социальных учетных систем трансграничного уровня в ШОС и двусторонних Российско-Китайских проектах

В Шанхайской организации сотрудничества можно выделить следующие направления деятельности в области создания и развития кибер-социальных учетных систем трансграничного уровня:

В Российской Федерации в 2006 году за счет бюджетных средств ФЦП «Электронная Россия» созданы необходимые программно-технические и организационно-правовые решения по обеспечению трансграничной интероперабельности различных кибер-социальных учетных систем. Решение было успешно продемонстрированы в рамках общественной приемки в Санкт-Петербурге и международных конференций в Польше, Молдове, Узбекистане, России.

На базе данных решений Российской стороной на третьем заседании специальной рабочей группы по современным информационным и телекоммуникационным технологиям при комиссии старших должностных лиц Шанхайской Организации Сотрудничества (СРГ СИТТ КСДЛ ШОС), состоявшемся в Бишкеке в сентябре 2007 года был предложен проект «Организации электронного трансграничного взаимодействия с использованием электронной цифровой подписи» (далее - Проект ЭЦП-ШОС) в качестве «пилотного», что по правилам ШОС дает преимущества «приоритетного» проекта. Области применения данного решения в рамках формирующего общего экономического пространства в интересах оптимизации бизнес-процессов за счет повышения оперативности документооборота электронной торговли, государственных закупок, телемедицины, дистанционного образования, мобильных платежей, а также в процедурах контроля государственных контролирующих органов (ГКО) на границе: (пограничного, таможенного, транспортного, миграционного, ветеринарного, фитосанитарного, санитарного), патентной и других актуальных сферах деятельности. Предложение было рассмотрено в рамках 3-го заседания специальной рабочей группы СИТТ ШОС, получило общее одобрение.

Протокол данного заседания СРГ СИТТ предусматривает ряд конкретных мероприятий по реализации проекта ЭЦП-ШОС, в том числе создание экспертной рабочей группы, с участием экспертов от каждой из стран ШОС, проведение испытаний в контуре Россия-Кыргызстан, анализ проектных документов, предложенных экспертам Российской стороной (в

том числе проекта международного соглашения), планирование финансовых вложений в рамках бюджетов заинтересованных стран. Так же протоколом 3 заседания СРГ Российская сторона определена координатором данного проекта, и определен порядок представления материалов экспертными группами стран руководству СРГ и координатору проекта.

В целях проработки деталей проекта сформирована экспертная группа. Российская сторона в качестве координатора представила другим участникам СРГ необходимые исходные данные.

Проект поддержан на заседании Совета глав правительств /премьер-министров/ государств-членов ШОС (02.10.2007 г., г. Ташкент). Совместное коммюнике по итогам заседания гласит:

«...9. Главы правительств констатировали, что реализация отобранного Специальной рабочей группой по современным информационным и телекоммуникационным технологиям "пилотного" проекта "Организация электронного трансграничного взаимодействия с использованием электронной цифровой подписи" позволит активизировать инвестиционную деятельность в рамках ШОС в сфере высоких технологий. Выражена готовность поощрять в рамках ШОС взаимодействие в наукоемких отраслях и формирование современных производств на основе совместных инвестиционных проектов».

По-прежнему актуальным остается вопрос выработки функциональных приоритетов для использования на основе «пилотного» проекта по трансграничному взаимодействию с использованием ЭЦП. По мнению российской стороны в таком качестве могут рассматриваться, как указано выше, электронная торговля, государственные закупки, системы дистанционного образования (в том числе в рамках проекта «Университет ШОС»), телемедицинские проекты, рассматриваемые специальной рабочей группой КСДЛ ШОС по здравоохранению, процедуры контроля ГКО на границе. Эти направления входят в состав экономической политики стран-членов ШОС, активно реализуются в других развитых странах мира и могут дать быстрый и существенный социально экономический эффект. Кроме того, практическая реализация этих направлений позволит ускорить решение других прикладных задач.

Другой приоритетной задачей является формирование международного правового поля стран-членов ШОС для взаимного признания электронных документов с использованием принципов, изложенных в Гаагской конвенции 1961 года «Об апостилях», но в применении к глобальному электронному пространству. Проект соответствующего соглашения представлен российской стороной в формате СРГ по информационным технологиям.

В рамках ШОС к данному проекту проявили интерес СРГ по электронной торговле и СРГ по международной информационной безопасности. Во время работы 4-го совещания СРГ по электронной торговле 18-19 февраля 2008 г. в Пекине обсуждался вопрос применения сервисов

обеспечения доверия в интересах электронной торговли стран-членов ШОС. Делегация посетила Китайский Центр электронной коммерции при Министерстве коммерции КНР. Представленные Китайской стороной решения свидетельствуют о том, что необходимая инфраструктура в КНР имеется, но вопросы обеспечения трансграничности бизнес-процессов электронной торговли не реализованы. Вместе с тем, представители СРГ по электронной торговле, и прежде всего китайская сторона декларировали свою заинтересованность в реализации данных (трансграничных) сервисов. В ходе работы 4-го совещания СРГ по электронной торговле Российской стороной сделаны предложения по интеграции технологий электронной торговли, имеющихся у Российской стороны и сервисов электронной торговой площадки центра электронной коммерции КНР. Данные предложения представлены в протоколе работы 4-й СРГ по электронной коммерции.

24 апреля 2008 года в г. Ташкенте состоялось совещание экспертов по реализации пилотного проекта, в ходе которого была продемонстрирована работа пилотных зон Россия-Кыргзстан и Россия-Узбекистан на абстрактной модели трансграничного электронного документооборота.

О ходе работы по проекту Координатор информирует деловой совет ШОС. Состоялась рабочая встреча с представителем ДС, Сергеем Борисовичем Дурнопьяновым, Заместителем директора Департамента структурного и долгового финансирования Внешэкономбанка. В ходе встречи обсуждалась возможность финансирования работ по линии Межбанковского объединения ШОС. 11 сентября 2008 года в г. Иркутске состоялось заседание правления делового совета ШОС. На заседании по инициативе Координатора проекта (Российская сторона) сделан доклад о состоянии работ по проекту. Участники правления делового совета констатировали поддержку деловым советом данного проекта.

В ходе четвертого заседания Специальной рабочей группы по современным информационным и телекоммуникационным технологиям, состоявшемся в г. Екатеринбурге 17-18 октября 2008 г. Участники СРГ рассмотрели результаты работы по пилотному проекту «Организация электронного трансграничного взаимодействия с использованием электронной цифровой подписи» и приняли ряд решений, направленных на придание динамики развития проекта, прежде всего - на подготовку к подписанию «Соглашения об электронном трансграничном взаимодействии», как базового документа, определяющего возможность применения данных технологий в международных информационных процессах.

В рамках мероприятий Недели ИТ, проходившей в г. Владивостоке 22-26.09.2008 состоялись переговоры с участием представителей департамента связи и информатизации Приморского края, представителя специальной рабочей группы по современным информационным и телекоммуникационным технологиям при комиссии старших должностных

лиц Шанхайской Организации Сотрудничества (СРГ СИТТ КСДЛ ШОС) и делегацией народного правительства города Суйфэньхэ (КНР). В ходе переговоров представитель СРГ СИТТ КСДЛ ШОС проинформировал участников о ходе работ по пилотному (приоритетному) проекту ЭЦП-ШОС. Представители департамента связи и информатизации Приморского края и делегации народного правительства города Суйфэньхэ предложили выйти с инициативой на Координатора проекта ЭЦП-ШОС с предложением об организации пилотной зоны на основе информационного взаимодействия в рамках конкретных трансграничных бизнес-процессов Приморского Края и города Суйфэньхэ.

16 октября 2008 года в г. Санкт-Петербурге состоялось заседание экспертов по реализации пилотного проекта. Сторонами обсуждены замечания и предложения по проекту международного соглашения «Об электронном трансграничном взаимодействии» представленные Кыргызской и Казахской сторонами. По итогам обсуждения Стороны сочли целесообразным рекомендовать СРГ СИТТ использовать в качестве основы проект соглашения «Об электронном трансграничном взаимодействии» для дальнейшей доработки с учетом мнений (заключений) экспертов.

В период 2007-2008 г.г. проведены предварительные испытания технологии, предлагаемой для обеспечения прикладных информационных процессов свойствами подтверждения целостности, неотрекаемости авторства и, как следствие - юридической значимости электронных документов в пилотных зонах Россия-Казахстан, Россия-Кыргызстан и Россия-Узбекистан. Испытания показали работоспособность решения, его универсальность по отношению особенностям национальных реализаций.

По итогам данной работы имеется ряд поручений Правительства Российской Федерации по работам на этих направлениях, в том числе о практической реализации работ по пилотному проекту «ЭЦП ШОС». В настоящее время ведется подготовка к практической реализации поставленных задач.

5.7 БРИКС и ОЧЭС

Под эгидой Минэкономразвития России и с участием ЕЭК проведена серия Экспертных диалогов в форматах БРИКС, ОЧЭС и АСЕАН по электронной коммерции в 2015 - 2016 годах.

5.8 Азиатско-тихоокеанский регион

Наиболее активно данная тематика разрабатывается в Азиатско-тихоокеанском регионе во множестве форматов двустороннего и многостороннего сотрудничества. Ярким примером является Пан-Азиатский альянс по электронной коммерции (ПАА) [6].

Альянс основан в июле 2000 года компаниями Crimson Logic (Сингапур), TRADE-VAN Information Services Co. (Китайский Тайбэй), and

Tradelink Electronic Commerce Limited (Гонконг).

ПАА — это первый региональный альянс по электронной коммерции, цели которого — продвижение и обеспечение безопасных, надежных и защищенных ИТ-инфраструктур и сервисов для безбумажной торговли по всему миру, таких как:

- безопасная и надежная передача торговых и логистических документов с помощью взаимного признания сертификатов электронной подписи, выпущенных УЦ, входящими в Альянс;
- обеспечение взаимодействия сетевых решений для предоставления бизнес-сообществу доступа к различным приложениям для электронной торговли;
- создание Пан-Азиатского веб-портала для обеспечения глобального B2B- взаимодействия и общения.

В настоящее время в ПАА входят организации из 11стран Азиатского региона: China International Electronic Commerce Centre, CIECC (Китай), Trade-Van (Китайский Тайбэй), Trade Link (Гонконг), NACCS (Япония), KTNET (Южная Корея), TEDMEV (Макао), Dagang Net (Малайзия), Crimson Logic (Сингапур), CAT Telecom (Таиланд), Inter Commerce (Филиппины), EDI-I (Индонезия).

Вышеперечисленные организации являются крупнейшими провайдерами услуг в области электронной торговли в своих экономиках в сегментах B2B, B2G и G2G.

ПАА предоставляет набор сервисных предложений, которые строятся вокруг международных технических стандартов, технологий информационной безопасности на соответствующей правовой основе. При этом на практике реализуется безопасный трансграничный электронный документооборот и обмен данными между пользователями через членов Альянса.

В ПАА обмен документами для трансграничных сделок может осуществляться просто и эффективно в электронном виде посредством защищенной инфраструктуры. Кроме того, пользователи смогут повторно использовать соответствующие данные из полученных документов для применения и представления торговых или нормативных деклараций местным органам управления экономик ПАА.

Можно привести следующие примеры реализованных в ПАА проектов:

- Документооборот между импортерами и экспортерами.
  - Обмен заказами на поставку, счетами-фактурами и предварительными уведомлениями об отгрузке для текстильной промышленности. Проект разработан для гонконгской компании — производителя одежды TAL Apparel Limited и ее поставщиков из Тайваня, в частности, текстильной компании Tai Yuen Textile Co. Решение реализовано участниками ПАА Tradelink Electronic Commerce Limited (Гонконг) и TRADE-VAN

Information Services Co. (Китайский Тайбэй).

- Обмен упаковочными листами, счетами-фактурами и коносаментами для поставок стали для автомобильной промышленности. Проект разработан для японского поставщика стали Metal One Corporation и автомобильной корпорации Hyundai Motors. Решение реализовано компаниями KTNET (Южная Корея) и TEDIANET (Япония).

- Документооборот между экспедиторскими и логистическими компаниями. Обмен и повторное использование данных о доставке и торговых данных для подготовки и подачи деклараций экспорта/импорта между бизнес-сообществами Сингапура и Малайзии. Сетевое решение реализовано компаниями Crimson Logic (Сингапур) и Dagang Net (Малайзия).
- Взаимное признание национальных инфраструктур открытых ключей (PKI). В ПАА существует специальная политика сертификации и авторизации удостоверяющих центров из экономик Альянса. На основе таких УЦ построена инфраструктура использования и взаимного признания сертификатов электронной подписи для всех электронных транзакций в сети ПАА.
- Сервис отслеживания грузов. Данный сервис позволит транспортным компаниям определять статус груза и будет внедрен в существующие трансграничные электронные сервисы. В настоящее время сервис проходит тестирование с участием клиентов компаний KTNET (Южная Корея) и TRADE-VAN Information Services Co. (Китайский Тайбэй).

ПАА занимается разработкой технических стандартов, протоколов связи и обменом сообщениями внутри сети Альянса, а также правовыми аспектами: разработкой договоров, спецификаций, процедур для обеспечения юридической значимости электронных транзакций среди участников ПАА.

Услугами и электронными решениями ПАА пользуются более 150 000 компаний на азиатском рынке.

ПАА активно сотрудничает с группой по электронной торговле АТЭС, является членом Австралийской федерации борьбы против пиратства (AFACT). Началось сотрудничество с Европой через Азиатско-Европейский Альянс по электронной торговле (ASEAL).

Из более свежих примеров можно упомянуть Trans Pacific Partnership - Транстихоокеанское партнёрство— преференциальное торговое соглашение между 12-ю странами Азиатско-Тихоокеанского региона, целью которого является снижение тарифных барьеров, а также регулирование внутренних правил в странах-участницах в таких областях как трудовое право, экология, интеллектуальная собственность и ряде других.[7]

6 Обобщение международного опыта обеспечения интероперабельности трансграничного информационного юридически-значимого взаимодействия

Таким образом, США, Европа и страны Азиатско-Тихоокеанского региона реализуют единую криптографическую политику в сфере создания единых региональных цифровых пространств и показывают очевидную тенденцию выхода на глобальный уровень. Криптографические алгоритмы RSA в настоящее время являются стандартом де-факто в системах информационной безопасности рекомендованых CCITT (Consultative Committee in International Telegraphy and Telephony – Международным консультативным комитетом в области телеграфии и телефонии, МККТТ), в рекомендациях X.509, используется во многих международных стандартах (S-HTTP, PEM, S-MIME, S/WAN, SSL, SWIFT, ANSI X.9.31 и т.д.) в системах обслуживания кредитных карточек, в операционных системах, для защиты сетевых протоколов взаимодействия и пр.

Национальное законодательство стран, обладающих собственными криптографическими школами, как правило, определяет необходимость использования национальных криптографических стандартов для решения критических, с точки зрения безопасности, задач, в том числе – для обеспечения юридической силы электронных документов. Это правило вступает в противоречие с описанными выше, развиваемыми под эгидой администрации США и их союзников тенденции создания однополярного криптографического пространства.

Российской Федерацией и другими государствами-членами ЕАЭС в последнее время предпринят ряд шагов по созданию и продвижению подхода к обеспечению трансграничного электронного документооборота на платформе трансграничного пространства доверия (ТПД) с ключевым конструктивным элементом – доверенной третьей стороной (ДТС) согласно международному стандарту X.842.

Указанный подход представляет собой информационную шину, на основании которой возможно обеспечить интеграцию национальных криптографических решений.

Идеи ТПД и ДТС удалось существенно продвинуть в рамках таких международных форматов, как ЕАЭС, ЭСКАТО, СЕФАКТ, ЮНСИТРАЛ и других. Стоит отметить, что большое количество стран поддерживают российский подход в качестве альтернативы активно продвигаемой американской стороной собственной модели обеспечения информационной безопасности.

Целесообразно рассматривать ТПД в качестве инфраструктурной поддержки для функционирования системы концентраторов (хабов) сервисов электронной коммерции в соответствии с моделью BUY-SHIP-PAY, по аналогии с практикой упомянутого выше Паназиатского альянса по электронной коммерции. Данные хабы, концентрируя все сервисы цифровой

экономики, позволяют наиболее простым и неконфликтным способом решить проблему прослеживаемости товаров при разворачивании соответствующей информационно-аналитической системы «поверх» сервисов.

7 Электронная коммерция на Евразийском пространстве

Учитывая изложенное в разделах 5-6, становится очевидной инициатива по созданию Евразийского альянса по электронной коммерции на платформе частно-государственного партнерства. Это позволит комплексно решить вопросы привлечения бизнеса для частичного снятия нагрузки с бюджета, мягкой защиты экономических интересов России, а также на конструктивной основе обеспечить решение вопросов международной информационной безопасности в глобальном информационном пространстве.

В плане практической реализации целесообразно:

- государству взять на себя вопросы разработки технических требований по информационной безопасности и формирование нормативной основы;
- бизнесу осуществить разработку функционального хаба электронной коммерции в рамках импортозамещения, используя имеющиеся международные наработки;
- использовать существующую инфраструктуру для организации работы с клиентами (Почта России, сеть нотариальных контор, сеть удостоверяющих центров).

Как отмечалось выше формирование Альянса целесообразно производить совместно с функциональной логистической составляющей и кибер-физическими системами:

- создание современного транспортного коридора в указанной географии на основе мультимодальных технологий;
- обеспечение поддержки логистических технологий со стороны Умных транспортных кибер-систем или промышленного Интернета.

Экономическая связанность в рамках межрегиональной географии (от Атлантики до Тихого океана) предполагает развитие современных логистических технологий для всех видов транспорта (железнодорожного, авиационного, речного и морского, а также автомобильного и трубопроводного). При этом уникальное геополитическое положение России в центре этого мирового региона создает хорошие предпосылки для повышения роли страны в глобальной экономике, в том числе на основе инновационных технологий, к которым относятся ИКТ. Наращивание транспортной и информационной связанности в важнейшем регионе мира будет способствовать экономической интеграции региона и предоставлению качественных трансграничных услуг населению и организациям, находящихся в различных юрисдикциях.

С другой стороны, сочетание этих двух важнейших инфраструктур (логистика и ИКТ) может придать дополнительный импульс для развития транспортной отрасли России и стран ближнего зарубежья, радикальному сокращению издержек временного и финансового характера на обслуживание бумажного документооборота, становящегося все большим анахронизмом, и пересечение пунктов пропуска для всех видов транспортных средств. Инновационные решения по обеспечению трансграничного юридически значимого документооборота, отработанные на постсоветском пространстве, в последующем могут быть тиражированы на европейском и азиатско-тихоокеанском направлениях. Это находится в контексте задач, поставленных Президентом Российской Федерации и решаемых на практике в рамках Евразийского экономического союза [9].

Таким образом:

1. Анализ зарубежных источников показал детальную теоретическую проработанность класса кибер-физических систем и некоторое общее описание кибер-социальных систем, прежде всего в онтологическом плане и применительно к телемедицинским системам недокументированного типа. Это позволяет обобщить практику создания систем электронного правительства, механизмов единого окна и их аналогов на основе описания в качестве самостоятельного класса кибер-социальных учетных систем.

2. В России и ЕЭК имеются уникальные наработки в области создания трансграничного пространства доверия, как сложной гуманитарно-технологической системы международного уровня. Эти подходы получили признание и поддержку в других регионах мира и в структурах ООН.

3. Уникальное географическое положение России и других государств-членов ЕАЭС позволяет выдвинуть инициативу по созданию Евразийского альянса по электронной коммерции в увязке с современными логистическими технологиями.

4. Совместное создание в рамках Альянса обоих типов кибер-систем, физических и социальных, позволит существенно сократить инвестиции путем формирования общих инфраструктур, прежде всего телекоммуникационных и работы с данными. Кроме того, это позволит говорить о частичном импортозамещении в результате использования отечественных информационно-безопасных разработок в сфере построения доверенных сервисов, а также обеспечить управляемость при масштабном внедрении зарубежных кибер-физических систем.

8 Исследование и анализ возможностей построения трансграничного пространства доверия на централизованных или децентрализованных принципах

Для целей поддержки ЕЦП трансграничное пространство доверия может сегментироваться по признаку централизованного или децентрализованного управления сервисами доверия.

8.1 Централизованная модель построения инфраструктуры доверия

Определенное развитие на протяжении ряда последних лет получила централизованная модель, разработка которой ведется в форматах СНГ, ЕАЭС, СЕФАКТ, ЭСКАТО ООН и ЮНСИТРАЛ. Ее можно обозначить как нейтральную международную среду для отдельных стран и их объединений, устойчивую по отношению к политическим, экономическим, социальным и иным влияниям и интересам отдельно взятых ее участников.

Доверие строится в централизованной модели на общественных отношениях, институционализированных самими же участниками соответствующей инфраструктуры доверия. Централизованная модель основывается на выполнении всеми её участниками между ними же согласованных Требований при проведении периодического независимого аудита уполномоченных операторов сервисов доверия.

Таким образом, необходимый уровень доверия между участниками (в том числе – конечными пользователями) инфраструктуры доверия, основанной на централизованной модели, достигается благодаря априорно институционализированным отношениям между странами-участницами этой инфраструктуры доверия. Эта институционализация охватывает юридические и организационные аспекты, влияющие и на технико-технологические аспекты интероперабельности и информационной безопасности.

Существенными особенностями централизованной модели доверия являются:

- ее естественное, и поэтому легкое, сопряжение с традиционно существующими институтами (включая идентификацию субъектов электронного взаимодействия),
- государственно-коммерческое сотрудничество в рамках инфраструктуры доверия,
- ее естественная масштабируемость (прием новых участников / выход из инфраструктуры доверия),
- равноправность и недискриминационность сотрудничества в инфраструктуре доверия,
- многовариантность выбора уровня квалификации отдельных сервисов доверия (например, низкий, средний, высокий).

Подходы к построению нейтральной среды находят отражение в ряде международных документов, среди которых следующие:

Договор о Евразийском экономическом союзе (Подписан в г. Астане 29.05.2014)[18];

Проект рекомендации Центра ООН по упрощению торговых процедур (СЕФАКТ) «Об обеспечении юридически значимого трансграничного электронного взаимодействия»[19];

[18] http://www.consultant.ru/document/cons_doc_LAW_163855/

Проект регионального межправительственного соглашения об упрощении процедур трансграничной безбумажной торговли Экономической и социальной комиссии ООН стран Азии и Тихого океана (ЭСКАТО)[20];

Пакет документов в области формирования и функционирования трансграничного пространства доверия государств-участников СНГ[21].

Практическая реализация нейтральной международной среды на платформе Доверенной третьей стороны в настоящее время активно проводится в рамках Евразийской экономической комиссии. Разработан проект архитектуры трансграничного пространства доверия, который включает набор централизованно предоставляемых электронных сервисов. Продолжается обсуждение государствами-членами ЕАЭС их состава в контексте согласованного обеспечения вопросов международной и национальной информационной безопасности.

8.2 Децентрализованная модель построения инфраструктуры доверия

Необходимый уровень доверия может также обеспечиваться инфраструктурами доверия, построенными по децентрализованной модели.

Одной из технологий, позволяющей реализовать децентрализованную модель, является *блокчейн (blockchain)* технология. Идея блокчейн-технологии максимально проста — это огромная распределенная база данных общего пользования, которая функционирует без централизованного руководства. В случае с биткоином, проверкой транзакций занимаются так называемые майнеры — участники системы, которые подтверждают подлинность совершенных действий, а затем формируют из записей транзакций блоки. В настоящее время в обществе развернуты активные дискуссии по вопросу перспективности использования блокчейн в массовых сервисах[22].

Доверие строится в децентрализованной модели на общественных отношениях, возникающих между участниками децентрализованной инфраструктуры доверия, основанных на неконтролируемости решающего большинства узлов блокчейн-системы[23] и их равноправности.

Таким образом мы видим, что децентрализованная модель установления доверия также требует институционализации, несмотря на то, что неконтролируемость решающего большинства узлов блокчейн-системы и их равноправность в значительной мере поддерживается (но не

---

19 http://www1.unece.org/cefact/platform/download/attachments/55378391/Rec+draft+v.0.91+08.09.15.pdf

20 http://www.unescap.org/our-work

21 http://www.rcc.org.ru/work/informatiz/trans/index

22 http://www.gazeta.ru/tech/2016/02/01/8038769/blockchain.shtml

23 „blockchain“-система: какая-либо конкретная реализация „blockchain“-технологии

обеспечивается полностью) математическими / технологическими, а не организационными (как в централизованной модели) методами.

Поскольку сам процесс майнинга сопряжен со сложными математическими задачами, майнеры должны иметь в своем арсенале довольно мощные компьютеры. В руках этих участников и находится распределенная база данных, состоящая из «цепочки блоков». Распределенный характер базы данных на основе блокчейна и позволяет контролировать достоверность транзакций без надзора каких-либо институционализированных (например, финансовых) регуляторов.

Основное преимущество блокчейна перед традиционными транзакциями — отсутствие посредников (например, в лице банков). Сейчас все операции с деньгами, документами или другими данными неизбежно проходят через посредников. Банки, государственные органы или же нотариусы постоянно подтверждают подлинность проделанных операций.

Блокчейн не имеет центрального органа, поэтому транзакции проверяются всеми участниками системы. Именно это позволяет избавиться от посредников и тем самым упростить процедуру. Программный код сети открыт, и любой может обратиться к нему, но личность и другая персональная информация остаются тайной. Все, что видят создатели блоков, — данные по каждой конкретной операции.

Проще говоря, если блокчейн-технологию внедрить в повседневную жизнь, то контроль по фиксации операций со стороны банков, госорганов, аудиторов, контролеров, страховых компаний или регистраторов будет либо нужен в существенно меньшем объеме, либо вовсе не нужен.

В будущем государства могут институционализировать определенные блокчейн-системы и взять на вооружение данные, заверенные с помощью институционализированного блокчейна, как доказательства в различных процессах, в том числе и судебной практике, поскольку технология не принимает какую-либо фальсификацию. Российские специалисты занимаются разработкой шлюза для взаимодействия с биткоин-блокчейн для нотаризации событий.

8.3 Влияние внедрения блокчейн-систем на общество

Следует заметить, что правовая база любой юрисдикции в прошлом, настоящем и будущем основывается на идентификации физических и юридических лиц. Это является имманентным, неотторжимым свойством права, как социально-организующей функции человеческого общества, так как пользователями правовой системы являются именно физические и юридические лица, как подмножество ее субъектов. Сбор налогов для поддержания функционирования общества как такового и сохранение баланса между защитой общества от угроз и свободой выбора для его членов также основываются на идентификации физических и юридических лиц.

Широкое внедрение блокчейн-систем в различные сферы общественной жизни может существенно повлиять как на инфраструктурную

организацию общества, так и на процедуры его регулирования. Если блокчейн-системы будут институционально интегрированы и, следовательно, результаты их действия будут признаваться в качестве доказательств в правосудии, это приведет, например, к уменьшению объема функций исполнительной власти из-за перенятия блокчейн-системами некоторых, а то и многих ее институциональных функций.

Например, одна из центральных функций государства – фиксация отношений собственности между физическим или юридическим лицом и каким-либо активом (asset) – может быть перенята блокчейн-системами. Обеспечение соблюдения отношений собственности останется, однако в ведении правосудия.

Сокращение объема функций исполнительной власти автоматически приведет к уменьшению ее представительского авторитета. Этот процесс, как любое существенное изменение структур и функций в этой сфере, может сопровождаться политической нестабильностью.

Кроме того, возможным в перспективе представляется появление следующих факторов:

уменьшение роли нотариата, особенно в области подтверждения юридически значимых статусов субъектов и объектов права, так как фиксация этих статусов может быть перенята блокчейн-системами. Правовая оценка юридически значимых статусов останется в ведении правосудия;

драматическое уменьшение роли поставщиков (предоставителей) финансовых услуг, особенно тех, которые в основном занимаются посредничеством при проведении платежной транзакции между покупателем и продавцом (это в особенности коснется банков и платежных площадок в интернете);

изменение конкурентной ситуации в международной экономике в пользу развивающихся стран. Фиксация собственности блокчейн-системами (например, на землю, другую движимость и недвижимость) способствовало бы появлению в этих странах кредитоспособных хозяйственных субъектов (собственников), что, в свою очередь, привело бы к ростовому скачку их экономик.

Следует обратить внимание еще на одно явление, которое имманентно блокчейн-технологии, по крайней мере в ее сегодняшнем виде. Для создания новых значимых (то есть валидных) блоков в блокчейн-системе используются методы Proof-of-Work и Proof-of-Stake.

Метод Proof-of-Work требует тем меньше вычислительных ресурсов (экспоненциально), чем раньше участник системы к ней присоединился. Таким образом, ранние участники системы получают существенные ресурсные преимущества, что несколько противоречит заявленному равноправию участников. Для поддержания принципа равноправия, конкретные блокчейн-системы, использующие Proof-of-Work, могут вводить как дополнительные технические, так и технико-организационные средства. Например, в системе bitcoin к ним относятся targeting, регулирующий с

помощью специального системного параметра трудоемкость создания новых значимых (т.е. валидных) блоков, и мотивация майнеров[24] (получением bitcoins) для увеличения количества независимых пользователей системы.

Метод Proof-of-Stake мотивирует к накоплению контролирующих атрибутов системы в одних руках с целью перенятия контроля над системой, что противоречит принципу децентрализации системы.

Любая из этих реализаций – без введения дополнительных технических и организационных мер противодействия – с необходимостью приведет к возникновению олигархической системы, в которой небольшая группа ее участников сможет (и будет) контролировать поведение системы. Уровень доверия к этой системе будет зависеть от уровня доверия к тому, что группа олигархов не злоупотребляет своим положением в системе. Это противоречит изначально заявленным принципам неконтролируемости решающего большинства узлов системы и их равноправности. Более того, плакатное декларирование этих принципов вуалирует имманентную склонность сегодняшних реализаций блокчейн-технологии к образованию форм олигархии.

8.4 Вопросы конвергенции

Предложенная в проекте рекомендации Центра ООН по упрощению торговых процедур (СЕФАКТ) «Об обеспечении юридически значимого трансграничного электронного взаимодействия» нейтральная международная среда, контролируемая клубом юрисдикций на равноправных началах, а не одним государством, является, на наш взгляд, более универсальной в отношении приложения в различных областях человеческого общества. В отношении установления доверия, она соединяет преимущества относительного равноправия децентрализованных технологий и преимущества относительно легкой институциональной интегрируемости и легкой масштабируемости централизованных систем.

Централизованная система, построенная на нейтральной среде, кроме прочего, легко взаимодействует с системами идентификации лиц (и может их легко интегрировать при необходимости) и, таким образом, может гибко регулировать баланс «идентификация – анонимность».

Блокчейн-технология, наряду с другими технологиями, может эффективно использоваться для реализации частных задач, для решения которых она предоставляет адекватную среду. Как было обосновано выше, самое естественное приложение блокчейн-технологии – анонимные ценные бумаги, включая деньги, сертификаты происхождения ценных активов (драгоценностей, произведений искусства, дорогих автомобилей и т.п.) и другие анонимные оборотные средства.

---

[24] участники системы, подтверждающие подлинность совершенных транзакций, а затем формирующие из записей транзакций блоки.

Неверно утверждать, что одна из рассмотренных выше моделей в любом случае подходящая, а другая заведомо влечет негативные проявления. Логика развития общества приводит к существованию исторических фаз с различным уровнем взаимного доверия между его отдельными членами, группами и общественными институтами. Фактическое или ощущаемое отсутствие необходимой степени взаимного доверия и другие мотивации делают неизбежной незаконную деятельность при использовании конкретной технологии, что и вызывает регулятивное вмешательство со стороны общества.

Оптимальной стратегией того, что касается предотвращения негативных последствий использования цифровых валют, могло бы стать появление общественно-приемлемых альтернатив тому, что стимулирует их принятие, а это, прежде всего, анонимность транзакций, безопасность (полнота и неподделываемость истории всех завершенных транзакций) и доступность, которые интересны массовым пользователям.

В приемлемости со стороны общества на данном историческом этапе и заключаются предпосылки для конвергенции между двумя подходами.

Основная институциональная проблема децентрализованной модели, построенной на блокчейн-технологии, заключается в том, что невозможно локализовать информационные системы – распределенные реестры и закрепить за ними уполномоченных операторов, которые могут подлежать международному правовому регулированию. С другой стороны, централизованные реестры – учетные системы допускают естественное, и поэтому легкое, сопряжение с традиционно существующими институтами. Соответственно можно построить правовую модель и предложить ее международному сообществу для регулирования, что и происходит в рамках СЕФАКТ, ЭСКАТО, ЕАЭС и СНГ, как описано выше.

Нейтральная международная среда, контролируемая клубом юрисдикций на равноправных началах, а не одним государством, является в обозримой перспективе более универсальной в отношении приложения в различных областях человеческого общества. В отношении установления доверия, она соединяет преимущества относительного равноправия блокчейна, как децентрализованной технологии, и преимущества относительно легкой институциональной интегрируемости и легкой масштабируемости централизованных систем.

Однако это не означает, что децентрализованные решения нужно запретить или отпустить «в свободное плавание». Децентрализованная модель установления доверия также требует институционализации, несмотря на то, что неконтролируемость решающего большинства узлов блокчейн-системы и их равноправность в значительной мере поддерживается (но не обеспечивается полностью) математическими / технологическими, а не организационными – как в централизованной модели – методами. По блокчейн-технологии однако пока в мире не предложена модель правового

регулирования, что является определенным барьером на пути развития глобального информационного общества, и на этот вызов надо отвечать.

Пока не очень понятно, как использовать блокчейн-технологию в рамках, например, электронного правительства в ближайшей обозримой перспективе, без радикальной смены парадигмы взаимодействия власти и общества. С другой стороны, эту технологию можно и нужно легализовать в тех сферах, где она может эффективно использоваться для реализации частных задач, для решения которых она предоставляет адекватную среду. Как указывалось выше (см. «Децентрализованная модель построения инфраструктуры доверия»), самое естественное приложение блокчейн-технологии – анонимные ценные бумаги, включая деньги, сертификаты происхождения ценных активов и другие анонимные оборотные средства. Другой сферой ее возможного применения может быть, например, урегулирование споров в режиме онлайн.

Оптимальным решением является конвергенция и выработка непротиворечивых моделей международного правового регулирования, нацеленных на достижение общественного блага, использование разносторонних преимуществ и недопущение негативных проявлений.

8.5 Вопросы реализации

Практическую реализацию двухсегментного трансграничного пространства доверия невозможно проводить без тесной увязки с функциональными сервисами, то есть эту проблему следует рассматривать в общем контексте цифровой экономики. Результатом могут стать две различные правовые модели для централизованного-децентрализованного учетов, которые также требуют более широкого концепта прикладных сервисов.

Правовому регулированию подлежат объекты и субъекты прав. К субъектам можно отнести все категории лиц (физические, юридические, уполномоченные) и организации (органы власти всех уровней, судебные, страховые и нотариальные инстанции), а также операторов информационных систем. К объектам – информационные системы и рабочие места, включая средства подписи и доступа. Между субъектами и объектами прав возникают правовые отношения – в первую очередь по поводу функциональных приложений. Эти правовые отношения, однако, могут также включать аспекты доверия и безопасности, что может рассматриваться как опция к торговле, медицине и образованию. Само по себе доверие бессмысленно – оно всегда относится к кому-то или чему-то. Именно поэтому блокчейн-технология появилась в связке с цифровой валютой – биткоинами. Как известно, технологии сами по себе не подлежат правовому регулированию, а являются сферой специфического технического регулирования, которое находится вне компетенции таких субъектов регулирования, как Комиссия ООН по праву международной торговли (ЮНСИТРАЛ), в ведении которой

находится проблематика институционализации двухсегментного трансграничного пространства доверия.

Целесообразно предложить инициативу по разработке проекта Конвенции ООН об использовании трансграничного пространства доверия для цифровой экономики (проект Конвенции представлен в приложении к данному сборнику). Такого рода вклад может быть сделан в профильную Рабочую группу IV (Электронная коммерция) ЮНСИТРАЛ.

При этом в качестве возможного решения проблемы двух правовых моделей доверия можно предложить следующий подход: нейтральная международная среда, контролируемая клубом юрисдикций на равноправных началах, и ее общая инфраструктура доверия строится на принципе международного регулирования, в то время как сервисы на основе блокчейн-технологии предоставляются на основе саморегулирования при дозированном международном контроле с целью недопущения нежелательных для общества эффектов.

Таким образом, ключевым вызовом в отношении реализации централизованной модели станет поиск консенсуса по регламенту организации нейтральной международной среды, тогда как ключевым вызовом в отношении реализации децентрализованной модели станет поиск приемлемых форм такого регулятивного вмешательства, которое не станет существенным препятствием для применения блокчейн-технологии, надежно устранив негативные социальные проявления путем локального государственного контроля.

9 Исследование архитектуры формирования трансграничного пространства доверия, основанной на централизованных принципах, на примере Евразийского экономического союза

Трансграничное пространство доверия (ТПД) государств-членов Евразийского экономического союза (ЕАЭС) может рассматриваться как большая и сложная гуманитарно-технологическая система, предназначенная для институционально гарантированной охраны законных прав и интересов граждан и организаций, взаимодействующих в рамках отношений, возникающих при формировании, отправке, передаче, получении, хранении и использовании электронных документов.

В условиях экономической глобализации и повсеместного распространения сети Интернет ТПД ЕАЭС может рассматриваться в качестве отдельного домена, который взаимодействует с аналогами в других регионах мира, при условии сохранения установленного уровня доверия для граждан и организаций, находящихся в юрисдикции государств-членов ЕАЭС (масштабироваться с использованием нейтральных межгосударственных шлюзов).

Проводимая в рамках Экономической и социальной комиссии ООН по странам Азии и Тихого океана (ЭСКАТО) работа, позволяет рассматривать совершенствование ТПД (improving trans-boundary trust environment) в

качестве одного из универсальных принципов трансграничного безбумажного документооборота, наряду с другими основополагающими принципами ООН, выработанными Комиссией ООН по праву международной торговли (ЮНСИТРАЛ), такими как технологическая нейтральность, функциональная эквивалентность и не дискриминация.

При этом ТПД, как принцип, может означать следующее:

- реализацию на практике взаимного доверия между странами в рамках трансграничного безбумажного документооборота при сохранении цифрового суверенитета;

- общую информационную безопасность стран-участников ТПД при обеспечении равнопрочности национальных доменов доверия;

- выработку общей политики обеспечения взаимного доверия в рамках совместных координационных советов регуляторов;

- возможность совместного использования существующих и перспективных организационных, правовых и технологических механизмов реализации отдельных доменов доверия на основе нейтральных междоменных шлюзов;

- обеспечение взаимного трансграничного признания электронных документов (легализации) при выполнении критериев их эквивалентности бумажным аналогам.

Корректное и системное описание архитектуры ТПД предполагает ее описание на следующих взаимно увязанных уровнях:

1. Технологический уровень - описание доверенных сервисов, предназначенных для инженерно-технической поддержки информационных процессов, обеспечиваемых в рамках ТПД ЕАЭС.

2. Институциональный уровень – описание организационно-правовых механизмов, необходимых и достаточных для гарантированной охраны законных прав и интересов граждан и организаций государств-членов ЕАЭС.

3. Процессно-проектный уровень – описание вариантов информационных процессов инфраструктурного характера, предназначенных для придания качества юридической значимости электронным документам в рамках общих процессов функционального характера в рамках ЕАЭС, выбор оптимальных решений и их отражение в проектной документации.

4. Нормативно-правовой уровень – закрепление описания отдельных элементов архитектуры ТПД и их взаимосвязей в совокупности технических требований, регламентов, положений, правил, стандартов, рекомендаций и других правоустанавливающих документах, принимаемых в рамках ЕАЭС с последующей гармонизацией в национальных законодательствах государств-членов.

Перечень доверенных сервисов и организационно-правовых механизмов должен закрепляться в разрабатываемых документах стратегического характера. Разработка проектов документов процессно-проектного и нормативно-правового уровня является предметом дальнейших работ, проводимых по планам ЕАЭС.

В таблице, приводимой ниже, описывается возможный состав доверенных сервисов и организационно-правовых механизмов.

№ п/п	Доверенные сервисы (ДС)	Организационно-правовые механизмы	Информационные процессы, описываемые в рамках НИР и других работ по планам ЕАЭС	Закрепление в документах
1.	Сервис доверенной третьей стороны (ДТС)	- лицензирование деятельности, связанной с предоставлением ДС; - аккредитация операторов, предоставляющих ДС; - сертификация программно-аппаратных комплексов и средств, с использованием которых предоставляется ДС; - проверка (аудит) выполнения Требований к созданию, развитию и функционированию трансграничного пространства доверия; - обеспечительная политика деятельности операторов, предоставляющих ДС; - тарифная политика операторов, предоставляющих ДС; - страхование рисков, связанных с предоставлением ДС; - признание электронных документов, издаваемых с использованием ДС, в страховой деятельности; - признание электронных документов, издаваемых с использованием ДС в судебной деятельности; - другие организационно-правовые механизмы, связанные с предоставлением ДС.	Формализованное описание вариантов сквозного информационного процесса взаимодействия между клиентами в различных юрисдикциях (с использованием нотариального и/или апостильного заверения подписи и без них). Обоснование подходов к гармонизации организационно-правовых механизмов, связанных с предоставлением ДС, в государствах-членах ЕАЭС. Определение возможностей по адаптации международных судебных и страховых механизмов для работы с электронными документами, издаваемыми в различных юрисдикциях. Предложения по международной стандартизации сервиса ДТС. Модель угроз.	1. Технические требования к ПАК ДТС (связано с п.6). 2. Регламенты оператора и уполномоченных лиц ДТС (с использованием нотариального заверения подписи и без него). 3. Положение о гармонизации организационно-правовых механизмов, связанных с предоставлением ДС[25], в государствах-членах ЕАЭС. 4. Положение об участии ЕАЭС и государств-членов в международных организациях, регулирующих вопросы судебной и страховой деятельности. 5. Положение о комиссии по проверке компонентов общей инфраструктуры документирования информации в электронном виде на соответствие требованиям к созданию, развитию и функционированию трансграничного пространства доверия[26]. 6. Требования к созданию, развитию и функционированию трансграничного пространства доверия[27]. 7. Другие документы.
2.	Сервис удостоверяющего центра (УЦ) ТПД		Технический проект и смета на создание и эксплуатацию. Модель угроз.	Регламент уполномоченных лиц УЦ. Политика безопасности

[25] Является актуальным для всех ДС.
[26] Является актуальным для всех ДС.
[27] Является актуальным для всех ДС.

				УЦ.
3.	Сервис национальной инфраструктуры открытых ключей		Разработка предложений по гармонизации сервисов национальных инфраструктур открытых ключей. Модель угроз.	Рекомендации по построению национальных инфраструктур открытых ключей.
4.	Сервис доверенного времени		Обоснование конфигурации предоставления сервиса доверенного времени (централизованная или децентрализованная). Технический проект и смета на создание и эксплуатацию (в случае выбора централизованной конфигурации). Модель угроз.	Технические требования к ПАК доверенного времени (в случае выбора децентрализованной конфигурации). Регламент оператора.
5.	Сервис подтверждения статусов (полномочия и правомочия физических лиц, правовой статус юридических лиц, право подписи, других статусов) субъектов информационного взаимодействия		Обоснование конфигурации предоставления сервиса подтверждения статусов субъектов информационного взаимодействия с учетом взаимодействия с унаследованными и перспективными (ЕАГД, НСИ) информационными системами интеграционного и национальных сегментов. Модель угроз.	Требования, рекомендации, регламенты, положения по результатам обоснования и модели угроз.
6.	Сервис заверения подлинности отдельных фрагментов контента электронного документа (место издания и другие)		Обоснование юридической модели сервиса заверения подлинности отдельных фрагментов контента электронного документа[28]. Модель угроз.	Требования, рекомендации, регламенты, положения по результатам обоснования и модели угроз.
7.	Совокупность сервисов на клиентском уровне, используемых для информационного взаимодействия в рамках общих процессов ТПД: - комплексная эмиссия средств доступа и подписи (производство, дистрибуция, персонализация,		Обоснование сервисов на клиентском уровне, прежде всего с точки зрения простоты использования и соблюдения требований по информационной безопасности. Обоснование конфигурации предоставления клиентских сервисов с учетом взаимодействия с унаследованными и	Требования, рекомендации, регламенты, положения по результатам обоснования и модели угроз.

[28] Целесообразно рассматривать вместе с сервисами нотариального и/или апостильного заверения.

	выдача, утилизация); - эмиссия устройств чтения средств доступа и подписи; - идентификация и аутентификация субъектов информационного взаимодействия; - клиентский интерфейс для различных операционных систем; - другие клиентские сервисы.		перспективными (ЕСИА) информационными системами интеграционного и национальных сегментов. Модель угроз.	
8.	Сервис внешнего интерфейса для информационного взаимодействия с гражданами и организациями стран, не входящих в ТПД ЕАЭС		Разработка подходов к созданию и функционированию типовых нейтральных междоменных шлюзов. Предложения по международной стандартизации типовых нейтральных междоменных шлюзов. Модель угроз.	Положение об организации информационного взаимодействия с гражданами и организациями стран, не входящих в ТПД ЕАЭС.
9.	Интерфейс встраивания доверенных сервисов в функциональные информационные системы, поддерживающие общие процессы, единое окно и системы межведомственного взаимодействия		Обоснование конфигурации предоставления сервиса взаимодействия с учетом унаследованных и перспективных (СМЭВ) информационных систем интеграционного и национальных сегментов. Модель угроз.	Рекомендации по построению национальных сегментов по результатам обоснования и модели угроз (в случае необходимости).
10.	Сервис доверенного архивного хранения электронных документов		Обоснование конфигурации предоставления сервиса доверенного архивного хранения электронных документов (централизованная или децентрализованная). Технический проект и смета на создание и эксплуатацию (в случае выбора централизованной конфигурации). Модель угроз.	Технические требования к ПАК доверенного архивного хранения электронных документов (в случае выбора децентрализованной конфигурации). Регламент оператора.

10 Исследование и анализ возможностей формирования глобального трансграничного пространства доверия

1. Целью исследования является выявление проблем и подходов к их решению для последующего обсуждения в рамках разработки семейства Рекомендаций по формированию и функционированию ТПД (Рекомендации ТПД) в специализированных структурах ООН и профильных международных организациях. Рекомендации ТПД могут быть нацелены на обеспечение институциональных гарантий прав и законных интересов находящихся под юрисдикцией государств-членов ООН граждан и организаций при совершении ими юридически значимых информационных транзакций в электронном виде с использованием Интернет и других открытых ИКТ-систем массового использования.

2. Упомянутые выше институциональные гарантии предлагается обеспечить в результате деятельности специализированных операторов, которые могут:

2.1. Предоставлять пользователям набор доверенных инфраструктурных ИКТ-сервисов.

2.2. Функционировать в рамках установленных правовых режимов, которые могут включать ограничения, связанные с обработкой персональных данных и другие рамочные условия.

3. Предлагается выполнить описание различных возможных правовых режимов:

3.1. Основанных на международных соглашениях (конвенциях) и/или на международном регулировании прямого действия;

3.2. Основанных на коммерческих договорах и/или торговых обычаях.

3.3. Без специального международного регулирования.

Правовые режимы могут дополнительно поддерживаться со стороны традиционных институтов (государственных органов, судебного урегулирования споров, страхования рисков, нотариата и других) для взаимного признания электронных документов, формируемых с помощью доверенных инфраструктурных ИКТ-сервисов.

Установленные правовые режимы могут также налагать специальные требования по материальному и финансовому обеспечению деятельности специализированных операторов в случае нанесения ими ущерба пользователям, включая разглашение персональных данных.

Вопросы институциональных гарантий и правых режимов для формирования и функционирования региональных и глобальных доменов ТПД для целей предоставления прикладных сервисов (общих процессов) на инфраструктурной основе этих доменов ТПД, предлагается рассмотреть в рамках отдельной Конвенции ЮНСИТРАЛ.

4. Предлагается выполнить описание возможных наборов доверенных инфраструктурных ИКТ-сервисов в зависимости от критичности поддерживаемых ими прикладных сервисов (общих процессов). Доверенные инфраструктурные ИКТ-сервисы и их возможные уровни доверия могут определяться операторами прикладных информационных систем в зависимости от угроз, рисков, установленных правовых режимов и пользовательских требований (предпочтений). Для целей обеспечения требуемых уровней доверия операторы прикладных информационных систем могут действовать в рамках нейтральной международной среды, определяемой заданным международным сообществом правовым режимом. Предлагается выполнить описание организационных инфраструктур, необходимых для формирования и поддержки нейтральной международной среды.

Общие положения: а) по формированию и функционированию региональных и глобальных доменов ТПД, б) по прикладным сервисам (приложениям), предоставляемым в рамках этих доменов, а также в) по наборам доверенных инфраструктурных ИКТ-сервисов могут быть рассмотрены в Рекомендации СЕФАКТ по обеспечению юридически значимых доверенных трансграничных электронных транзакций.

Описание отдельных доверенных инфраструктурных ИКТ-сервисов может стать предметом рассмотрения в технических стандартах и рекомендациях ITU, JTC-1, ETSI и других органах международной и региональной стандартизации в области информационных технологий.

5. Наборы идентификационных признаков субъектов электронного взаимодействия могут определяться правовыми режимами деятельности специализированных ID-операторов и/или операторами прикладных информационных систем, и поддерживаться со стороны операторов доверенных инфраструктурных ИКТ-сервисов (подмножеством которых являются специализированные ID-операторы). Деятельность операторов (всех категорий) может регулироваться специальными организационными и техническими требованиями, направленными, кроме прочего, на защиту персональных данных, коммерческой, врачебной тайны и других видов информации ограниченного доступа.

Наборы идентификационных признаков пользователей и сами идентификационные процедуры могут служить основой для определения уровней доверия, устанавливаемых в форме идентификационных схем, которые в свою очередь, могут стать содержательной основой для регулирования взаимодействия между различными доменами ТПД.

6. Предлагается выполнить описание механизмов взаимодействия между отдельными государственными образованиями (странами), и возможно их международными объединениями (здесь упоминается только для полноты возможных вариантов), с другими международными форматами в рамках формирования общего ТПД.

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

6.1.1. Полноформатное присоединение государственного образования (страны) к существующему правовому режиму на основе международных соглашений и/или международного регулирования прямого действия, в рамках которого задача формирования регионального ТПД уже решена (или находится в процессе реализации) для целей обеспечения прикладных сервисов (общих процессов) на инфраструктурной основе этого ТПД.

6.1.2. Частичное присоединение государственного образования (страны) к существующему правовому режиму на основе международных соглашений и/или международного регулирования прямого действия в части, касающейся формирования и функционирования регионального домена ТПД для целей обеспечения прикладных сервисов (общих процессов) на инфраструктурной основе этого ТПД.

6.2. На основе взаимодействия между различными международными объединениями:

6.2.1. На первом этапе группы государственных образований (стран) создают обособленные региональные домены ТПД для целей обеспечения прикладных сервисов (общих процессов) на инфраструктурной основе этих ТПД.

6.2.2. На втором этапе вырабатываются протоколы доверенного взаимодействия между обособленными региональными доменами ТПД для целей взаимного признания (выравнивания) различных правовых режимов. Это взаимное признание должно увязывать институциональные гарантии и требования по информационной безопасности, которые установлены в каждом из международных форматов, возможно на основе нейтрального

междоменного шлюза (НМШ), который функционирует в рамках специального правового режима при совместном аудите со стороны взаимодействующих региональных доменов ТПД.

6.3. На основе взаимодействия между отдельными государственными образованиями (странами) со своими аналогами или международными объединениями:

6.3.1. На первом этапе отдельные государственные образования (страны) формируют обособленное национальное трансграничное пространство доверия (ПД-Н), функционирующее в рамках установленного национального правового режима.

6.3.2. На втором этапе вырабатываются протоколы доверенного взаимодействия между этим ПД-Н и обособленными одним или несколькими региональными доменами ТПД для целей взаимного признания (выравнивания) различных правовых режимов. Это взаимное признание должно увязывать институциональные гарантии и требования по информационной безопасности, которые установлены в ПД-Н и в одном или нескольких региональных доменах ТПД, возможно на основе НМШ, который функционирует в рамках специального правового режима при совместном аудите со стороны взаимодействующих ПД-Н и одного или нескольких региональных доменов ТПД.

7. Предлагается выполнить описание домен-образующих механизмов, аналогично приведенному в пункте 6, для правовых режимов, основанных на коммерческих соглашениях и/или торговых обычаев.

8. Предлагается выполнить описание механизмов формирования глобального ТПД, основанного на интеграции различных региональных доменов ТПД и отдельных ПД-Н в матрицу, образуемую по следующим признакам:

8.1. Прикладным сервисам (общим процессам) и географическим пределам.

8.2. Различным правовым режимам и их модификациям.

9. Предлагается привести описание подходов к формированию нейтральных междоменных[29] шлюзов, как ключевых элементов формирования матрицы глобального ТПД.

[29] Домены могут также быть представлены отдельными государствами; в этом случае нейтральный междоменный шлюз будет межгосударственным

Целью создания таких шлюзов является обеспечение взаимодействия между различными доменами глобального ТПД, причем формирование шлюзов может учитывать все необходимые аспекты: юридический, организационный и технологический.

Процедуры и процессы взаимодействия между различными доменами глобального ТПД должны поддерживать уровень доверия между этими доменами, необходимый для взаимного признания (легализации) электронных документов и данных, издаваемых в различных юрисдикциях (доменах).

Таким образом, нейтральные междоменные шлюзы позволят установить и поддерживать глобальные юридически значимые информационные процессы в рамках глобального ТПД.

Для достижения указанного уровня доверия междоменные шлюзы должны эксплуатироваться в нейтральной, т.е. внедоменной (наддоменной) международную среде.

Такая нейтральная международная среда должна находиться в нейтральном правовом поле, определяемом, например, Конвенцией ООН или международным соглашением отдельных стран или объединений стран.

Документы, определяющие необходимое, в том числе для эксплуатации шлюзов, нейтральное правовое поле, должны, среди прочего, определить роль нейтрального международного оператора нейтрального междоменного шлюза. Этот международный оператор должен действовать в рамках указанного правового поля, выполнять установленные этим правовым полем требования и подвергаться международному аудиту на предмет выполнения этих требований.

Представляется также необходимым, что документы, определяющие указанное нейтральное правовое поле, должны также определить роль нейтрального международного регулятора, осуществлящего, среди прочего, координацию взаимодействия нейтральных международных операторов.

Таким образом, нейтральные междоменные шлюзы позволят установить и поддерживать глобальные юридически значимые информационные процессы в рамках глобального ТПД, осуществляемые через совокупность нейтральных междоменных шлюзов, т.е. через нейтральную междоменную шину. Эксплуатация этой нейтральной междоменной шины будет осуществляться одним или многими нейтральными международными операторами и регулироваться нейтральным международным регулятора, действующимии на основе соответствующих международных документов.

Подходы к формированию нейтральных междоменных шлюзов могут учитывать существование различных возможных уровней взаимодействия между отдельными доменами ТПД. В частности, может быть открыта возможность формирования шлюзов как на исключительно юридически-

организационном уровне, так и на комплексном, юридически-организационно-технологическом уровне.

Подходы к формированию нейтральных междоменных шлюзов могут учитывать использование профилей перехода от одного домена ТПД к другому. Эти профили перехода могут учитывать уровни доверия схем идентификации, используемых во взаимодействующих доменах, см. пункт 5.

Описание нейтральных междоменных шлюзов может стать предметом технических стандартов или рекомендаций ITU и JTC-1.

10. Потребности развития глобальной экономики, особенно в кризисные периоды, настоятельно требуют активизации интеграционных процессов в различных экономических и социальных сферах при поддержке со стороны современных ИКТ-технологий, основанных на инновациях. На преодоление подобных вызовов нацелена предлагаемая разработка семейства Рекомендаций ТПД.

Изложенная выше логика уже нашла отражение в проекте рекомендации Центра ООН по упрощению торговых процедур (СЕФАКТ) «Об обеспечении юридически значимого трансграничного электронного взаимодействия»[30];

11 Исследование и анализ функциональных требований к доверенной третьей стороне Российской Федерации

Одним из основных механизмов, обеспечивающих функционирование ТПД является Доверенная третья сторона (ДТС) Российской Федерации.

Работы по созданию ДТС РФ в рамках реализации мероприятий государственной программы Российской Федерации «Информационное общество (2011 - 2020 годы)» выполняются в два этапа:

На первом этапе (2014-2016 годы) создается прототип программно-аппаратного комплекса (ПАК) ДТС в соответствии с пунктом 1.7 Плана мероприятий по созданию и развитию национального сегмента Российской Федерации интегрированной системы государств - участников Таможенного союза, утвержденного Первым заместителем Председателя Правительства Российской Федерации И.И. Шуваловым 30 июля 2014г. № ИШ-П10-5760 (далее – План мероприятий). Документационное обеспечение для функционирования прототипа ПАК ДТС должно осуществляться в соответствии с отдельным Планом Правительства Российской Федерации.

---

30 http://www1.unece.org/cefact/platform/download/attachments/55378391/Rec+draft+v.0.91+08.09.15.pdf

В результате реализации первого, пилотного этапа должны быть отработаны технико-технологические решения прототипа ПАК ДТС, функционирующего на основе временных регламентов и положений, утверждаемых приказами Минкомсвязи России. Выявленные недостатки и предложения по совершенствованию прототипа ПАК ДТС должны быть учтены при развертывании полнофункционального ДТС Российской Федерации.

На втором этапе (2015 – сентябрь 2017 года) создается ДТС Российской Федерации в соответствии с пунктами 1.8 и 1.10 Плана мероприятий, а также пунктом V.3 Рабочего плана разработки актов и международных договоров в соответствии с Договором о Евразийском экономическом союзе от 29 мая 2014 года. Нормативно-правовое обеспечение для функционирования ДТС Российской Федерации должно осуществляться в соответствии с отдельным Планом Правительства Российской Федерации. Этот этап реализуется по отдельным планам Минкомсвязи России, согласованным с Комиссией Евразийского экономического союза.

В результате реализации второго этапа ДТС Российской Федерации должен быть готов к предоставлению институционально гарантированных электронных сервисов гражданам и организациям Российской Федерации на основе правового режима, определяемого актами Евразийского экономического союза и законодательства Российской Федерации[31].

Основным функциональным требованием к созданию и функционированию ДТС РФ является обеспечение гарантий реализации законных интересов и прав граждан и организаций Российской Федерации при их юридически значимом трансграничном информационном взаимодействии на основе электронных документов с гражданами и организациями, находящимися в юрисдикции других государств-участников Евразийского экономического союза (далее – ЕАЭС) и должностными лицами Комиссии ЕАЭС (далее – Комиссия), на основании соответствующего Договора, а также если это предусмотрено другими международными соглашениями с участием Российской Федерации.

Достижение гарантий при реализации основного функционального требования в рамках сквозного бизнес-процесса, затрагивающего различные юрисдикции, предполагает равную прочность и взаимную зависимость общего результата от всех составляющих компонент, как в рамках институционально-правовой деятельности уполномоченных лиц и организаций, так и в рамках технического обеспечения их деятельности.

Основное функциональное требование должно обеспечиваться через реализацию на практике следующих положений, которые в своей совокупности являются необходимыми и достаточными условиями обеспечения таких гарантий:

---

[31] Предоставление институционально гарантированных сервисов ДТС Российской Федерации и их развитие осуществляются, начиная с января 2018 года, в рамках последующих этапов работ.

- институциональная деятельность уполномоченных Правительством Российской Федерации лиц и организаций[32], поддерживаемая работами уполномоченного оператора ДТС РФ, которые проводятся на основе регламентированного разграничения ответственности и полномочий по реализации основного функционального требования и на принципах согласованной тарифной и обеспечительной политики;

- выполнение Требований к созданию, развитию и функционированию трансграничного пространства доверия, утверждаемых в соответствии с пунктом 18 Приложения 3 к Договору о создании ЕАЭС (далее – Требования к ТПД)[33];

- выполнение положений Концепции использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов, Стратегии развития трансграничного пространства доверия и Планов мероприятий, направленных на реализацию указанных Концепции и Стратегии;

- функционирование ДТС РФ в качестве отдельной подсистемы электронного правительства России, как его международный интерфейс, который организационно интегрируется и технологически взаимодействует с другими инфраструктурными компонентами;

- взаимодействие ДТС РФ с ДТС других государств-участников и ДТС Комиссии ЕАЭС на принципе равнопрочности принимаемых решений в области информационной безопасности;

- обязательная инфраструктурная поддержка со стороны ДТС РФ функциональных информационных систем российских органов государственного и муниципального управления при их взаимодействии с участниками юридически значимого трансграничного электронного документооборота в государствах-участниках ЕАЭС и в Комиссии;

- рекомендованная инфраструктурная поддержка со стороны ДТС РФ российских физических и юридических лиц, при их взаимодействии с участниками юридически значимого трансграничного электронного документооборота в государствах-участниках ЕАЭС и в Комиссии[34];

---

[32] Решением Совета ЕЭК от 18 сентября 2014 г. № 73 утверждена Концепция использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов, в рамках которой предполагается разработка модельного кодекса института международного электронного нотариата на основе сервисов и служб доверенной третьей стороны.

Постановлением Правительства Российской Федерации от 24 июля 2014 г. № 698 Минкомсвязи России поручено выполнение функций доверенной третьей стороны при обмене электронными документами в случаях, если ее участие в таком обмене предусмотрено международными договорами Российской Федерации.

До принятия, указанного выше Модельного кодекса, для целей настоящих ФТ ДТС РФ используются понятия - уполномоченный орган в области ДТС РФ, уполномоченные лица уполномоченного органа в области ДТС РФ.

[33] До принятия указанных требований в рамках работ по тестированию прототипа ДТС в Российской Федерации используются временные требования технико-технологического и организационно-регламентного характера. Нормативно-правовое закрепление на территории Российской Федерации они получают после утверждения международно признанных Требований к ПД-Т.

[34] Указанные функции могут выполнять другие ДТС, если они выполняют Требования к ПД-Т и если это предусмотрено законодательством Российской Федерации.

- обеспечение международного признания деятельности уполномоченных лиц и органов ДТС РФ по заверению, хранению и выдаче по запросу электронных документов, эмитированных в рамках ЕАЭС, а также на основе других международных соглашений Российской Федерации, со стороны международных судебных органов и страховых компаний;

- использование удостоверяющего центра Комиссии для обеспечения сертификатами ключей подписи для взаимодействия уполномоченных ДТС интеграционного и национальных сегментов интегрированной системы в соответствии с Концепцией использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов[35].

Наряду с выполнением указанных выше положений, основное функциональное требование структурируется в пакете частных требований технико-технологического, организационно-регламентного и нормативно-правового характера на клиентском, национальном и наднациональном уровнях в рамках сквозного бизнес-процесса, затрагивающего различные юрисдикции.

На клиентском уровне:

- варианты требований и рекомендаций к различным типам автоматизированных рабочих мест пользователей, возможно на различных операционных системах (Windows, Linux, iOS, Android, другие), а также для персонального использования или интегрированных в функциональные государственные информационные системы;

- варианты требований и рекомендаций по подключению клиентов к серверной части ДТС, на основе использования сети Интернет, выделенных каналов связи и/или общей шины;

- требования и рекомендации к средствам доступа и идентификации, включая отдельные компоненты инфраструктуры эмиссии, в том числе производство, персонализацию, эмиссию, дистрибуцию, утилизацию;

- порядок получения сертификатов ключей подписи для участия в трансграничном информационном взаимодействии;

- требования и рекомендации к средствам чтения средств доступа и идентификации;

- требования и рекомендации к разработке клиентского интерфейса с учетом достижения качества интуитивной понятности для массового пользователя и возможной интеграции с массовыми офисными продуктами;

В случае, если ДТС предоставляет сервисы поддержки трансграничного электронного документооборота со странами, с которыми у Российской Федерации отсутствуют соответствующие международные соглашения, реализация основного функционального требования не гарантируется, даже если это предусмотрено торговыми обычаями.

[35] Данный аспект реализации основного функционального требования актуален в рамках ЕАЭС. Не исключается принятие других архитектурных решений на наднациональном уровне в рамках других международных соглашений, в том числе на основе взаимного признания электронных подписей уполномоченных лиц ДТС, основанных на различных национальных стандартов криптографических алгоритмов.

- Правила документирования информации на клиентском уровне и доступа к серверной части ДТС (инструкция пользователям);

- Порядок представления электронных документов, эмитированных пользователем и заверенных ДТС в рамках трансграничного электронного документооборота, в государственные органы, судебные инстанции и страховые компании;

- Рекомендации пользователям по получению справочной информации в отношении процедур и правил трансграничного электронного документооборота и ведению личного кабинета с обеспечением защиты персональных данных;

- другие требования и рекомендации.

На национальном уровне:

- технико-технологические требования к программно-аппаратному комплексу ДТС РФ (временные требования к прототипу ДТС до утверждения Требований к ТПД);

- унифицированный административный регламент деятельности уполномоченных органов и лиц в области ДТС РФ (временный регламент деятельности уполномоченных органов и лиц до утверждения Требований к ТПД);

- порядок назначения и регламент работ оператора ДТС в Российской Федерации;

- договор между уполномоченным органом и оператором ДТС РФ с детальным разграничением ответственности и полномочий;

- рекомендации по гармонизации деятельности национальных органов по аккредитации, сертификации и лицензированию деятельности, связанной с функционированием ДТС, в случае если это предусмотрено утвержденными Требованиями к ТПД;

- требования к системе идентификации и аутентификации участников информационного взаимодействия в рамках трансграничного пространства доверия (временный порядок взаимодействия с ЕСИА до утверждения Требований к ТПД);

- порядок взаимодействия ДТС РФ с компонентами единого пространства доверия Российской Федерации и СМЭВ;

- порядок взаимодействия ДТС РФ с ЕАГД Российской Федерации и системой НСИ ЕАЭС в части мониторинга статуса участников информационного взаимодействия в рамках ТПД;

- порядок обеспечения участников информационного взаимодействия в рамках ТПД источником доверенного времени (временный порядок получения меток времени от ИС ГУЦ до утверждения Требований к ТПД);

- другие требования, рекомендации и нормативные правовые акты Российской Федерации.

На наднациональном уровне:

- Договор о создании ЕАЭС, другие международные соглашения с участием Российской Федерации;

- Модельный кодекс института международного электронного нотариата на основе сервисов и служб доверенной третьей стороны[36];
- Требования к ТПД;
- Положение о комиссии по проверке компонентов общей инфраструктуры документирования информации в электронном виде на соответствие Требованиям к ТПД;
- требования к созданию и функционированию удостоверяющего центра Комиссии ЕАЭС для обеспечения сертификатами ключей подписи для взаимодействия уполномоченных ДТС интеграционного и национальных сегментов интегрированной системы[37];
- Положение о системе НСИ Комиссии ЕАЭС в части обеспечения нормативно-справочной информацией задач, решаемых ТПД;
- решения Комиссии ЕАЭС, принимаемые установленным порядком.

12 Исследование и анализ механизма единого окна в рамках Евразийского экономического союза с учетом международного опыта

Тема использования механизма единого окна обусловлена факторами глобализации мировой экономики и бурным развитием информационно-коммуникационных технологий (далее – ИКТ). Единое окно – это термин, обозначающий механизм предоставления услуг для граждан и бизнеса. Использование механизма единого окна имеет целью снизить время вынужденного общения граждан и (или) бизнеса с государством, и характеризуется тем, что оказание государственных и муниципальных услуг концентрируется в одном месте, начиная от подачи заявления, до выдачи результатов решения исполнительного или иного органа.

Важной составляющей механизма единого окна является минимизация количества документов, которые заявитель должен предоставлять в орган власти для принятия решения. Это достигается построением развитой инфраструктуры эффективного межведомственного взаимодействия, причём как на одном уровне власти (по горизонтали), так и межуровневого взаимодействия (по вертикали). Как правило, при предоставлении государственной услуги необходима информация из разных органов, включая разные уровни власти.

При использовании механизма единого окна, от заявителя скрывается процесс межведомственного информационного обмена, заявитель перестаёт

---

[36] Для решения задач масштабирования ПД-Т на постсоветском, европейском и азиатско-тихоокеанском направлениях в соответствии с положениями Стратегии ПД-Т возможно потребуется принятие соответствующей международной конвенции по аналогии с Конвенцией 1961 года об апостилях.

[37] С оговоркой о возможности использования схемы на основе взаимного признания электронных подписей уполномоченных лиц ДТС, основанных на различных национальных стандартах криптографических алгоритмов.

быть курьером для доставки информации о себе из одного ведомства в другое. Заявитель сдаёт один раз минимально необходимый набор документов в одном месте, одной формы, в одну службу, одному специалисту, далее служба самостоятельно осуществляет все процедуры согласований и оформления.

Механизм единого окна получает широкое распространение благодаря применению современных ИКТ в практике государственного управления, так как содержать большое количество курьеров невыгодно как государству, так и гражданам.

ИКТ позволяют организовать относительно недорогой информационный межведомственный обмен в рамках оказания государственных услуг и удешевить использование механизма единого окна. При этом появляется возможность разделять территориально офисы по взаимодействию с заявителями (фронт-офисы) и офисы, где происходит обработка информации и принятие решений органами власти (бэк-офисы).

Немаловажным является также повышение оперативности процедур информационного обмена и, следовательно, оперативности предоставления коммерческих или государственных услуг.

Так как широкое применение механизма единого окна возможно благодаря применению современных ИКТ, этот механизм является важной частью электронного правительства.

Помимо физических точек доступа к различным службам механизма единого окна, посредством применения современных ИКТ, можно реализовать возможность обращения, не выходя из дома через Интернет-порталы, терминалы с сенсорными дисплеями, call-центры, интерактивные справочные службы, точки беспроводного доступа и др. При этом необходимо обеспечивать доступность и простоту транзакций для пользователей (заявителей).

Документы и опыт ООН по формированию механизма единого окна. Механизм единого окна начал рассматриваться структурами ООН в контексте решения задачи по упрощению процедур торговли.

Практическое руководство по упрощению процедур торговли для национальных экономик было разработано Европейской экономической комиссией Организации Объединенных Наций (ЕЭК ООН), при участии Центра Организации Объединенных Наций по упрощению процедур торговли и электронным деловым операциям (СЕФАКТ ООН) и при финансовой поддержке Шведского агентства международного сотрудничества в области развития (СИДА)[38].

Наиболее распространенное определение единого окна приводится в Рекомендации ЕЭК ООН № 33. Согласно данному определению, единое окно

[38] Официальный сайт Европейской экономической комиссии ООН. Адрес в сети: URL: http://tfig.unece.org/RUS/about.html (Дата обращения 02.04.2016).

— это система, позволяющая представителям сферы торговли и транспорта предоставлять стандартизированную информацию и документы в единый пункт приема с целью соблюдения нормативных требований, касающихся импорта, экспорта и транзита грузов. Если информация предоставляется в электронной форме, то индивидуальные элементы данных следует предоставлять лишь один раз[39].

Абстрагировавшись от роли механизма единого окна, как платформы, среды или инструмента, его можно охарактеризовать с точки зрения услуг, которые оказываются участникам торговой деятельности и государственным органам. Услуги, предоставляемые посредством механизма единого окна, выражаются в упрощении обмена торговой информацией между участниками торговой деятельности и государственными структурами с целью получения соответствующих разрешений, лицензий, сертификатов и согласований. В рамках механизма единого окна участники торговой деятельности или их агенты могут подавать документы и сведения в электронной или бумажной форме, используя единую точку приема данных.

Рекомендация № 33 и дополняющие ее руководящие принципы стали одним из первых документов, описывающих создание механизма единого окна. Рекомендация была разработана на основе анализа и обобщения опыта существующих механизмов единого окна в различных странах, в том числе в США, на Маврикии и в Швеции. В данном документе впервые представлены и обсуждаются различные технологические и организационные модели механизма единого окна, перечисляются преимущества данного механизма, как для участников торговой деятельности, так и для органов государственного управления, перечислены возможные услуги с использованием механизма единого окна. Практические меры, а также стандарты и инструменты, направленные на внедрение механизма единого окна, представляют собой непосредственный интерес для Евразийского экономического союза (ЕАЭС)[40].

В 2006 году Европейская экономическая комиссия ООН инициировала создание репозитория (фонда лучших практик), который включает в себя практические примеры существующих механизмов единых окон. Данный репозиторий дает дополнительную информацию об опыте создания

---

[39] Рекомендация и руководящие принципы по созданию механизма «единого окна» для улучшения эффективного обмена информацией между торговыми организациями и государственными органами. Рекомендация № 33. ООН. Европейская экономическая комиссия. Центр по упрощению процедур торговли и электронным деловым операциям (СЕФАКТ ООН). Нью-Йорк, Женева, 2005. Адрес в сети: URL: http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352r.pdf (Дата обращения 02.04.2016).

[40] Адрес в сети: URL: http://tfig.unece.org/RUS/contents/recommendation-33.htm (Дата обращения 02.04.2016).

механизма единого окна различными странами. Репозиторий лучших практик размещен на официальном сайте ЕЭК ООН[41].

Механизм единого окна в сфере торговли может стать важным инструментом упрощения торговых процедур. При условии эффективного применения данного механизма с его помощью можно существенно упростить процедуры и формальности, связанные с подачей документов и сбором данных. Основные выгоды, которые сулит участникам проект по формированию механизма единого окна, заключаются в следующем:

государство: рост государственных доходов, соблюдение установленных правил, более эффективное и рациональное распределение ресурсов, улучшение торговой статистики;

субъекты торговли: ускоренная таможенная очистка, более прозрачный, предсказуемый и дебюрократизированный процесс таможенного оформления;

таможенная служба: более эффективная работа персонала благодаря усовершенствованной инфраструктуре, рост таможенных доходов, более структурированная и контролируемая рабочая среда и более профессиональное отношение сотрудников к своим обязанностям;

экономика в целом: более прозрачная и эффективная деятельность органов власти, а также снижение уровня коррупции в связи с ограниченными возможностями для физического контакта уполномоченных лиц и агентов торговли.

По подсчетам таможенной службы Республики Корея, в 2010 году благодаря внедрению механизма единого окна она дополнительно принесла в бюджет порядка 18 млн. долларов США, при этом общий положительный эффект от мер по упрощению процедур торговли был оценен почти в 3,47 млрд. долларов США. Национальный механизм единого окна Сингапура под названием «TradeNet» с 1989 года объединяет более 35 пограничных агентств, существенно повышая эффективность деятельности государственных органов. По утверждениям таможенной службы Сингапура, на каждый принесенный в бюджет доллар таможня тратит лишь один цент, обеспечивая доходность в 99%[42].

Важную роль в формировании механизма единого окна играет Рекомендация № 34 ЕЭК ООН «Упрощение и стандартизация данных для международной торговли»[43]. Данная рекомендация содержит руководящие

---

[41] Адрес в сети: URL: http://www.unece.org/cefact/single_window/welcome.html (Дата обращения 02.04.2016).

[42] Всемирный банк, «Трансграничная торговля», доклад «Ведение бизнеса» (Всемирный банк, 2012 г.). С документом можно ознакомиться по адресу в сети: URL: http://www.doingbusiness.org/reports/global-reports/~/media/FPDKM/Doing%20Business/Documents/Annual-Reports/English/DB12-Chapters/Trading-Across-Borders.pdf. (Дата обращения 02.04.2016).

[43] Упрощение и стандартизация данных для международной торговли. Рекомендация № 34. ООН. Европейская экономическая комиссия. Первое издание. Принята Центром по упрощению процедур торговли и электронному бизнесу

принципы, описывающие, каким образом информационные требования правительства могут быть стандартизированы и согласованы.

Рекомендация № 34 предлагает процесс, направленный на упрощение и стандартизацию наборов данных, что позволит облегчить процесс обмена информацией между участниками торговой деятельности и правительством. Согласно данной рекомендации, процесс упрощения и стандартизации должен включать в себя четыре этапа:

сбор данных – подготовка национального перечня торговых данных на основе текущих потребностей правительственных ведомств в данных и информации с использованием автоматизированных систем и документов с целью охвата всех требований, касающихся процедур международной торговли, связанных с импортом, экспортом и транзитом;

определение данных – подготовка набора данных с указанием названия, определения и формата представления (текстовой формат или код) каждого элемента данных;

анализ – осуществление анализа потребности в информации и в элементах данных для установления их фундаментальной важности и возможности демонстрации их использования;

согласование – подготовка консолидированного перечня определенных и проанализированных торговых данных через процесс согласования.

Соблюдение последовательных этапов позволяет правительствам стран снизить потребности в официальной и нормативной информации путем устранения избыточности и дублирования элементов данных. В рамках практической реализации такого процесса может быть эффективно использован инструмент концентраторов (хабов) сервисов электронной коммерции, описываемый ниже.

Еще одним основанием для реализации на практике механизма единого окна является Рекомендация ЕЭК ООН № 35 “Выработка правовой основы механизма единого окна в международной торговле”[44]. Целью данной Рекомендации является определение руководящих принципов и предоставление контрольного перечня общих правовых вопросов, которые возникают в ходе внедрения механизма единого окна.

Данная Рекомендация была разработана в качестве дополнения к Рекомендации ЕЭК ООН № 33 по созданию механизма единого окна в международной торговле. Рекомендация № 35 основана на опыте внедрения механизма единого окна в разных странах, она также рассматривает

Организации Объединенных Наций (СЕФАКТ ООН). Женева, февраль 2011. Адрес в сети: URL: http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec34/ECE_TRADE_400_DataSimplificationand_Rec34R.pdf. (Дата обращения 02.04.2016).

[44] Адрес в сети: URL: http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec35/Rec35_ECE_TRADE_401_EstablishingLegalFrameworkforSingleWindow_R.pdf (Дата обращения 02.04.2016).

соответствующие аспекты правовой основы для национальных и региональных механизмов единого окна.

Данный документ рекомендует провести анализ текущей правовой основы, определить пробелы и выработать меры по устранению данных пробелов. В приложении I и II Рекомендации № 35 содержится контрольный перечень, а также руководящие принципы по данному контрольному перечню, которые служат справочными материалами для проведения анализа пробелов. Рекомендация побуждает административные органы учитывать международные стандарты, международные правовые акты, включая необязательные нормативные акты, при внесении изменений в собственную правовую основу. В приложении III к данной рекомендации приводится перечень полезных ссылок.

Правовая основа механизма единого окна определяется как комплекс мер, которые могут потребоваться для решения юридических вопросов, связанных с национальным и международным обменом торговыми данными. Она включает в себя следующие аспекты: защита данных, полномочия на доступ и обмен данными между государственными учреждениями, идентификация, аутентификация и авторизация, вопросы качества данных, вопрос ответственности, электронные документы, электронное архивирование, право интеллектуальной собственности и право собственности на базу данных. Правовая основа также включает в себя нормативные положения, касающиеся организационных договоренностей между сторонами, владельцами и пользователями механизма единого окна, положения, касающиеся разрешения споров и арбитража, а также вопросов конкуренции.

В Рекомендации ЕЭК ООН № 35 подчеркивается важность использования электронной подписи, как наиболее распространенного способа обеспечения безопасности электронных платежей на основе использования криптографических технологий, таких как шифрование и электронные подписи. Электронная подпись – это набор данных, прикрепленный к электронному сообщению, позволяющий гарантировать его аутентичность, идентифицировать подписавшее его лицо и привязать содержание документа к подписавшему его лицу (защищая, таким образом, получателя от риска того, что отправитель будет отрицать свою причастность к данному сообщению). Электронная подпись является эффективным средством гарантии аутентичности и целостности любого документа в течение его срока действия.

Электронная подпись имеет влияние в течение всех этапов жизненного цикла электронных документов в торговле, включая:

создание: чтобы обеспечить аутентичность и целостность документа, электронная подпись должна применяться при создании счета-фактуры и других видов электронных документов в торговле;

обмен: для получателя, чтобы проверить подлинность электронной подписи, информация, позволяющая проверить подпись, должна быть

отправлена вместе со счетом-фактурой и другими видам электронных документов в торговле,

акцептование: чтобы проверить аутентичность и целостность полученного счета-фактуры и других видов электронных документов в торговле, получатель может (в зависимости от национального законодательства) проверять подлинность электронной подписи с использованием имеющейся информации;

хранение: счета-фактуры и другие виды электронных документов в торговле должны храниться в течение срока, определенного местными налоговыми органами, при этом аутентичность происхождения и целостность данных должны быть обеспечены для всех хранимых счетов-фактур и других видов электронных документов в торговле.

Комиссия ООН по международной торговле (ЮНСИТРАЛ) разработала Типовой закон об электронной торговле и Типовой закон об электронных подписях, чтобы предоставить национальным законодателям набор международно признанных правил, нацеленных на устранение юридических препятствий и повышение юридической предсказуемости в электронной торговле, а также на упрощение использования электронной подписи[45].

Внедрение решений в области электронных подписей приносит значительные выгоды:

предоставляет глобальное решение по выставлению электронных счетов-фактур и других видов электронных документов в торговле с соблюдением местного законодательства;

поддерживает процессы, связанные с дебиторской и кредиторской задолженностью;

устраняет капитальные затраты компании на создание соответствующего архива электронных счетов-фактур и других видов электронных документов в торговле;

максимально повышает безопасность путем использования защищенных электронных документов и высокозащищённых соединений;

снижает ИКТ затраты и упрощает ИКТ инфраструктуру;

устраняет транзакционные барьеры и проблемы, связанные с выставлением счетов-фактур и других видов электронных документов в торговле.

Однако, применение электронной подписи в сфере торговли сопряжено с определенными трудностями. Помимо сложности и высокой стоимости внедрения электронной подписи, это:

отсутствие взаимного признания со стороны национальных сертифицирующих органов;

---

[45] Адрес в сети: URL: http://tfig.unece.org/RUS/contents/e-signature.htm (Дата обращения 02.04.2016).

отсутствие прозрачности относительно оснований для приемлемости электронной подписи для трансграничной торговли, что приводит к тому, что в некоторых странах корпорации вводят так называемые двойные подписи – одна для страны отправителя и одна для собственной страны покупателя;

некоторые европейские страны (например, Германия, Италия, Польша, Португалия, Испания и Венгрия) требуют квалифицированные подписи на основе сертификатов, выданных реальным лицам.

Следует отметить, что принцип использования трансграничного пространства доверия, предложенный в Договоре о Евразийском экономическом союзе, нацелен на устранение описанных проблем.

Задачи и планы ЕАЭС по созданию механизма единого окна. С учетом накопленного международного опыта и профильных Рекомендаций ЕЭК ООН в части механизма единого окна решением Высшего Евразийского экономического совета от 29 мая 2014 г. № 68 одобрены «Основные направления развития механизма единого окна в системе регулирования внешнеэкономической деятельности», которые учитывают специфику данного интеграционного объединения и конкретизируют постановку задач[46].

Под единым окном в этих Основных направлениях понимается механизм взаимодействия между государственными органами, регулирующими внешнеэкономическую деятельность, и участниками внешнеэкономической деятельности, который позволяет участникам однократно представлять документы в стандартизованном виде через единый пропускной канал для последующего использования заинтересованными государственными органами и иными организациями в соответствии с их компетенцией при проведении контроля за осуществлением внешнеэкономической деятельности.

Применение механизма единого окна в рамках ЕАЭС позволит:

для государственных органов государств-членов, регулирующих внешнеэкономическую деятельность:

повысить качество и сократить сроки предоставления государственных услуг и осуществления государственных функций;

повысить уровень управления рисками и минимизировать случаи несоблюдения участниками внешнеэкономической деятельности требований, установленных законодательством государств-членов;

сократить расходы бюджетов государств-членов на предоставление государственных услуг и осуществление государственных функций;

упростить административные процедуры и повысить их эффективность;

для участников внешнеэкономической деятельности:

---

[46] Адрес в сети: URL: http://www.eurasiancommission.org/ru/act/tam_sotr/Pages/mdsw.aspx (Дата обращения 02.04.2016).

сократить стоимостные и временные издержки, связанные с обработкой информации и документов, необходимых для осуществления внешнеэкономической деятельности;

упростить технологию информационного взаимодействия с государственными органами, регулирующими внешнеэкономическую деятельность;

оптимизировать ресурсы, в том числе трудовые, при осуществлении внешнеэкономической деятельности;

повысить транспарентность и предсказуемость бизнес-процессов, связанных с внешнеэкономической деятельностью.

В Решении № 68 от 29 мая 2014 года намечены основные направления развития механизма единого окна в системе регулирования внешнеэкономической деятельности, такие как:

сближение подходов по развитию национальных механизмов единого окна;

развитие национальных механизмов единого окна;

взаимное признание электронных документов, необходимых для осуществления внешнеэкономической деятельности;

организация информационного взаимодействия.

В данном решении механизм единого окна рассматривается в триединстве правовых, организационных и технологических аспектов. Очевидно, что инструмент правовой аналитики может эффективно использоваться для изучения существующей практики в государствах-членах ЕАЭС, оптимизации организационных и технологических решений с последующим закреплением результатов проведенного реинжиниринга в национальных законодательствах и нормативных актах ЕАЭС.

Реализация Основных направлений развития механизма единого окна в системе регулирования внешнеэкономической деятельности предусмотрена в Решении Высшего Евразийского экономического совета от 8 мая 2015 г. № 19, которым утвержден План мероприятий на 6-летний период, с 2015 по 2020 год включительно[47]. Основное содержание Плана мероприятий сводится к следующему.

1. Правовые предпосылки и основания.

Настоящий план разработан во исполнение Решения Высшего Евразийского экономического совета от 29 мая 2014 г. № 68 «Об Основных направлениях развития механизма единого окна в системе регулирования внешнеэкономической деятельности» и основывается на положениях Договора о Евразийском экономическом союзе от 29 мая 2014 года (далее – Договор о Союзе), международных договоров и актов в области внешнеэкономической деятельности, составляющих право Евразийского экономического союза (далее - Союз), а также нормах, правилах и принципах

[47] Адрес в сети: URL: http://www.eurasiancommission.org/ru/act/tam_sotr/Pages/sw.aspx (Дата обращения 02.04.2016).

Всемирной торговой организации, международных рекомендациях Организации Объединенных Наций и Всемирной таможенной организации.

2. Регуляторные задачи.

Вводится определение «государственных процедур», как деятельности государственных органов государств-членов в соответствии с их компетенцией, связанной с регулированием правоотношений в сфере внешнеэкономической деятельности, при осуществлении государственных функций (административных процедур) и предоставлении государственных услуг заинтересованным лицам.

3. Целеполагание.

Целью реализации настоящего плана является формирование организационно-правовых и технических основ для создания условий развития и сближения национальных механизмов единого окна, а также организации их взаимодействия на наднациональном уровне при построении эффективной системы регулирования внешнеэкономической деятельности на территории Союза.

4. Формирование эталонной модели единого окна.

Эталонная модель учитывает положения международных стандартов Всемирной таможенной организации и рекомендаций Организации Объединенных Наций, интегрирует опыт построения современных моделей механизма единого окна, используя прогрессивные организационно-правовые, технические и технологические решения.

5. Организационный механизм.

5.1. На подготовительном этапе определяется организационный механизм выполнения настоящего плана, проводится анализ текущего состояния проектов, направленных на создание национальных механизмов единого окна, определяются необходимые организационно-правовые, технологические и технические требования по созданию и (или) развитию национальных механизмов единого окна, а также оцениваются перспективы их сближения.

5.2. На этапе разработки на основе заключений, сформированных на подготовительном этапе, готовятся предложения по оптимизации государственных процедур, связанных с внешнеэкономической деятельностью, и бизнес-процессов, унификации состава сведений, включаемых в электронные документы, необходимые для осуществления внешнеэкономической деятельности, а также разрабатываются и принимаются решения и рекомендации по сближению или развитию национальных механизмов единого окна, совершенствованию положений актов, входящих в право Союза, регулирующих внешнеэкономическую деятельность, и законодательства государств-членов, в том числе утверждается детальное описание функций и архитектуры эталонной модели, перечень государственных процедур и услуг, охватываемых эталонной моделью.

5.3. На этапе реализации принимаются решения по внедрению или развитию национальных механизмов единого окна, обеспечению надлежащего информационного взаимодействия посредством интегрированной системы, а также реализуется комплекс организационно-технологических, правовых и технических мероприятий, обеспечивающих осуществление взаимного признания, унификации, стандартизации и гармонизации электронных документов, необходимых для осуществления внешнеэкономической деятельности, и их использование государственными органами и (или) уполномоченными организациями государств-членов.

Предложения по формированию Евразийского альянса по электронной коммерции. Для перевода проекта формирования механизма единого окна в практическую плоскость важно рассмотреть его в увязке с другими проектами информационного обеспечения, которые реализуются в настоящее время в ЕАЭС и соотнести их с уже реализованными в мире.

В настоящее время в рамках ЕАЭС решается несколько взаимоувязанных задач:

1. Обеспечение прослеживаемости движения товаров до конечного потребителя.

2. Формирование цифровой экономики.

3. Развитие интегрированной информационной системы Союза на платформе ИИСВВТ[48].

4. Создание, функционирование и развитие трансграничного пространства доверия.

5. Формирование механизма единого окна, а также ряд других проектов информационной поддержки интеграционных процессов в рамках ЕАЭС и для взаимодействия с основными экономическими регионами мира.

На реализацию совокупности информационных проектов оказывают существенное влияние следующие факторы:

изначально отсутствовала задача прослеживания товаров до конечного потребителя, чем наносится экономический ущерб, прежде всего России, которая вынужденно находится в режиме взаимных санкций;

ограниченное бюджетное финансирование в связи с кризисом;

недостаточная активность бизнеса;

необходимость противодействия политике отдельных стран по использованию безальтернативных решений в рамках цифровой экономики в различных регионах мира.

Для повышения эффективности работ целесообразно использовать международный опыт, лучшие мировые практики и аналоги.

Наиболее активно данная тематика разрабатывается в Азиатско-тихоокеанском регионе во множестве форматов двустороннего и

[48] Интегрированная информационная система взаимной и внешней торговли Таможенного союза.

многостороннего сотрудничества. Ярким примером является Пан-Азиатский альянс по электронной коммерции (ПАА)[49].

Альянс основан в июле 2000 года компаниями Crimson Logic (Сингапур), TRADE-VAN Information Services Co. (Китайский Тайбэй), and Tradelink Electronic Commerce Limited (Гонконг).

ПАА — это первый региональный альянс по электронной коммерции, цели которого — продвижение и обеспечение безопасных, надежных и защищенных ИТ-инфраструктур и сервисов для безбумажной торговли по всему миру, таких как:

безопасная и надежная передача торговых и логистических документов с помощью взаимного признания сертификатов электронной подписи, выпущенных УЦ, входящими в Альянс;

обеспечение взаимодействия сетевых решений для предоставления бизнес-сообществу доступа к различным приложениям для электронной торговли;

создание Пан-Азиатского веб-портала для обеспечения глобального B2B- взаимодействия и общения.

В настоящее время в ПАА входят организации из 11стран Азиатского региона: China International Electronic Commerce Centre, CIECC (Китай), Trade-Van (Китайский Тайбэй), Trade Link (Гонконг), NACCS (Япония), KTNET (Южная Корея), TEDMEV (Макао), Dagang Net (Малайзия), Crimson Logic (Сингапур), CAT Telecom (Таиланд), Inter Commerce (Филиппины), EDI-I (Индонезия).

Вышеперечисленные организации являются крупнейшими провайдерами услуг в области электронной торговли в своих экономиках в сегментах B2B, B2G и G2G.

ПАА предоставляет набор сервисных предложений, которые строятся вокруг международных технических стандартов, технологий информационной безопасности на соответствующей правовой основе. При этом на практике реализуется безопасный трансграничный электронный документооборот и обмен данными между пользователями через членов Альянса.

В настоящее время торговые документы для трансграничной сделки заполняются в бумажном виде и передаются по электронной почте или факсу. В ПАА обмен документами для трансграничных сделок может осуществляться более просто и эффективно в электронном виде посредством защищенной инфраструктуры. Кроме того, пользователи смогут повторно использовать соответствующие данные из полученных документов для применения и представления торговых или нормативных деклараций местным органам управления экономик ПАА.

Примеры реализованных проектов:

1. Документооборот между импортерами и экспортерами.

---

[49] Адрес в сети: URL: http://paa.net/ (Дата обращения 02.04.2016)

1.1. Обмен заказами на поставку, счетами-фактурами и предварительными уведомлениями об отгрузке для текстильной промышленности. Проект разработан для гонконгской компании — производителя одежды TAL Apparel Limited и ее поставщиков из Тайваня, в частности, текстильной компании Tai Yuen Textile Co. Решение реализовано участниками ПАА Tradelink Electronic Commerce Limited (Гонконг) и TRADE-VAN Information Services Co. (Китайский Тайбэй).

1.2. Обмен упаковочными листами, счетами-фактурами и коносаментами для поставок стали для автомобильной промышленности. Проект разработан для японского поставщика стали Metal One Corporation и автомобильной корпорации Hyundai Motors. Решение реализовано компаниями KTNET (Южная Корея) и TEDIANET (Япония).

2. Документооборот между экспедиторскими и логистическими компаниями. Обмен и повторное использование данных о доставке и торговых данных для подготовки и подачи деклараций экспорта/импорта между бизнес-сообществами Сингапура и Малайзии. Сетевое решение реализовано компаниями Crimson Logic (Сингапур) и Dagang Net (Малайзия).

3. Взаимное признание национальных инфраструктур открытых ключей (PKI). В ПАА существует специальная политика сертификации и авторизации удостоверяющих центров из экономик Альянса. На основе таких УЦ построена инфраструктура использования и взаимного признания сертификатов электронной подписи для всех электронных транзакций в сети ПАА.

4. Сервис отслеживания грузов. Данный сервис позволит транспортным компаниям определять статус груза и будет внедрен в существующие трансграничные электронные сервисы. В настоящее время сервис проходит тестирование с участием клиентов компаний KTNET (Южная Корея) и TRADE-VAN Information Services Co. (Китайский Тайбэй).

ПАА занимается разработкой технических стандартов, протоколов связи и обменом сообщениями внутри сети Альянса, а также правовыми аспектами: разработкой договоров, спецификаций, процедур для обеспечения юридической значимости электронных транзакций среди участников ПАА.

Услугами и электронными решениями ПАА пользуются более 150 000 компаний на азиатском рынке.

ПАА активно сотрудничает с группой по электронной торговле АТЭС, является членом Австралийской федерации борьбы против пиратства (AFACT). Началось сотрудничество с Европой через Азиатско-Европейский Альянс по электронной торговле (ASEAL).

Аналогичные подходы реализуются в Европе, где приняты, реализуются и модернизируются дорожные карты по цифровой экономике. на основе Regulation of the European Parliament and of the Council on electronic

identification and trust services for electronic transactions in the internal market (project – eIDAS)[50].

Российской Федерацией в последнее время предпринят ряд шагов по созданию и продвижению подхода к обеспечению трансграничного электронного документооборота на платформе трансграничного пространства доверия (ТПД) с ключевым конструктивным элементом – доверенной третьей стороной (ДТС) согласно международному стандарту X.842.

Указанный подход представляет собой информационную шину, на основании которой возможно обеспечить интеграцию национальных криптографических решений.

Идеи ТПД и ДТС удалось существенно продвинуть в рамках таких международных форматов, как ЕАЭС, ЭСКАТО, СЕФАКТ, ЮНСИТРАЛ и других. Стоит отметить, что большое количество стран поддерживают российский подход в качестве альтернативы активно продвигаемой американской стороной собственной модели обеспечения информационной безопасности.

Целесообразно рассматривать ТПД в качестве инфраструктурной поддержки для функционирования системы концентраторов (хабов) сервисов электронной коммерции в парадигме BUY-SHIP-PAY, по аналогии с практикой упомянутого выше Паназиатского альянса по электронной коммерции. Данные хабы, концентрируя все сервисы цифровой экономики, позволяют наиболее простым и неконфликтным способом решить проблему прослеживаемости товаров при разворачивании соответствующей информационно-аналитической системы «поверх» сервисов.

Учитывая изложенное, можно выдвинуть инициативу по созданию Евразийского альянса по электронной коммерции на платформе государственно-частного партнерства. Это позволит комплексно решить вопросы привлечения бизнеса для частичного снятия нагрузки с бюджета, мягкой защиты экономических интересов России, а также на конструктивной основе обеспечить решение вопросов международной информационной безопасности в глобальном информационном пространстве.

В плане практической реализации целесообразно:

государству взять на себя вопросы разработки технических требований по информационной безопасности и формирование нормативной основы;

бизнесу осуществить разработку функционального хаба электронной коммерции в рамках импортозамещения, используя имеющиеся международные наработки;

использовать существующую инфраструктуру для организации работы с клиентами (Почта России, сеть нотариальных контор).

---

[50] Адрес в сети: URL: https://ec.europa.eu/digital-single-market/en/trust-services-and-eid (Дата обращения 02.04.2016).

Учитывая лидирующую роль России в ЕАЭС, тематику международной информационной безопасности, а также необходимость скорейшего решения проблемы прослеживаемости товаров, представляется обоснованным инициировать указанный проект под патронажем Президента Российской Федерации и назначить представителя Российской Федерации Главным конструктором системы.

Реинжиниринг и единое окно. Лидерами государств-членов ЕАЭС поставлена задача по созданию системы национальных «единых окон». Разработан план на период до 2020 года. При этом нельзя допустить узкую трактовку этого проекта, целесообразно выработать общее понимание того, что суть «единого окна» это реинжиниринг, который требуется проводить в увязке разных фрагментов:

- национальном (5 экономик) и трансграничном (ЕАЭС);
- административном и предпринимательском;
- национальными сегментами ИИСС и электронными правительствами в целом (5 экономик);
- для России это усложняется структурой услуг на федеральном, региональном и муниципальном уровнях.

В целом для России, как ведущей экономики в ЕАЭС, реинжиниринг представляется наиболее сложной задачей. Для её решения необходимо создать эффективный организационный механизм, который из международного опыта может состоять из трёх компонент:

- профессионального центра компетенции, который не связан с реформируемыми организациями, а нацелен на достижение максимальной общей эффективности;
- ответственного федерального органа исполнительной власти, который проводит процедуры согласования предложений Центра компетенции с реформируемыми организациями;
- руководителя Правительства Российской Федерации на уровне не ниже вице-премьера, который обладает полномочиями по снятию оставшихся разногласий между реформируемыми организациями.

Подобная структура управлением реинжинирингом существует в Республике Казахстан с 2010 года и показала свою эффективность.

Отсутствие подобного механизма может привести к выхолащиванию взаимоувязанных идей реинжиниринга и «единого окна» и непроизводительным затратам на реализацию этих проектов.

Интероперабельность, стандарты и единое окно. Задача формирования механизма единого окна на платформе ТПД может быть отнесена к качественно новым явлениям современности, поскольку в такой постановке она не ставилась пока нигде в мире. Это обусловлено, прежде всего, следующими факторами:

- обеспечение трансграничного юридически значимого электронного документооборота для всех жителей планеты представляет собой задачу создания большой и сложной гуманитарно-технологической информационной системы, аналогов которой нет в мире;

- такая система по определению не может строиться «на пустом месте», она должна объединить большое количество (тысячи) унаследованных информационных систем в разных странах, при этом стандарты обеспечения такой глобальной интероперабельности отсутствуют.

Исходя их обозначенных выше тезисов, приступать к проблеме интероперабельности ИКТ целесообразно на основе выработки основополагающих принципов, которые возможно издать в форме одной из рекомендаций органа по международной стандартизации, например СЕФАКТ.

Работа в этом направлении начата. Так, в целях продвижения инициативы Российской Федерации о рассмотрении экономиками АТЭС проблематики достижения взаимосвязанности экономик АТЭС посредством ИКТ, зафиксированной во Владивостокской Декларации АТЭС 2012 года «Интеграция в целях роста, инноваций и процветания», в рамках заседания APEC TEL 48 был реализован российский самофинансируемый проект «Интероперабельные ИКТ: семантические, лингвистические и другие аспекты», в форме семинара.

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). В общем, был представлен весь спектр: бизнес, учёные, правительство и международные чиновники.

Ключевыми проблемами для достижения взаимосвязанности экономик АТЭС на основе современных ИКТ были признаны:

- решение вопросов интероперабельности ИКТ, используемых для обеспечения международной электронной торговли, логистических цепочек поставок, других информационных систем, в том числе используемых для управления в чрезвычайных ситуациях и на основе информационного взаимодействия человека с окружающей средой;

- решение вопросов международного юридически значимого обмена электронными документами для поддержки вышеупомянутых процедур;

- формирование трансграничного пространства доверия для охраны прав и законных интересов граждан, и организаций, находящихся под юрисдикцией государств и экономик, входящих в АТЭС, ЕЭК, СНГ, ШОС, Европейский союз, БРИКС и другие международные форматы, при обмене критически важными данными, в том числе персональными.

В завершении семинара состоялся заинтересованный обмен мнениями по этим вопросам, который показал чрезвычайную актуальность темы, поднятой Россией, для развития экономики в азиатско-тихоокеанском и других регионах мира, а также необходимость снятия многочисленных

барьеров на пути формирования единого экономического и человеческого пространства от Атлантики до Тихого океана. Участниками был принят проект решения семинара, включающий предложенный Россией расширенный набор универсальных принципов достижения интероперабельности ИКТ.

1. Unification. Interoperable ICT use unified organizational and technical infrastructures enabling cross-border electronic document interchange.

2. Scalability. Interoperable organizational and technical infrastructures should maintain the capacity to enroll new participants enabling them to quickly start operating resp. using the system. These infrastructures should also enable their users to choose a set of services matching user's needs.

3. Equal reliability of the infrastructure, which applies common minimal security requirements to all of its participants.

4. Legalization of electronic documents, ensuring that issued e-documents are equally recognized by respective jurisdictions.

5. Client-friendly architecture, which includes simple, clear, and handy user interfaces and unified system of accesses to the services of electronic documents interchange.

6. Systematization , which includes following components:

- consistency of organizational, legal and technical arrangements;
- consistency in reliability structures and infrastructure systems;
- moving from bilateral interoperability arrangements towards multi-vectored ones, where appropriate;
- agreed linguistic algorithms and technologies for information systems.

В дальнейшем указанные принципы интероперабельности ИКТ планируется издать в форме рекомендации СЕФАКТ в рамках инициируемого Россией проекта «Recommendation for ensuring legally significant trusted trans-boundary electronic interaction».

На этой основе в последующем должны быть проведена серьезная работа по международной стандартизации и формированию торговых обычаев для полноценного функционирования Евразийского альянса по электронной коммерции. Очевидно, что оба уровня стандартизации должны быть согласованы между собой в целях обеспечения глобальной интероперабельности ИКТ.

Понятийный аппарат в рамках единого окна. Решение вопросов стандартизации и интероперабельности в рамках формирования механизма единого окна на платформе ТПД предполагает выработку непротиворечивого глоссария базовых понятий. Определенная основа для этого предоставляется в Приложении № 3 к Договору о Евразийском экономическом союзе. В тоже время требуется некоторое дополнение глоссария. Ниже приводится аналитика этого вопроса.

В Приложения № 3 к Договору о ЕАЭС имеются следующие определения:

«информационная система» – совокупность информационных технологий и технических средств, обеспечивающих обработку информационных ресурсов;

«учетная система» – информационная система, которая содержит информацию из правоустанавливающих документов субъектов электронного взаимодействия и с использованием которой составляются или выдаются юридически значимые электронные документы;

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 в рамках Союза;

«общий процесс в рамках Союза» – операции и процедуры, регламентированные (установленные) международными договорами и актами, составляющими право Союза, и законодательством государств-членов, которые начинаются на территории одного из государств-членов, а заканчиваются (изменяются) на территории другого государства-члена;

«электронный документ» – документ в электронном виде, заверенный электронной цифровой подписью (электронной подписью) и отвечающий требованиям общей инфраструктуры документирования информации в электронном виде.

«электронный вид документа» – информация, сведения, данные, представленные в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи и обработки с использованием информационно-коммуникационных технологий с соблюдением установленных требований к формату и структуре.

Кроме того, в Приложения № 3 к Договору о ЕАЭС имеются следующие положения:

электронный документ, оформленный по правилам и требованиям документирования, утверждаемым Советом Комиссии, признается равным по юридической силе аналогичному документу на бумажном носителе, заверенному подписью либо подписью и печатью;

отсутствует определение электронного сообщения.

В следующей таблице приведен анализ этих определений и положений.

Определения и положения из Договора	**Анализ**
«информационная система» – совокупность информационных технологий и технических средств, обеспечивающих обработку информационных ресурсов;	1. Сравнивая эти определения можно сделать вывод, в рамках ИИСС используются две категории информационных систем – учетные и другие.

«учетная система» – информационная система, которая содержит информацию из правоустанавливающих документов субъектов электронного взаимодействия и с использованием которой составляются или выдаются юридически значимые электронные документы;	2. Категория «другие» не имеет в Договоре дальнейшего структурирования. При необходимости можно это сделать в документах более низкого уровня, например, в ТЗ на ИИСС дать определение информационно-справочных систем, которые обеспечивают жизненный цикл информации, сведений, данных, но не электронных документов. Также ввести три вида информационно-справочных систем соответственно для информации, сведений, данных. 3. Критерием отнесения информационных систем к той или иной категории является наличие или отсутствие в них информации из правоустанавливающих документов. 3. Цель учетных систем – обеспечение жизненного цикла электронных документов. 4. Цель других информационных систем – обеспечение жизненного цикла других разновидностей контента (информация, сведения, данные – обозначены в определении «электронного вида документа»).
«электронный документ» – документ в электронном виде, заверенный электронной цифровой подписью (электронной подписью) и отвечающий требованиям общей инфраструктуры документирования информации в электронном виде. «электронный вид документа» – информация, сведения, данные, представленные в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи и обработки с	1. Сравнивая первые два определения, подтверждается вышеприведенная логика 4-х видов контента (электронные документы, информация, сведения, данные). 2. При этом только первый вид (электронные документы) жестко соотносится с учетными системами, использованием ЭЦП и общей инфраструктурой документирования информации в электронном виде. 3. Соответственно остальные три вида контента (информация, сведения, данные) не требуют использования ЭЦП и других компонент этой общей инфраструктуры. 4. Анализ положения по юридический

использованием информационно-коммуникационных технологий с соблюдением установленных требований к формату и структуре; электронный документ, оформленный по правилам и требованиям документирования, утверждаемым Советом Комиссии, признается равным по юридической силе аналогичному документу на бумажном носителе, заверенному подписью либо подписью и печатью;	силе показывает, что информация, сведения, данные в электронном виде не равны по юридической силе документу на бумажном носителе, заверенному подписью, либо печатью и подписью. Следовательно, только учетные системы могут оперировать с электронными документами, в которых содержится информация из правоустанавливающих документов субъектов электронного взаимодействия. 5. Учетные системы и электронные документы жестко соотнесены с правилами и требованиям документирования. Информационно-справочные системы могут функционировать и без этого.
«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 в рамках Союза;	1. И учетные системы и общая инфраструктура жестко соотнесены с электронными документами и только эта триединая конструкция обеспечивает необходимые и достаточные условия для придания юридической силы. 2. Информация, сведения, данные в электронном виде, циркулирующие в информационно-справочных системах, не имеют юридической силы.
«общий процесс в рамках Союза» – операции и процедуры, регламентированные (установленные) международными договорами и актами, составляющими право Союза, и законодательством государств-членов, которые начинаются на территории одного из государств-членов, а заканчиваются (изменяются) на территории другого государства-члена;	1. Понятие общего процесса представляет собой динамическую последовательность операций и процедур и не равнозначно понятию информационных систем, как статической совокупности технологий и средств. Их соотношение – динамика общих процессов поддерживается статикой информационных систем. 2. Общий процесс не соотносится жестко ни с учетными, ни с информационно-справочными (другими) системами. Следовательно, можно выделить две типа общих процессов. Критерий для разграничения аналогичный – содержится или нет

	информация из правоустанавливающих документов. 3. Из определения следует, что общий процесс не может поддерживаться только одной информационной системой (независимо от их категорий). Всегда - только совокупность национальных и интеграционных. Их операторы принципиально разные.
электронное сообщение – определение отсутствует в Договоре	1. Электронное сообщение может содержать или не содержать в себе любой из 4-х видов контента (электронные документы, информация, сведения, данные). 2. Сообщение не является самостоятельным видом, а является только телекоммуникационной (транспортной) фазой в обеспечении жизненного цикла любого из самостоятельных видов.

Общие выводы по анализу:

1. В Договоре выделены две категории информационных систем в рамках ИИСС – учетные и другие. Разграничительным признаком является обработка информации из правоустанавливающих документов.

2. Учетные системы жестко увязаны с:

- электронными документами;
- информацией из правоустанавливающих документов;
- использованием ЭЦП и общей инфраструктурой документирования информации в электронном виде;
- равенством по юридической силе электронного документа аналогичному документу на бумажном носителе, заверенному подписью либо подписью и печатью;
- правилами и требованиям документирования;
- по совокупности приведенного выше – с трансграничным пространством доверия и соответственно с требованиями из пункта 18 Протокола.

Учетные системы поддерживают только те общие процессы, в которых обрабатывается информация из правоустанавливающих документов.

3. Другие информационные системы могут быть структурированы в зависимости от видов контента (информация, сведения, данные), как классы информационно-справочных систем. Определение можно дать в ТЗ на ИСС. У них нет жесткой увязки с перечисленным в пункте 2. Следовательно,

требования к ним существенно ниже. Они могут функционировать вне трансграничного пространства доверия.

4. Вся приведенная логика основана исключительно на тезисах из Договора. Для полноты системного описания потребуется ввести в ТЗ на ИСС только две новые сущности – электронных сообщений и информационно-справочных систем. И увязать основное целеполагание ИИСС с учетными системами, вспомогательное – с информационно-справочными. Это необходимо, поскольку набор требований к ним и соответственно их технических реализаций принципиально различаются. Кроме того, это ключевой функциональный аспект ИИСС в системном плане. Всё остальное должно расти из этого корня.

5. ИИСС представляет собой совокупность учетных и информационно-справочных систем. Учетные системы требуют обязательной поддержки со стороны трансграничного пространства доверия.

Для целей формирования единого окна в рамках ЕАЭС предлагается дополнить глоссарий следующими определениями:

Информационно-справочная система - информационная система с использованием которой обрабатывается информация, сведения, данные, используемые в рамках Евразийского экономического союза и которая не содержит информацию из правоустанавливающих документов субъектов электронного взаимодействия.

Информационные объекты - все виды электронных документов, информации, данных, сведений и электронных сообщений в рамках процессов и процедур механизма единого окна в рамках ЕЭК.2. Информация – вспомогательные информационные объекты аудио и визуального характера, используемые для обеспечения основной деятельности Комиссии.

Данные – информационные объекты, зафиксированные в информационно-справочных системах.

Сведения – информационные объекты, предоставляемые из информационно-справочных систем, по запросам физических, юридических и уполномоченных лиц.

Информация – вспомогательные информационные объекты аудио и визуального характера, используемые для обеспечения основной деятельности Комиссии.

Электронные сообщения – информационные объекты всех видов (информация, сведения, данные), которые в том числе могут содержать или не содержать электронные документы, передаваемые от отправителя к получателю по информационно-телекоммуникационной сети.

13 Исследование и анализ возможности использования института нотариата для поддержки функционирования трансграничного пространства доверия

В настоящее время появилась настоятельная необходимость придать проведенным технологическим наработкам в области формирования ТПД

институциональный характер в целях защиты прав и законных интересов граждан и юридических лиц, вступающих в юридически значимое, в том числе трансграничное информационное взаимодействие.

Для такой постановки задачи на постсоветском пространстве имеются определенные основания:

1. Решение Совета Евразийской экономической комиссии от 18 сентября 2014 года N 73 «О Концепции использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов»[51], в пункте VI.1 которой в частности отмечается следующее.

«В целях реализации настоящей Концепции должны быть разработаны и приняты соответствующие документы, направленные на унификацию правовых требований к операторам доверенных третьих сторон и порядку их деятельности, которые в дальнейшем могут быть рекомендованы к имплементации в законодательство государств-членов. В состав таких документов может входить, в том числе модельный кодекс института международного электронного нотариата на основе сервисов и служб доверенных третьих сторон государств-членов».

2. Постановление Экспертного совета МПА СНГ-РСС от 11 ноября 2014 года № 6 «О предложениях Экспертного совета МПА СНГ-РСС в перспективный план модельного законотворчества в Содружестве Независимых государств на 2016-2020 годы».

В этой связи имеется две альтернативные возможности:

- проинтегрировать возможности, предоставляемые современными доверенными ИКТ-сервисами, с одним из традиционных институтов, например, нотариальным;

- предпринять усилия к формированию нового института, основанного не на общественных отношениях, а на технологиях.

В качестве основы для выбора ниже проводится сравнение имеющихся технологических наработок с российским законодательством о нотариате.

Для целей дальнейшего исследования действия, совершаемые нотариусами, могут быть квалифицированы на две группы, по специальной и общей направленности.

К специальным нотариальным действиям, имеющим конкретный характер, могут быть отнесены:

удостоверение сделки;

выдача свидетельства о праве собственности на долю в общем имуществе супругов;

наложение и снятие запрещения отчуждения имущества;

удостоверение факта нахождения гражданина в живых;

удостоверение факта нахождения гражданина в определенном месте;

---

[51] http://www.tks.ru/news/law/2014/10/08/0006

удостоверение тождественности гражданина с лицом, изображенным на фотографии;

передача заявления и (или) иных документов физических и юридических лиц другим физическим и юридическим лицам;

принятие в депозит денежных сумм и ценных бумаг;

совершение исполнительных надписей;

совершение протестов векселей;

предъявление чеков к платежу и удостоверение неоплаты чеков;

совершение морских протестов;

обеспечение доказательств;

регистрация уведомлений о залоге движимого имущества;

выдача выписок из реестра уведомлений о залоге движимого имущества;

выдача дубликатов нотариальных свидетельств, исполнительных надписей и дубликатов документов, выражающих содержание нотариально удостоверенных сделок;

представление документов на государственную регистрацию прав на недвижимое имущество и сделок с ним;

удостоверение тождественности собственноручной подписи инвалида по зрению с факсимильным воспроизведением его собственноручной подписи;

выдача свидетельств о праве на наследство;

принятие мер по охране наследственного имущества;

удостоверение решений органов управления юридических лиц.

К общим нотариальным действиям, имеющим преимущественно документоведческий характер, могут быть отнесены:

свидетельствование верности копий документов и выписок из них;

свидетельствование подлинности подписи на документах;

свидетельствование верности перевода документов с одного языка на другой;

удостоверение времени предъявления документов;

принятие на хранение документов;

удостоверение сведений о лицах в случаях, предусмотренных законодательством Российской Федерации;

удостоверение равнозначности электронного документа документу на бумажном носителе;

удостоверение равнозначности документа на бумажном носителе электронному документу.

С нотариальными действиями общего характера тесно связаны правила их совершения, к которым относятся:

установление личности обратившегося за совершением нотариального действия;

проверка правоспособности юридических лиц, а также полномочий на совершение нотариального действия;

совершение нотариальных действий на основании электронного документа.

Важным является международный аспект нотариальных действий. Нотариус принимает документы, составленные в соответствии с требованиями международных договоров, а также совершает удостоверительные надписи в форме, предусмотренной законодательством других государств, если это не противоречит международным договорам Российской Федерации.

Нотариальные действия общего характера и связанные с ними правила их совершения, включая международный аспект, могут быть поставлены в соответствие с сервисами ТПД, описанными в проекте разработанной для целей Евразийской экономической комиссии Архитектуры ТПД.

Ниже в таблице приводятся результаты такого сопоставления.

№ п/п	Нотариальные действия общего характера и связанные с ними правила их совершения	Сервисы трансграничного пространства доверия
1.	Свидетельствование подлинности подписи на документах *свидетельствуя подлинность подписи, нотариус удостоверяет, что подпись на документе сделана определенным лицом, но не удостоверяет фактов, изложенных в документе*	Сервис доверенной третьей стороны (ДТС) Сервис удостоверяющего центра (УЦ) ТПД Сервис национальной инфраструктуры открытых ключей
2.	Установление личности обратившегося за совершением нотариального действия	Совокупность сервисов на клиентском уровне, используемых для информационного взаимодействия в рамках общих процессов ТПД: - комплексная эмиссия средств доступа и подписи (производство, дистрибуция, персонализация, выдача, утилизация); - эмиссия устройств чтения средств доступа и подписи; - идентификация и аутентификация субъектов информационного взаимодействия; - клиентский интерфейс для различных операционных систем; - другие клиентские сервисы.
3.	Удостоверение времени предъявления документов	Сервис доверенного времени

4.	Проверка правоспособности юридических лиц, а также полномочий на совершение нотариального действия	Сервис подтверждения статусов (полномочия и правомочия физических лиц, правовой статус юридических лиц, право подписи, других статусов) субъектов информационного взаимодействия
5.	Принятие на хранение документов	Сервис доверенного архивного хранения электронных документов
6.	Свидетельствование верности копий документов и выписок из них Свидетельствование верности перевода документов с одного языка на другой Удостоверение сведений о лицах в случаях, предусмотренных законодательством Российской Федерации Удостоверение равнозначности электронного документа документу на бумажном носителе Удостоверение равнозначности документа на бумажном носителе электронному документу Совершение нотариальных действий на основании электронного документа	Сервис заверения подлинности отдельных фрагментов контента электронного документа (место издания и другие)
7.	Международный аспект нотариальных действий	Сервис внешнего интерфейса для информационного взаимодействия с гражданами и организациями стран, не входящих в ТПД ЕАЭС

Этот перечень может быть в свою очередь классифицирован, как: работа с реквизитами (п.п. 1 – 4), с контентом (п. 6), архивное хранение (п. 5) и международный интерфейс (п. 7), что является необходимым и достаточным набором юридически значимых действий и соотнесенных с ними доверенных сервисов для массового перехода от бумажного к электронному документообороту, в том числе в трансграничной форме.

Другим важным заключением является то, что юридически значимые сервисы ТПД имеют все признаки традиционных нотариальных действий, но совершаемых не на бумаге, а с использованием современных ИКТ. В этой связи широко обсуждаемая категория Доверенной третьей стороны не имеет самостоятельного правового содержания, а является только инструментом для обеспечения деятельности специальной категории уполномоченных лиц.

Из этого следует, что институт нотариата, сформированный веками, может быть эффективно использован для «укрепления» электронных доверенных сервисов. Альтернатива этому пути – выращивание нового института на основе появившихся новых технологий представляется тупиковым. В этом плане генезис нотариата, как общественного института, может рассматриваться как замена информационного юридически значимого интерфейса с бумажного на электронную форму. А в условиях глобализации масштабирование этих подходов за национальные границы имеет характер цивилизационного явления.

В последнее время на законодательном уровне в Российской Федерации и ряде стран Содружества Независимых Государств сделаны решительные шаги в направлении широкого внедрения элементов электронного нотариата, предполагающего постепенный переход к оформлению, фиксации и хранению нотариальных актов непосредственно в электронной форме, а также – иные формы использования современных информационных технологий в нотариальной деятельности (например в Российской Федерации - использование аудио- и видеозаписей в нотариальном производстве, регистрация нотариальных действий в Едином реестре нотариальных действий, непосредственное взаимодействие с публичными реестрами, органами государственной власти в рамках СМЭВ, и др.).

В условиях резкой активизации интеграционных тенденций на постсоветском пространстве у института нотариата имеются все возможности поддержать политическую волю лидеров и предложить инновационные подходы по обеспечению юридической значимости широкого спектра трансграничных информационных транзакций в экономической и социальной сферах. Такая потребность растет год от года и является актуальной для всех регионов мира. Страны постсоветского пространства являются лидерами в этом направлении наряду с европейским и азиатско-тихоокеанском регионами. Все необходимые законодательные и технологические предпосылки для такого рывка имеются, как показано в настоящей аналитической записке. Требуется синергетическое слияние усилий государств и нотариальных сообществ для придания институциональных качеств современным информационно-безопасным технологиям.

14 Исследование и анализ возможности использования института урегулирования споров для поддержки функционирования трансграничного пространства доверия

В настоящее время функционирование института международного коммерческого арбитражного суда осуществляется на основе доминирующего использования документов, предоставляемых истцами и ответчиками в бумажной форме. Это определено международным законодательством, которое формировалось, начиная с 1958 года.

Однако вопрос использования современных информационных технологий в международной практике уже ставится в повестку дня профильных структур ООН.

Проблемами урегулирования споров в режиме онлайн применительно к трансграничным электронным коммерческим сделкам занимается Рабочая группа III ЮНСИТРАЛ «Урегулирование споров в режиме онлайн» (далее сокращенно – УСО). Работа в указанном направлении ведется с декабря 2010 года, в актуальной повестке дня – рассмотрение и принятие Процессуальных правил УСО.

Данная проблема была инициирована глобальными мировыми торговыми площадками и платежными системами, такими как e-Bay, Pay-Pal, alibaba.com и другими, а также разработчиками программного продукта платформы УСО, например, из Чехии. На подобных электронных торговых площадках совершаются миллионы сделок на суммы, как правило, не превышающие 2000 Евро. При этом возникающие конфликтные ситуации разрешаются не на основе права о международном арбитраже, а в соответствии с корпоративными правилами. Работа по разработке процессуальных правил УСО под эгидой ООН нацелена на устранение этого пробела в международном праве.

При использовании режима онлайн на всех этапах процедуры УСО при совершении тех или иных информационных транзакций предполагается отсутствие непосредственного контакта участников информационного взаимодействия, традиционного для арбитражного рассмотрения споров, когда основным средством идентификации является паспорт или другой документ, удостоверяющий личность. При этом возникает проблема надежной дистанционной идентификации участников информационного обмена. К числу последних можно отнести истцов, ответчиков, нейтральную сторону, операторов платформы УСО и провайдеров сервисов УСО.

На обоснование этой проблемы нацелен доклад Минкомсвязи России (прилагается), который был подготовлен и представлен в основных тезисах на заседании Рабочей группы III ЮНСИТРАЛ, состоявшемся в ноябре 2011 года в Вене. Представленная российская позиция по вопросам надежной идентификации нашла адекватное отражение в п.8 итогового документа[52]. Также предполагается, что по российской инициативе в последующем будет налажено в рамках ЮНСИТРАЛ взаимодействие Рабочей группы III с Рабочей группой IV «Электронная торговля», работающей над схожей проблематикой. Настоящая статья представляет собой попытку обосновать ряд предложений, направленных на решение проблемы поиска критериев надежной идентификации участников информационного обмена в рамках процедур УСО (далее сокращенно – Критерии).

Для выработки указанных Критериев необходимо обозначить основные компоненты системы идентификации участников информационного обмена

[52] A/CN.9/WG.III/XXIV/CRP.1/Add3. (Нужна полная ссылка!).

при совершении ими информационных транзакций в рамках процедуры УСО. К таковым компонентам можно отнести:

типовой процесс доступа участников информационного обмена к совершению информационных транзакций в рамках процедуры УСО – типовой процесс доступа;

набор идентификационных признаков, которыми может быть формализовано описан субъект права (физическое или юридическое лицо), для целей дистанционной идентификации участников информационного обмена при совершении ими информационных транзакций в рамках процедуры УСО – идентификационные признаки;

средство доступа участника информационного обмена к совершению информационных транзакций в рамках процедуры УСО – средство доступа;

операторы сервисов идентификации участников информационного обмена при совершении ими информационных транзакций в рамках процедуры УСО – операторы сервисов ID[53].

Типовой процесс доступа может включать следующие этапы:

1. Адекватную самоидентификацию участников информационного обмена до начала той или иной информационной транзакции в рамках процедур УСО.

2. Обязательную регистрацию участников информационного обмена в информационной системе оператора платформы УСО или в информационной системе оператора сервисов ID.

3. Реализацию платформой УСО сервиса доступа участников информационного обмена к совершению ими информационных транзакций в рамках УСО путем соотнесения предъявленных субъектом права идентификационных признаков с зарегистрированными аналогами[54] в отношении этого субъекта прав.

4. Регламентированную фиксацию результатов процедуры доступа в информационной системе оператора платформы УСО и предоставление информации о фактах доступа в случае конфликтной ситуации.

Исходя из описания типового процесса доступа, можно сделать следующие выводы.

Для процедур УСО недостаточным представляется только самоидентификация участников информационного обмена, например, на основе nickname (псевдонима); необходимо также зарегистрировать участников информационного обмена в регламентированном порядке у уполномоченного оператора, разновидностями которого являются: оператор

---

[53] Функции оператора сервисов ID могут выполняться операторами платформы УСО на децентрализованной основе. В тоже время оптимальным представляется формирование централизованного оператора сервисов ID для обеспечения этим функциональным назначением ряда платформ УСО, что обусловлено удобством пользователей, которые могут находиться в различных юрисдикциях, а также унификацией регламентов ID-процедур.

[54] Подтверждение прав доступа к платформе УСО целесообразно осуществлять также при использовании централизованных сервисов ID сторонних операторов.

платформы УСО – на децентрализованной основе, или оператор сервисов ID – на централизованной основе, создаваемые в интересах ряда платформ УСО;

В случае централизации сервисов ID для ряда платформ УСО, все они должны реализовывать Унифицированные требования по доступу участников информационного обмена к совершению ими информационных транзакций в рамках УСО;

В случае централизации сервисов ID для ряда платформ УСО, представляется целесообразной регламентация на клиентском уровне путем формирования единых Правил доступа участников информационного обмена к совершению ими информационных транзакций в рамках УСО;

В целях защиты персональных данных, коммерческой, врачебной тайны и других видов информации ограниченного доступа в том числе при их трансграничной передаче целесообразно подвергать операторов централизованных ID сервисов, а также операторов платформ УСО в части реализации ими ID сервисов, регламентированному аудиту со стороны независимых международных аудиторов.

Набор идентификационных признаков в принципе характеризуется огромным многообразием, от nickname (псевдонима) до любых биометрических данных, вплоть до анализа ДНК. Учитывая специфику УСО (споры по сделкам, не превышающим 2000 Евро), необходимо выработать такой набор идентификационных признаков, которые с одной стороны могут обеспечить надежный контроль доступа участников информационного обмена к совершению ими информационных транзакций в рамках УСО. С другой стороны, стоимость ID сервисов для участников информационного обмена должна быть существенно ниже стоимости сделки.

В общем виде идентификационные признаки участников информационного обмена могут быть распределены по трем группам:

информационные персональные данные, например ФИО, а также в противоположность - анонимный nickname или псевдоним, кроме того - связка логин-пароль; внутренний и внешний IP-адрес; MAC-адрес; доменное имя, E-mail и другие;

биометрические персональные данные (отпечаток пальца, фотография, сетчатка глаза, тембр голоса и другие);

технические идентифицирующие данные (Sim-карта, смарт-карта/usb-идентификатор, RFID-метка и другие).

Разнообразие идентификационных признаков позволяет выстроить их по возрастанию сложности реализации и стоимости. При этом для УСО может быть выбрано конкретное решение, на основе того, что модель угроз определяется небольшими (до 2 тыс. евро) суммами сделок (например, Middle-решение). В то же время из соображений технологической нейтральности нецелесообразно в разрабатываемых Процессуальных правилах УСО закреплять тот или иной конкретный набор. Целесообразно решить эту проблему путем указания на необходимость регламентации ID

сервисов соответствующими операторами и организации системы аудита за их деятельностью.

Средство доступа представляет собой привязанный к участнику информационного обмена агрегатор идентификационных признаков всех типов (информационных, биометрических и технических). В простейшем случае средством доступа является обычная клавиатура, например для ввода связки логин-пароль. Более сложным, но универсальным, случаем является ID-карта гражданина, имеющаяся во многих странах мира.

Очевидно, что средства доступа, выбираемые для использования в рамках УСО, должны быть увязаны с уже упомянутыми компонентами системы:

Регламентами деятельности соответствующих операторов ID сервисов;

Унифицированными требованиями по доступу УИВ к совершению ими информационных транзакций в рамках УСО;

Правилами доступа участников информационного обмена к совершению ими информационных транзакций в рамках УСО.

Тем самым может быть обеспечена интероперабельность различных платформ УСО в части ID сервисов, облегчен аудит в части соблюдения требований по защите персональных данных и соответственно – удобство для пользователей в различных странах при адекватной охране их прав.

Фиксация результатов процедуры доступа, как и в вышеописанных случаях, может иметь различную реализацию, от log-файлов до совершения регламентированных записей в специализированных учетах, имеющих служебный характер. Подход и в настоящем случае основывается на принципе технологической нейтральности, что предполагает указание в Процессуальных правилах УСО на необходимость регламентированной фиксации результатов процедуры доступа.

Приведенное выше описание основных компонент системы идентификации участников информационного обмена при совершении ими информационных транзакций в рамках процедуры УСО позволяет выйти на формулирование требований к данным процедурам, прежде всего в правовой, не технологической плоскости:

1. В центр проблемы необходимо поставить необходимость защиты персональных данных участников информационного обмена при совершении ими информационных транзакций в рамках процедуры УСО. Механизмом реализации этого требования должны являться регламентация деятельности операторов, работающих с такими персональными данными, а также независимый международный аудит за предоставлением ими ID сервисов.

2. Необходимо обозначить возможность предоставления ID сервисов как в централизованном исполнении (на основе специализированных операторов), так и в децентрализованном исполнении (на основе совмещения ID сервисов с основными задачами платформы УСО).

3. В случае централизованного использования ID сервисов целесообразно отразить вопрос обеспечения интероперабельности на основе

унифицированных требований по доступу участников информационного обмена к совершению ими информационных транзакций в рамках УСО, а также разработки и принятия единых Правил доступа к совершению ими информационных транзакций в рамках УСО.

Представляется, что данные требования могут носить универсальный, прежде всего с правовой точки зрения, характер, поскольку формулируются на основе принципа технологической нейтральности. В этой связи они могут быть актуальны также и для деятельности Рабочей группы IV ЮНСИТРАЛ «Электронная торговля» в рамках регулирования вопросов инфраструктурного обеспечения трансграничных электронных коммерческих сделок. Речь в общем случае может идти о создании в сети Интернет универсальной трансграничной инфраструктуры доступа к различным функциональным приложениям, требующим надежной дистанционной идентификации.

Проблема формирования глобальной онлайновой системы урегулирования коммерческих споров на основе идентификации участников информационного взаимодействия относится к числу актуальных и пока не решенных вопросов трансграничного электронного взаимодействия.

В Конвенции ООН об использовании электронных сообщений в международных договорах используется принцип функционального эквивалента на основе определения критериев, в соответствии с которыми электронные сообщения могут рассматриваться как эквивалент бумажных сообщений. В частности, в ней предусмотрены конкретные требования, которым должны отвечать электронные сообщения, для того чтобы они могли служить тем же целям и выполнять те же функции, свойственные определенным понятиям в традиционной системе бумажного оборота, например, понятиям "письменная форма", "подлинный экземпляр", "подпись" и "запись".

Начало процедуры урегулирования споров в системе онлайн предполагает взаимную идентификацию сторон спора (истца, ответчика, поставщика услуг УСО и нейтральной стороны), в рамках которой может использоваться электронная или цифровая подпись. Следует отметить, что термин "электронная подпись" отличается от термина "цифровая подпись". Электронная подпись относится к любому виду подписи, который служит для идентификации и удостоверения подлинности личности пользователя, включая управление идентификационными данными.

В статье 2 (a) Типового закона об электронных подписях электронная подпись определяется как «данные в электронной форме, которые содержатся в сообщении данных, приложены к нему или логически ассоциируются с ним и которые могут быть использованы для идентификации подписавшего в связи с сообщением данных и указания на то, что подписавший согласен с информацией, содержащейся в сообщении данных».

При цифровой подписи, как правило, используются такие методы шифрования, как инфраструктура открытых ключей (ИОК), для обеспечения эффективной реализации которой требуется наличие специальных технических средств.

Управление идентификационными данными можно определить как систему процедур, мер и технических средств, предназначенных для управления сроками допуска и полномочиями пользователей и их электронными идентификационными данными. Проверка идентификационных данных лица или субъекта, запрашивающего дистанционный доступ к системе, являющегося автором электронного сообщения или подписавшего электронный документ, относятся к той сфере, которая получила название "управление идентификационными данными". Цели системы управления идентификационными данными достигаются посредством следующих трех процессов: идентификации, удостоверения подлинности и проверки полномочий[55]

Эти подходы хорошо коррелируют с запиской Секретариата ЮНСИТРАЛ, подготовленной к 44-й сессии «Текущая и возможная будущая работа в области электронной торговли»[56], в которой была высказана мысль о необходимости создания "структуры доверия", позволяющей обеспечить выполнение как оперативных требований, т.е. как технических спецификаций, процедур, стандартов, директивных установок и правил, так и функциональных требований к системе идентификации, а также принятие правовых норм, необходимых для создания заслуживающей доверия идентификационной системы[57].

Было далее указано, что правовые нормы, образующие такую структуру доверия, могут устанавливаться в законодательном порядке либо носить договорный характер. Договоры могут конкретизировать нормы закона, а в случаях, когда это допускается, также видоизменять их. Секретариатом было разъяснено, что в рамках структуры доверия правовые нормы выполняют тройственную функцию. Во-первых, они придают спецификациям, стандартам и правилам, регулирующим различные аспекты оперативных требований, юридически обязательный характер в отношении всех сторон. Во-вторых, они определяют юридические права и обязанности сторон, конкретизируют правовой риск, принимаемый на себя участниками структуры доверия (в частности, в связи с предоставлением гарантий, ответственностью за убытки и рисками, которым подвергаются личные данные). И, следует особенно подчеркнуть, *предоставляют средства правовой защиты в случае возникновения споров между сторонами, включая*

---

[55] См. документы ЮНСИТРАЛ A/CN.9/692 и A/CN.9/728.

[56] См. документ ЮНСИТРАЛ A/CN.9/728.

[57] На своих 34-й и 35-й сессиях ЮНСИТРАЛ постановила, что ее будущая работа в области электронной торговли будет включать дальнейшие исследования и изучение вопроса урегулирования споров в режиме онлайн и что Рабочая группа II (Арбитраж и согласительная процедура) будет взаимодействовать с Рабочей группой IV (Электронная торговля) в связи с возможной будущей работой в этой области.

механизмы урегулирования споров и исполнения решений, права, касающиеся расторжения соглашений, а также размеры компенсации ущерба, *штрафные санкции и другие формы ответственности* – именно это является предметом рассмотрения настоящей рабочей группы III ЮНСИТРАЛ. Наконец, в некоторых случаях правовые нормы могут регулировать также содержание оперативных требований.

Таким образом, можно сделать вывод о том, что проблема УСО является одним из трех аспектов правовых норм трансграничной инфраструктуры доверия, которая в свою очередь, наряду с правовыми нормами, должна реализовывать комплекс технологических и организационных требований.

В дальнейшем в упомянутом документе A/CN.9/728 эти идеи находят свое развитие. В частности, выявлена связь между системами идентификации и использованием электронных подписей. Отмечалось, что в отношении ряда услуг, связанных с электронными подписями, таких, как удостоверение времени подписания и гарантия целостности содержания, до сих пор отсутствует единый правовой режим и что эти услуги актуальны также в контексте управления использованием идентификационных данных.

В итоге широкую поддержку получило мнение о важности вопросов управления использованием идентификационных данных для содействия трансграничным электронным сделкам, а также о необходимости надлежащего решения связанных с этим правовых проблем. Было отмечено, что, хотя на национальном уровне соответствующая работа ведется, практически отсутствуют инициативы, посвященные транснациональным юридическим аспектам управления использованием идентификационных данных. Была также высказана мысль о том, что ЮНСИТРАЛ в силу ее мандата, членского состава и экспертного потенциала располагает идеальными возможностями для работы над этими правовыми вопросами. Было добавлено, что такая работа позволила бы также дополнительно прояснить сферу применения положений о юридической силе подписи, которые содержатся в существующих текстах ЮНСИТРАЛ, и облегчила бы решение вопросов управления использованием идентификационных данных в контексте других тем, представляющих потенциальный интерес для ЮНСИТРАЛ – таких, как мобильная торговля, электронные передаваемые записи и электронные механизмы единого окна.

Вопросами «единого окна» в рамках ООН активно занимается Центр по упрощению процедур торговли и электронным деловым операциям (СЕФАКТ), который поддерживает деятельность, направленную на усиление возможности деловых кругов, торговых и государственных организаций в развитых, развивающихся и странах с переходной экономикой эффективно обмениваться товарами и соответствующими услугами. Его главная задача заключается в содействии национальным и международным сделкам посредством упрощения и согласования процессов, процедур и информационных потоков, и тем самым способствовать росту мировой

торговли, в том числе на основе трансграничных электронных коммерческих сделок.

Последнее является предметом рассмотрения в части УСО. Видимо можно констатировать, что рассматриваемый круг вопросов носит комплексный характер, те или иные аспекты которого находятся в фокусе рассмотрения различных международных форматов, как ООН, так и региональных, о чем пойдет речь ниже. Возвращаясь к теме СЕФАКТ можно отметить следующее.

В декабре 2010 года на очередной сессии этого формата в Женеве был рассмотрен проект 37-й Рекомендации СЕФАКТ «Рекомендация в отношении функциональной совместимости подписанных цифровых документов». По данному проекту был подготовлен ряд существенных российских замечаний, наряду с которыми в конструктивном плане предложено использовать соответствующий понятийный аппарат. Это обусловлено тем, что представленная к рассмотрению редакция 37-й Рекомендации СЕФАКТ, на наш взгляд, не демонстрирует системного подхода к решению такой многоаспектной проблемы, а также ориентирована на использование только одного национального алгоритма электронной подписи, что не соответствует российским подходам в области информационной безопасности.

Российские предложения, содержавшиеся в докладе Минсвязи России, были с интересом восприняты разработчиками 37-й Рекомендации, в настоящее время продолжается их активное обсуждение, и предпринимаются попытки выработать общую точку зрения.

Как отмечалось выше, затронутый комплекс вопросов находится в активной проработке в ряде региональных международных форматов, среди которых можно назвать Содружество Независимых Государств, Шанхайскую организацию сотрудничества и Евразийскую экономическую комиссию. В настоящий момент можно отметить некоторые итоги:

разработана и одобрена в формате СНГ Модель формирования и функционирования в сети Интернет трансграничного пространства доверия;

разработана и ведется обсуждение в формате СНГ Методологии системного проектирования, как дальнейшее развитие указанной выше Модели;

по инициативе китайской стороны начата проработка вопросов построения международного центра электронной торговли в формате ШОС на основе трансграничного пространства доверия;

имеется также ряд других результатов, в частности проведение российского семинара по трансграничному пространству доверия в Сан-Франциско в формате АТЭС, который получил высокие оценки, например со стороны экономик Канады, Мексики и Тайваня.

Ключевые идеи этих региональных разработок полностью соответствуют изложенным выше подходам III и IV рабочих групп ЮНСИТРАЛ и в какой-то степени развивают выдвинутые идеи. Описаны

базовые конструкты трансграничного пространства доверия, учетных систем, электронных передаваемых записей. Последняя компонента предназначена для предоставления сервисов документирования информации и доступа к учетным системам, а также некоторых вспомогательных сервисов. Все сервисы могут иметь различные сценарии в спектре от Light до Heavy реализаций.

Поскольку при создании глобальной онлайновой системы урегулирования споров предполагается рассмотрение многочисленных споров между коммерсантами и между коммерсантами и потребителями только на незначительные суммы, поэтому для электронных коммерческих трансграничных споров потребуются упрощенные механизмы, которые не потребуют таких затрат средств, времени и усилий, которые были бы непропорциональны экономической стоимости спора.

В этой связи, на наш взгляд, целесообразно для идентификации сторон спора в начале процедуры УСО использовать только Light сценарии сервисов доверия, предоставляемых на основе структуры (или общей инфраструктуры) доверия, в понимании упомянутых выше документов ЮНСИТРАЛ и региональных разработок, предложенных Российской Федерацией.

Резюмируя изложенное, полагаем целесообразным использование в рамках начала процедуры УСО, а возможно и при последующих информационных транзакциях, соответствующей структуры доверия. Для выработки более конкретных рекомендаций в последующем организовать взаимодействие в рамках III и IV рабочих групп ЮНСИТРАЛ с участием разработчиков 37-й Рекомендации СЕФАКТ.

15 Исследование и анализ возможности использования института страхования рисков для поддержки функционирования трансграничного пространства доверия

Данное направление институциональной поддержки функционирования ТПД является наименее проработанным по сравнению с тремя другими фундаментальными институтами, описанными выше, как начальная постановка задач по обеспечению гарантированного приема электронных документов в трансграничном режиме со стороны органов власти, судов и нотариата.

Это объясняется тем, что страховые компании строят свой бизнес по профилям рисков, в которых известна статистика по количеству страховых случаев, среднему возмещаемому ущербу при закладывании в расчеты прибыли компаний от ведения страховой деятельности.

Такой статистики в рамках деятельности по предоставлению сервисов операторами доверенных трансграничных сервисов пока не имеется. Этот рынок только нарождается. Тем не менее требуется дополнительная исследовательская работа в данном направлении.

Библиография

[1] Куприяновский В. П., Намиот Д. Е., Синягов С. А. Кибер-физические системы как основа цифровой экономики //International Journal of Open Information Technologies. - 2016. -Т. 4. - №. 2. - С. 18-25.

[2] Sheth A., Anantharam P., Henson C. Physical-cyber-social computing: An early 21st century approach //IEEE Intelligent Systems. – 2013. – Т. 28. – №. 1. – С. 78-82.

[3] Waldron M. Adopting electronic records management: European strategic initiatives //Information Management Journal. – 2004. – Т. 38. – №. 4. – С. 30-35.

[4] Liu Z. et al. Cyber-physical-social systems for command and control //IEEE Intelligent Systems. – 2011. – Т. 26. – №. 4. – С. 92-96.

[5] Baheti R., Gill H. Cyber-physical systems //The impact of control technology. – 2011. – Т. 12. – С. 161-166.

[6] Pan Asian E-commerce Alliance http://paa.net Retrieved: Aug, 2016

[7] Lee E. Y. J. Trans-Pacific Partnership (TPP) as a US Strategic Alliance Initiative under the G2 System: Legal and Political Implications //JE Asia & Int'l L. – 2015. – Т. 8. – С. 323.

[8] eIDAS project https://ec.europa.eu/digital-single-market/en/trust-services-and-eid Retrieved: Aug, 2016

[9] А.А. Домрачев, С.Н. Евтушенко, А.В. Петров, В.П. Куприяновский, Д.Е. Намиот «Об инновационных инициативах государств-членов ЕАЭС в области построения глобальной цифровой экономики» // International Journal of Open Information Technologies ISSN: 2307-8162 vol. 4, no. 10, 2016

[10] А.А. Домрачев, В.Б.Исаков, И.А.Фургель «Формирование единых региональных цифровых пространств с использованием трансграничного пространства доверия» // http://d-russia.ru/formirovanie-edinyx-regionalnyx-cifrovyx-prostranstv-s-ispolzovaniem-transgranichnogo-prostranstva-doveriya.html 06.07.2016

[11] Общая инфраструктура доверия для юридически значимого трансграничного электронного взаимодействия: Часть 1: «Модель формирования и функционирования в сети Интернет трансграничного пространства доверия государств-участников СНГ», разработанная Минкомсвязи РФ и одобренная на 17-м заседании Координационного совета государств – участников СНГ по информатизации при РСС (02.06.2011г., г. Ереван, Республика Армения, решение № 17/3). http://www.rcc.org.ru/userdocs/docs/Model-PD-T.pdf

[12] Общая инфраструктура доверия для юридически значимого трансграничного электронного взаимодействия: Часть 2: «Методология формирования и функционирования в сети Интернет трансграничного пространства доверия», разработана по заказу и под руководством

Министерства связи и массовых коммуникаций РФ, одобрена на 18-ом заседании Координационного совета государств-участников СНГ по информатизации при РСС (05.11.2012 г., г. Баку, Республика Азербайджан, решение № 47/18-9).
http://www.rcc.org.ru/userdocs/docs/Metodologiya_PD-T.pdf

[13] Общая инфраструктура доверия для юридически значимого трансграничного электронного взаимодействия: Часть 3: «Концепция разработки и принятия проектов документов для координации и аудита деятельности ее участников», разработана по заказу ОАО «Ростелеком».
http://www.rcc.org.ru/userdocs/docs/Kontseptsiya_19_11_12.pdf,
www.rcc.org.ru/userdocs/docs/Prilojeniya_k_Kontseptsii_19_11_12.rar.

Приложение
ПРОЕКТ

Конвенция о трансграничном пространстве доверия при трансграничном электронном взаимодействии

Государства-участники настоящей Конвенции,

подтверждая свою убежденность в том, что развитие информационно-коммуникационных технологий является условием устойчивого экономического роста и повышения качества жизни граждан,

отмечая, что электронное взаимодействие повышает эффективность государственного управления и коммерческой деятельности, укрепляет внешнеэкономические связи, открывает доступ к новым возможностям для ранее удаленных сторон и рынков и играет тем самым основополагающую роль в содействии экономическому развитию как на национальном, так и на международном уровнях,

учитывая, что проблемы, возникающие ввиду неопределенности технологического и правового регулирования использования электронных документов при взаимодействии между государственными и муниципальными органами, физическими лицами и организациями государств - участниц Конвенции, представляют собой препятствие для развития электронного взаимодействия,

будучи убеждены в том, что создание доверия между всеми участниками электронного взаимодействия является необходимым условием его развития,

полагая, что единообразные правила должны основываться на уважении свободы выбора сторонами соответствующих информационных носителей и технологий с учетом принципов технологической нейтральности и функциональной эквивалентности в той мере, в которой избранные сторонами средства отвечают цели соответствующих норм права,

признавая возможность и целесообразность построения как централизованной, так и децентрализованной систем доверия и использования их для ускорения прогресса и в рамках цифровой экономики, в том числе целях доверенного осуществления электронной торговли и транспорта, электронного разрешения споров, создания электронных правительств и других электронных государственных услуг, реализации дистанционного обучения, электронного здравоохранения, электронных реестров всевозможного назначения, электронных финансовых услуг,

согласились о нижеследующем:

Глава I. СФЕРА ПРИМЕНЕНИЯ

Статья 1
Сфера применения

1. Настоящая Конвенция определяет основные характеристики трансграничного пространства доверия - совокупности нормативных и организационно-технических условий по установлению доверия при трансграничном информационном взаимодействии органов государственной власти и местного самоуправления государств – участников настоящей Конвенции (далее - государства-участники), физических и юридических лиц, находящихся на территории различных государств-участников, в электронном виде.

2. Ни государственная принадлежность участников трансграничного электронного взаимодействия, ни их гражданский и правовой статус, ни характер электронных документов и электронных сообщений, которыми они обмениваются, не принимаются во внимание при определении применимости настоящей Конвенции.

3. Трансграничное пространство доверия охватывает следующие сегменты:

1) централизованный, охватывающий нормативные и организационно-технические условия по установлению доверия при обмене электронными документами, что предполагает установление обязательных для государств-участников требований к порядку деятельности операторов доверенных сервисов, к программно-аппаратным средствам, используемым в целях осуществления трансграничного электронного взаимодействия операторами доверенных сервисов, и процедуры подтверждения соответствия операторов доверенных сервисов и программно-аппаратных средств установленным требованиям;

2) саморегулируемый, охватывающий нормативные и организационно-технические условия по установлению доверия при обмене электронными сообщениями с использованием распределенных баз данных и формированием блоков данных, что предполагает организацию трансграничного электронного взаимодействия на принципах саморегулирования.

4. Трансграничное пространство доверия используется его участниками в целях установления и обеспечения необходимого уровня доверия между его участниками при предоставлении и использовании цифровых услуг (сервисов). Выбор конкретного сегмента трансграничного пространства доверия или их комбинации согласно части 3 статьи 1 настоящей Конвенции зависит от характера конкретных цифровых услуг (сервисов), уровень доверия при оказании которых должен обеспечиваться трансграничным пространством доверия.

Глава II. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 2
Определения

1. Для целей настоящей Конвенции:

1) «участники трансграничного пространства доверия» означает органы государственной власти и местного самоуправления государств – участников, Координационный Совет, операторы доверенных сервисов, операторы распределенных баз данных, физические лица и организации, находящиеся на территории любого из государств-участников;

2) "электронное сообщение" означает любую информацию, подготовленную, отправленную, полученную или хранимую с помощью электронных, магнитных, оптических или аналогичных средств;

3) "электронный документ" означает электронное сообщение, обладающее необходимыми и достаточными реквизитами для признания его юридически значимым, достоверность и подлинность которого удостоверена оператором доверенных сервисов в соответствии с настоящей Конвенцией;

4) «записи транзакций» означают электронные сообщения, прошедшие проверку подлинности у операторов распределенных баз данных, включенные этими операторами в действительный блок данных, не подлежащие изменению и составляющие в совокупности действительный блок данных;

5) «доверенные сервисы» означает услуги, подтверждающие достоверность и подлинность электронных документов и (или) их отдельных реквизитов, в том числе включая, но не ограничиваясь услуги, связанные с созданием и использованием электронной подписи, электронной печати, электронные отметки времени и доставки, аутентификация веб-сайтов;

6) «трансграничное электронное взаимодействие» означает осуществляемый с помощью информационных систем обмен электронными сообщениями и (или) электронными документами между участниками трансграничного пространства доверия;

7) "Координационный совет" означает создаваемый государствами-участниками в соответствии с настоящей Конвенцией орган, устанавливающий обязательные для государств-участников требования к порядку деятельности операторов доверенных сервисов, к программно-аппаратным средствам, используемым в целях осуществления трансграничного электронного взаимодействия операторами доверенных сервисов, и процедуры подтверждения соответствия операторов доверенных сервисов и программно-аппаратных средств установленным требованиям, а также выполняет иные функции, установленные настоящей Конвенцией;

8) «место нахождения» означает место, указанное участником трансграничного пространства доверия как место своего нахождения, а при

отсутствии такого указания – место жительство физического лица или место инкорпорации юридического лица;

9) «оператор доверенных сервисов» означает оказывающее услуги доверенных сервисов - в рамках централизованного сегмента трансграничного пространства доверия - физическое лицо или организация, соответствующие требованиям, установленным Координационным советом и получившие подтверждение о соответствии указанным требованиям в установленном Координационным советом порядке;

10) «операторы распределенных баз данных (майнеры)» означают обладающие необходимыми программно-аппаратными средствами физические или юридические лица (в том числе действующее анонимно), участвующие - в рамках саморегулируемого сегмента трансграничного пространства доверия - в записи транзакций и проверяющие их подлинность, формирующие блоки данных в распределенных базах данных и проверяющие их полноту;

11) «пользователь» означает орган государственной власти или местного самоуправления государства-участника, физическое лицо или организация, являющее отправителем или получателем электронных сообщений и электронных документов, в том числе с использованием услуг саморегулируемого сегмента трансграничного пространства доверия;

12) "информационные системы" означает системы для подготовки, отправления, получения, хранения или иной обработки электронных сообщений, включая электронные документы, в целях трансграничного электронного взаимодействия;

13) «электронная подпись / печать» означает данные в электронной форме, физически или логически ассоциированные с другими электронными данными, документирующие определенное отношение между подписантом и этими электронными данными и позволяющие третьему лицу впоследствии установить наличие этого отношения.

14) „подписант“ означает физическое (для электронной подписи) или юридическое (для электронной печати) лицо, осуществляющее подпись электронного документа с помощью своей электронной подписи/печати;

15) «квалифицированный сертификат электронной подписи / печати» - подтверждение в электронной форме, связывающее данные для проверки электронной подписи / печати с физическим (подпись) или юридическим (печать) лицом, подтверждающее, как минимум, его личность, выданное оператором доверенных сервисов, прошедшего процедуру подтверждения соответствия согласно части 5 статьи 8 настоящей Конвенции и удовлетворяющее требованиям, установленным Координационным советом;

16) «электронная отметка времени» - данные в электронной форме, связывающие другие электронные данные с определенным моментом времени и документирующие, что эти электронные данные в этот момент времени существовали, и позволяющие третьему лицу впоследствии установить этот факт;

17) «электронный сервис доставки с подтверждением получения» - сервис, позволяющий передавать данные между третьими сторонами электронными средствами и предоставляет доказательство относительно обработки передаваемых данных, включая подтверждение отправления и получения данных, и который защищает передаваемые данные от рисков утраты, кражи, повреждения или несанкционированных изменений;

18) «квалифицированный сертификат аутентификации веб-сайтов» - подтверждение в электронной форме, позволяющее аутентифицировать веб-сайты, связывающее веб-сайт с физическим или юридическим лицом, которому это подтверждение было выдано, выданное оператором доверенных сервисов, прошедшего процедуру подтверждения соответствия согласно части 5 статьи 8 настоящей Конвенции и удовлетворяющее требованиям, установленным Координационным советом.

Статья 3
Толкование

1. При толковании настоящей Конвенции надлежит учитывать ее международный характер и необходимость содействовать достижению единообразия в ее применении, а также соблюдению добросовестности при трансграничном электронном взаимодействии и иных принципов, установленных статьей 5 настоящей Конвенции.

2. Вопросы, относящиеся к предмету регулирования настоящей Конвенции, которые прямо в ней не разрешены, подлежат разрешению в соответствии с общими принципами, на которых она основана, а при отсутствии таких принципов - в соответствии с правом, применимым в силу норм международного частного права.

Статья 4
Принципы

Осуществление трансграничного электронного взаимодействия в рамках трансграничного пространства доверия осуществляется на основании следующих принципов, которые применяются в обоих сегментах трансграничного пространства доверия:

1) технологическая нейтральность;

2) функциональная эквивалентность;

3) защита информации ограниченного доступа, то есть охраняемой на основании норм международного права и национального законодательства государств-участников информации, включая коммерческую тайну и персональные данные, при осуществлении трансграничного электронного взаимодействия;

4) использование любой информации, документов, сообщений, в том числе блоков данных в распределенных базах данных, исключительно в целях, не противоречащих нормам международного права и нормам национального законодательства государств-участников.

Глава III. КООРДИНАЦИОННЫЙ СОВЕТ

Статья 5
Функции Координационного совета

1. Координационный совет является органом, выполняющим функции управляющего органа в централизованном сегменте трансграничного пространства доверия и функции координатора в саморегулируемом сегменте трансграничного пространства доверия.

2. В централизованном сегменте трансграничного пространства доверия Координационный совет утверждает:

1) требования к порядку деятельности операторов доверенных сервисов, в том числе к страхованию гражданской ответственности и аудиту операторов доверенных сервисов;

2) требования к программно-аппаратным средствам, используемым в целях осуществления трансграничного электронного взаимодействия;

3) процедуры подтверждения соответствия операторов доверенных сервисов и программно-аппаратных средств установленным требованиям (аудит);

4) правила ответственности операторов доверенных сервисов;

5) правила разрешения споров в рамках трансграничного пространства доверия;

6) требования к органам и (или) лицам, осуществляющим подтверждение соответствия операторов доверенных сервисов и программно-аппаратных средств установленным требованиям (аудит);

7) иные документы, предусмотренные настоящей Конвенцией.

3. Государства-участники соглашаются в соответствии с настоящей Конвенцией исполнять или обеспечивать исполнение актов Координационного совета, принятых в соответствии с частью 2 настоящей статьи, находящимися под их юрисдикцией органами государственной власти и местного самоуправления, пользователями, операторами доверенных сервисов.

4. В саморегулируемом сегменте трансграничного пространства доверия Координационный совет:

1) утверждает рекомендательный порядок подтверждения присоединения операторов распределенных баз данных к соответствующим базам данных;

2) утверждает порядок уведомлений Координационного совета об инцидентах с информацией в распределенных базах данных, то есть об

использовании электронных сообщений, записей транзакций, блоков данных в распределенных базах данных в целях, противоречащих нормам международного права и нормам национального законодательства государств-участников;

3) организует подачу операторами распределенных баз данных уведомлений в Координационный совет о добровольном принятии на себя операторами распределенных баз данных обязательств о выполнении требований настоящей Конвенции в части обеспечения использования любой информации, документов, сообщений, в том числе блоков данных в распределенных баз данных исключительно в целях, не противоречащих нормам международного права и нормам национального законодательства государств-участников, и в части информирования Координационного совета об инцидентах с информацией в распределенных базах данных.

5. Решения и документы, принимаемые Координационным советом в рамках саморегулируемого сегмента трансграничного пространства доверия, носят рекомендательный характер.

Статья 6

Создание и порядок функционирования Координационного совета

1. Координационный совет состоит из уполномоченных представителей государств-участников, назначаемых государствами-участниками на срок четыре года. Каждое государство-участник может назначить одного уполномоченного представителя.

2. Координационный совет может учреждать такие вспомогательные органы, какие он найдет необходимыми для выполнения своих функций.

3. Каждый член Координационного совета имеет один голос.

4. Решения Координационного совета по вопросам регламента его работы считаются принятыми, когда за них поданы голоса не менее двух третей членов Координационного совета.

5. Решения Координационного совета об утверждении актов, указанных в части 2 настоящей статьи, считаются принятыми, когда за них поданы голоса не менее трех четвертей членов Координационного совета.

6. Координационный совет устанавливает свой регламент, включая порядок избрания своего Председателя, процедуру поддержания взаимного доверия между ответственными представительствами государств-участников трансграничного пространства доверия, процедуру принятия решений в отношении утверждения документов, указанных в статье 5 настоящей Конвенции.

Глава IV. УЧАСТНИКИ ТРАНСГРАНИЧНОГО ПРОСТРАНСТВА ДОВЕРИЯ

Статья 7

Органы государственной власти и местного самоуправления государств-участников

1. Органы государственной власти и местного самоуправления государств-участников участвуют в трансграничном электронном взаимодействии при выполнении публичных функций, возложенных на них национальным законодательством государств-участников, в соответствии с правилами, установленными настоящей Конвенцией и принятыми в соответствии с ней актами Координационного совета.

2. Органы государственной власти и местного самоуправления государств–участников вправе самостоятельно принимать решение о порядке участия в саморегулируемом сегменте трансграничного пространства доверия.

3. Органы государственной власти и местного самоуправления вправе устанавливать дополнительные требования по сравнению с требованиями, установленными настоящей Конвенцией и принятыми в соответствии с ней актами Координационного совета, но не противоречащие им, в целях осуществления электронного взаимодействия, в случаях, установленных Координационным советом.

Статья 8

Операторы доверенных сервисов

1. Операторы доверенных сервисов являются участниками централизованного сегмента трансграничного пространства доверия.

2. Операторы доверенных сервисов могут оказывать услуги доверенных сервисов как на территории отдельных государств-участников, так и на территории всех государств-участников.

3. Операторы доверенных сервисов обязаны соответствовать требованиям, установленным Координационным советом в зависимости от охвата территории (все или отдельные государства-участники), на которой операторы доверенных сервисов оказывают услуги, и подтверждать соответствие установленным требованиям в порядке, установленном Координационным советом.

3. Операторы доверенных сервисов обязаны размещать для всеобщего сведения в сети Интернет любую информацию, связанную с получением или изменением статуса оператора доверенных сервисов. Операторы доверенных сервисов обязаны предоставлять любую информацию, связанную с инцидентами при осуществлении трансграничного электронного взаимодействия, уполномоченным органам государственной власти

государств-участников и Координационному совету. Порядок и сроки предоставления информации, связанной с инцидентами при осуществлении трансграничного электронного взаимодействия, устанавливает Координационный совет.

4. Операторы доверенных сервисов обязаны страховать гражданскую ответственность в порядке, установленном Координационным советом.

5. Операторы доверенных сервисов обязаны проходить процедуру подтверждения соответствия (независимый аудит соответствия) операторов доверенных сервисов и программно-аппаратных средств установленным требованиям в порядке, установленном Координационным советом.

Статья 9
Независимый аудит соответствия. Страхование

1. Услуги доверенных сервисов имеют право оказывать только операторы доверенных сервисов, прошедшие независимый аудит соответствия.

2. Аудит соответствия проводят органы или организации, уполномоченные в установленном Координационным советом порядке.

3. Операторы доверенных сервисов осуществляют страхование гражданской ответственности в соответствии с требованиями, установленными Координационным советом.

Статья 10
Операторы распределенных баз данных

1. Операторы распределенных баз данных являются участниками саморегулируемого сегмента трансграничного пространства доверия.

2. Операторы распределенных баз данных организуют трансграничное электронное взаимодействие друг с другом и с пользователями на принципах саморегулирования и самостоятельно обеспечивают выполнение требований настоящей Конвенции об использовании любой информации, документов, сообщений, в том числе блоков данных в распределенных базах данных исключительно в целях, не противоречащих нормам международного права и нормам национального законодательства государств-участников, и об информировании Координационного совета об инцидентах с информацией в распределенных базах данных.

3. Операторы распределенных баз данных признаются выполняющими требования настоящей Конвенции об использовании любой информации, документов, сообщений, в том числе блоков данных в распределенных баз данных исключительно в целях, не противоречащих нормам международного права и нормам национального законодательства государств-участников, и об информировании Координационного совета об инцидентах с информацией в распределенных базах данных в случае добровольной подачи

операторами уведомлений в Координационный совет о добровольном соблюдении указанных требований. Порядок подачи соответствующих уведомлений и порядок ведения перечня операторов распределенных баз данных – участников трансграничного пространства доверия устанавливается Координационным советом.

4. Взаимодействие операторов распределенных баз данных и Координационного совета, а также операторов распределенных баз данных и пользователей может осуществляться без идентификации юридических и физических лиц, являющихся операторами распределенных баз данных и пользователями.

5. В случае получения Координационным советом информации о нарушении оператором распределенной базы данных требований настоящей Конвенции, указанных в части 2 настоящей статьи, оператор распределенной базы данных исключается из публично доступного в сети Интернет перечня операторов распределенных баз данных – участников трансграничного пространства доверия.

Статья 11
Пользователи

1. Пользователи являются участниками обоих сегментов трансграничного пространства доверия.

2. В зависимости от использования определенного сегмента трансграничного пространства доверия, пользователи осуществляют обмен электронными сообщениями и электронными документами с учетом правил, установленных Координационным советом и операторами доверенных сервисов, или с учетом правил, установленных операторами распределенных баз данных, соответственно.

Глава V. ИНФРАСТРУКТУРА ТРАНСГРАНИЧНОГО ПРОСТРАНСТВА ДОВЕРИЯ

Статья 12
Программно-аппаратный комплекс операторов доверенных сервисов

1. Операторы доверенных сервисов используют для оказания услуг только оборудование, сертифицированное в соответствии с частью 5 статьи 8 и частью 1 статьи 9.

2. Функциональные требования к программно-аппаратному комплексу операторов доверенных сервисов и требования к сертификации оборудования с учетом принципа технологической нейтральности устанавливаются Координационным советом в соответствии с частью 5 статьи 8 и частями 1 и 2 статьи 9.

Статья 13
Программно-аппаратный комплекс операторов распределенных баз данных

Операторы распределенных баз данных самостоятельно определяют требования к программно-аппаратным комплексам, необходимым для проверки подлинности и полноты записей транзакций, создания, хранения и проверки полноты блоков данных.

Статья 14
Программно-аппаратный комплекс пользователей

Пользователи обязаны самостоятельно обеспечивать соответствие программно-аппаратных комплексов, используемых при осуществлении трансграничного электронного взаимодействия, требованиям, установленным операторами доверенных сервисов.

Глава VI. ДОВЕРЕННЫЕ СЕРВИСЫ В РАМКАХ ЦЕНТРАЛИЗОВАННОГО СЕГМЕНТА ТРАНСГРАНИЧНОГО ПРОСТРАНСТВА ДОВЕРИЯ

Статья 15
Электронная подпись

1. Электронная подпись не может считаться не имеющей юридических последствий или признаваться недопустимым доказательством в судебном разбирательстве только на том основании, что она имеет электронную форму или не соответствует требованиям квалифицированной электронной цифровой подписи.

2. Усиленная электронная подпись должна соответствовать следующим требованиям:

а) должна быть уникальным образом связана с подписантом;

б) должна давать возможность идентифицировать подписанта;

в) должна быть создана с использованием данных создания электронной подписи, которые подписант с высоким уровнем уверенности использует под единоличным контролем;

г) должна быть связана с данными, в отношении которых она проставляется, таким образом, чтобы изменение таких данных после проставления подписи можно было обнаружить.

3. Квалифицированная электронная подпись – это усиленная электронная подпись, базирующаяся на квалифицированном сертификате электронной подписи и созданная с помощью программно-аппаратных

средств, сертифицированных согласно части 5 статьи 8. Квалифицированная электронная подпись имеет такие же юридические последствия, что и собственноручная подпись.

Статья 16
Электронная печать

1. Электронная печать не может считаться не имеющей юридических последствий или не может быть признана недопустимым доказательством в судебном разбирательстве только на том основании, что она имеет электронную форму или не соответствует требованиям квалифицированной электронной печати.

2. Усиленная электронная печать должна соответствовать следующим требованиям:

а) должна быть уникальным образом связана с автором печати;

б) должна давать возможность идентифицировать автора печати;

в) должна быть создана с использованием данных создания электронной печати, которые с высоким уровнем уверенности используются под единоличным контролем автора печати;

г) должна быть связана с данными, в отношении которых она проставляется, таким образом, чтобы изменение указанных данных после проставления печати можно было обнаружить.

3. Квалифицированная электронная печать– это усиленная электронная печать, базирующаяся на квалифицированном сертификате электронной печати и созданная с помощью программно-аппаратных средств, сертифицированных согласно части 5 статьи 8. Квалифицированная электронная печать создает презумпцию целостности данных и подтверждения источника происхождения данных, которые заверяет такая квалифицированная электронная печать.

Статья 17
Электронные отметки времени

1. Электронная отметка времени не может считаться не имеющей юридических последствий и не может быть признана недопустимым доказательством в судебном разбирательстве только на том основании, что она имеет электронную форму или не соответствует требованиям квалифицированных электронных отметок времени.

2. Квалифицированная электронная отметка времени создает презумпцию точности указанных даты и времени и целостности данных, наличие которых заверяет такая квалифицированная электронная отметка времени.

3. Квалифицированная электронная отметка времени должна соответствовать следующим требованиям:

а) должна привязывать дату и время к данным таким образом, чтобы разумно исключалась возможность незаметного изменения данных;

б) должна быть основана на источнике, указывающем точное время и соотносимом с универсальным глобальным временем;

в) должна быть заверена усиленной электронной подписью или печатью оператора доверенных сервисов, прошедшего процедуру подтверждения соответствия согласно части 5 статьи 8, или иным аналогичным способом.

Статья 18
Сервис заказной доставки

1. Данные, отправленные и полученные с помощью электронного сервиса доставки с подтверждением получения, не могут считаться не имеющими юридических последствий или не могут быть признаны недопустимым доказательством в судебном разбирательстве только на том основании, что они имеют электронную форму или не соответствуют требованиям квалифицированных электронных сервисов доставки с подтверждением получения.

2. Данные, отправленные и полученные с помощью квалифицированного электронного сервиса доставки с подтверждением получения, создают презумпцию целостности данных, отправки таких данных идентифицированным отправителем, получения таких данных идентифицированным получателем, точности даты и времени отправки и получения, указанных квалифицированным электронным сервисом доставки с подтверждением получения.

3. Квалифицированные электронные сервисы доставки с подтверждением получения должны соответствовать следующим требованиям:

а) они предоставляются одним или несколькими операторами доверенных сервисов, прошедшими процедуру подтверждения соответствия согласно части 5 статьи 8 настоящей Конвенции;

б) с высоким уровнем надежности обеспечивают идентификацию отправителя;

с) они обеспечивают идентификацию получателя до предоставления данных;

в) отправка и получение данных заверяются усиленной электронной подписью или печатью оператора доверенных сервисов таким образом, чтобы исключить возможность незаметного внесения изменений в данные;

г) любые изменения данных, осуществляемые с целью отправки или получения данных, явным образом доводятся до сведения отправителя и получателя,

д) дата и время отправки, получения данных и внесения в них каких-либо изменений указываются с помощью квалифицированной электронной отметки времени.

Статья 19
Аутентификация веб-сайтов

1. Квалифицированные сертификаты аутентификации веб-сайтов должны содержать:

а) указание на то, что сертификат был выдан в качестве квалифицированного сертификата аутентификации веб-сайтов как минимум в формате, подходящем для автоматической обработки;

б) данные, позволяющие однозначным образом идентифицировать оператора доверенных сервисов, который выдает квалифицированный сертификат;

в) имя или псевдоним физического лица либо наименование и регистрационный номер юридического лица;

г) частичные данные адреса (как минимум город и страна) физического или юридического лица, которому был выдан сертификат;

д) доменные имена, принадлежащие физическому или юридическому лицу, которому был выдан сертификат;

е) данные о начале и окончании срока действия сертификата;

ж) идентификационный номер сертификата, который должен быть уникальным для конкретного оператора доверенных сервисов;

з) усиленная электронная подпись или печать квалифицированного оператора доверенных сервисов, выдающего сертификат;

и) место нахождения сервисов, которые могут использоваться для получения сведений о статусе сертификата.

Статья 20
Другие доверенные сервисы

1. Координационный совет может дополнительно включить в сферу своего регулирования другие доверенные сервисы, не указанные в статьях 15-19 настоящей Конвеции.

2. Регулирование других доверенных сервисов должно осуществляться аналогично регулированию доверенных сервисов, указанных в статьях 15-19 настоящей Конвенции.

Статья 21
Признание доверенных сервисов третьих стран и международных организаций

1. Услуги доверенных сервисов, оказываемые операторами доверенных сервисов, уполномоченными в соответствии с законодательством третьих стран или международных организаций, могут признаваться юридически эквивалентными услугам доверенных сервисов, оказываемыми операторами доверенных сервисов, прошедшими процедуру подтверждения соответствия согласно части 5 статьи 8 настоящей Конвенции, в случае заключения между Координационным советом и уполномоченным органом соответствующей третьей страны или международной организацией соглашения в соответствии с частью 2 настоящей статьи.

2. Указанные в пункте 1 настоящей статьи соглашения должны обеспечивать, в частности, что:

1) требования, предъявляемые к операторам доверенных сервисов в третьей стране или международной организации, не ниже требований, предъявляемых к операторам доверенных сервисов, оказывающих услуги доверенных сервисов в соответствии с настоящей Конвенцией;

2) третья страна или международная организация, заключившая соглашения, признает на своей территории (под своей юрисдикцией) юридическую эквивалентность услуг, оказываемых операторами доверенных сервисов, прошедшими процедуру подтверждения соответствия согласно части 5 статьи 8 настоящей Конвенции, и услуг, оказываемых операторами доверенных сервисов, уполномоченными в соответствии с законодательством третьей страны или международной организации, с которой заключено соответсвтующее соглашение.

Глава VII.
ЗАЩИТА ПРАВ И ИНТЕРЕСОВ УЧАСТНИКОВ ТРАНСГРАНИЧНОГО ЭЛЕКТРОННОГО ВЗАИМОДЕСТВИЯ

Статья 22
Судебная защита

1. Электронные документы и электронные сообщения, включая результаты использования доверенных сервисов, описанных в статьях 15 – 20 настоящей Конвенции, принимаются как доказательство во всех судах, арбитражных судах государств-участников.

2. Субъективное право, удостоверенное электронным документом, имеет такую же судебную защиту, как и право, удостоверенное документом в бумажной форме.

Статья 23
Внесудебная защита

1. Координационный совет утверждает правила административного разбирательства споров, возникающих в ходе трансграничного электронного взаимодействия в рамках централизованного сегмента трансграничного пространства доверия.

2. Участники трансграничного электронного взаимодействия вправе заключать двусторонние и многосторонние соглашения о порядке рассмотрения споров, возникающих при осуществлении трансграничного электронного взаимодействия.

Глава VIII. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Статья 24
Иные соглашения

1. Государства-участники настоящей Конвенции добровольно принимают на себя обязательство привести в соответствие заключенные между ними многосторонние или двусторонние соглашения в отношении трансграничного электронного взаимодействия в соответствии с настоящей Конвенцией.

Статья 25
Ратификация Конвенции

1. Настоящая Конвенция открыта до «__»_____ года для подписания от имени любого члена Организации Объединенных Наций, а также от имени любого государства, которое является или впоследствии станет членом какого-либо специализированного учреждения Организации Объединенных Наций, или любого другого государства, которое будет приглашено Генеральной Ассамблеей Организации Объединенных Наций.

2. Настоящая Конвенция подлежит ратификации, и ратификационные грамоты депонируются у Генерального секретаря Организации Объединенных Наций.

3. Любое государство вправе присоединиться к настоящей Конвенции, и грамоты о присоединении депонируются у Генерального секретаря Организации Объединенных Наций.

4. Любое государство может при подписании или ратификации настоящей Конвенции или при присоединении к ней заявить, что эта Конвенция распространяется на все или некоторые территории, за международные отношения которых оно несет ответственность. Такое

заявление вступает в силу одновременно с вступлением в силу настоящей Конвенции в отношении этого государства.

Статья 26
Вступление в силу

1. Настоящая Конвенция вступает в силу на девяностый день, считая со дня депонирования третьей ратификационной грамоты или грамоты о присоединении.

2. Для каждого государства, ратифицирующего настоящую Конвенцию или присоединяющегося к ней после депонирования третьей ратификационной грамоты или грамоты о присоединении, настоящая Конвенция вступает в силу на девяностый день после депонирования этим государством своей ратификационной грамоты или грамоты о присоединении.

Статья 27
Денонсация

1. Любое Договаривающееся государство может денонсировать настоящую Конвенцию письменным уведомлением на имя Генерального секретаря Организации Объединенных Наций. Денонсация вступает в силу через год со дня получения этого уведомления Генеральным секретарем.

2. Любое государство, которое сделало заявление или уведомление на основании статьи 25, может в любое время впоследствии заявить в уведомлении на имя Генерального секретаря Организации Объединенных Наций, что действие настоящей Конвенции в отношении соответствующей территории прекратится через год со дня получения этого уведомления Генеральным секретарем.

3. Настоящая Конвенция будет применяться в отношении арбитражных решений, дела о признании и приведении в исполнение которых были начаты до вступления в силу денонсации.

Статья 28
Уведомления

Генеральный секретарь Организации Объединенных Наций уведомляет государств-участников о нижеследующем:

а) о подписании и ратификациях;

б) о присоединениях согласно;

в) о дне вступления настоящей Конвенции в силу;

г) о денонсациях и уведомлениях.

Статья 29
Язык

1. Настоящая Конвенция, русский, английский, испанский, китайский и французский тексты которой являются равно аутентичными, хранится в архиве Организации Объединенных Наций.

Статья 30
Оговорки

Согласно настоящей Конвенции никакие оговорки не допускаются.