

РЕАЛИЗАЦИЯ КОНЦЕПЦИИ «ТРЕТЬЕЙ ДОВЕРЕННОЙ СТОРОНЫ» НА БАЗЕ ТЕХНОЛОГИЙ ГОСУДАРСТВЕННОЙ ЭЛЕКТРОННОЙ ПОЧТОВОЙ СИСТЕМЫ

Д.К. Овсянникова, к.э.н., Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, d.ovsyannikova@digital.gov.ru;

А.В. Шишов, АО «Почта России», Alexander.Shishov@russianpost.ru;

А.М. Кухаренко, Московский технический университет связи и информатики, a.m.kukharenko@mtuci.ru.

УДК 656.8

Аннотация. В данной статье авторами рассматриваются технологии государственной электронной почтовой системы (далее также – ГЭПС) в части их применимости при построении доверенного пространства юридически значимых коммуникаций участников гражданско-правовых и административно-правовых отношений.

Ключевые слова: электронная подпись; третья доверенная сторона; юридически значимые коммуникации; государственная электронная почтовая система; почтовая связь.

IMPLEMENTATION OF THE CONCEPT OF «THIRD TRUSTED PARTY» ON THE BASIS OF TECHNOLOGIES OF THE STATE ELECTRONIC POSTAL SYSTEM

Daria Ovsyannikova, Candidate of Economic Sciences, Ministry of Digital Development, Communications and Mass Media of the Russian Federation;

Aleksandr Shishov, Russian Post JSC;

Alexandra Kukharenko, Moscow Technical University of Communications and Informatics.

Annotation. In this article the authors consider the technologies of the state electronic mail system in terms of their applicability in building a trusted space of legally significant communications of participants in civil law and administrative law relations.

Keywords: electronic signature; third trusted party; legally significant communications; state electronic postal system; postal service.

Введение

Законодательство Российской Федерации содержит ряд правовых норм, регулирующих правоотношения по применению информационных технологий при обеспечении юридически значимых коммуникаций. Вместе с тем такие нормы носят разрозненный характер, содержатся в правовых актах различного уровня и различных сфер правоприменения.

Указанные положения при этом направлены на регулирование составляющих элементов процесса, не обеспечивая единого регулятивного пространства для «полного цикла» электронного взаимодействия, который должен включать в себя подпроцессы создания, подписания, обмена, обработки, хранения и уничтожения электронных документов, а также закрепление фактов действий (бездействий), осуществленных в рамках таких подпроцессов [1].

В ответ на сохраняющуюся неопределенность правового ландшафта в области обеспечения единого цикла электронного взаимодействия, учитывая невозможность кодификации разрозненных норм, органы государственной власти

предпринимают попытки решения указанной проблемы через закрепление межотраслевой суперсущности – «доверенной третьей стороны» (далее также – ДТС), в задачи которой должно входить обеспечение пространства доверия между различными участниками делового оборота. При этом на уровень ДТС делегируются полномочия, реализация которых силами самих участников коммуникации может быть затруднена вследствие угрозы недобросовестных действий сторон [2].

Однако в законодательстве Российской Федерации отсутствуют единообразные решения по построению и функционированию системы доверенных цифровых юридически значимых коммуникаций по схеме «полного цикла». Вышесказанное обуславливает актуальность проведенного исследования.

Объектом исследования выступают технологии государственной электронной почтовой системы. Предметом исследования является применимость технологий государственной электронной почтовой системы при построении доверенного пространства юридически значимых коммуникаций участников гражданско-правовых и административно-правовых отношений.

Целью данного исследования является определение возможности построения доверенного пространства юридически значимых коммуникаций участников гражданско-правовых и административно-правовых отношений на базе технологий ГЭПС.

Для достижения указанной цели в исследовании будет решен ряд задач:

- 1) составление перечня технологий ГЭПС, обеспечивающих исполнение функций, связанных с коммуникациями участников делового оборота;
- 2) проведения анализа технологий на предмет их необходимости и достаточности для построения доверенного пространства.

Полный цикл документооборота

Законодательство Российской Федерации рассматривает документ как сумму следующих квалифицирующих признаков: материальный носитель, зафиксированная на нем информация и реквизиты, позволяющие определить или идентифицировать экземпляр документа¹. Таким образом, состав содержащейся документированной информации не влияет на свойство «документности». Вместе с тем в экономической деятельности использованию подлежат только документы, влекущие или подтверждающие возникновение определенных прав и обязанностей участников такой деятельности. Так, документированная форма свойственна договорам, закрепляющим сделку в письменной форме. И хотя документированная форма вызывает повышенные транзакционные издержки на заключение сделки, она обеспечивает их снижение для процессов администрирования сделки, которые в свою очередь, включают исполнение договорных условий, оспаривание фактов их исполнения и учет фактов коммерческой деятельности.

Рассматривая жизненный цикл сделки, П. Рожков выделяет этапы прокьюремента (возникновение потребности в сделке, формулирование условий, поиск и проверка контрагента), подготовки и согласования текста договора, его подписания (создания) и доставки участникам, исполнения (включая оспаривание), учета и прекращения. Таким образом, договорная деятельность представляет собой не столько факт закрепления сторонами определенных условий в конкретный момент, сколько распределенную во времени структуру, которая выстраивается на

¹Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов».

основе узловых событий на треке жизненного цикла сделки и особого типа связей, скрепляющих такие события (факты) между собой [3].

Уязвимость любого из этих элементов способна привести к разрушению всей структуры при внешнем злонамеренном воздействии (к примеру, в случае если недобросовестный поставщик ищет возможность избежать ответственности за срыв сделки за счет попытки признания ее условий недействительными). При этом можно констатировать определенную делопроизводственную асимметрию, при которой количество юридически значимых документов, необходимых для закрепления и формализации указанных узлов и связей, возрастает по мере продвижения по указанным этапам [4].

Для упрощения реализации этапов жизненного цикла сделки участники делового оборота обращаются к рыночному предложению соответствующих услуг юристов, сервисов электронного документооборота, удостоверяющих центров, электронных архивов. Вместе с тем в текущих рыночных условиях организации, предоставляющие соответствующие услуги, сосредоточены на развитии узкой специализации на одном-двух из всех этапов жизненного цикла сделки. Это не только повышает совокупные затраты на пользование такими услугами, но и вызывает новые проблемы, к примеру, связанные с отсутствием взаимного роуминга между операторами электронного документооборота или с различиями в используемых форматах машиночитаемых доверенностей к электронным документам². Взамен поставщики таких услуг способны предложить более содержательные и многогранные способы пользования услугами, что востребовано, в основном, в исключительных нетиповых случаях.

Единая экосистема

Объединение подпроцессов, входящих в жизненный цикл сделки, в рамках единой экосистемы цифровых сервисов позволит устранить избыточные затраты участников делового оборота, снять риски контрагента и компрометации чувствительных данных, а также обеспечить единое пространство доверия для участников коммуникации различного уровня [5].

Претендентами на статус такой экосистемы могут считаться структура Доверенной третьей стороны по Федеральному закону «Об электронной подписи», Единый портал государственных и муниципальных услуг (ЕПГУ) и Государственная электронная почтовая система (ГЭПС).

Законодательство Российской Федерации определяет³ ДТС как юридическое лицо, осуществляющее деятельность по проверке электронной подписи в электронных документах в конкретный момент времени в отношении лица, подписавшего электронный документ, для обеспечения доверия при обмене данными и электронными документами. Электронной подписью является «информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и, которая используется для определения лица, подписывающего информацию»⁴.

Технология электронной подписи позволяет обеспечить неизменность электронного документа, установление личности подписанта, установление даты и

² Приказ Минцифры России от 18.08.2021 № 858 «Об утверждении единых требований к машиночитаемым формам документов о полномочиях».

³ Федеральный закон от 27.12.2019 № 476-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи», Федеральный закон «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

⁴ Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

времени создания документа. Вместе с тем указанная технология сама по себе не обеспечивает возможность проверки полномочий лица, подписавшего электронный документ, проверки фактов надлежащего направления и получения электронных документов, обеспечения процедур корректного хранения и уничтожения документов [6, 7].

Таким образом, текущая реализация ДТС «электронной подписи» не позволяет поддержать полный цикл документа и требует расширения или реинтерпретации для обеспечения всех потребностей участников делового оборота.

Единый портал государственных и муниципальных услуг (далее – ЕПГУ), изначально задуманный как способ «выпрямления» взаимодействия государства и граждан, в последние годы претендует на включение в контур своего влияния не только административно-правовых, но и гражданско-правовых отношений [8]. Указанный мотив прослеживается от реализации функции «запись к врачу» до последних законодательных инициатив по превращению личного кабинета пользователя ЕПГУ в центр обмена «юридически не значимыми» сообщениями между пользователями. Однако превращению ЕПГУ в единую экосистему электронных коммуникаций препятствует государственный статус этой системы и, как следствие, наблюдается отсутствие защиты конфиденциальных данных, передаваемых оператору ЕПГУ, от использования таких данных в целях государственного управления.

Оператор ГЭПС является оператором почтовой связи. Все почтовые отправления, посредством которых документы передаются между контрагентами, регистрируются, а факт их перемещения фиксируется автоматизировано и может быть подтвержден документально. При этом обеспечивается тайна почтовой связи⁵, а несанкционированный доступ к содержимому почтовых отправлений влечет за собой уголовное наказание⁶. Указанные преимущества распространяются как на бумажные, так и на электронные почтовые отправления [9, 10].

Технологии ГЭПС

ГЭПС представляет собой информационную систему организации федеральной почтовой связи, предназначенную для обмена почтовыми отправлениями, пересылаемыми в форме электронного документа, с возможностью гибридной доставки таких отправлений. Гибридная доставка предусматривает возможность преобразования почтового отправления из электронного документа в отправление на бумажном носителе и оцифровку бумажных почтовых отправлений в форму электронного документа. Принципы такого обмена закреплены в Правилах оказания услуг почтовой связи⁷, а постановлениями Правительства Российской Федерации⁸ ГЭПС прямо предписана к использованию ряду органов исполнительной власти при реализации их функций.

⁵ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).

⁶ Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ.

⁷ Утверждены приказом Минкомсвязи России от 31.07.2014 № 234.

⁸ Постановления Правительства Российской Федерации от 19.06.2021 № 947 «Об утверждении Правил направления экземпляров постановлений и копий решений по жалобам на постановления по делу об административном правонарушении и материалов, полученных с применением работающих в автоматическом режиме специальных технических средств, имеющих функции фото- и киносъемки, видеозаписи, или средств фото- и киносъемки, видеозаписи, лицу, в отношении которого возбуждено дело об административном правонарушении, в форме электронного документа, подписанного усиленной квалифицированной электронной подписью уполномоченного должностного лица, с использованием Единого портала государственных и муниципальных услуг», от 17.08.2021 № 1358 «Об использовании федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» для информирования граждан и организаций о направлении им от государственных органов, органов местного самоуправления, государственных и муниципальных учреждений, иных организаций,

Рассмотрим технологии и особенности ГЭПС, обосновывающие обретение ГЭПС статуса экосистемы, обеспечивающей полный цикл документооборота и наиболее содержательную реализацию концепции ДТС на практике.

Среди требований к таким технологиям можно выделить не только соответствие нормативным правовым актам и обычаям делового оборота, но и необходимость обеспечения всех этапов жизненного цикла документа в целом, а не отдельных его этапов [11, 12]. При этом к ДТС не применяются требования обеспечения этапов, которые, хотя и относятся к жизненному циклу сделки, тем не менее не подразумевают необходимости их фиксации. К примеру, не требуется сохранение истории редакторских правок по проекту договора до момента его представления на согласование контрагента.

В части прокьюременты от ДТС требуется аутентифицировать и идентифицировать участвующих в заключении сделки субъектов, обеспечить удостоверение личности физических лиц, подтвердить их правоспособность и полномочия действовать от имени юридических лиц (при необходимости). Этот этап позволяет уже на этапе подготовки договора значительно снизить риск контрагента [13]. Юридическая значимость действий, реализуемых на данном этапе, обеспечивается за счет совокупности технических, организационных и логистических преимуществ ГЭПС. К таковым относятся: сервис использования удаленной идентификации участников электронного взаимодействия посредством подтвержденных учетных записей ЕСИА (федеральная государственная информационная система «Единый портал государственных и муниципальных услуг/функций»), сервис выдачи простых электронных подписей «Почты России»⁹ *Pochta.ID*, сервис выдачи УКЭП аккредитованным удостоверяющим центром «Почты России», право использования сервисов проверки контрагентов СПАРКС, Прима-Информ.

Ключевым преимуществом организации федеральной почтовой связи является всероссийская сеть из более чем 38 000 отделений почтовой связи, в каждом из которых можно легитимно удостоверить личность посетителя с юридически значимым закреплением факта удостоверения личности. Отметим, что такой возможностью пользуются, в том числе Госуслуги в целях подтверждения учетной записи пользователя. Удостоверив личность руководителя организации и проверив его полномочия посредством сервисов ЕСИА и ЕГРЮЛ ФНС России, ГЭПС предоставляет руководителю возможность как личного участия в дальнейшем информационном взаимодействии, так и делегирования такого участия работникам организации, чья личность также устанавливается оператором [14].

В части согласования договора ГЭПС предоставляет возможность обмена регистрируемыми почтовыми отправлениями, подписанными усиленными квалифицированными электронными подписями либо, как допускают Правила оказания услуг почтовой связи, простой электронной подписью [15]. Файлы почтовых отправлений хранятся в ГЭПС с возможностью доступа отправителя и адресата к оригиналу направленного почтового отправления бессрочно. Указанный сервис также применим и при подписании договора. Несмотря на то, что почтовое отправление с текстом договора может быть подписано сторонами простой электронной подписью, такой договор, тем не менее, будет считаться заключенным в силу части 2 статьи 434 Гражданского кодекса Российской Федерации, в соответствии с которой Договор в письменной форме может быть заключен путем

осуществляющих публично значимые функции, уведомлений и (или) документов в почтовых отправлениях в форме электронного документа».

⁹ Правил оказания услуг почтовой связи, утвержденных приказом Минкомсвязи России от 31.07.2014 № 234.

обмена письмами. Задача ГЭПС в указанном процессе состоит в том, чтобы проверить неизменность содержимого двух почтовых отправок и удостоверить личности участников подписания (процедура, реализованная на этапе прокьюременты) [16].

В ряде случаев законодательство требует направить договор (его копию) контрагенту или третьим лицам. Сервис ГЭПС обеспечивает это требование за счет предоставления доступа к файлу ровно в том виде, в котором он был разослан между контрагентами, а юридическая значимость такого направления обеспечивается за счет фиксации фактов доступа к хранимому почтовому отправлению (электронному документу) и невозможностью такого доступа без надлежащего установления личности. При этом участники правоотношений также имеют возможность получить бумажную копию договора, воспользовавшись сервисом гибридизации (печати) почтовых отправок. Исполнение договора фиксируется в электронной форме посредством обмена электронными закрывающими документами, при этом в организации федеральной почтовой связи – операторе ГЭПС действует проект по предоставлению услуг оператора ЭДО, результаты которого могут быть использованы при обеспечении функционирования ГЭПС как ДТС. Комплекты документов, подготовленных в рамках взаимодействия между контрагентами, могут быть загружены в электронный архив ГЭПС. При этом учитывая, что сервисы ГЭПС и ЭДО предоставляются в настоящее время как самостоятельные, интеграция их в единый процесс документооборота обеспечивает перспективу синергетического эффекта [17].

В процессе исполнения договора создаются закрывающие документы – акты и накладные. Вместе с тем для подпроцессов оспаривания событий по сделке важны не только факты наличия документов, но и факты инициации их подписания, отказа от их подписания сторонами. Оператор почтовой связи по правовому содержанию своей деятельности не только доставляет почтовое отправление от отправителя адресату, но и обеспечивает фиксацию действий отправителя и адресата, направленных на отправку, получение или уклонение от получения (неявку за почтовым отправлением). Надлежащая фиксация уклонения от получения почтового отправления реализована за счет широкой сети отделений почтовой связи: непосредственно по почтовому адресу адресата доставляются извещения о поступлении почтовых отправок. Факт неявки за почтовым отправлением или выраженный в иной форме отказ от получения, тем не менее, в дальнейшем приравнивается судами как факт надлежащего извещения адресата о поступлении ему информации, содержащейся в направленных документах^{10,11}. Таким образом, оператор ГЭПС имеет рыночное преимущество в вопросах обеспечения оспаривания за счет фиксации фактов действий (бездействий) с документами.

Подпроцессы учета и хранения обеспечиваются за счет функций бессрочного хранения электронных документов, обеспечения актуальности их электронных подписей¹². При этом значимым элементом является фиксация

¹⁰ В соответствии с абз. 2 ст. 165.1 ГК РФ «сообщение считается доставленным и в тех случаях, если оно поступило лицу, которому оно направлено (адресату), но по обстоятельствам, зависящим от него, не было ему вручено или адресат не ознакомился с ним».

¹¹ В соответствии с п. 64 Постановления Пленума Верховного Суда РФ от 23.06.2015 № 25 «О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации».

¹² Сервис будет реализован в рамках исполнения требований проектируемого федерального закона о внесении изменений в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации (в части использования и хранения электронных документов), законопроект № 1173189-7.

оператором ГЭПС действий над хранимым документом: такие действия осуществляются с подтверждением личности лица, получающего доступ, метки времени такого доступа. Удобство сервиса также обеспечивается за счет поисковых фильтров и возможности создания «публичных ссылок» на документ с правом предоставления конкретным лицам или распространения на неограниченный круг лиц.

При реализации указанных подпроцессов в рамках экосистемы доверенной третьей стороны каждому значимому действию оператор ГЭПС присваивает свой идентификатор (ШПИ для направляемых документов и *hid* для фактов действий с ними).

Заключение

Технологии ГЭПС способны обеспечить полный цикл электронного документооборота. Ключевыми технологиями, гарантирующими доверие контрагентов в рамках ДТС, являются: подтверждение лица, коммуницирующего в пространстве доверия, проверка его правоспособности, независимая фиксация фактов в рамках подпроцессов жизненного цикла документооборота, неизменность документов и гарантия их доставки адресату, надлежащие уведомления контрагентов о юридически значимых событиях, хранение электронных документов и возможность подтверждения всех фактов, зафиксированных ДТС, при взаимодействиях с третьими сторонами (судами, проверяющими и контролирующими органами).

Таким образом, авторами определена возможность построения доверенного пространства юридически значимых коммуникаций участников гражданско-правовых и административно-правовых отношений на базе технологий ГЭПС.

Литература

1. Корниенко А.А. Повышение эффективности функционирования службы доверенной третьей стороны // Защита информации. Инсайд, 2018. – № 1 (79). – С. 49-54. – EDN YRENKH.
2. Лошкарев А.В. Правовые аспекты регулирования цифровой среды доверия // Международный журнал гуманитарных и естественных наук, 2020. – № 9-2 (48). – С. 172-175. – DOI 10.24411/2500-1000-2020-11053. – EDN RWZEVN.
3. Цикл сделки: что это такое и как его сократить // Журнал «Генеральный директор» URL: <https://www.gd.ru/articles/10798-tsikl-sdelki> (дата обращения: 26.06.2023).
4. Абдыгалиев А.А. Взаимное признание электронной цифровой подписи странами Евразийского экономического союза в сфере государственных закупок // Молодой исследователь: вызовы и перспективы: Сборник статей по материалам ССVII международной научно-практической конференции, Москва, 06 апреля 2021 года. Том 12 (207). – Москва: Общество с ограниченной ответственностью «Интернаука», 2021. – С. 58-67. – EDN GMDQRB.
5. Конева Н.С. Цифровизация государства и государственной власти // Право цифровой среды: Монография. Под редакцией Т.П. Подшивалова, Е.В. Титовой, Е.А. Громовой. – Москва: Общество с ограниченной ответственностью «Перспект», 2022. – С. 232-244. – EDN XSMNUE.
6. Курусев К.Н. Проблемы и перспективы использования электронной подписи в Российской Федерации // Актуальные проблемы публичного права: Сборник научных трудов Всероссийской научно-практической конференции, Владимир, 23 мая 2019 года – 24 мая 2020 года / Редколлегия: О.Н. Дядькин (пред.) [и др.]. Том

- Выпуск 10. – Владимир: Общество с ограниченной ответственностью «Издательство «Шерлок-Пресс», 2020. – С. 245-250. – EDN JVMVBU.
7. Проблемы и перспективы применения электронной цифровой подписи в международной // *Advances in Science and Technology*: сборник статей XXXVI международной научно-практической конференции, Москва, 30 апреля 2021 года. – Москва: Общество с ограниченной ответственностью «Актуальность.РФ», 2021. – С. 290-293. – EDN CUNDRY.
8. Алексеева А.И. доверенная третья сторона // *Электронный бизнес: проблемы, развитие и перспективы*. Материалы XIX Всероссийской научно-практической интернет-конференции, Воронеж, 28-29 мая 2021 года. Под редакцией В.В. Давниса. – Воронеж: Воронежский государственный университет, 2021. – С. 136-139. – EDN FNNOID.
9. Соловяненко Н.И. Правовой формат цифрового взаимодействия и сервисы электронной подписи в Республике Саха (Якутия) // *Роль Республики Саха (Якутия) в развитии российской федеративной государственности: Сборник докладов участников круглого стола*, Москва, 12 апреля 2022 года. – Казань: Общество с ограниченной ответственностью «Бук», 2022. – С. 117-120. – EDN LXCERM.
10. Варламова Л.Н. Международный опыт стандартизации хранения электронных документов: доверенная третья сторона // *Делопроизводство*, 2022. – № 2. – С. 91-95. – EDN LKOSJU.
11. Смирнов Е.Е. Электронная подпись станет надежнее // *Аудитор*, 2020. – Т. 6. № 4. – С. 3-9. – DOI 10.12737/1998-0701-2020-3-9. – EDN DLIPBL.
12. Чурсина Т.И., Крысенкова Н.Б. Тенденции цифровизации исполнительной власти в зарубежных странах: Научно-практическое пособие. Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. – Москва: Инфотропик Медиа, 2021. – 222 с. – ISBN 978-5-9998-0366-5. – EDN QTFHAJ.
13. Терещенко Л.К. Единая цифровая среда доверия как условие формирования цифровой экономики // *Информационное право*, 2020. – № 4. – С. 12-15. – EDN GGZMUU.
14. Фролова А.В. Использование электронной подписи в международном таможенном информационном обмене: проблемы и пути их решения // *Цифровая таможня и «Единое окно»: тренды и содержание: Сборник материалов научно-практической конференции*, Москва, 12 мая 2017 года / ГКО УВО «Российская таможенная академия». – Москва: Российская таможенная академия, 2017. – С. 87-90. – EDN ZVENOR.
15. Кустов В.Н., Силантьева Е.С. Технологии использования сервисов валидации электронной подписи в трансграничном электронном документообороте // *Мягкие измерения и вычисления*, 2020. – Т. 32. – № 7. – С. 54-77. – EDN GZHJFC.
16. Фортунатов А.Н. Цифровизация власти или власть цифровизации? // *Власть в XXI веке. Социокультурные аспекты политических процессов: Монография*. Под общ. ред. М.И. Рыхтика, А.Н. Фортунатова. – Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2020. – С. 37-47. – EDN RRAHHR.
17. Имамвердиев Я.Н. Архитектура инфраструктуры доверия электронным документам в среде электронного государства // *Телекоммуникации*, 2011. – № 11. – С. 18-26. – EDN ONHVXL.