Технологические подходы к обеспечению юридически значимого взаимодействия в облачных услугах

С.Л. Горелик, В.С. Ляпер

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Общество с ограниченной ответственностью «Компания «Демос»
samgor46@gmail.com, vitaly@lyaper.com

Аннотация

В настоящей статье дается обзор технологических подходов для обеспечения юридически значимых электронных взаимодействий, применимых для современных типов электронных услуг (в том числе облачных услуг).

Рассматривается понятие юридической значимости электронных взаимодействий в контексте технической реализации, классифицируются типы электронных взаимодействий, предлагается технологический сценарий использования технических средств, на основе серверных реализаций услуг информационной безопасности.

Введение

Юридическая значимость для электронных взаимодействий означает, что все действия, совершенные с их помощью, могут быть, в случае необходимости, предъявлены в виде доказательств в судебном или административном разбирательстве.

Большинство существующих систем основаны на современных криптографических алгоритмах и реализуются на аппаратно-программном уровне. Широкое развитие «облачных» технологий, которые основаны на использовании распределенных систем, требует специального подхода к реализации, чтобы эффективно использовать преимущества последних. Фундаментальный принцип распределённых систем - **для пользователя система должна выглядеть как нераспределённая система** [1], - должен неукоснительно соблюдаться. Из этого принципа вытекает ряд требований к технической реализации, которые должны учитываться при создании систем обеспечения юридической значимости в электронных коммуникациях.

К наиболее быстро растущим сегментам IT рынка, в которых принцип юридической значимости особенно актуален, можно отнести следующие:

- электронная и мобильная коммерция;
- финансовые и платежные системы;
- системы государственных и ведомственных услуг;
- системы межведомственного документооборота;
- системы защиты приоритетов и авторских прав.

Увеличение спроса на электронные услуги и развитие цифровых технологий связи привело к массовому переходу на web-mail и отказ от технологии server-mail, то есть, к видоизменению привычной концепции предоставления услуг клиент-сервер на «облачные» услуги.

Высокая доступность и простота использования делают их весьма привлекательными, но есть определенные препятствия их массовому внедрению, которые до сих пор являются предметом дискуссий технических специалистов, юристов и государственных чиновников.

В реальном мире уже выработаны механизмы, позволяющие построить между людьми договорные отношения, придать им юридически значимый статус и в дальнейшем защитить интересы субъектов этих отношений, а также, при необходимости, разрешить их в суде. Когда пользователь оказывается в периметре электронных услуг, все становится гораздо сложнее – механизмы, аналогичные привычным (нотариат, подпись, печать) либо не выработаны, либо не внедрены. Совершенно ясно, что сосуществование «электронной» и «бумажной» технологий будет продолжаться еще достаточно долгое время и должно учитываться в разработках.

Между тем, поскольку все больше действий из реального мира, таких как, заключение сделок, платежные транзакции или деловая переписка совершаются с помощью электронных услуг, возникает необходимость придания им юридической значимости. **Принцип аналогии электронного и бумажного (традиционного) документооборота** [2] является одним из важнейших для успешного внедрения современных технологий. Этот принцип формулируется следующим образом: между системой существующего бумажного документооборота и системой юридически значимого электронного докумен-

Труды XV Всероссийской объединенной конференции «Интернет и современное общество» (IMS-2012), Санкт-Петербург, Россия, 2012.

тооборота действует принцип соответствия (аналогии) юридических требований и регламентов.

1. Электронные средства обеспечения юридической значимости

Как было отмечено ранее, появляется все больше видов электронных коммуникаций, которые могут стать предметом судебных или административных отношений и должны, поэтому, быть юридически значимы.

Федеральное законодательство [3] устанавливает несколько видов электронной подписи (простую, усиленную неквалифицированную и усиленную квалифицированную).

В любом виде электронная подпись должна:

- обеспечить установление факта изменения подписанного электронного документа после момента его подписания (подлинность);
- обеспечить практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

В настоящей работе, в основном, рассматриваются электронные взаимодействия трех видов субъектов: граждане (C), бизнес (B) и государство (G), причем, основное внимание уделяется системам C2C, C2B (B2C), C2G (G2C), главной особенностью которых является участие физических лиц в качестве одного из участников взаимодействия. Причины, по которым основное внимание уделено именно физическим лицам, следующие:

- достаточно большое количество транзакций во всех сегментах, связано с физическими лицами, выступающими как независимые граждане или как сотрудники организаций и предприятий;
- для массового использования необходимо создание простых механизмов, которые были бы понятны как с технической, так и с юридической точек зрения, пользователям (такие механизмы в настоящее время очень ограничены – именно поэтому принцип аналогии бумажного и электронного документооборота очень важен);
- стоимость услуг на приобретение и эксплуатацию усиленной квалифицированной подписи, которая применяется во взаимодействии между предприятиями и организациями (типа B2B и B2G) слишком высока для массового использования гражданами, а предлагаемая для указанных целей система в портале госуслуг имеет не удобный интерфейс и не покрывает все потребности рынка.

Следует отдельно подчеркнуть, что, несмотря на то, что определяются несколько видов электронной подписи, каждый из них, при соблюдении определенных условий может являться гарантией юридической значимости электронного взаимодействия. Так, например, простая электронная подпись может обеспечивать юридическую значимость, если между субъектами, использующими такую подпись, заключено соглашение, в котором определено использование простой электронной подписи в качестве подтверждения юридической значимости.

Однако, понятие простой подписи появилось сравнительно недавно, и практика её использования пока не столь велика. В то же время, простая (и, в некоторой степени, усиленная) подпись привлекательна для реализации взаимодействий с участием граждан, так как использует более простые и дешевые средства электронной подписи.

Средства электронной подписи – это технологические решения, с помощью которых создается и проверяется подпись. Традиционно для этих целей используются связки из программных и аппаратных компонентов. К аппаратным компонентам относятся персональные устройства типа смарт-карт или криптографических токенов, обладающие собственной памятью, процессором, с встроенными криптографическими средствами.

Привычные средства электронной подписи отличаются рядом технических ограничений, которые не позволяют им найти широкое распространение среди «домашних» пользователей. Можно выделить следующие ключевые ограничения при использовании токенов и смарт-карт как средств электронной подписи:

- необходимо наличие специальных разъемов (для токенов обычно это USB типа A) или специальных устройств-считывателей, которые позволяют работать со смарт-картами (такие разъемы есть не на всяких устройствах, например с находящими все большее распространение планшетными компьютерами традиционные средства ЭП несовместимы);
- необходимо предустанавливать на пользовательской системе специализированное ПО – Crypto Service Provider (CSP) – для вызова функций токена или смарт-карты, соответствующее ПО существует не под все виды аппаратных платформ и операционных систем;
- стоимость использования такого средства ЭП складывается обычно из двух факторов – стоимости CSP и самого токена, а также стоимости сертификата ключа ЭП, выдаваемого аккредитованным удостоверяющим центром.

Перечисленные выше ограничения по использованию средств электронной подписи отражаются на распространении ЭП среди различных групп пользователей. Основное применение электронной подписи в сфере B2B – участие в различного рода торгах, а также государственных закупках. По данным удостоверяющих центров, количество сертификатов ЭП выпущенных для этих целей в некоторых случаях уже переваливает за миллион [4]. При этом, в случае взаимодействия, в котором участвуют физические лица, например использование электронной подписи при доступе на портал государственных услуг, число выданных ключей электронных подписей составляет по некоторым данным на июль 2012 г. незначительный процент потенциальных пользователей [5].

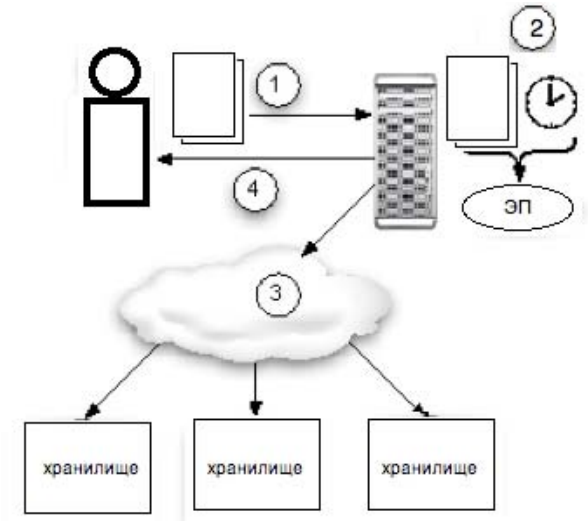

Рис 1. Заверение документа электронной цифровой печатью

На основании анализа существующих тенденций и имеющегося опыта, с учетом сформулированных выше требований, предлагается следующая схема для реализации цифровой подписи в рассматриваемом классе задач (рис 1) [3].

Заверение документа электронной печатью производится следующим образом:

1. Отправка документа через Интернет на сайт, выдающий электронные печати.
2. Создание электронной печати на основе документа, времени его поступления на сайт (и идентификатора пользователя).
3. Размещение копий электронной печати в независимых хранилищах (на не модифицируемых носителях).
4. Передача пользователю копии электронной печати.

2. Средства юридической значимости, применимые для облачных услуг

Низкое распространение среди «домашних» пользователей технологий электронной подписи объясняется как стоимостью такого решения, так и невысокой степенью его удобства. К этому добавляется невозможность использования существующих средств ЭП с мобильными коммуникаторами и планшетными компьютерами, которые многие пользователи все чаще предпочитают в качестве альтернативы обычным компьютерам.

Таким образом, для физических лиц требуются средства электронной подписи нового типа, которые лишены перечисленных выше недостатков, просты в использовании и обеспечивают мобильность пользователей. В идеале, с прицелом на дальнейшее развитие, услуги предоставления электронной подписи также станут облачными и, тем самым, станут доступнее для массового пользователя.

Решением может стать использование средств электронной подписи на стороне сервера, вместо привычных клиентских – токенов и смарт-карт. Электронная подпись на стороне сервера – концепция использования электронной подписи без её привязки к физическому носителю ключа электронной подписи, пригодная для использования в облачных платформах и с любым пользовательским устройством доступа (в т.ч. мобильный телефон или планшет).

Технология электронной подписи на стороне сервера основывается на нескольких базовых принципах (рис.2):

- ключ электронной подписи хранится на удаленном сервере с использованием аппаратных средств защиты, гарантирующих доступ к ключу только пользователя, которому этот ключ принадлежит;
- ключ никогда не покидает защищенный периметр сервера в открытом виде, все операции с ключом подписи, в том числе непосредственно формирование электронной подписи выполняются внутри аппаратного модуля безопасности в защищенной памяти, наружу выдается только результат криптографического преобразования с использованием ключа;
- доступ к ключу электронной подписи производится только после аутентификации пользователя, аутентификация основывается на многофакторной схеме с использованием стойких механизмов аутентификации;
- каждая операция с ключом электронной подписи требует подтверждения со стороны пользователя;
- передача документа для подписи и её подтверждение должны производиться по независимым каналам связи.

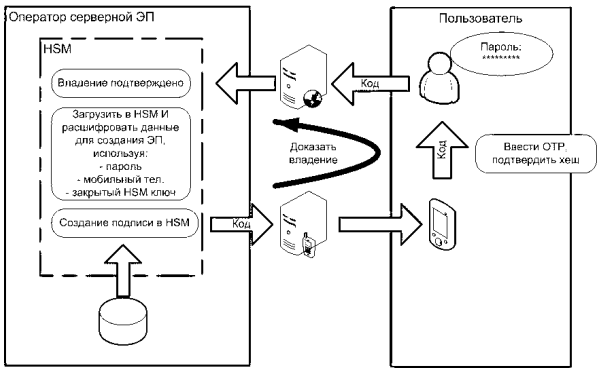

Рис. 2. Схема реализации электронной подписи на стороне сервера [6].

Процедура регистрации пользователя в системе электронных коммуникаций является одним из важнейших компонентов, от структуры которого и качества интерфейсов зависит usability системы.

В настоящее время в большинстве приложений (в том числе, в банковских и государственных услугах) обязательна **первичная (полная) регистрация** пользователя, во время которой производится его аутентификация на основе предъявляемого документа и привязка выдаваемого идентификатора к

его личности [2]. В государственных услугах используется в качестве идентификатора номер СНИЛС, а, в дальнейшем, предполагается использование Универсальной Электронной Карты и Мобильного Телефона (коммуникатора) [7]. В любом случае юридическая значимость в полном объеме может быть достигнута только после реализации указанной процедуры первичной регистрации. Однако, в практических применениях возможны подходы, использующие процедуру **предварительной регистрации** [2, 8, 9], в которой до момента необходимости совершения каких-либо взаимодействий, требующих юридической ответственности участников, допускается привязка пользователя к идентификатору без процедуры его аутентификации. Полная регистрация производится только тогда, когда пользователь начинает использовать услуги, требующие аутентификации. Такой подход существенно повышает привлекательность и доступность ряда электронных услуг.

Ключи, пароли и другие дополнительные идентификаторы, которые хранятся в облачном хранилище, доступны пользователю в течение пользовательской сессии через предъявление основного идентификатора, полученного при первичной (и, иногда, при предварительной регистрации).

При аутентификации пользователя может быть задействован дополнительный фактор в виде одноразового пароля, присылаемого пользователю на телефон [10]. Система аутентифицирует пользователя, определяет связанный с пользователем номер мобильного телефона и перенаправляет пользователя на страницу создания электронной подписи, где пользователь загружает на сервер документ, который он хотел бы подписать.

Для полученного документа система (в «электронной канцелярии») считает значение хеш-функции, и генерирует одноразовый пароль (OTP – one-time-password), который вместе с значением хеш-функции передается пользователю через SMS. Посчитанное значение хеш-функции также отображает на веб-форме с которой работает пользователь.

Получив SMS с хеш-значением и одноразовым паролем, пользователь сверяет полученное значение и то, которое он видит на экране. Теперь он может подтвердить транзакцию подписи, введя в форму значение полученного одноразового пароля и нажав кнопку «Подписать». Передача одноразового пароля и хеш-значения необходимы, чтобы доказать, что пользователь в данный момент хочет подписать документ.

После получения подтверждения транзакции подписи от пользователя, система загружает в память аппаратного модуля безопасности (HSM – Hardware Security Module, устройство для безопасного хранения ключей и выполнения криптографических операций, в т.ч. электронной подписи) закрытый ключ пользователя и документ, который надо подписать. Подпись формируется внутри модуля безопасности, в закрытой памяти, тем самым избегается использование ключа в незащищенном сегменте. Подписанный документ возвращается пользователю в виде, доступном для скачивания, создание электронной подписи завершено.

Столкнувшись впервые с электронной подписью на стороне сервера, многие пользователи оказываются в растерянности – концепция использования своего ключа электронной подписи в удаленном режиме несколько расходится с привычной схемой, когда ключ всегда при тебе. В этой связи закономерно возникают некоторые вопросы, ответы на самые популярные из них приводятся ниже.

Каким образом обеспечивается защищенность ключа пользователя?

В сервисе электронной подписи на стороне сервера безопасности ключей уделяется особое внимание поскольку сам пользователь не может влиять на безопасность ключа на сервере, задача сервиса обеспечить достаточный уровень информационной безопасности, чтобы такая необходимость отпала. Для обеспечения информационной безопасности в сервисах электронной подписи используются специализированные аппаратные средства – Hardware Security Module (HSM – аппаратный модуль безопасности).

HSM – это устройство, которое обеспечивает безопасность ключей пользователя, а также позволяет производить операции с этими ключами, не раскрывая самого ключа в открытой памяти и вообще вовне этого устройства. Ближайшая аналогия с HSM – это большая смарт-карта, которая доступна всем пользователям системы. Все операции с ключами пользователей внутри HSM разделяются по идентификаторам пользователя, таким образом гарантируется, что вы получите доступ только к своему ключу. Перед использованием своего ключа пользователь должен аутентифицироваться и только после этого он сможет получить доступ к функциям, работающим с его ключом пользователя. Сами ключи пользователя никогда не покидают пределов HSM, даже такая операция, как загрузка ключей, может не производиться по соображениям безопасности, ключи могут генерироваться непосредственно внутри HSM, таким образом гарантируется, что они никогда не будут скомпрометированы.

Ключ лежит на стороне сервера, а токен всегда с собой – разве вторая схема безопасней?

Хранение ключа подписи самим пользователем несет в себе определенные риски. В подписываемом при первичной регистрации собственноручной подписью или ее законным аналогом договоре, указывается, что передача ключа третьим лицам является зоной ответственности пользователя и рассматривается как выдача им доверенности на проведение соответствующих операций).

В случае серверной ЭП ключ находится всегда внутри HSM (как печать в сейфе) и никогда оттуда не выходит, а доступ к нему гарантируется хорошо защищенными средствами, полученными при первичной идентификации и аутентификации.

Как гарантируется, что только пользователь сможет воспользоваться своим ключом?

Чтобы воспользоваться своим ключом, пользователю надо авторизоваться с помощью своего идентификатора, полученного при первичной регистрации (например, через получение на мобильный телефон одноразового кода). Кроме того, в системе ЭП на стороне сервера реализуется подтверждение каждой транзакции с помощью одноразового пароля, передаваемого пользователю через SMS, что обеспечивает дополнительный оперативный контроль использования своего ключа.

Насколько предложенная схема соответствует требованиям законодательства?

Предложенная схема полностью соответствует требованиям закона от 06.04.2011 N 63-ФЗ «Об электронной подписи», базовый вариант подписи, которая реализуется в схеме – простая электронная подпись. Стоит отметить, что требования закона, предъявляемые к усиленной и квалифицированной электронной подписи, касаются главным образом вопросов связанных с сертификатом ключа подписи и аккредитацией удостоверяющего центра, выпустившего сертификат. Таким образом, предложенная схема, без изменения при взаимодействии с соответствующим удостоверяющим центром может быть расширена до уровня усиленной квалифицированной электронной подписи.

3. Сценарии применения средств юридической значимости для облачных услуг

Технологические достоинства рассмотренного сервиса электронной подписи (например, не нужно запоминать большое количество паролей и иметь несколько аппаратных носителей) делают эту схему привлекательной для использования. Данная схема также позволит различным группам пользователей значительно сэкономить и получить новые технологические возможности.

Для граждан – простых пользователей – нет необходимости покупать дорогие токены и ПО к ним, срок жизни виртуального токена практически не ограничен, можно использовать мобильные телефоны и планшеты и получать на них подписанные документы, которые соответствуют требованиям законодательства и подпись под ними проверяется стандартными средствами.

Для бизнеса – это в первую очередь возможность аутсорсинга инфраструктуры электронной подписи. Сейчас чтобы обеспечить сотрудников организации средствами ЭП, необходимо устанавливать дополнительное ПО, прописывать регламенты использования ЭП, следить за жизненным циклом токенов и смарт-карт, в случае серверной электронной подписи все эти действия не нужны, организация получает сервис «под ключ» от поставщика такой услуги. Таким образом, можно снизить капитальные затраты на использование электронной подписи в организации с полным сохранением всех возможностей, которые предоставляет использование ЭП.

Для государства – важнейшим преимуществом использования серверной ЭП является возможность охватить очень широкую аудиторию пользователей (на текущий момент это 70 млн. пользователей сети Интернет, 150 млн SIM-карт у мобильных пользователей) государственными услугами, которые требуют юридически значимого взаимодействия. При этом, возможно организовать возврат инвестиций в систему электронной серверной подписи для государства за счет включения стоимости транзакции подписи в обычную государственную пошлина, взимаемую за услугу.

Отметим, что технология серверной ЭП на сегодняшний день является наиболее подходящей для использования в облачных услугах всех типов, вне зависимости от того, кто их предоставляет бизнес или государство. С учетом закрепившейся тенденции к переходу в облака это делает указанный подход весьма актуальным в сложившихся условиях.

Что касается непосредственно услуг и бизнес-сценариев использования электронной подписи на стороне сервера, следует отметить, что это в первую очередь уже привычные услуги с использованием ЭП – электронный документооборот (ЭДО), подача документов в ведомства и организации. Кроме того, среди услуг и сценариев использования электронной подписи на стороне сервера можно выделить относительно новые варианты использования технологии.

Системы облачного документооборота, которые в настоящее время получают все большее распространение, в т.ч. в государственных органах. Ключевым моментом использования облачных систем ЭДО является работа через тонкого клиента (веб-браузер), когда использование традиционных средств ЭП затруднено. Как было рассмотрено выше в настоящей статье сценарий использования ЭП на стороне сервера позволяет применять её для облачных систем ЭДО;

Электронная почтовая служба, как её частный случай Государственная электронная почтовая служба (ГЭПС) – концепция client-server email, к которой мы привыкли, когда есть сервер электронной почты, общение с которым происходит посредством клиентского приложения, уходит в прошлое, сейчас все предпочитают читать почту в окне браузера. В таком случае, традиционные средства обеспечения целостности и конфиденциальности сообщений, такие как S-MIME, становятся не актуальными, требуется встраивать средства информационной безопасности в серверное приложение. Решить эту проблему можно как раз с использованием электронной подписи на стороне сервера.

Электронное взаимодействие с клиентами, электронные платежи, электронный биллинг – использование даже простой ЭП на стороне сервера при работе с клиентами, может существенно упростить взаимодействие клиента и поставщика услуг. При первичном заключении договора на предоставление услуг достаточно включить пункт соглашения об использовании простой ЭП, чтобы полностью

перевести дальнейшее взаимодействие с клиентом в электронную форму. Таким образом, клиент сможет совершать юридически значимые сделки, проводить платежи, требующие его аутентификации, получать различного рода выписки и финансовые документы, подписанные электронной подписью. При этом, организация, использующая такую схему взаимодействия с клиентом, уже начинает экономить только за счет того, что вместо бумажных транзакций используются более дешевые электронные.

В переходный период через сертифицированные центры (например, нотариусов) может быть обеспечена юридически значимая услуга перевода электронных документов в «бумажные» и наоборот, что позволит резко расширить существующий рынок юридически значимых электронных коммуникаций и ускорить переход на электронный документооборот.

Государственные электронные услуги, в первую очередь, требуют обязательной юридической значимости всех выполняемых действий. При этом число пользователей государственных электронных услуг в конечном счете не меньше трудоспособного населения страны. Обеспечить такое число пользователей средствами ЭП без существенных затрат можно только используя ЭП на стороне сервера, когда стоимость клиентской части минимальна, и получение средств ЭП максимально упрощено. С использованием средств ЭП на стороне сервера можно также решить важнейшие проблемы предоставления государственных электронных услуг – аутентификацию пользователя и контроль целостности документов, принимаемых в электронном виде.

Заключение.

Следует отметить, что современные тенденции в инфокоммуникациях – переход к облачным технологиям, рост количества транзакций требующих юридической значимости, – диктуют необходимость обеспечивать юридическую значимость для новых облачных услуг. При этом существующие средства такие, как электронная подпись на клиенте, оказываются непригодными для облачных услуг, а, иногда, просто неприменимыми для пользователей мобильных устройств (мобильные телефоны, коомуникаторы, планшеты).

Назрела необходимость в новом, подходе к обеспечению юридически значимого взаимодействия, когда средства электронной подписи привязываются не только к физическому носителю, а к пользователю. В этом случае, обеспечение юридической значимости возможно на всех уровнях электронных взаимодействий вне зависимости от того, кто является субъектом этих взаимодействий – физическое лицо, бизнес или государство.

Литература

[1] Таненбаум Э., ван Стеен М. Распределенные системы. Принципы и парадигмы. СПб.: Питер, 2003.

[2] Комплексное исследование вопросов обеспечения граждан Российской Федерации и органов государственной власти электронной почтовой связью. // Отчёт о научно-исследовательской работе. Шифр темы ЦА/05-10, № госрегистрации 01201065830.

[3] Федеральный закон № 63-ФЗ «Об электронной подписи».

[4] Выдано рекордное количество сертификатов электронной цифровой подписи // Удостоверяющий центр СКБ «КОНТУР» [Электронный ресурс]. URL: http://ca.skbkontur.ru/about/news/127/ (дата обращения 14.09.2012).

[5] «Почта России» будет выдавать ЭЦП для доступа к порталу госуслуг [Электронный ресурс]. URL: http://www.itsec.ru/newstext.php?news_id=85867 (дата обращения 14.09.2012).

[6] Kustor P. Austrian mobile phone signature // Centre for eGovernance Development [Электронный ресурс]. URL: http://www.cegd.eu/public/files/eeeGovDays_Kustor.pdf (дата обращения 14.09.2012).

[7] Государственная программа "Информационное общество (2011 - 2020 годы)" // Департамент государственных целевых программ и капитальных вложений Минэкономразвития России [Электронный ресурс]. URL: http://fcp.economy.gov.ru/cgi-bin/cis/fcp.cgi/Fcp/ViewFcp/View/2012/369/ (дата обращения 14.09.2012).

[8] Горелик С.Л. Система дистанционной экспресс регистрации субъектов и документов. Заявка на патент № 2012109045, приоритет от 12.03.2012 г. Решение о регистрации патента от 14.05.2012 г.

[9] Научно-технический отчет по проекту «Честный интернет». Свидетельство о регистрации: 07N-4R-RJ. Дата: 01.05.2011. Электронный регистратор «COPYTRUST» .

[10] Aloul F., Zahidi S., El-Hajj W. Two Factor Authentication Using Mobile Phones // Fadi Aloul's Home Page [Электронный ресурс]. URL: http://www.aloul.net/Papers/faloul_aiccsa09.pdf (дата обращения 14.09.2012).

Technical Approaches for Relevant in Law Electronic Communications in Cloud Services

S. Gorelik, V. Lyaper

In the present article the review of technological approaches for ensuring relevant in law electronic interactions applicable for modern types of electronic services (including cloudy services) is given. The concept of the relevant in law electronic interactions of a context of technical realization is considered, types of electronic interactions are classified, the technological scenario of use of means, on the basis of server realization of services of information security is offered.