Об одной реализации системы электронного документооборота с юридической значимостью

О. А. Славин, И. М. Янишевский

Институт системного анализа Российской академии наук,
Россия, 117312 Москва, пр. 60-летия Октября, 9

В статье на примере системы сбора заявок на проведение государственных и муниципальных закупок рассматриваются автоматизированные системы обмена электронными документами, обеспечивающие юридическую значимость на основе применения электронной цифровой подписи и сервисов удостоверяющего центра. Показано, каким образом в ассоциации государственных организаций реализуются следующие характеристики электронных документов: авторство, неотказуемость от подписания, целостность и т. п. Описано, как именно реализуется юридическая значимость электронных документов как для пользователей, работающих в системе, так и для внешних пользователей.

Введение

Рассматривая вопросы реализации юридически значимого электронного документооборота, мы будем использоваться следующие определения:

- *система электронного документооборота* (СЭД) — автоматизированная система для обеспечения делопроизводства (регистрации, учета, хранения, списания документов) и обмена документами в электронной форме [1]. Обычно под СЭД понимают программное обеспечение (ПО), хотя есть смысл рассматривать и иные виды обеспечения СЭД, такие как техническое и нормативно-правовое;
- *внутренний пользователь СЭД* — пользователь, присоединившийся к правилам работы системы, т. е. являющийся сотрудником организации, которая эксплуатирует данную СЭД;
- *неприсоединившийся пользователь СЭД* — физическое лицо, не присоединившееся к правилам работы системы, но просматривающее

созданные в СЭД электронные документы без возможности их модификации;

- *корпоративная СЭД* — такая СЭД, электронные документы которой не предназначены для использования внешними субъектами;
- *доверие к электронному документу* (ЭД) — отношение, основанное на уверенности в соответствии использования электронного документа заранее известному набору требований, аналогичных требованиям к бумажным документам;
- *юридическая значимость электронного документа* — признак документа, позволяющий ссылаться на него как на имеющего юридическую силу, и использовать данный электронный документ для обоснования своих действий либо защиты своих прав в судебном порядке.

В общем виде СЭД не способны обеспечить юридическую значимость электронного документа [2]. Основные причины этого состоят в отсутствии регламентации на уровне законодательства РФ порядка получения, передачи и хранения электронных документов.

Возможен и альтернативный взгляд на принципиальную возможность использования электронных документов. В работе [5] указывается, что «письменными доказательствами являются содержащие сведения об обстоятельствах, имеющих значение для рассмотрения и разрешения дела, акты, договоры, справки, деловая корреспонденция, иные документы и материалы, выполненные в форме цифровой, графической записи, в том числе полученные посредством факсимильной, электронной или другой связи либо иным позволяющим установить достоверность документа способом» (Федеральный закон РФ от 14.11.2002 г. № 138-ФЗ «Гражданский процессуальный кодекс РФ», ст. 71 // СЗ РФ от 18.11.2002 г. № 46, ст. 4532). Это обстоятельство, по мнению авторов [5], позволяет утверждать, что «электронные документы также представляют собой письменную форму на новой технологической основе».

Сказанное означает, как минимум, возможность создания отдельных СЭД, обеспечивающих юридическую значимость электронных документов в конкретных условиях функционирования СЭД. Известен способ [3], состоящий в регулировании отношений между пользователями корпоративной СЭД на основе договора присоединения к регламенту работы системы. Эффективность этого способа гарантируется Гражданским кодексом РФ (Федеральный закон РФ от 14.11.2002 г. № 138-ФЗ «Гражданский процессуальный кодекс РФ», ст. 426 ГК РФ), при этом договор в целом или его отдельные статьи не должны противоречить законам и иным правовым актам РФ. В этом случае пользователи, не присоединившиеся к СЭД, не могут создавать и изменять электронные документы внутри системы, сле-

довательно, судебное разбирательство относительно электронного документа в этих ситуациях не возникает. Случай оспаривания неприсоединившимся субъектом подлинности опубликованных электронных документов может разрешаться в суде на основании бумажных копий электронных документов, которые заверяются печатью организации и подписью руководителя.

Популярными являются попытки придания документам юридической значимости с помощью электронной цифровой подписи (ЭЦП). При этом используются возможности инфраструктуры открытых ключей (ИОК, PKI) для решения задачи обеспечения доверия к электронным документам, подписанным цифровой подписью пользователями, обладающими сертификатами открытых ключей, выданными удостоверяющими центрами (УЦ). Существенна роль УЦ, которые публикуют регламент работы пользователей, в частности поддерживающие сервисы целостности и неотказуемости от совершенных действий, что способствует приданию юридической силы электронным документам, подписанным ЭЦП.

В настоящей работе мы рассмотрим весь комплекс проблем, обеспечивающих реализацию СЭД с юридической значимостью. Рассмотрение будет производиться на примере системы, предназначенной для сбора заявок на проведение государственных и муниципальных закупок и планирование подготовки закупок в субъекте РФ или муниципальном образовании РФ, т. е. СЭД является частью автоматизированной системы проведения государственных закупок, описанных в [3, 4]. Будет показано, что юридическая значимость реализуется на основе следующей совокупности возможностей электронного документа:

- *авторство* электронного документа, обеспечиваемое ЭЦП;
- *обеспечение неотказуемости* от подписания в прошлом некоторого электронного документа с проставленной личной ЭЦП *конечного субъекта* (т. е. владельца закрытого ключа ЭЦП);
- *проверка целостности*, т. е. отсутствие изменений в электронном документе и всех его свойствах;
- *обеспечение актуальности содержимого* электронного документа, принятого из другой организации;
- *архивное хранение* электронного документа;
- *обеспечение конфиденциальности*, реализуемой за счет шифрования информации;
- *верификация средствами СЭД*, т. е. с помощью программного обеспечения, входящего в состав СЭД;
- *верификация альтернативными средствами*, не входящими в состав СЭД.

1. Использование инфраструктуры открытых ключей для создания СЭД сбора заявок и планирования государственных и муниципальных закупок

Рассмотрим процессы, обеспечивающие сбор заявок на проведение закупок и подготовку публикации извещений о проведении муниципальных и государственных закупок. Организационная схема одного из таких процессов приведена на рис. 1.

Совокупность организаций и их взаимодействие соответствуют модели, приведенной в [6]. Множество организаций упорядочено отношениями подчинения: для каждой организации, кроме уполномоченного органа на проведение закупок, существует *вышестоящая организация*, принимающая входные заявки на размещение госзаказа и создающая на их основе сводные документы. Бумажные документы передаются из одной организации в другую как в конвертах, так и в открытом виде. Последнее возможно, если в документах не содержится закрытой информации, например данные в заявках о проводящихся закупках уже опубликованы в законе о закупках на текущий год. В случае, когда в документе содержатся персональные данные, документ должен быть передан в конверте.

При проектировании СЭД должны быть учтены различные способы электронного взаимодействия между организациями — участниками документооборота:

- постоянное подключение к серверу вышестоящей организации;
- электронная почта;
- отсутствие выхода в Интернет.

В результате создаваемая СЭД должна обладать такими видами обеспечения, чтобы электронные аналоги бумажных документов (заявка, письмо с отказом, документация для публикации) и системные электронные документы (такие как пакет обновления настроек и справочников, системный журнал) обладали легитимностью с точки зрения пользователей СЭД. Легитимность должна быть обеспечена при всех способах подключения. Для обеспечения юридической значимости не менее важна легитимизация электронных документов вне СЭД, прежде всего с точки зрения их использования в судах.

Рассмотрим различные аспекты создания СЭД с применением ЭЦП для описанной организационной структуры. Отметим, что нормативно-правовая база не может основываться в полной мере на Федеральном законе № 1-ФЗ от 10.01.2002 «Об электронной цифровой подписи». Действительно, гл. I, п. 2, ст. 1 указанного закона гласит: «Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении

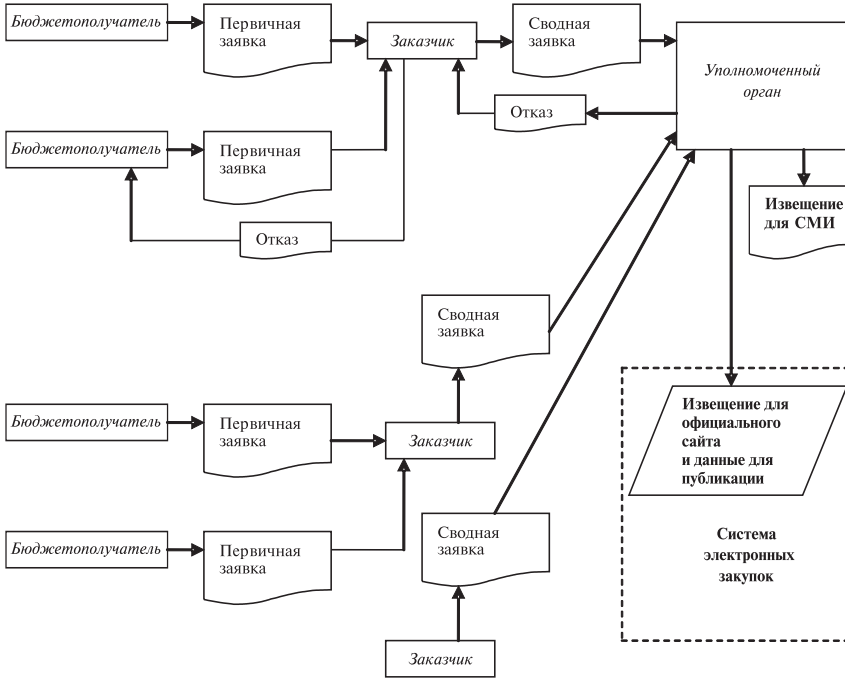

Рис. 1. Организационная схема процессов подготовки проведения закупок

гражданско-правовых сделок, и в других предусмотренных законодательством Российской Федерации случаях». Обмен документами между организациями не относится к числу сделок. Правовые же отношения, такие как подача налоговой декларации в электронном виде или участие в конкурсе поставок для государственных нужд (и иные отношения, перечисляемые в федеральных законах), также не имеют отношению к документообороту. Иными словами, отношения, возникающие в процессе обмена электронными документами, в законе об ЭЦП прямо не урегулированы, а применение гражданского законодательства, регулирующего сходные отношения по аналогии, неочевидно для участников обмена. Тем самым нормативное обеспечение СЭД должно включать регламенты и методики работы пользователей СЭД, устанавливающие типовые процедуры работы с электронными документами на протяжении всего жизненного цикла электронного документа, и требования к выполнению этих операций. Разумеется, регламенты и методики должны максимально соответствовать Федеральному закону № 1-ФЗ и полностью соответствовать регламенту и политике безопасности удостоверяющих центров, выдающих сертификаты и ключи.

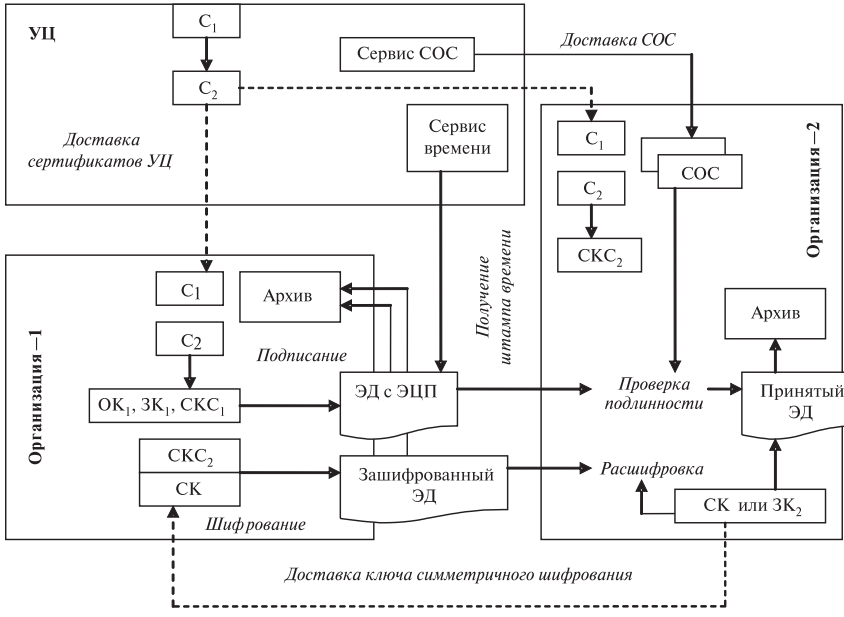

Рис. 2. Схема ИОК

Отметим необходимое соответствие в части гл. IV, п. 1, ст. 16 рассматриваемого закона. «Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, а также организации, участвующие в документообороте с указанными органами, используют для подписания своих электронных документов электронные цифровые подписи уполномоченных лиц указанных органов, организаций». Иными словами, правом подписи электронных документов должны быть наделены руководители организаций.

Организационное обеспечение СЭД, а точнее, каждой из организаций, использующих систему, должно быть построено на базе инфраструктуры открытых ключей (ИОК). Это обусловлено необходимостью реализации ЭЦП на основе открытого ключа (гл. I, ст. 3 Федерального закона № 1-ФЗ). Домен доверия ограничивается пользователями СЭД и некоторым числом неприсоединившихся пользователей. Схема ИОК организаций — участников системы приведена на рис. 2.

На приведенной схеме C_1 означает самоподписанный сертификат УЦ, C_2 — сертификат уполномоченного лица УЦ, СК — секретный (*закрытый*) ключ симметричного шифрования, $СКС_1$ и $СКС_2$ — сертификаты уполномоченных лиц — руководителей организаций 1 и 2 соответственно. Сертификаты C_1 и C_2 должны быть переданы в организации доверенным

способом, сертификат $СКС_2$ — из организации 2 в организацию 1. Подписание ЭЦП документа включает получение штампа времени, а проверка подлинности — получение списка отозванных сертификатов (СОС) с помощью соответствующих сервисов УЦ. Асимметричное шифрование использует сертификат открытого ключа $СКС_2$, симметричное — ключ, известный обеим организациям. Мы рассматриваем возможность применения симметричного шифрования по той причине, что в ГОСТ Р34.10–94, который «определяет процедуры выработки и проверки электронной цифровой подписи на базе асимметрического криптографического алгоритма с применением функции хеширования», отсутствует упоминание термина «шифрование», что может быть интерпретировано как невозможность применения алгоритма ГОСТ Р34.10–94 для шифрования. Разумеется, иная интерпретация, разрешающая применять указанный алгоритм для шифрования, разрешает процедуру шифрования с помощью открытого ключа $СКС_2$ аналогично процедуре подписания ЭЦП.

Отметим, что приведенная на рис. 2 ИОК является простейшей из возможных, так как задействован один-единственный УЦ, путь валидации также является простейшим из возможных и состоит из пути ($СКС_1$, $С_2$, $С_1$) или ($СКС_1$, $С_1$). В дальнейшем под УЦ понимаем УЦ, выдающий сертификаты и ключи пользователям СЭД.

Описанная ИОК требует работы администратора безопасности СЭД, отвечающего за сохранность сертификатов в соответствующих хранилищах и контролирующего доставку сертификатов и ключей доверенным способом.

Разбор конфликтов, носящих технический и организационный характер, возлагается на комиссии, составленные из представителей обеих организаций, персонала сопровождения СЭД и персонала УЦ.

Верификация (проверка подписанного или зашифрованного документа) должна быть возможной и для организации, которая не присоединена к СЭД. Методика проверки может отличаться от аналогичной методики для организации, которая использует систему.

Описанная ИОК позволяет реализовать сформулированные выше требования к СЭД:

- *проверку целостности* электронного документа и всех его свойств после подписания ЭЦП с помощью средств криптографической защиты информации (СКЗИ);
- *обеспечение неотказуемости* от подписания электронного документа с помощью СКЗИ и сервисов УЦ;
- *архивное хранение* электронных документов;
- *шифрование* конфиденциальной и персональной информации с помощью СКЗИ;

- *верификация средствами системы* с помощью прикладного ПО СЭД;
- *верификация альтернативными средствами*, не входящими в состав СЭД.

Программное обеспечение для подписания, шифрования и верификации электронного документа состоит из следующих элементов:

$ПО_1$ — СКЗИ (криптопровайдер);

$ПО_2$ — компонента доступа к сервису штампов времени УЦ;

$ПО_3$ — компонента доступа к сервису скачивания СОС;

$ПО_4$ — приложения, не входящие в СЭД и обеспечивающие разбор конфликтов и верификацию электронного документа;

$ПО_5$ — приложения, входящие в СЭД и обеспечивающие подписание, шифрование, разбор конфликтов и верификацию электронного документа.

Следует отметить, что внутри СЭД необходимы компоненты **$ПО_1$**, **$ПО_2$**, **$ПО_3$** и **$ПО_5$**, а в организации, не присоединившейся к СЭД, — **$ПО_1$**, **$ПО_4$**.

Доверие к программному обеспечению пользователей обеспечивается по-разному. Присоединившиеся пользователи доверяют программному обеспечению вследствие положений договора о присоединении к СЭД, вследствие постоянного опыта работы с СЭД, а также из-за комплекса мероприятий по обслуживанию рабочих мест, на которых установлены средства шифрования.

При этом доверия к СЭД со стороны неприсоединившегося пользователя не требуется, хотя не исключается использование **$ПО_5$** при проведении экспертизы при судебном разбирательстве. Доверие неприсоединившегося пользователя к своему комплекту ПО обеспечивается самим фактом его использования до момента проверки конкретного электронного документа, разумеется, если неприсоединившаяся организация уже обладает СКЗИ. Если же неприсоединившаяся организация, которая нуждается в проверке электронного документа, еще не обладает СКЗИ, то необходима установка сертифицированных СКЗИ. В последнем случае в качестве **$ПО_5$** могут быть использованы компоненты верификации разработчика устанавливаемых СКЗИ.

Отдельно стоит рассмотреть случай работы судебных экспертов с электронным документом, извлеченным из СЭД. Основным способом установления авторства подписи и проверки целостности электронного документа является использование программного обеспечения разбора конфликтов, являющегося частью ПО УЦ. Дополнительный способ описан в предыдущем абзаце.

Применение ЭЦП и средств шифрования накладывает повышенные требования к техническому обеспечению СЭД, такие как требования к хранению ключей и оснащению рабочих мест, на которых установлены средства криптографии.

Реализованная таким образом СЭД обеспечивает следующие возможности документооборота:

- ускорение обмена документами в электронной форме;
- упрощение архивного хранения документов в электронной форме;
- механизм обеспечения авторства и неизменности документа.

Последняя возможность является более простой для пользователя (организации), обладающего СКЗИ и установившего путь валидации, состоящий из цепочки $С_2$—$СКС_1$ или $С_1$—$С_2$—$СКС_1$, поскольку требуется обращение только в УЦ, а сертификат СКС извлекается из электронного документа. Для организации (участника размещения заказа, судебного эксперта) из субъекта РФ, в котором развернут УЦ, процедура доверенной передачи сертификатов УЦ является упрощенной из-за географической близости организаций.

Для реализации описанной СЭД необходимо выполнение следующих требований к нормативно-правовому обеспечению СЭД и УЦ.

1. В договоре присоединения к регламенту СЭД должны быть статьи, в которых:

- устанавливается возможность обмена только электронными документами, причем стороны обязуются не оспаривать законность и действительность электронного документа только на том основании, что они совершены в электронной форме;
- признается, что электронный документ, подписанный ЭЦП, сформированный в СЭД, имеет юридическую силу;
- стороны обязуются обеспечивать информационную безопасность и защиту электронных документов, а также рабочих мест, на которых производится подписание электронного документа ЭЦП;
- стороны обязуются применять политику безопасности в отношении сертификатов и ключевых пар, которая соответствует установленной УЦ политике безопасности.

2. Регламент СЭД должен включать «Порядок использования электронных документов».

3. Регламент УЦ должен описывать положения политики безопасности, в частности положения, имеющие отношения к подписчикам (владельцам сертификатов):

- обязательства УЦ и подписчика;
- процедуры решения споров (конфликтов);
- обязательства ведения реестра сертификатов;
- политика раскрытия информации официальным представителям правоохранительных органов;

- приостановление и аннулирование сертификата, смена секретного (закрытого) ключа;
- ведение архива в УЦ;
- генерация и инсталляция ключевых пар;
- защита ключевых пар;
- формы сертификатов и списка СОС;
- процедуры изменения политики безопасности УЦ.

Требования политики безопасности УЦ могут привести к возникновению требований к техническому обеспечению СЭД, например таких как:

- требования к техническим средствам рабочих мест, на которых производится подписание электронного документа ЭЦП;
- требования к носителям для хранения секретных ключей пользователей СЭД.

Требования к программному обеспечению СЭД будут рассмотрены в следующем разделе настоящей статьи.

Иными словами, предложенный способ построения СЭД обеспечивает юридическую значимость электронного документа, понимаемую как реализацию доверия к электронным документам, сформированных в СЭД и защищенных процедурами шифрования и подписания ЭЦП, причем проверки авторства и неизменности электронного документа не являются более сложными, чем аналогичные проверки бумажных документов.

2. Особенности программного обеспечения СЭД с юридической значимостью электронных документов

В этом разделе приводятся требования к ПО для работы с ЭЦП и шифрованием, необходимые для работы описанной выше СЭД.

Одним из главных требований к ПО для работы с ЭЦП и шифрованием является наличие сертифицированного СКЗИ на предмет соответствия требованиям ГОСТ 28147–89, ГОСТ Р34.10–94, ГОСТ Р34.10–2001, ГОСТ Р34.11–94 и требованиям ФСБ России к СКЗИ класса КС1. Прежде всего отметим, что в РФ все без исключения сертифицированные СКЗИ являются платными и выбор может зависеть от различных причин, прежде всего от совместимости с программными средствами УЦ. В нашей работе мы использовали СКЗИ **КриптоПро CSP**, которое полностью поддерживает следующие возможности операционных систем Windows:

- создание подписи;
- проверка подписи;
- получения доказательств достоверности подписи.

Кроме собственно СКЗИ **КриптоПро CSP** мы использовали:

- библиотеку **cpcrlupdate.dll** (разработана компанией **КриптоПро**) получения СОС из пункта доверия сертификата, распространяемую на условиях freeware;
- утилиту «приложения командной строки» (ПКС) **cryptcp.exe**, приобретаемую отдельно от СКЗИ **КриптоПро CSP**.

Отметим, что дополнительные программные компоненты не являются сертифицированными, доверие к ним основывается исключительно на доверии к организации-разработчику КриптоПро. Также нами была использована библиотека **CAPICOM** для обеспечения доступа к хранилищам сертификатов. На основе перечисленных программных компонент была разработана библиотека **CT_CrypoAPI**, структура которой приведена на рис. 3.

Библиотека **CT_CrypoAPI** реализует высокоуровневые функции:

- подписать документ, создав сообщение, в котором, в частности, содержится штамп времени и образ исходного документа (при необходимости);
- проверить сообщение (в частности, скачать СОС и проверить, отозван ли сертификат подписавшего) и извлечь содержащийся в нем документ;
- зашифровать сообщение;
- расшифровать сообщение;
- получить штамп времени;
- передать пописанный документ в электронный архив УЦ.

Разработка библиотеки, как модуля, предоставляющего высокоуровневые сервисы различным приложениям ПО СЭД, не является единственно возможным вариантом проектирования. Альтернативным путем является покупка аналогичного модуля, например компоненты «**ЭЦП процессор**». В нашем случае мы отказались от закупки по причине большой стоимости компоненты «**ЭЦП процессор**», требующую лицензирования для каждой из организаций, количество которых в описываемой системе может достигать нескольких сотен.

Другими программными компонентами, необходимыми для интеграции с УЦ, являются:

- **КриптоПро TSP,** предназначенная для организации сервера штампов времени;
- **КриптоПро OCSP,** предназначенная для организации сервера онлайновой проверки статусов сертификатов.

Разработанная библиотека предполагает онлайновое подключение к следующим сервисам УЦ: оперативной проверки статусов сертификатов и доверенного времени.

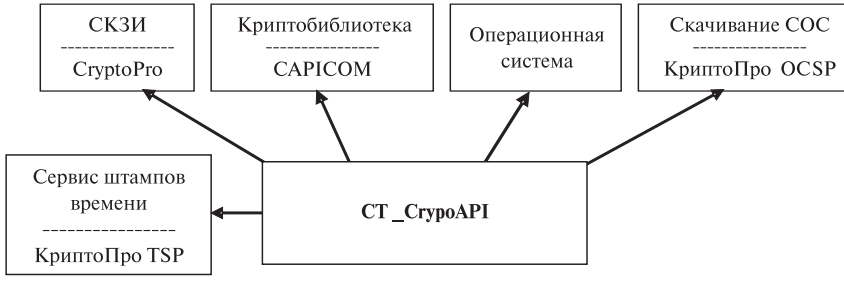

Рис. 3. Схема работы библиотеки CT_CryroAPI

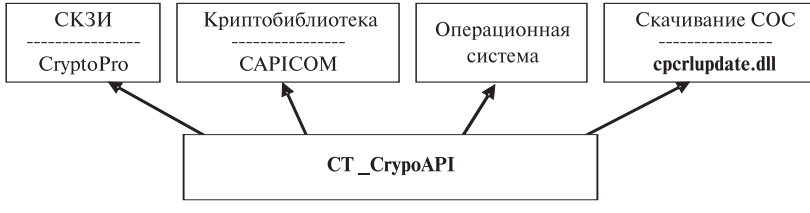

Рис. 4. Схема упрощенного режима работы библиотеки CT_CryroAPI

В отсутствии доступа к сервисам УЦ возможен упрощенный режим работы библиотеки **CT_CryroAPI** (рис. 4), в котором реализованы следующие высокоуровневые функции:

- подписать электронный документ, создав сообщение, в котором, в частности, содержится метка (не штамп) времени;
- проверить подпись и извлечь из сообщения содержащийся в нем документ (при необходимости);
- зашифровать электронный документ;
- расшифровать сообщение.

Структура сообщения спроектирована исходя из критерия совместимости с утилитой ПКС **cryptcp.exe**, которая не поддерживает усовершенствованную ЭЦП (CADES). Возможные структуры сообщения приведены на рис. 5.

В сообщениях, приведенных на рис. 5, должны находиться:

- данные, представляющие собой ZIP-архив, состоящий из одного или нескольких электронных документов и иных файлов;
- сертификат конечного пользователя;
- ЭЦП;
- штамп времени.

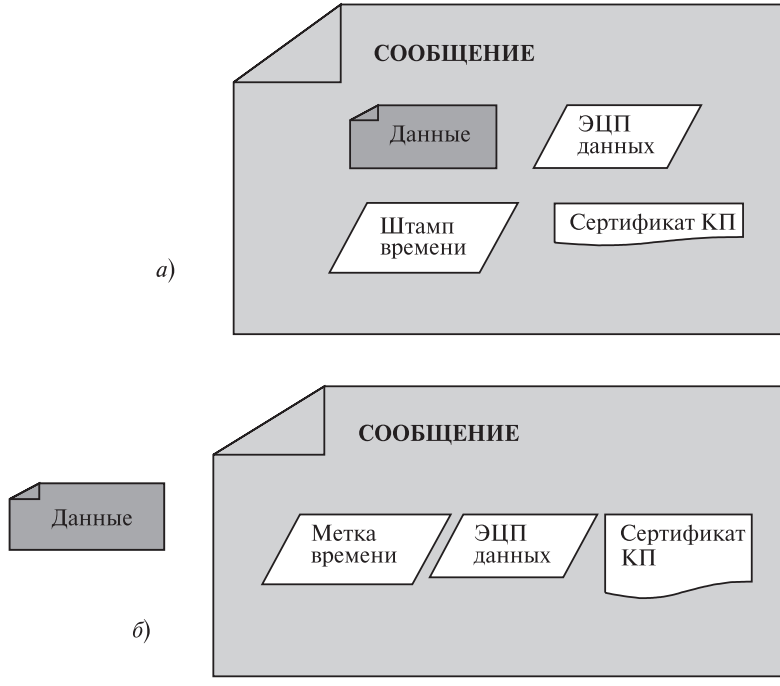

Рис. 5. Возможные структуры сообщения библиотеки CT_CryproAPI:

а) сообщение, содержащее образ подписанного файла;
б) сообщение, не содержащее образа подписанного файла

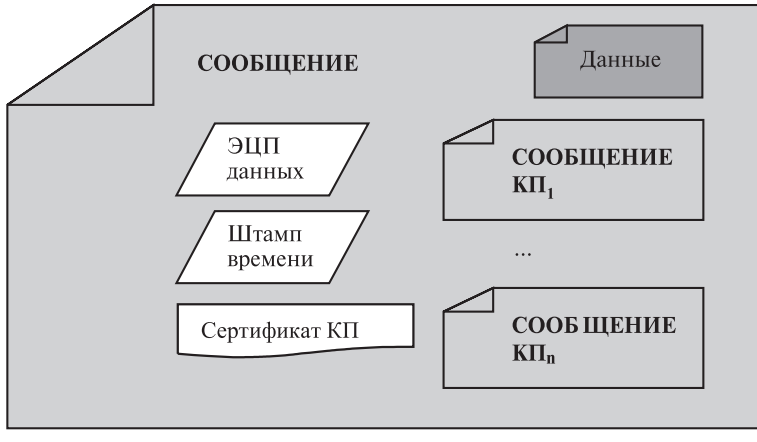

Рис. 6. Возможные структура сообщения с несколькими подписчиками

В сообщениях, приведенных на рис. 5, присутствует одна единственная ЭЦП одного подписчика. Однако возможно подписание электронного документа ЭЦП нескольких подписчиков. На рис. 6 представлена структура сообщения, содержащая:

- данные (ZIP-архив, содержащий один или несколько электронных документов);
- сообщения нескольких конечных пользователей, не содержащие данных, то есть сформированные по схеме рис. 5*б*;
- ЭЦП *основного подписчика*, то есть конечного пользователя, который заверяет данные и сообщения остальных подписчиков;
- штамп времени;
- сертификат основного подписчика.

ЭЦП основного подписчика формируется после подготовки всех сообщений $КП_1$–$КП_n$.

К АРМ, которые используют библиотеку **CT_CryproAPI** (а вместе с ним СКЗИ) предъявляются следующие дополнительные требования по безопасности:

- установленное ПО не должно содержать средств разработки и отладки приложений;
- установленное ПО не должно содержать компонент, позволяющих осуществлять несанкционированный доступ к системным ресурсам;
- необходимо проводить контроль целостности и легальности установленных копий ПО с помощью программ контроля целостности.

Рассмотрим сценарий отправки пакета исходящих электронных документов из произвольной организации, присоединившихся к СЭД. Используются два рабочих места: АРМ Специалиста и АРМ Руководителя организации. Сценарий отправки состоит из следующих этапов:

- специалист на своем АРМе выполняет всю содержательную работу по подготовке исходящих документов;
- руководитель, на АРМе которого установлены СКЗИ и сертификат УЦ, инициирует процесс подписания ЭЦП и шифрования пакета документов, предоставляя свой закрытый ключ на внешнем носителе информации, при этом подписание/шифрование осуществляется только в том случае, если сертификат ЭЦП руководителя действителен;
- ПО СЭД объединяет все документы, входящие в пакет, создавая один файл данных, который подписывается и шифруется личной ЭЦП руководителя, в результате чего образуется сообщение (см. рис. 5), содержащее образ пакета исходящих документов, ЭЦП, штамп (метка) времени и сертификат подписавшего.

При изменении исходящих документов сообщение удаляется. После отправки сообщения в вышестоящую организацию (или его публикации) исходящие документы, породившие сообщение, не могут быть изменены средствами СЭД, они помещаются в архив, из которого не могут быть удалены.

Сценарий приема входящих электронных документов реализуется на одном рабочем месте регистратора и состоит из следующих этапов:

- переданное по электронным каналам связи сообщение поступает на АРМ Регистратора, на котором установлены СКЗИ и сертификат УЦ;
- на АРМ Регистратора проверяется принятое сообщение, включая, целостность, проверки сертификата, причем СОС скачивается с адреса, извлеченного из сертификата подписчика.

В результате должно быть принято решение — корректно ли принятое сообщение. Из корректного сообщения извлекается пакет входящих документов и регистрируется в СЭД, сообщение помещается в архив, из которого не может быть удалено. Для некорректного сообщения отправителю направляется квитанция с указанием причины отказа в регистрации.

3. Обсуждение предложенного решения

Рассмотрим свойства предлагаемого решения, рассматриваемые с точки зрения различных пользователей и сведенные в таблицу (табл. 1).

Очевидно, что достоинства использования электронных документов с ЭЦП делают возможным обеспечение доверия к СЭД со стороны всех рассмотренных групп пользователей. Также отметим, что для пользователя, не доверяющего УЦ, обеспечить доверие к ЭЦП невозможно. Такому пользователю можно предложить использовать бумажные копии электронных документов, заверенные руководителями соответствующих организаций. В то же самое время недоверие пользователя к УЦ, уполномоченное лицо которого находится в едином реестре уполномоченного федерального органа исполнительной власти в области электронной цифровой подписи [7], может объясняться только психологическими причинами, а не толкованием нормативно-правовой базы ЭЦП.

Выводы

Описанные в статье принципы разработки СЭД, используемой несколькими организациями, позволяют обеспечить юридическую значимость, понимаемую как легитимность электронного документа со стороны как пользователей СЭД, так и неприсоединившихся пользователей.

Легитимность СЭД обеспечивается как легитимностью ИОК, включающей один УЦ, так и разработкой нормативно-методического обеспе-

Таблица 1

Свойства решения

Роль	Пользователь СЭД	Участник размещения	Судебный эксперт
Аналогия с бумажными документами	Традиционный сценарий подготовки, подписания, передачи и регистрации внутреннего документа СЭД	Равноценность документации, подписанной ЭЦП, копии бумажной документации	Электронный документ, рассматриваемый как доказательство, обладает всеми необходимыми реквизитами бумажного документа
Преимущества электронного документа	Архивное хранение	Подлинность документации или изменений к документации, полученных электронным способом	Надежный способ определения даты подписи электронного документа. Надежный автоматизированный способ проверки целостности и авторства электронного документа. Способ обеспечения неотказуемости
Недостатки электронного документа	–	Нет возможности получить документацию иным способом, кроме электронного	необходимость в СКЗИ и ПО для осуществления проверок
Необходимость СКЗИ и иного ПО для работы с ЭЦП	В составе СЭД	При необходимости проверки электронного документа	При необходимости проверки электронного документа при нежелании воспользоваться услугами УЦ
Причины доверия к электронному документу	Подписание договора присоединения к СЭД.	Электронный документ, подписанный ЭЦП, является оригиналом, а бумажная распечатка — копией	Несколько альтернативных способов проверок авторства и целостности электронного документа с помощью ПО различных производителей
Причины недоверия	–	Психологические	Отсутствие регламентации на уровне законодательства РФ порядка получения, передачи и хранения электронного документа

чения, технического обеспечения, общего и специального программного обеспечения.

Аналогичным образом могут быть построены СЭД, предназначенные, в частности, для обмена документами между государственными организациями, входящими в ассоциацию, решающую общие для всех организаций задачи, в масштабах домена доверия с одним УЦ.

Авторы выражают благодарность А. Ю. Боженову за ценные обсуждения.

Литература

1. *Арлазаров В. Л., Емельянов Н. Е.* Системы обработки документов. Основные компоненты // Труды ИСА РАН «Управление информационными потоками». М.: URSS, 2002. С. 3–20.
2. Доклад о применении цифровой подписи в электронном документообороте в работе государственных органов по обращениям граждан и организаций. [Электронный ресурс]: http://wiki.elrussia.ru/index.php/Доклад_о_применении_цифровой_подписи_и_электронном_документообороте_в_работе_государственных_органов
3. *Хлебутин П. С., Славин О. А.* Автоматизированная система размещения госзаказа Cognitive Лот // Труды ИСА РАН «Системный подход к управлению информацией». М.: КомКнига/URSS, 2006. Т. 23. С. 116–131.
4. *Горбунов-Посадов М. М.* Электронные государственные закупки в России // Информационные технологии и вычислительные системы. 2003. № 1–2. С. 128–144.
5. *Боженов А. Ю., Семилетов С. И.* Организация процедур конвертования в системе электронных закупок: реализация и правовое обеспечение // Сборник трудов ИСА РАН «Системный подход к управлению информацией». М.: КомКнига/URSS, 2006. С. 132–155.
6. *Акимова Г. П., Пашкин М. А., Славин О. А.* Специфика документооборота электронной торговли // Сборник трудов ИСА РАН «Документооборот. Прикладные аспекты». М.: URSS, 2005. С. 12–20.
7. Реестр уполномоченного федерального органа исполнительной власти в области электронной цифровой подписи. [Электронный ресурс]: http://www.reestr-pki.ru