Организация процедур конвертования в системе электронных закупок: реализация и правовое обеспечение

А. Ю. Боженов, С. И. Семилетов

В статье рассматриваются методы и механизмы обеспечения конфиденциальности коммерческой информации, которые могут быть использованы при организации и проведении открытых и закрытых конкурсов по закупкам для государственных нужд в электронной форме в режиме интерактивного удаленного доступа.

В настоящее время все большее количество сделок совершается в электронном виде без участия бумажных носителей. Это приводит к тому, что механизмы, обеспечивающие конфиденциальность информации, разработанные для «бумажного» формата, необходимо перенести на формат электронных документов. Требуется разработать адекватную им замену, которая позволила бы достичь не меньшего уровня сохранности и защиты электронных документов, обращающегося на всех этапах проведения конкурса.

При проведении открытых или закрытых конкурсов по закупкам для государственных нужд, организатор конкурса в соответствии с требованиями Федерального закона от 21.07.2005 г. № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд» получает закрытые заявки с предложениями от потенциальных поставщиков, которые, в целях обеспечения установленных Законом требований, должны быть запечатаны в конверты. Целостность конвертов может заверяться печатями поставщиков-участников конкурса. Заявка в конверте содержит конкретные предложения участника конкурса по предполагаемым поставкам, неизвестные до поры другим участникам конкурса, а также организатору торгов, и вскрывается в соответствии с установленными правилами в момент проведения и подведения итогов конкурса. Победителем конкурса объявляется поставщик, заявка которого содержит наилучшие предложения по условиям конкурса.

Ограничение доступа к содержанию заявки и защита информации в запечатанных конвертах является важным условием конкурса, поскольку в

случае утечки информации о предложении конкурента до проведения конкурса, отдельные лица в корыстных целях могут повлиять на результаты конкурса в пользу заранее установленного поставщика. При этом пострадает как заказчик в лице государства, который будет вынужден тратить дополнительные бюджетные средства, так и остальные участники конкурса, потерявшие контракты.

Для электронных заявок закон устанавливает процедуру открытия доступа к заявкам на участие в конкурсе, находящимся в информационной системе общего пользования, поданным в форме электронных документов и подписанным в соответствии с нормативными правовыми актами Российской Федерации.

В настоящей работе предпринята попытка предложить протоколы организации процедур электронного конвертования (т. е. заключения электронных документов в электронные аналоги конвертов) при проведении электронных открытых или закрытых конкурсов по закупкам для государственных нужд, гарантирующие конфиденциальность коммерческой информации, а также проверить их на юридическую чистоту и соответствие требованиям Федерального закона от 21.07.2005 г. № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд» (далее по тексту Закон «О размещении заказов…»).

1. Правовое обеспечение процедур конвертования

В настоящее время основными документами нормативно-правовой базы конкурсной организации закупок продукции, работ и услуг являются Гражданский кодекс Российской Федерации и Федеральный закон «О размещении заказов…».

Указанный Закон при организации и проведении конкурсов устанавливает и регламентирует процедуру конвертования заявок участников конкурса и их вскрытия при подведении итогов конкурса. На первом этапе в соответствии с п. 2 ст. 25 этого Закона заявка на участие в открытом конкурсе оформляется участником конкурса в письменной форме и подается в запечатанном конверте в порядке, предусмотренном организатором открытого конкурса в конкурсной документации. При этом организатор открытого конкурса берет на хранение запечатанный конверт с заявкой до момента проведения конкурса и выдает расписку в получении заявки на участие в открытом конкурсе с указанием даты и времени ее получения[1].

[1]Федеральный закон от 21.07.2005 № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд» // СЗ РФ. 25.07.2005 г.. № 30 (ч. 1), ст. 3105.

На втором этапе, в соответствии со ст. 26 указанного Закона в момент проведения конкурса и подведения его итогов, запечатанные конверты с заявками участников конкурса представляются конкурсной комиссии на ее заседании в предусмотренном конкурсной документацией месте и время. При этом все присутствующие члены конкурсной комиссии и участники конкурса имеют возможность убедиться в целостности запечатанных конвертов. Председатель конкурсной комиссии в предусмотренное конкурсной документацией время вскрывает конверты с заявками на участие в открытом конкурсе в присутствии членов комиссии и участников конкурса. При этом при вскрытии конвертов с заявками присутствующим участникам открытого конкурса объявляются наименования, адреса участников открытого конкурса, цены и описание предлагаемых ими товаров (работ, услуг) и вся эта информация заносятся в протокол проведения открытого конкурса.

В Законе «О размещении заказов…», а также иных нормативно-правовых актах Российской Федерации дефиниция «письменная форма» находит очень широкое употребление, но ни один из них законодательно не определяет это понятие. Исторически требование соблюдения «письменной формы» появилось как альтернатива «устной форме» общения людей и обращения информации и сложилось как обычай делового оборота. Как правило, данный термин употребляется, когда законодатель регулирует те или иные публично-правовые или гражданско-правовые отношения и, в частности, когда устанавливает порядок реализации прав и обязанностей тех или иных субъектов отношений и устанавливает порядок документирования этих отношений. Поскольку в Законе «О размещении заказов…» (как и в целом в действующем законодательстве) термин «письменная форма» не определен, а употребления электронных форм представления документов как письменных доказательств законодательно установлены[2], то можно утверждать, что электронные документы также

[2] Письменными доказательствами являются содержащие сведения об обстоятельствах, имеющих значение для дела, договоры, акты, справки, деловая корреспонденция, иные документы, выполненные в форме цифровой, графической записи или иным способом, позволяющим установить достоверность документа» (ФЗ РФ «Арбитражный процессуальный кодекс Российской Федерации» от 24.07.2002 г. № 95-ФЗ, ст. 75 // СЗ РФ от 29.07.2002 г. № 30, ст. 3012).

«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. К письменным доказательствам относятся приговоры и решения суда, иные судебные постановления, протоколы совершения процессуальных действий, протоколы судебных заседаний, приложения к протоколам совершения процессуальных действий (схемы, карты, планы, чертежи)» (ФЗ РФ «Гражданский процессуальный кодекс РФ» от 14.11.2002 г. № 138-ФЗ, ст. 71 // СЗ РФ от 18.11.2002 г. № 46, ст. 4532).

представляют собой письменную форму на новой технологической основе и подпадают под предмет данного Закона.

Указанный Закон допускает проведение конкурсов и аукционов, обмен сведениями между организатором и участниками конкурса в письменной форме, в том числе в форме электронных документов в соответствии с требованиями этого Федерального закона. Процедуры конвертования заявок участников конкурса и вскрытия конвертов при проведении конкурсов по указанному Закону устанавливают порядок организации оборота традиционных документов на бумажном носителе как воплощением письменной формы.

Для электронных заявок Закон устанавливает процедуру открытия доступа к заявкам на участие в конкурсе, находящимся в информационной системе общего пользования, поданным в форме электронных документов и подписанным в соответствии с нормативными правовыми актами Российской Федерации.

Из вышесказанного следует, что организация и проведение конкурсов по закупкам для государственных нужд на основе применения современных информационно-коммуникационных технологий, оборота электронных документов и автоматизации всех конкурсных процедур с переводом их в электронный формат, не противоречит нормам действующего законодательства, если эти процедуры отвечают установленным требованиям Закона «О размещении заказов…». Однако, Закон не устанавливает требований к защите и безопасности размещенных в информационной системе закрытых электронных заявок, поданных на конкурсное рассмотрение.

Это пробел означает, что с точки зрения обеспечения надежности защиты содержания поданных конкурсных заявок от несанкционированной утечки информации и, соответственно, обеспечения равноправия участников конкурса, использование предложенной Законом электронной процедуры открытия доступа к поданным электронным конкурсным заявкам не обеспечивает юридическую чистоту проведения конкурса и уступает процедуре вскрытия конвертов с конкурсными заявками на бумажном носителе, поскольку сервер информационной системы, в котором будут размещаться электронные конкурсные предложения участников конкурса (заявки), как правило, находится вне контроля конкурсной комиссии и доступ к информационной системе, серверу, имеет достаточно много должностных или уполномоченных третьих лиц. Соответственно, риск утечки информации достаточно большой.

На наш взгляд, все элементы электронных процедур в полной мере должны отвечать требованиям, соответствовать установленным и отработанным процедурам проведения конкурсов на основе оборота традиционных документов, а процедура вскрытия электронных заявок конкурсной комиссией должна четко и однозначно документироваться, быть такой же надежной и подконтрольной для всех участников конкурса, как и процедура конвертования и вскрытия запечатанных бумажных конвертов.

Предлагаемый способ реализации процедуры электронного конвертования конкурсных заявок в полной мере обеспечивает юридическую чистоту проведения конкурса в электронной форме и отвечает, а по многим параметрам и превосходит, требованиям установленной процедуре конвертования конкурсных заявок и вскрытия запечатанных бумажных конвертов.

2. Обзор способов организации электронного конвертования

Рассмотрим различные схемы организации шифрования и защиты данных, применяющиеся в современной практике. Все способы организации электронного конвертования основываются на известных методах шифрования данных электронных документов, при которых формируется новый выделяемый файл, содержащий зашифрованные данные исходного документа и исполняющий по аналогии функцию запечатанного электронного конверта. Рассмотрим эти методы:

2.1. Шифрование симметричным ключом

Под ключом понимается некоторый (обычно не очень большой) бинарный массив данных, создаваемый на основе некоторого протокола. При шифровании симметричным ключом один и тот же ключ используется как для шифрования, так и для дешифрования данных. Примерами симметричных протоколов являются международные алгоритмы AES, RC2, Triple DES и отечественный ГОСТ 28147-89. К достоинствам таких алгоритмов можно отнести их высокую криптостойкость (устойчивость к взлому) и скорость работы, однако такие алгоритмы плохо применимы при обмене зашифрованной информацией при наличии большого и постоянно меняющегося круга респондентов (участников конкурсов), поскольку ключ должен быть известен обеим сторонам, передающим файл. Будучи перехвачен во время передачи от одной стороны к другой, ключ позволит расшифровать любые скрытые данные (см. рис. 1). К сожалению, в условиях открытой сети интеренет невозможно гарантировать надежность канала между отправителем и получателем, поэтому участники обмена должны использовать другие способы передачи ключа (личная встреча, курьерская служба), что чрезмерно усложняет процесс подготовки к передаче данных. Более того, каждый из участников конкурса должен обладать уникальным ключом, который может быть использован только один раз, поскольку велик риск утечки ключа в момент дешифрации полученной информации. Таким образом, поддержание инфраструктуры обмена ключами превращается в трудноразрешимую задачу.

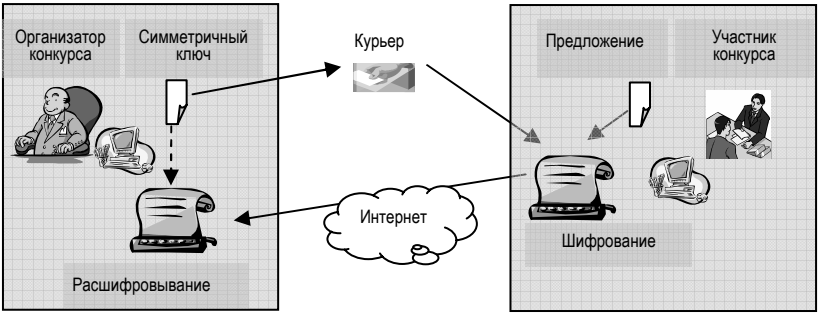

Рис. 1. Схема с симметричным ключом

2.2. Несимметричное шифрование (шифрование с открытым ключом)

В данной схеме для работы с данными используется два связанных ключа (открытый и закрытый). При шифровании с открытым ключом, данные, зашифрованные одним ключом из пары, могут быть расшифрованы только вторым, причем знание ключа, использовавшегося для шифрования данных, не может помочь в задаче подбора ключа расшифровки. К таким алгоритмам относятся международные RSA, DSA и российские ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001 (конечно, это стандарты ЭЦП, но могут быть применены и для шифрования). Недостатками данных алгоритмов, по сравнению с симметричными, является худшая стойкость к взлому, что вынуждает использовать значительно более длинные ключи, что в свою очередь приводит к серьезному проигрышу в скорости работы. Учитывая данные недостатки, в современной практике принято шифровать с помощью таких алгоритмов не сами защищаемые данные, а симметричный (называемый в данном контексте сессионным) ключ, который был использован для шифрования данных. То есть, сначала данные зашифровываются при помощи симметричного алгоритма, после чего сессионный ключ, размеры которого обычно не превышают 32 байт, зашифровывается несимметричным алгоритмом.

Несимметричные алгоритмы решают проблему обмена ключами. При таком подходе лицо, желающее получить зашифрованные предложения (в нашем случае — организатор конкурса), создает ключевую пару и сохраняет один из ключей, называемый закрытым, в надежном месте. Второй ключ, открытый, выкладывается в общий доступ или рассылается участникам конкурса, которые и используют его для шифрования своих предложений. Этот ключ един для всех участников в рамках одного конкурса, поскольку не может быть использован для дешифрации данных и не позволяет одним участникам «подглядеть» информацию, зашифрованную другими.

2.3. ЭЦП и сертификаты

Необходимо упомянуть ещё один вопрос, связанный с применением открытых ключей. На пути от организатора конкурса к участнику открытый ключ может быть перехвачен злоумышленником и подменен на другой, относящийся к созданной им самим ключевой паре. Если данный факт пройдет незамеченным, то поставщик законвертует (зашифрует) свою заявку этим «фальшивым» ключом и отправит её организатору. Данная сконвертованная заявка может быть вновь перехвачена злоумышленником, расшифрована известным ему закрытым ключом, после чего вновь сконвертована «правильным» ключом организатора и отправлена к нему. При этом факт утечки останется сторонами незамеченным. Чтобы избежать подобной ситуации используется механизм сертификатов открытых ключей, применяемый также и при использовании электронной цифровой подписи в соответствии с положениями Федерального закона «Об электронной цифровой подписи»[3].

Понятие электронной подписи тесно связано с понятием несимметричного шифрования с одной лишь разницей — в данном случае открытым делается не шифрующий, а расшифровывающий ключ ключевой пары. При этом вместе с самим сообщением посылается его зашифрованная копия. Получатель при помощи открытого ключа расшифровывает зашифрованное сообщение и сравнивает с оригиналом. Поскольку, не зная закрытого ключа, невозможно зашифровать сообщение так, чтобы после расшифровки открытым ключом оно оказалось идентичным оригиналу, авторство сообщения считается проверенным.

Как уже говорилось выше, в реальной жизни несимметричные алгоритмы не применяются для шифрования больших объемов данных. Поэтому в случае подписывания сообщения предварительно вычисляется его хэш, т. е. уникальный отпечаток, который впоследствии и шифруется. Алгоритмы вычисления хэша (такие как MD5 или ГОСТ Р 34.11-94) должны обеспечивать невозможность подбора текста к заранее известному результату хеш-функции. В этом случае оказывается невозможным изменить сообщение так, чтобы в измененном виде ему соответствовал тот же хэш.

Механизм сертификатов использует механизм электронной подписи для безопасной доставки открытых ключей шифрования участникам конкурса. Упрощенно данную модель можно представить в следующем виде:

- На компьютер участника конкурса надежным образом устанавливается открытый ключ подписи организатора конкурса.

[3] Федеральный закон от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи» (принят ГД ФС РФ 13.12.2001) // СЗ РФ от 14.01.2002 г. № 2, ст. 127.

- Открытый ключ, который будет использоваться для шифрования данных конкурса участниками, подписывается закрытым ключом ЭЦП организатора и отправляется участникам.
- Участники, при помощи имеющегося у них открытого ключа ЭЦП организатора проверят подлинность пришедшего к ним открытого ключа шифрования конкурса.

Также механизм применения сертификатов поддерживает возможность выстраивать цепочки доверия, когда один сертификат используется для заверения другого. Применительно к нашему случаю это означает, что у нас исчезает необходимость защищать среду передачи и обеспечивать безопасные условия рассылки открытых ключей. Реализуется это следующим образом — в момент установки на компьютер участника устанавливается самоподписанный сертификат так называемого удостоверяющего центра. Устанавливается он, обычно, с компакт-диска, происхождение которого не вызывает сомнений. При генерации организатором конкурса ключевой пары, его открытый ключ подписывается закрытым ключом удостоверяющего центра, парным к установленному на компьютере участника, и в виде сертификата высылается по открытым каналам связи (см. рис. 2).

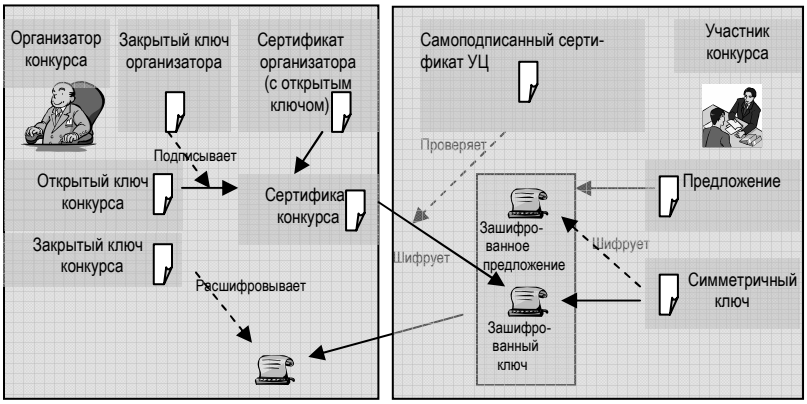

Рис. 2.Схема с несимметричным ключом

2.4. Метка времени (Time Stamping)

Рассмотрим вопрос обеспечения привязки ко времени различных манипуляций с данными. Для юридической оценки событий, фактов часто бывает необходимо не только убедиться в том, что тот или иной файл

электронного документа не изменялся с момента его подписания, но и знать точную дату подписания. Решением этой задачи является установка меток времени при работе с электронными документами. Реализуется этот процесс следующим образом:

1. При помощи одной из хеш-функций, описанных ранее, для файла заявки участника конкурса создается хэш.
2. Хэш отправляется по каналам связи в уполномоченную организацию, оказывающую услуги по заверению электронных документов или проставляющей метки времени (time stamp server), где к ней добавляется независимая информация о текущем времени, а затем подписывается ЭЦП должностного лица этой организации. Такой организацией может быть специализированная государственная или коммерческая организация, реализующая функцию «электронного нотариуса», либо эту функцию может исполнять удостоверяющий центр. Подписанная комбинация из хэша и информации о дате и времени называется меткой времени.
3. Метка времени отправляется обратно, сохраняется рядом с интересующим нас файлом электронной заявки и может быть в дальнейшем использована для подтверждения или проверки даты последней модификации файла.

Как видно из вышеприведенного протокола, важнейшей задачей является обеспечение подлинности даты, проставляемой уполномоченной организацией. Данную задачу возможно решить в рамках комплекса удостоверяющих центров (УЦ). Для её решения применяются как организационные (регламенты и правила), так и аппаратные средства системы единого времени Российской Федерации (специальное оборудование отсчета времени, не допускающее его «перевод» на значительный интервал, контроль физического доступа к оборудованию).

3. Протоколы практической реализации процедур конвертования и обработки конкурсных заявок

3.1. Протокол конвертования и обработки заявок с использованием симметричного шифрования и удостоверяющих центров

Рассмотрим один из наиболее трудно реализуемых на практике вариант работы с заявками участников конкурса. Он предполагает наличие доступного, стабильно работающего и независимого удостоверяющего центра (УЦ):

1. Организатор торгов объявляет о начале конкурса и оповещает об этом УЦ.
2. Каждый участник торгов, принимающий участие в конкурсе, лично обращается в УЦ, который создает симметричный ключ конвертования (шифрования) предложения на данный конкурс для данного участника. Копия ключа остается на хранение в УЦ. Сохранность копии обеспечивается регламентами УЦ.
3. При помощи специальной программы участники конвертуют (шифруют) свои заявки с предложениями полученными ключами и отправляют их организатору торгов, либо лично приносят зашифрованные данные на дискетах, которые затем вводятся в систему организатором торгов.
4. К моменту завершения конкурса председатель конкурсной комиссии организатора торгов посылает в УЦ запрос на получение набора ключей по данному конкурсу.
5. УЦ по запросу передает (пересылает) председателю конкурсной комиссии организатора торгов набор ключей участников конкурса.
6. Председатель конкурсной комиссии организатора «вскрывает» поступившие сконвертованные заявки при помощи полученных ключей.

Оценка протокола

1. Организатор торгов и каждый участник конкурса по данной схеме должен вступить в отношения с УЦ и заключать с УЦ дополнительный разовый возмездный договор об оказании услуг (привязанный к проводимому конкурсу), что существенно усложняет процедуру подготовки конкурсного предложения, подготовки заявок и их конвертование, собственно процедуру проведения конкурса, а также повышает накладные расходы.

2. В виду того, что все ключи хранятся в УЦ, существенным недостатком данной схемы является то, что не исключена возможность сговора должностных лиц организатора торгов и УЦ и несанкционированная передача ключей участников конкурса. Соответственно, есть риск того, что должностные лица организатора торгов могут получить несанкционированный и недоказуемый доступ к заявкам участников конкурса до момента подведения итогов конкурса и незаконно использовать эту информацию для получения нужного результата при подведении итогов конкурса, что противоречит требованиям Закона «О размещении заказов…».

3. При реализации данного протокола необходимым условием работы организатора торгов при компрометации им ключей должна быть его материальная ответственность за нарушение установленных Законом правил проведения конкурсов, сопоставимая со стоимостью разыгрываемых на конкурсе контрактов.

4. Предложенный протокол не предусматривает независимого от сторон документирования (фиксации) времени отправления, получения и вскрытия электронных конвертов с заявками участников, что может послужить источником фальсификации времени подачи заявки и, соответственно, незаконного недопущения участника к конкурсу, либо допущения к конкурсу заявителя, подавшему заявку после установленного времени и, соответственно, не обеспечивает возможности доказать заинтересованным сторонам в спорах те или иные действия или бездействия организатора торгов, УЦ или участников конкурса.

5. Регламентация действий и процедур всех субъектов отношений, участвующих или обеспечивающих проведение конкурса по данной схеме потребует от организатора торгов значительных затрат административных и материальных ресурсов, разработки достаточно большого количества сложных локальных нормативно-правовых актов в части юридического обеспечения процедур проведения конкурса (порядок взаимодействия с УЦ, порядок генерации ключей, порядок хранения ключей, порядок передачи ключей, порядок конвертования заявок, порядок вскрытия конвертов, порядок ведения протокола, порядок внесудебного разрешения споров и пр.) и соответствующего программного обеспечения, которые в целом не смогут создать как интерактивную, так и очную среду доверия и равноправия для всех ее участников. Регламентация реализации данного протокола не обеспечивает юридическую чистоту процедур электронного конвертования и не в состоянии обеспечить выполнение требований по организации конвертования, установленных Законом «О размещении заказов…».

Вывод: реализация процедур конвертования по данному протоколу создает почву для коррупции, не обеспечивает юридической чистоты и не отвечает требованиям конвертования, установленным Законом «О размещении заказов…».

3.2. Протокол конвертования и обработки заявок с использованием симметричного шифрования без удостоверяющего центра

Можно предложить протокол без УЦ:

1. Организатор торгов объявляет о начале конкурса.
2. Каждый участник торгов, принимающий участие в конкурсе, на своем компьютере при помощи специальной программы, входящей в комплект конкурсной документации, создает симметричный ключ конвертования (шифрования) заявок для данного конкурса, записывает его на сменный носитель и охраняет его под свою ответственность.

3. При помощи специальной программы участники конвертуют (шифруют) свои заявки с предложениями созданными ключами и отправляют по открытым каналам связи (в т. ч. и посредством сети Интернет) электронный конверт с заявкой организатору торгов, либо лично приносят его на дискетах, CD-дисках, флэш-накопителях, которые затем вводятся в автоматизированную систему организатором торгов.
4. Во время проведения конкурсной комиссией процедуры подведения итогов конкурса участники отправляют председателю конкурсной комиссии свои ключи конвертования в том же порядке, как и электронные конверты.
5. Председатель конкурсной комиссии организатора торгов при помощи полученных ключей «вскрывает» поступившие электронные конверты с заявками участников конкурса.

Оценка протокола

1. Казалось бы, достоинством данного протокола является большая защищенность электронных конвертов. По этой схеме специализированное программное обеспечение по генерации ключей конвертования будет формироваться организатором торгов и передаваться участникам конкурса в составе конкурсной документации. Соответственно ответственность организатора торгов по проведению процедур конвертования сведена к минимуму, а вся ответственность по охране ключей конвертования и обеспечению защищенности электронных конвертов будет лежать на участниках конкурса.

Однако в этой схеме повышается риск того, что в рассылаемом специализированном программном обеспечении организатора торгов могут быть заложены программные закладки, несанкционированно копирующие и передающие сгенерированные ключи конвертования, либо саму заявку, что позволит получить несанкционированный и труднодоказуемый доступ к заявкам участников конкурса до момента подведения итогов конкурса и незаконно использовать эту информацию для получения нужного результата при подведении итогов конкурса. А это противоречит требованиям по конвертованию, установленных Законом «О размещения заказов…».

Без государственных гарантий и системы государственной сертификации аппаратных и программных средств организатора и участников торгов реализация данного протокола не сможет обеспечить необходимый уровень доверия и защищенности процедур электронного конвертования.

2. Предложенный протокол также не предусматривает независимого от сторон документирования (фиксации) времени отправления, получения и вскрытия электронных конвертов с заявками участников.

При использовании данного протокола требуется обязательное личное присутствие поставщиков в момент «вскрытия конвертов», поскольку

при пересылке по сети ключ по злому умыслу или по техническим причинам может не дойти до адресата. В случае отсутствия ключа заявка не будет расшифрована, а участник не сможет принять участие в конкурсе.

Вывод: реализация процедур конвертования по данному протоколу без дополнительной сертификации программного и аппаратного обеспечения не полностью обеспечивает юридической чистоты и не вполне отвечает требованиям конвертования, установленным Законом «О размещении заказов…».

3.3. Протокол конвертования и обработки заявок с использованием несимметричного шифрования

Рассмотрим ещё один протокол для реализации процедуры конвертования и схемы защиты информации.

1. При объявлении конкурса организатор торгов в присутствии нотариуса или уполномоченного представителя незаинтересованной организации (электронного нотариуса) создает пару ключей конвертования (открытый и закрытый) для объявленного конкурса, формирует сертификат открытого ключа конвертования и помещает его в реестр действующих сертификатов открытых ключей конвертования, доступный для сверки всем участникам конкурса через сеть Интернет.
2. Закрытый ключ помещается на сменный носитель (дискета, flash drive, CD), опечатывается и передается нотариусу или уполномоченному представителю сторонней и незаинтересованной в результатах конкурса организации (электронному нотариусу) на хранение под их ответственность.
3. Сертификат открытого ключа конвертования, содержащий открытый ключ и подписанный ЭЦП председателя конкурсной комиссии, помещается в реестр действующих сертификатов и передается совместно со специализированной программой всем участникам конкурса в пакете с конкурсной документацией через веб-сервер организатора торгов.
4. При помощи специализированной программы участники конкурса формируют в установленном конкурсной документацией порядке электронную заявку в xml-формате и конвертуют ее при помощи открытого ключа конкурса.
5. Сформированный электронный конверт отсылается организатору торгов на его сервер и хранится там до момента подведения итогов конкурса.
6. В момент начала работы конкурсной комиссии по подведению итогов конкурса нотариус или уполномоченный представитель незаинтересо-

ванной организации передает председателю конкурсной комиссии носитель с закрытым ключом конвертования по проводимому конкурсу.

7. Председатель конкурсной комиссии, используя закрытый ключ конвертования, вскрывает представленные на конкурс электронные конверты с заявками участников конкурса и подводит итоги конкурса.

К достоинствам данной схемы можно отнести простоту и удобство её использования. Поскольку работа с закрытым ключом конвертования ведется на системе организатора торгов, то несколько упрощается решение задачи обеспечения гарантий безопасности создания и хранения ключа.

Единственным слабым местом данной схемы, как и схемы с симметричным шифрованием и УЦ, является проблема возможного несанкционированного доступа к закрытому ключу конвертования и его утечки.

Оценка протокола

1. По этой схеме открытый и закрытый ключи конвертования будут формироваться организатором торгов. Открытый ключ конвертования передается участникам конкурса в составе конкурсной документации, а закрытый ключ передается на хранение нотариусу или уполномоченному представителю сторонней незаинтересованной вы результатах конкурса организации под ее ответственность. Нотариус или сторонняя незаинтересованная в результатах конкурса организацией, оказывает услугу организатору торгов на условиях заключенного между ними договора об оказании услуг.

При реализации данного протокола, если не будет предусмотрена государственная сертификация и поверка специализированного программного и аппаратного обеспечения, есть риск того, что у организатора торгов может остаться несанкционированная копия закрытого ключа конвертования, что позволит получить отдельным должностным лицам организатора торгов несанкционированный и труднодоказуемый доступ к заявкам участников конкурса до момента подведения итогов конкурса и незаконно использовать эту информацию для получения нужного результата при подведении итогов конкурса, что противоречит требованиям по конвертованию Закона «О размещении заказов…».

Без государственных гарантий и проведения государственной сертификации аппаратных и программных средств организатора торгов реализация данного протокола не сможет обеспечить необходимый уровень доверия и защищенности процедур электронного конвертования.

2. По этой схеме есть риск того, что возможен сговор должностных лиц организатора торгов и нотариуса или уполномоченного представителя незаинтересованной сторонней организации. Соответственно, должностные лица организатора торгов могут получить несанкционированный и труднодоказуемый доступ к заявкам участников конкурса до момента под-

ведения итогов конкурса и незаконно использовать эту информацию для получения нужного результата при подведении итогов конкурса. Соответственно, при заключении договора между организатором торгов и нотариусом или сторонней организации необходимо устанавливать ответственность за компрометацию закрытого ключа конвертования, сопоставимую с порядком разыгрываемых конкурсных контрактов.

При реализации данного протокола необходимым условием работы организатора торгов при компрометации им ключей должна быть его материальная ответственность за нарушение установленных Законом правил проведения конкурсов, сопоставимая со стоимостью разыгрываемых на конкурсе контрактов.

3. Предложенный протокол также не предусматривает независимого от сторон документирования (фиксации) времени отправления, получения и вскрытия электронных конвертов с заявками участников, что может послужить источником фальсификации времени подачи заявки и, соответственно, незаконное недопущение участника к конкурсу, либо допущение по сговору заявителя к конкурсу, подавшему заявку после установленного времени и, соответственно, существенно усложняет возможности доказать заинтересованным сторонам в спорах те или иные действия или бездействия организатора торгов или участников конкурса.

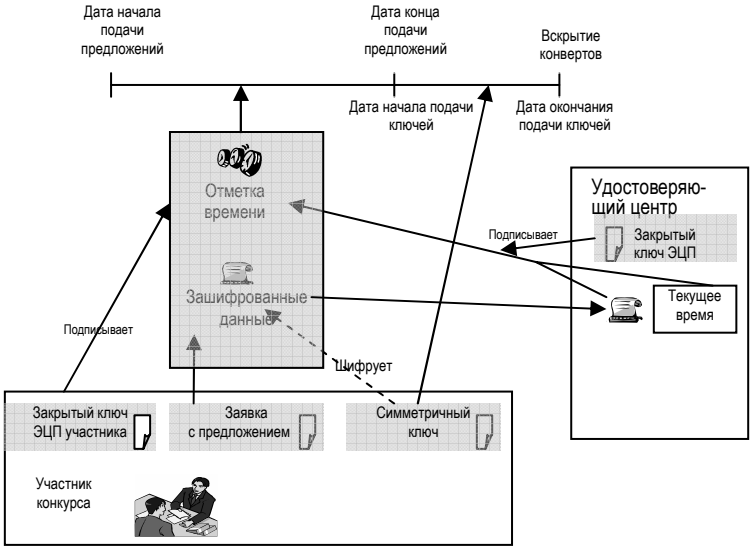

Рис. 3. Схема с несимметричным ключом и сервером времени

4. Регламентация действий и электронных процедур организатора торгов и участников конкурса по данной схеме также потребует от организатора торгов значительных затрат административных и материальных ресурсов, разработки достаточно большого количества сложных локальных нормативно-правовых актов в части юридического обеспечения процедур проведения конкурса (порядок генерации ключей и паролей, порядок хранения и передачи закрытых ключей и паролей, порядок открытых передачи ключей, порядок конвертования заявок, порядок вскрытия конвертов, порядок ведения протокола, порядок внесудебного разрешения споров и пр.) и соответствующего программного обеспечения, которые в целом не в состоянии создать ни интерактивную, ни очную среду доверия и равноправия для всех ее участников.

Вывод: реализация процедур конвертования по данному протоколу в целом обеспечивает юридическую чистоту и отвечает требованиям по конвертованию, установленным Законом «О размещении заказов…», но потребует существенных затрат на разработку регламентов и иных внутренних нормативных правовых актов, реализующих административно-правовое обеспечение процесса торгов.

3.4. Протокол конвертования и обработки заявок с использованием симметричного шифрования и независимого сервера времени

Для использования данного протокола следует несколько изменить процедуру проведения конкурса, однако это позволит гарантировать надежность и использовать все преимущества автоматизированной системы и интерактивной среды реализации. Перечислим шаги протокола:

1. Организатор торгов в конкурсной документации, помимо даты и времени начала, и окончания подачи заявок, даты и времени вскрытия конвертов, устанавливает в числе прочего дату и время начала и окончания подачи ключей конвертования. Конкурсная документация пакетом вместе со специализированным программным обеспечением, обеспечивающим реализацию процедуры конвертования, передается участникам конкурса.
2. На интервале от времени начала до времени окончания подачи заявок каждый участник, принимающий участие в конкурсе, создает у себя при помощи специальной программы симметричный ключ конвертования заявок на объявленный конкурс, записывает его на сменный носитель и охраняет его под свою ответственность. При помощи специальной программы участники конвертуют свои заявки созданными ключами, далее посредством сети Интернет используя независимый

сервер времени сторонней организации (например, УЦ), проставляют метку времени на своих электронных конвертах (см. п. 2.4), затем подписывают их своей ЭЦП и отправляют организатору торгов. В случае отсутствия доступа в сеть Интернет у кого-либо из участников, они могут очно принести свои электронные конверты с заявками на электронных носителях в порядке, установленном конкурсной документацией, на которые затем в их присутствии организатором торгов устанавливается отметка времени и которые затем вводятся в систему организатором торгов.

3. На интервале от времени начала до времени окончания подачи ключей участники присылают посредством сети Интернет либо приносят лично свои ключи конвертования.
4. В момент подведения итогов председатель конкурсной комиссии вскрывает поступившие конверты с заявками участников при помощи полученных ключей.
5. По окончанию конкурса любой из его участников имеет возможность получить полный набор подписанных зашифрованных предложений, присланных на конкурс, и ключей от них, проверить подписи, метки времени, расшифровать и убедиться в том что предложения содержат ту же информацию, что и была оглашена при принятии решения по победителю конкурса.

Поскольку период подачи ключей может составлять несколько дней, риск попытки сорвать процесс участия и вскрытия электронных конвертов кого-либо из участников конкурса путем блокировки тем или иным способом каналов связи между участником и организатором торгов сводится к минимуму.

Простановка независимой и защищенной ответственностью УЦ метки времени существенно уменьшает риск подлога заявок на протяжении периода подачи ключей. Предположим, злоумышленник перехватил один или несколько из ключей, переданных поставщиками. У злоумышленника, участвующего в конкурсе, может появиться соблазн расшифровать предложения других участников присланными ими ключами, просмотреть содержащиеся в них данные, а затем подменить свое предложение так, чтобы выиграть конкурс. Данная ситуация оказывается невозможной, поскольку злоумышленник будет не в состоянии поставить на свой конверт с измененной заявкой метку времени, попадающую в интервал подачи зашифрованных предложений.

Постановка ЭЦП делает невозможной ситуацию исключения поставщика из числа участников. Злоумышленник может попытаться модифицировать метку времени на предложениях других поставщиков так, чтобы казалось, что предложение было подано после даты окончания подачи

предложений. В предлагаемой схеме это невозможно, поскольку каждое зашифрованное предложение вместе с отметкой времени подписывается ЭЦП подавшего его поставщика.

Оценка протокола

1. По этой схеме специализированное программное обеспечение, позволяющее генерировать ключ конвертования, будет передаваться участникам конкурса в составе конкурсной документации. При этом организатор торгов будет нести ответственность за это специализированное программное обеспечение, а вся ответственность по охране ключей конвертования, конвертование и обеспечение защищенности электронных конвертов будет лежать на самих участниках конкурса.

2. Сторонняя организация в рамках гражданского договора об оказании услуг между ней и организатором торгов будет нести ответственность за достоверность фиксации отметок времени на электронных конвертах участников конкурса.

3. Реализация процедуры конвертования заявок участников конкурса по этой схеме отвечает требованиям по конвертованию Закона «О размещении заказов…» за исключением одного момента. Так на интервале от времени начала до времени окончания подачи ключей есть риск того, что организатор торгов может несанкционированно до начала установленного времени вскрыть конверты участников конкурса. При этом организатор торгов существенно повлиять на ход процедуры проведения конкурса будет не в состоянии. Однако будет возможна ситуация, когда организатор торгов в отдельных случаях, имея незаконный доступ к закрытой информации конвертов с заявками, в нарушение установленных требований по конвертованию Закона «О размещении заказов…», может принять решение об отмене или переносе в этого конкурса и тем самым повлиять на результаты проведения конкурса.

Вывод: реализация конвертования по данному протоколу не обеспечивает полной юридической чистоты, соответствующей требованиям Закона «О размещении заказов…». Для обеспечения соответствия процедур электронного конвертования по данному протоколу необходима будет комплексная реализация ряда аппаратно-технических, программных технических и административно-организационных мероприятий, а также принятия необходимых нормативных правовых документов на уровне руководителя субъекта Российской Федерации и иных локальных нормативных правовых документов организатора торгов, удостоверяющего центра или иной организации, оказывающей услуги удостоверения (сверки) документов и фиксации отметок времени на электронных документах при проведении процедур электронного конвертования и вскрытия конвертов участников конкурса.

3.5. Протокол конвертования и обработки заявок с использованием несимметричного шифрования, удостоверяющего центра и независимого сервера времени

Учитывая все вышеприведенные соображения, может быть предложен ещё один вариант для реализации процедуры конвертования и схемы защиты информации.

1. При объявлении конкурса нотариус или уполномоченное должностное лицо сторонней и незаинтересованной в результатах конкурса организации (электронного нотариуса), используя специализированное сертифицированное программное обеспечение, полученное от организатора торгов, создает (генерирует) пару ключей для шифрования закрытого ключа конвертования по открываемому конкурсу. Закрытый ключ шифрования формируется непосредственно на сменном носителе (дискета, flash drive, CD).
2. Сменный носитель с закрытым ключом шифрования и закрытым ключом конвертования открываемого конкурса опечатывается нотариусом или уполномоченным должностным лицом незаинтересованной организации и сдается на охраняемое хранение. Открытый ключ конвертования нотариус или сторонняя организация пересылает посредством сети Интернет организатору торгов.
3. Организатор торгов полученный открытый ключ вписывает (помещает) в формируемый сертификат, подписывает его ЭЦП председателя конкурсной комиссии и размещает в реестре действующих сертификатов открытых ключей конвертования, доступном для сверки всем участникам конкурса через сеть Интернет.
4. Открытый ключ конвертования в пакете конкурсной документации вместе со специализированной программой конвертования через вебсервер организатора торгов рассылается всем участникам конкурса. Участники конкурса при помощи специализированной программы формируют в установленном конкурсной документацией порядке электронную заявку в xml-формате и конвертуют ее при помощи открытого ключа конкурса. Затем участники конкурса посредством сети Интернет, используя сервер времени нотариуса или независимой организации, проставляют отметку времени на своих электронных конвертах и подписывают их своей ЭЦП.
5. Сформированный электронный конверт отсылается организатору торгов на его сервер и хранится там до момента подведения итогов конкурса.
6. В момент начала работы конкурсной комиссии по подведению итогов конкурса нотариус или уполномоченный представитель незаинтересо-

ванной сторонней организации получает и распечатывает электронный носитель с охраняемым ключом. Затем посредством сети Интернет пересылает закрытый ключ конвертования конкурса организатору торгов.

7. Председатель конкурсной комиссии, используя полученный ключ шифрования, вскрывает представленные на конкурс электронные конверты с заявками участников конкурса и подводит итоги конкурса.

Предложенная схема обеспечивает высокий уровень защиты информации и автоматизации процедур конвертования. Единственным её недостатком по сравнению с предыдущей является возможность срыва подведения итогов конкурса путем нарушения линий связи между организатором конкурса и нотариусом.

Оценка протокола

1. По этой схеме закрытый ключ конвертования будет формироваться и храниться до подведения итогов конкурса нотариусом или сторонней незаинтересованной в результатах конкурса организацией под их ответственность и без непосредственного участия организатора торгов. Нотариус или сторонняя незаинтересованная в результатах конкурса организацией, оказывает услугу организатору торгов на условиях заключенного между ними договора об оказании услуг. Открытые ключи шифрования и конвертования передаются организатору торгов по любым открытым каналам связи. Открытый ключ конвертования передается участникам конкурса в составе конкурсной документации.

При реализации данного протокола, если не будет предусмотрена государственная сертификация и поверка специализированного программного и аппаратного обеспечения, есть риск того, что в специализированном программном обеспечении будет присутствовать программная закладка, позволяющая несанкционированно передавать копию генерируемых закрытых ключей, что позволит получить отдельным должностным лицам организатора торгов несанкционированный и труднодоказуемый доступ к заявкам участников конкурса до момента подведения итогов конкурса и незаконно использовать эту информацию для получения нужного результата при подведении итогов конкурса.

Эта проблема достаточно легко решается установлением государственной гарантии путем проведения государственной сертификации аппаратных и программных средств организатора торгов и их периодической поверкой, что позволит обеспечить при реализации данного протокола высокий уровень доверия и защищенности процедур электронного конвертования.

2. При реализации данного протокола необходимым условием работы нотариуса или должностных лиц незаинтересованной сторонней организации при компрометации ими закрытых ключей должна быть их матери-

альная и уголовная ответственность за нарушение установленных Законом правил проведения конкурсов, сопоставимая со стоимостью разыгрываемых на конкурсе контрактов.

3. Реализация предложенного протокола позволяет автоматизировать все этапы проведения конкурса и конкурсные процедуры в режиме реального времени и интерактивного присутствия участников конкурса, а также организовать возможность контроля всех процедур для любого участника конкурса как во время конкурса, так и после его проведения. Все это позволит обеспечить прозрачность, доверенную среду и юридическую чистоту конкурсных процедур.

4. Регламентация действий и электронных процедур организатора торгов, нотариуса или сторонней организации и участников конкурса по данной схеме также потребует от организатора торгов значительных затрат административных и материальных ресурсов, разработки достаточно большого количества сложных локальных нормативно-правовых актов в части юридического обеспечения процедур проведения конкурса. Однако пользовательское удобство организации работы для всех сторон, имеющих отношение к проводимому конкурсу, и экономия их времени стоит этих затрат.

Вывод: реализация процедур конвертования по данному протоколу наиболее полно обеспечивает юридическую чистоту процедур, отвечает потребностям современного информационного общества и отвечает требованиям по конвертованию, установленным Законом «О размещении заказов…».

4. Выводы

На основе рассмотренного материала можно дать следующие рекомендации:

- Протоколы, не включающие в себя использование сторонней организации (УЦ, нотариуса, сервера времени), не обеспечивают в полной мере выполнения требований по конвертованию, установленных Законом «О размещении заказов…». Однако они обладают большей простотой и гибкостью. Такие протоколы могут быть рекомендованы для проведения закупок вида B2B, когда фактор коррупции сводится к минимуму. В этом случае удобство и независимость от внешних факторов выгодно отличает протокол 3.3.
- Протоколы, не включающие в себя использование сервера времени также не обеспечивают в полной мере выполнения требований по конвертованию Закона «О размещении заказов…», поскольку не дает возможности вести гарантированное протоколирование действий участни-

ков конкурса. Это ограничение, опять же, не является критическим при проведении закупок коммерческими структурами. Вновь, в данной группе наибольшее предпочтение следует отдать протоколу 3.3.

- В роли УЦ должна выступать организация, независимая от организатора торгов. Таким образом, в регионах, в которых ещё не существует действующего УЦ, использование протоколов, включающих УЦ, будет затруднительно на первых этапах, поскольку потребует создания «с нуля» новой структуры. В условиях отсутствия стабильно работающего УЦ и наличия естественного для государственных закупок недоверия к организатору торгов, можно рекомендовать использование протокола 3.2.
- Использование протоколов, включающих хранение ключей в УЦ (или у нотариуса), потребует разработки дополнительного сложного комплекса регламентов взаимодействия организатора торгов, участников конкурса и УЦ, поскольку такая деятельность не входит в круг непосредственных обязанностей УЦ. Напротив, использование сервера времени не потребует никаких существенных дополнительных организационных мер. В виду всего вышесказанного протокол 3.4 выгодно отличается от остальных.
- В случае же отсутствия возможности пользоваться сервером времени, но при наличии независимого УЦ, следует использовать протокол 3.1.
- Протокол 3.5 требует наличия независимых и стабильных УЦ и сервера времени, однако выгодно отличается от протокола 3.1 большей простотой регламента взаимодействия с УЦ, от протокола 3.3 наличием документированных сведений о времени подачи и модификации заявок, от протокола 3.2 и 3.4 меньшим количеством используемых ключей и потому большей надежностью.

5. Заключение

Нами был предложен способ обеспечить конфиденциальность передачи и хранения конкурсных предложений в рамках конкурсов по закупкам для государственных нужд. Описанный способ рекомендован для внедрения в электронные торговые площадки, создаваемые в рамках ФПЦ «Электронная Россия» в мероприятиях № 53 «Разработка и создание системы информационно-маркетинговых центров» и № 54 «Разработка и создание опытного проекта интегрированной информационной инфраструктуры электронной торговли». Предложенные процедуры обеспечения конфиденциальности могут быть использованы также в других государственных и корпоративных автоматизированных системах, в которых требуется поддержание высокой степени секретности хранящихся в них данных.

Литература

1. Федеральный закон от 21.07.2005 г. № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».
2. Федеральный закон от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи».
3. ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Система электронной цифровой подписи на базе асимметричного криптографического протокола».
4. ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
5. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая».
6. *Бернет С., Пэйн С.* Криптография. Официальное руководство RSA Security. RSA Security's Official Guide to Cryptography. Бином, 2002.
7. *Аграновский А. В., Хади Р. А.* Практическая криптография. Протоколы и их программирование. Серия: Аспекты защиты. Солон-Пресс, 2002.
8. *Семилетов С. И.* Правовые проблемы организации электронного оборота документов в государственном управлении // Сборник ИГП РАН «Теоретические проблемы информационного права». М., 2006. С. 160–174.