науково-практичної конф. "Безперка інформації в інформаційно-телекомунікаційних системах".- К.: Видавництво "Інтерлінк", НДЦ "ТЕЗІС" НТУУ "КПІ", 2002. - С. 57. ***9.*** *Роштейн А. П., Штовба С. Д. Нечеткая надежность алгоритмических процессов. – Винница: Континент – ПРИМ, 1997. – 142 с.* ***10****. Мелихов А. Н., Берштейн Л. С., Коровин С. Я. Расплывчатые ситуационные модели принятия решений: Учебное пособие. - Таганрог: ТРТИ, 1986. - 92 с.* ***11.*** *Корченко А. Г., Рындюк В. А., Мелешко Е. А., Пацира Е. В. Исследование нечетких операций для применения в системах защиты информации // Матеріали V Міжнародн. науково-практичної конф. "Безпека інформації в інформаційно-телекомунікаційних системах".- К.: Вид-во "Інтерлінк", НДЦ "ТЕЗІС" НТУУ "КПІ", 2002. - С. 56.* ***12.*** *Корченко А. Г. Нечеткие арифметические операции с линейной аппроксимацией по локальным максимумам // Зб. наук. пр. ІПМЕ НАН України. Випуск 4. – Львів: Вид-во "Світ" при Львівському університеті, 1998. – С. 3-6.*

УДК 681.5

ОПЫТ ПРИМЕНЕНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ДЛЯ ЗАЩИТЫ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ В СИСТЕМЕ МЕЖБАНКОВСКИХ РАСЧЕТОВ ЦЕНТРАЛЬНОГО БАНКА РОССИЙСКОЙ ФЕДЕРАЦИИ

Игорь Устинов
ООО «Криптоком», г. Москва

Аннотация: **Рассматриваются теоретические проблемы применения электронной цифровой подписи для обеспечения юридической значимости электронных документов в системе межбанковских расчетов Центрального банка Российской Федерации.**
Summary: **This article describes theoretical problems of digital signature implementation for juridical significance of e-docs in the bank payment system of Russian Federation Central Bank.**
Ключевые слова: **Электронная цифровая подпись, юридическая значимость электронных документов.**

I Введение

Работы по созданию Автоматизированной системы банковских расчетов (АСБР) были начаты в Межрегиональном центре информатизации (МЦИ) при Центральном банке (ЦБ) в 1980 году. АСБР была призвана повысить скорость и надежность пересылки денег между банками. На начальном этапе АСБР функционировала параллельно с традиционной «бумажной» технологией осуществления платежей и дублировала ее функции. В то время АСБР обслуживала лишь банки, находящиеся в государственной собственности, поэтому задачи обеспечения безопасности расчетов возможно было решать организационно-техническими и режимными мерами.

Экономические и политические изменения в стране в конце 80-х и начале 90-х годов привели к резкому росту числа банков и выходу их из-под государственного контроля, что повлекло качественное усложнение задачи обеспечения информационной безопасности АСБР. Поэтому в 1992 году в рамках договора между Центральным Банком и Федеральным Агентством Правительственной Связи и Информации (ФАПСИ) при Президенте РФ были начаты работы по внедрению в АСБР средств защиты информации.

Важной составной частью этих работ являлось решение задачи придания электронному документу юридической значимости, то есть обеспечения возможности использовать электронный документ в качестве доказательства в арбитражном процессе.

II Описание АСБР

Структура АСБР была определена исходя из специфики решаемых ею финансовых задач и особенностей технической вооруженности пользователей на момент ее создания. Кратко эту структуру можно описать следующим образом.

Участниками АСБР являются банки, стоящие на расчетно-кассовом обслуживании в МЦИ. Для удобства описания сам МЦИ мы также будем относить к участникам системы.

АСБР состоит из информационных систем участников, объединенных в сеть с использованием коммутируемых каналов связи. Эта сеть имеет топологию «звезда», то есть банки обмениваются информацией только с МЦИ, информационные потоки между банками не предусмотрены. Информационный

обмен между банком и МЦИ организован в форме пересылки файлов во время сеанса связи, причем инициатором сеанса всегда является банк. В нормативных документах ЦБ информационная система участника, входящая в состав АСБР, называется **Абонентским пунктом**.

Банк отправляет в МЦИ так называемые рейсы. **Рейсом** называется файл, содержащий группу платежных поручений данного банка или его клиентов. Каждое платежное поручение является для МЦИ распоряжением на перевод денег с корреспондентского счета этого банка на корреспондентский счет банка получателя. Таким образом, пересылка рейсов является основной целевой функцией АСБР. В течение дня банк может передать в МЦИ до 99 рейсов. Каждый рейс имеет уникальный (в рамках текущего дня) номер.

В любой момент в течение дня банк имеет возможность вносить исправления в уже переданные рейсы. Для этого в МЦИ отправляется новый рейс с тем же номером. Новый рейс замещает старый, при этом обязательства сторон по старому варианту рейса отменяются. Данная процедура называется **отзывом рейса**. Если переданный банком отзывающий рейс пуст, это означает отмену ранее переданного рейса и обязательств сторон по нему.

Финансовая обработка полученных от банков рейсов производится ночью. В данной работе под **финансовой обработкой** понимается вся совокупность действий по целевому использованию информации, содержащейся в рейсе или ином электронном документе.

Утром следующего дня МЦИ передает банкам перечни документов, поступивших в кредит корреспондентского счета банка, расшифровки сальдо взаимных оборотов, реестры аннулированных документов, выписки из корреспондентских счетов, протоколы ошибок, протоколы отбраковки документов по результатам обработки в МЦИ и другие информационные документы.

III Постановка задачи

В соответствии с описанной структурой задача обеспечения информационной безопасности АСБР включает в себя обеспечение информационной безопасности составляющих ее внутренних информационных систем участников и организацию защищенного межсистемного взаимодействия. Однако участниками АСБР являются юридически самостоятельные и независимые организации, поэтому ни у МЦИ как координатора АСБР, ни у какой-либо иной организации нет ни юридической, ни технической возможности вмешиваться в организацию внутренней защиты информационной системы участника АСБР. Строго регламентироваться может лишь взаимодействие участников системы друг с другом.

Поэтому при создании системы защиты информации АСБР участники рассматривались как единые неделимые объекты. Такое решение обусловлено еще и тем, что регламентация работы АСБР осуществляется в форме договоров между МЦИ и коммерческими банками, в рамках которых каждая из сторон рассматривается как единое юридическое лицо.

В силу как специфики решаемых целевых задач (пересылка денег между пользователями), так и общей экономической ситуации в стране, АСБР обладает рядом особенностей, привнесших существенную новизну в разработку средств защиты в сравнении с ранее решавшимися криптографическими задачами. Из таких особенностей следует отметить:

- недоверие участников АСБР друг к другу, к координатору сети и к третьим лицам, в том числе к государственным институтам;
- недисциплинированность участников АСБР;
- потенциальная недобросовестность участников АСБР.

Следствием перечисленных факторов является то обстоятельство, что возникновение конфликтов между участников АСБР, связанных с пересылкой рейсов и иных электронных документов, следует рассматривать как штатную ситуацию.

Таким образом, обязательной частью разработки системы защиты АСБР должна была стать разработка механизмов выхода из конфликтных ситуаций. При этом следует отметить, что конфликт, связанный с пересылкой электронных документов, является проекцией на технический уровень экономического конфликта, связанного с прохождением платежа или иным финансовым действием, поэтому разрабатываемый механизм выхода из конфликтной ситуации должен быть максимально адекватен существующему арбитражному механизму разрешения экономических споров.

IV Разрешение конфликтов в системе межбанковских платежей в рамках традиционной «бумажной» технологии

К моменту начала работ по обеспечению информационной безопасности в АСБР собственно система осуществления межбанковских платежей существовала уже не одно десятилетие, поэтому, во-первых, было

известно, какие конфликты могут возникать в связи с функционированием этой системы и, во-вторых, существовали общепринятые процедуры разрешения этих конфликтов.

Как следует из приведенного выше описания, АСБР решает две целевые задачи: пересылку денег между банками и предоставление банкам информации о движении средств на их корреспондентских счетах. При решении обеих задач МЦИ как поставщик услуг совершает некоторые действия и несет по отношению к обслуживаемым банкам некоторые обязательства, банки же выступают лишь как потребители этих услуг. Поэтому конфликт в системе АСБР всегда заключается в том, что банк обвиняет МЦИ в неправомерности совершения или несовершения некоторого действия.

При этом МЦИ в рамках оказываемых услуг не обладает свободой принимать решения: любое действие МЦИ по пересылке денег может быть совершено только по поручению банка-отправителя, а при наличии такого поручения (при соблюдении ряда четко определенных условий) должно быть совершено. Аналогично содержание информации, которую МЦИ предоставляет банкам, однозначно определяется принятой в системе процедурой и не может изменяться по воле МЦИ.

Поэтому в обслуживаемой МЦИ системе межбанковских расчетов возможны три типа конфликтов:

1. банк обвиняет МЦИ в переводе денег без поручения банка;
2. банк обвиняет МЦИ в неосуществлении операции перевода денег при наличии соответствующего поручения;
3. банк обвиняет МЦИ в предоставлении недостоверной информации.

В рамках традиционной «бумажной» технологии указанные конфликты разрешаются следующим образом.

Для обоснования законности совершения операции перевода денег МЦИ должен доказать, что он получил от банка соответствующее поручение. Для возможности осуществления такого доказательства нормативными актами и договорами установлено, что поручение на перевод денег признается состоявшимся, если оно оформлено в виде документа фиксированного формата, скреплено подписями и печатью банка и передано в МЦИ. Также установлены сроки архивного хранения платежных документов, соответствующие срокам исковой давности по вопросам перевода денег между банками. Благодаря этим установлениям существует корректная процедура разрешения обсуждаемого конфликта, заключающаяся в требовании к МЦИ предъявить платежный документ банка, на основании которого был совершен перевод денег. Если МЦИ является добросовестным участником системы, он сможет извлечь из своего архива и предъявить в арбитраж платежный документ, обосновывающий любую его операцию. С другой стороны, если платежный документ предъявлен и арбитр убедился (возможно, с привлечением экспертов-криминалистов) в его подлинности и в том, что документ действительно подписан уполномоченными представителями банка, то можно утверждать, что соответствующее поручение действительно было передано банком в МЦИ.

Если банк обвиняет МЦИ в неисполнении своих обязательств по переводу денег, он должен доказать, что действительно поручал МЦИ осуществить эту операцию, то есть доказать, что он направлял в МЦИ соответствующий платежный документ. Для возможности осуществления такого доказательства установлено, что при получении платежного документа МЦИ возвращает банку второй экземпляр этого документа со своей отметкой о получении. Этот второй экземпляр выполняет функции квитанции и для него установлены те же сроки архивного хранения, что и для первых экземпляров. При такой организации процесса доставки платежных документов банк, если он действительно передавал в МЦИ поручение на перевод денег, сможет предъявить в арбитраже второй экземпляр соответствующего платежного документа. С другой стороны, если второй экземпляр платежного документа предъявлен и арбитр убедился (возможно, с привлечением экспертов-криминалистов) в подлинности имеющейся на нем отметки МЦИ о приеме первого экземпляра этого документа, то можно утверждать, что соответствующее поручение действительно было передано банком в МЦИ.

Обвинение МЦИ в недостоверности предоставленной информации порождает обязанность банка доказать, что некоторая ложная информация действительно была получена им от МЦИ. Для возможности осуществления такого доказательства установлено, что в рамках своих обязательств по обслуживанию банков в системе межбанковских расчетов МЦИ предоставляет информацию банкам в виде документов фиксированного формата, скрепленных подписями и печатью МЦИ. Тем самым для того, чтобы убедиться, что МЦИ действительно предоставил банку именно эту информацию, арбитр должен получить от банка соответствующий документ и проверить (возможно, с привлечением экспертов-криминалистов) его подлинность.

V Основные принципы обеспечения юридической значимости электронных документов в системе АСБР

Проанализировав сформулированные в предыдущем параграфе принципы обеспечения возможности корректного разбора конфликтов в рамках традиционной технологии межбанковских расчетов, можно выделить три основные свойства системы документооборота, которые делают возможным арбитражный разбор конфликта:

- возможность проверки подлинности документа;
- документальное подтверждения факта передачи документа (квитирование);
- обеспечение архивного хранения документов.

Поскольку в рамках работ по защите информации в АСБР изначально ставилась задача обеспечения возможности разбора конфликтов, связанных с электронными документами, в рамках существующих арбитражных процедур, необходимо было обеспечить наличие этих же свойств у циркулирующих в АСБР электронных платежных документов.

VI Обеспечение возможности доказательного подтверждения подлинности и авторства электронного документа

Криптографическим механизмом обеспечения доказательности подлинности и авторства электронного документа является электронная цифровая подпись (ЭЦП).

Известно множество алгоритмов ЭЦП (см., например, [1]), причем далеко не все из них являются стойкими к подделке подписи. Поэтому алгоритм ЭЦП, используемый для защиты электронных документов, должен быть тщательно и всесторонне проанализирован специалистами. Поскольку вопрос о подлинности электронного документа предстоит решать арбитру, не являющемуся специалистом в области криптографической защиты информации и, вследствие этого, не способному самостоятельно оценить ни стойкость применяемого алгоритма, ни качество и полноту его анализа, целесообразно использовать алгоритм ЭЦП, имеющий официальный статус. Поэтому параллельно с работами по внедрению средств защиты информации в АСБР ФАПСИ совместно с ВНИИстандарт решалась задача разработки и принятия государственного стандарта на алгоритм электронной цифровой подписи. Разработанный алгоритм был тщательно проанализирован специалистами ФАПСИ и принят в 1993 в качестве ведомственного стандарта ЦБ, а в 1994 году после некоторой доработки – в качестве Государственного стандарта Российской Федерации [2, 3].

Помимо криптографических качеств самого алгоритма ЭЦП для корректного решения вопроса о подлинности электронного документа арбитру необходима также уверенность в том, что технические средства, реализующие алгоритм ЭЦП, работают корректно. То есть нужен не только анализ собственно алгоритма ЭЦП, но и комплексный анализ технических средств ЭЦП. В связи с этим уже в процессе разработки государственного стандарта на алгоритм ЭЦП был поставлен вопрос о необходимости создания системы сертификации средств криптографической защиты информации с целью недопущения на эксплуатацию некачественной продукции. В последующие годы такая система была создана, обеспечена правовой и нормативной базой и в настоящее время все технические средства, реализующие алгоритмы ЭЦП, подлежат в России обязательной сертификации.

Решение задачи обеспечения возможности доказательного подтверждения подлинности и авторства электронного документа, однако, не ограничивается выбором качественного алгоритма ЭЦП и его реализации. Проблема состоит в том, что электронная цифровая подпись имеет одно качественное отличие от подписи собственноручной: она отчуждаема от своего владельца. Если обычная подпись под бумажным документом неотделима от человека, никто другой физически не сможет подделать подпись так, чтобы подделка не была обнаружена криминалистической экспертизой, то любой злоумышленник, завладевший секретным ключом, сможет вырабатывать электронные цифровые подписи так же хорошо, как и законный владелец этого ключа.

Поэтому система использования ЭЦП должна быть построена таким образом, чтобы секретный ключ подписи не был известен никому, кроме его владельца. В частности, каждый участник должен самостоятельно осуществлять процедуру генерации своих ключей.

Вторым следствием отчуждаемости ЭЦП является необходимость юридически корректного подтверждения принадлежности открытого ключа ЭЦП. То есть арбитр должен не только убедится в корректности ЭЦП под электронным документом, но и проверить, что использованный при проверке ЭЦП открытый ключ действительно принадлежит тому участнику системы, авторство которого проверяется.

Для юридического заверения принадлежности открытых ключей подписи участников в системе АСБР предложено свести задачу к уже имеющимся методам заверения, то есть распечатывать ключи на бумаге (в

шестнадцатиричном коде) и заверять мастичными печатями и собственноручными подписями ответственных лиц (таким образом созданный бумажный документ будем далее называть **контрольной записью**).

Данное решение, однако, обладает тем недостатком, что включает в себя принципиально неавтоматизируемые моменты, как то: формирование контрольной записи, ее физическую доставку противоположной стороне, сличение открытого ключа с контрольной записью и т. п. Поэтому заверение ключа посредством контрольной записи предложено применять только для первичных ключей пользователей.

Смена ключей производится по безбумажной технологии, при этом новый открытый ключ подписи заверяется на старом.

VII Документальное подтверждение факта передачи документа

Как отмечалось выше, при некоторых конфликтах арбитру необходимо проверить, был ли спорный электронный документ передан из банка в МЦИ.

В рамках традиционной технологии с бумажными документами подтверждением передачи документа является квитанция, роль которой исполняет второй экземпляр переданного документа с отметкой МЦИ о приеме первого экземпляра. При этом существенными являются следующие свойства квитанции.

Во-первых, квитанция однозначно отвечает на вопрос, быль ли квитируемый документ принят получателем или он был отвергнут. Квитанция может содержать также дополнительную информацию (например, причины непринятия документа), однако эта информация не является существенной при разрешении вопроса об ответственности сторон по документу. Данное требование легко переносится и на случай электронного документооборота.

Во-вторых, обеспечена возможность при арбитражном разбирательстве удостовериться в подлинности и неискаженности квитанции. Для того, чтобы квитанция на электронный документ обладала тем же свойством, она должна подписываться электронной цифровой подписью.

В-третьих, квитанция однозначно привязана к квитируемому документу. Это означает, что невозможно случайное или умышленное появление двух различных документов, которым могла бы соответствовать одна и та же квитанция. В случае электронного документооборота такую привязку можно было бы обеспечить по аналогии с платежными документами на бумаге, то есть включать в квитанцию копию квитируемого документа. Однако существование такого криптографического механизма, как функция хэширования, позволяет решать эту задачу более эффективно, а именно включать в квитанцию не сам квитируемый документ, а результат вычисления хэш-функции от этого документа. При этом арбитру для проверки соответствия квитанции некоторому документу достаточно вычислить хэш-вектор для этого документа и сравнить с хэш-ветором, записанным в квитанции. Доказанная в ходе криптографического анализа функции хэширования практическая неразрешимость задачи формирования двух различных текстов с одинаковым значением хэш-функции позволяет арбитру в случае совпадения хэш-векторов быть уверенным, что квитанция была выдана именно на этот документ.

Однако электронный документ обладает одной характерной чертой, качественно отличающей его от документа бумажного: для электронного документа возможно (и легко осуществимо) создание копий, неотличимых от оригинала. Это обстоятельство не позволяет полностью перенести традиционную технологию с использованием бумажных расчетных документов на случай электронного документооборота, поскольку возможность копирования документа делает возможным новую атаку, неосуществимую в рамках «бумажной» технологии.

Эта атака основана на том, что в исполнении рейса банку может быть отказано по какой-либо причине (реальная или мнимая ошибка в оформлении, недостаток средств на счете и т. п.). В рамках традиционной технологии неисполненный документ в таких случаях возвращается банку с пояснением причин отказа. При электронном же документообороте копия отвергнутого расчетного документа остается у МЦИ и банк не может быть уверен в том, что она не будет использована МЦИ для оправдания некорректных действий. Так, например, МЦИ имеет возможность под каким-либо предлогом отказать в исполнении корректно оформленного рейса и тем самым вынудить банк подготовить и послать новый рейс на те же платежи, а затем исполнить оба рейса, то есть списать с корреспондентского счета банка вдвое большую сумму.

Описанный выше механизм квитирования не решает эту проблему, поскольку задача однозначной привязки квитанции к квитируемому документу разрешима только для положительных квитанций. Для отрицательных же квитанций доказать их соответствие документу в общем случае оказывается невозможно, поскольку электронный документ может быть искажен во время передачи или умышленно модифицирован получателем. В этом случае в квитанции будет записано значение хэш-функции, не соответствующее отправленному документу. Документ, в результате, «зависает»: получатель, заявляет, что его не принял, однако отправитель не может этого доказать.

Для разрешения этой проблемы в АСБР предложено использовать имеющийся механизм отзыва рейса. Согласно типовому договору между МЦИ и банком администратор абонентского пункта банка должен на каждый отправленный им рейс либо добиться получения положительной квитанции, либо сформировать и отправить отзывающий рейс (исправленный вариант отвергнутого МЦИ рейса либо отменяющий его пустой рейс). Тем самым функции отрицательной квитанции при разрешении конфликтов выполняет положительная квитанция о приеме отзывающего рейса, на саму же отрицательную квитанцию возлагается лишь информационная функция.

VIII Организация надежного архивного хранения документов

Для обеспечения возможности корректного разрешения конфликтных ситуаций необходимо представить арбитру относящиеся к конфликту документы, как электронные, так и бумажные. Значит, должно быть организовано архивное хранение необходимых при разборе конфликта материалов: электронных документов и квитанций на них, контрольных записей на первичные ключи подписи и заявок на смену ключей, сертификатов и таблиц открытых ключей МЦИ.

Централизованное архивное хранение этих документов невозможно, так как держатель архива получает возможность путем уничтожения или искажения определенных документов влиять на результат разбора конфликтной ситуации. Поэтому при разработке системы применялся принцип заинтересованного хранения, согласно которому ответственность за хранение каждого конкретного материала возлагается на того пользователя системы, интересам которого будет нанесен ущерб при отсутствии этого материала во время разбора конфликта.

IX Заключение

Резюмируя сказанное, можно выделить шесть принципов, положенных в основу системы обеспечения юридической значимости электронных документов в АСБР.

1. Возможность конфликтов, связанных с электронными документами, требует доказательного заверения их подлинности и авторства. Криптографической основой для решения этой задачи является аппарат электронной цифровой подписи (ЭЦП). При этом используются стандартизированные алгоритмы ЭЦП и прошедшие сертификацию технические средства, реализующие эти алгоритмы.
2. Недоверие пользователей к кому бы то ни было, в том числе и к государственным учреждениям, традиционно выполнявшим функции выработки и распространения ключевой информации, предопределяет генерацию криптографических ключей самим владельцем этих ключей.
3. Процедуры регистрации и распространения открытых ключей должны включать в себя механизмы удостоверения их подлинности и принадлежности. К таким механизмам относятся заверение ключей электронной цифровой подписью на уже известных ключах, а для первичных ключ - распечатка на бумаге и заверение традиционными методами.
4. Организационная разобщенность и недисциплинированность участников АСБР не позволяет гарантировать добросовестность выполнения всеми участниками мероприятий по защите информации. Поэтому система защиты должна быть построена таким образом, чтобы нарушение участником требований информационной безопасности наносило ущерб только интересам этого участника.
5. Отсутствие доверенного держателя архива электронных документов требует распределенного хранения архивных документов, при этом ответственность за хранение каждого конкретного документа возлагается на того пользователя системы, интересам которого будет нанесен ущерб при отсутствии этого документа во время разбора конфликта.
6. Арбитражный характер разрешения конфликтных ситуаций предопределяет разработку таких механизмов выхода из конфликтов, связанных с электронными документами, который был бы понятен арбитру, не являющемуся специалистом в области защиты информации, и максимально адекватен механизму выхода из аналогичных конфликтов в случае использования бумажных документов.

Кроме того, для обеспечения самой возможности рассмотрения электронных документов в арбитраже должен быть создан необходимый юридический базис. Юридические аспекты электронного документооборота изучались Институтом государства и права РАН в рамках НИР, поставленной ФАПСИ. Результаты этих работ изложены в [4]. По результатам этой работы с одной стороны и выработанных криптографических решений выхода из конфликтных ситуаций с другой, во взаимодействии с юристами Центрального Банка был составлен «Типовой договор о расчетно-кассовом обслуживании банка в автоматизированной системе банковских расчетов», позволяющий обеспечить юридическую значимость электронных платежей. Заключение таких договоров началось в 1996 году, после чего межбанковские платежи в Московском регионе стали осуществляться на основании электронных платежных документов