**Правовое регулирование электронного документооборота**

Широкое внедрение компьютерной техники во все сферы деятельности человека привело к изменениям в обществе, пожалуй, не меньшим, чем промышленная революция XIX в. За несколько десятилетий ЭВМ превратились из чисто "вычислительных" машин в мощные системы по обработке, хранению, передаче информации.

В результате создания глобальных компьютерных сетей произошел настоящий переворот в области передачи и распространения информации. С использованием средств удаленного доступа стали проводиться торги, участники которых имеют возможность совершать сделки, не покидая своего офиса. Поручения о переводе денег могут передаваться в банк в виде компьютерных данных за считанные секунды. Чтобы заключить договор в письменной форме, уже необязательно писать его на бумаге и заверять подписью и печатью - достаточно заверить компьютерный файл с текстом договора электронной цифровой подписью и направить его по телекоммуникационным каналам партнеру.

Именно компьютеризация информационной деятельности помогла человечеству существенно ускорить процессы обработки, поиска, передачи информации, повысить надежность хранения больших ее массивов и тем самым преодолеть так называемый "второй информационный барьер".

Вместе с тем компьютеризация привела к возникновению целого ряда проблем, в том числе и правовых. Традиционные правовые системы создавались в эпоху, когда главенствующую роль в рыночном обмене занимали материальные товары ("индустриальная цивилизация"), а теперь, когда информация в стоимостном выражении стала существенной частью рынка, когда новые компьютерные технологии существенно изменили функционирование самого рынка, указанные системы часто уже не дают адекватных ответов на многие вопросы.

К числу таких проблем можно отнести следующие:

1) появление нового типа преступлений - преступлений в сфере компьютерной информации, связанных с несанкционированным доступом к компьютерной информации, созданием и распространением компьютерных вирусов и т.п.;

2) обеспечение правовой охраны программ для ЭВМ; определение правового режима компьютерной информации, баз данных;

3) регламентация доступа к базам данных, содержащим сведения о личной жизни граждан, определение ответственности за несанкционированное разглашение таких сведений;

4) правовое регулирование использования систем электронного документооборота и в связи с этим определение правового статуса электронных документов;

5) правовые проблемы, связанные с функционированием глобальных сетей, трансграничной передачей данных и трансграничными компьютерными преступлениями, и ряд других.

Обсудить все перечисленные проблемы в рамках одной статьи не представляется возможным. Мы рассмотрим лишь некоторые аспекты проблем, указанных в пп. 4 и 5.

**Системы электронного документооборота**

Развитие компьютерных технологий позволило во многих областях заменить бумажный документооборот безбумажным (электронным).

Первые системы электронного документооборота (ЭДО) появились в банковской сфере. В западной литературе такие системы получили название "системы электронного перевода денежных средств" (The Electronic Funds Transfer Systems (EFTS)). Одна из таких систем SWIFT1 функционирует с начала 1970-х годов.

В дальнейшем системы ЭДО стали широко применяться и для обмена другой коммерческой информацией. (Английское название таких систем Electronic Data Interchange, или сокращенно EDI.) Уже много лет такие системы используются для продажи и бронирования авиационных билетов; пятнадцать национальных союзов предприятий химической промышленности стран Западной Европы создали специальную организацию для осуществления обмена электронными документами; аналогичная организация была учреждена и западноевропейскими производителями автомобилей; транснациональная текстильная компания "Benetton" использует систему ЭДО для передачи необходимой информации между своими подразделениями, занимающимися продажей и производством продукции.

Даже эти несколько примеров показывают, насколько широк спектр применения систем безбумажного документооборота в коммерческой деятельности в индустриально развитых странах. И в такой сфере, как оформление таможенных документов, где, казалось бы, трудно избежать заполнения бумажных форм и бланков, в некоторых странах (например, во Франции, Норвегии) стало возможным представление деклараций в электронном виде. К проекту TVINN2 Норвежского таможенного управления присоединилось около семидесяти крупнейших норвежских компаний. В рамках этого проекта создана система ЭДО, позволяющая ее участникам использовать электронные таможенные декларации, которые направляются в таможенные органы из центральных офисов фирм по телекоммуникационным сетям.

В последние годы системы ЭДО стали активно внедряться и в нашей стране. Ряд крупных банков и банковских объединений (например Межбанковский финансовый дом) создают и используют в работе с клиентами и в межбанковском обмене указанные системы.

Очевидно, масштабы использования систем ЭДО в коммерческой деятельности будут увеличиваться благодаря множеству несомненных преимуществ этих систем перед традиционным документооборотом на бумажных носителях.

**Во-первых**, существенно возрастает скорость передачи и обработки информации. Правда, скорость выше только по сравнению с передачей бумажных документов по почте или с курьером, а такие средства обмена сообщениями, как телетайп и телефакс, позволяют обеспечить практически одинаковую с ЭДО скорость. Но и по сравнению с ними ЭДО имеет существенное преимущество. Системы ЭДО позволяют передавать структурированную определенным образом информацию, что в свою очередь позволяет автоматизировать обработку принимаемых сообщений. Естественно, при этом стороны должны предварительно договориться об обмене электронными документами и об их структуре. Проблема стандартизации документов в системах ЭДО является одной из важнейших на настоящий момент.

**Во-вторых**, значительно сокращается пространство, необходимое для хранения документации (например, вся "Большая советская энциклопедия" может быть записана на одном жестком магнитном диске персонального компьютера). Одновременно существенно упрощаются такие операции, как поиск необходимой информации, копирование документов.

**В-третьих**, использование систем ЭДО позволяет получить ощутимый экономический эффект. По оценкам американских фирм-производителей автомобилей, внедрение ЭДО позволяет сэкономить около 200 долл. на каждом автомобиле3. Суммарное годовое сокращение издержек благодаря использованию систем ЭДО в Норвегии оценивалось в 1989 г. в 5 млрд норв. кр.4 (около 1 млрд долл.).

Прежде чем перейдем к правовым аспектам использования систем ЭДО, остановимся вкратце еще на двух вопросах, имеющих непосредственное отношение к обсуждаемой теме.

Любой ли обмен данными в электронном виде можно считать электронным документооборотом?

Существуют два подхода к определению этого понятия. Первый подход (его можно назвать ЭДО в широком смысле) предполагает, что любой обмен компьютерными данными между различными субъектами можно считать ЭДО. В этом смысле, например, передача компьютерных файлов на дискете или система электронной почты, когда получаемая информация обрабатывается "вручную", подпадают под определение ЭДО. Например, П. Даукинс дает такое определение: "ЭДО есть передача коммерческой информации между организациями в электронном в иде и, в частности, между компьютерами различных организаций"5. При втором подходе (ЭДО в узком смысле) к подобным системам относят только передачу по каналам телекоммуникационной связи структурированной коммерческой информации, причем предполагается, что хотя бы первичная обработка сообщений производится автоматически, без участия человека. Д. Палмер пишет: "ЭДО - это передача структурированной деловой информации от компьютера к компьютеру"6. Приведем еще два определения: "ЭДО - это передача электронным способом структурированных в соответствии с согласованными стандартами сообщений между информационными системами"; "сообщение - это набор связанных между собой данных, структурированных в соответствии с согласованными стандартами; данные подготовлены в компьютерочитаемом формате и могут быть автоматически и однозначно обработаны; набор таких данных предназначен для передачи в электронном виде"7. Очевидно, таким требованиям удовлетворяют банковские системы, автоматизированные системы проведения торгов. В названных системах автоматически проверяется аутентичность документа, его допустимость, т. е. соответствие структуры документа согласованным стандартам, и возможно автоматическое выполнение определенных операций, предусмотренных для допустимых документов.

В дальнейшем в данной статье, если специально не будет оговорено другое, речь будет идти об ЭДО в широком смысле. Следует отметить, что в любом случае предполагается обмен деловой информацией между различными субъектами. Компьютерное же делопроизводство в рамках одной организации или частная переписка с использованием электронной почты, например, не подпадают под данное определение ЭДО.

Кто относится к субъектам электронного документооборота?

Принципиально возможны две схемы организации ЭДО. Первая схема предполагает прямую передачу данных участниками ЭДО без привлечения третьих лиц.

**Схема 1**

———————————————————————————————————————————————————————————

| Участник А | | Участник Б |

———————————————————————————————————————————————————————————

В этой ситуации стороны сами устанавливают "правила игры", т. е. определяют стандарты сообщений, выбирают оборудование и программное обеспечение, определяют процедуры разрешения конфликтов. При решении вопроса о распределении риска убытков здесь возможно участие третьих лиц (разработчиков программного обеспечения, поставщиков специального оборудования); подробнее эти вопросы будут рассмотрены в следующей статье. Более распространенной является вторая схема, в которой присутствует фирма-провайдер, обычно берущая на себя установку программного обеспечения и оборудования, контроль за их работой, следит за корректностью передачи данных, оказывает услуги по ведению архива передаваемых данных и т. п.

**Схема 2**

—————————————— —————————————— . . ——————————————

| Участник А | | Провайдер | | Участник В |

—————————————————————|——————————————|———————————————————|

. . | | . |

. . | | . |

—————————————— . . |——————————————|. . ——————————————|

| Участник Б | | Провайдер | | Участник Г |

————————————————————————————————————————————————————————

Для организации такого варианта ЭДО можно использовать две структуры договорных связей.

В первом случае обычно провайдер и несколько сторон создают начальную сеть ЭДО, в дальнейшем к ним может присоединиться произвольное количество новых участников. Здесь, как и в случае, представленном в схеме 1, участники ЭДО (а также провайдер) связаны между собой договором, в котором определены права и обязанности сторон, описаны процедуры разрешения конфликтов, распределение риска убытков. Поскольку функционирование системы ЭДО начинается после подписания такого договора, то данный договор заключается в традиционной письменной форме (на бумаге). Это обстоятельство, как будет показано далее, является существенным для признания арбитражными судами электронных документов в качестве доказательств.

Второй случай характерен для открытых сетей. Здесь участники ЭДО заключают договор только с провайдером. В такой ситуации участники (которые, возможно, физически располагаются даже на разных континентах, что затрудняет их непосредственное общение) могут заключить договор об использовании системы ЭДО в электронном виде. Упомянутый договор может содержать свои (отличные от общих) стандарты сообщений и другие положения, аналогичные описанным в предыдущем случае, но эти две модели организации систем ЭДО, похожие по сути, существенно различаются с точки зрения возможности использования электронных документов в качестве доказательств в суде.

Назовем теперь основные, на наш взгляд, юридические проблемы, которые могут возникнуть в процессе функционирования систем ЭДО. К ним относятся:

проверка подлинности электронного документа;

возможность использования электронных документов (ЭД) в качестве доказательств в арбитражных судах;

распределение риска убытков, которые могут возникнуть в процессе функционирования систем ЭДО;

взаимоотношения юридических лиц, использующих ЭДО, с аудиторскими фирмами, налоговыми и другими государственными органами, куда необходимо представлять отчетность о своей деятельности;

международноправовые проблемы, которые могут возникнуть, когда, например, два участника ЭДО и провайдер находятся в разных странах;

стандартизация;

защита информации в системах ЭДО.

Остановимся подробнее на первой из перечисленных проблем.

**Понятие электронного документа**

С точки зрения традиционного документооборота можно выделить две основные функции бумажного документа: информационную и доказательственную (т. е. возможность использовать его в качестве допустимого доказательства). Главной причиной, по которой именно бумажные документы выполняют эти функции, является то, что именно бумага была на протяжении многих столетий наиболее распространенным материальным носителем, используемым для передачи и хранения информации. В последние десятилетия ситуация резко изменилась, объемы передаваемых в электронном виде данных стремительно растут. Как отмечалось ранее, системы безбумажного документооборота получают все более широкое распространение в самых разных областях. В связи с этим важное значение приобретает определение правового статуса электронного документа - очерчивание областей, где возможно и допустимо его применение.

Прежде всего попытаемся сформулировать, что же такое традиционный документ (документ на бумажном носителе). Нам представляется, что наиболее полное и точное его определение дал В. Я. Дорохов: "Документ - письменный акт установленной или общепринятой формы, составленный определенными и компетентными учреждениями, предприятиями, организациями, должностными лицами, а также гражданами для изложения сведений о фактах или удостоверения фактов, имеющих юридическое значение, или для подтверждения прав и обязанностей"8.

Требования к документу, вытекающие из приведенного определения, можно разделить на три группы. Первая отражает информационную функцию документа: документом может быть не любая информация, зафиксированная на бумажном носителе, а только сведения определенного характера (это требование согласуется с приведенным ранее определением ЭДО). Вторая (требования к форме) группа - это, по существу, требования, обеспечивающие доказательственную функцию документа (реквизитами формы могут служить наличие печати и подписи определенного лица, персональные данные о лице, издавшем документ, а также требования к бумажному носителю, например, бумага с защитными знаками и т. п.). Третья группа (компетентность источника документа) как бы связывает первые две, придает юридическую значимость документу. Документ, изданный некомпетентным органом, подписанный не уполномоченным на то лицом либо анонимный, не может служить подтверждением изложенных в нем сведений о фактах, удостоверять факты или подтверждать права и обязанности.

Очевидно, легко обеспечить для данных, записанных в компьютерном формате, выполнение условий первой и третьей групп. Некоторые из требований к форме документа (например, соблюдение определенной последовательности изложения содержания и расположения текста ) тоже могут быть соблюдены. Другие требования второй группы (наличие печати организации, собственноручной подписи лица, специальный тип бумаги) принципиально неприемлемы для электронных документов вследствие специфической природы компьютерных носителей информации.

Именно физические характеристики электронных документов долгое время были объектом критики противников безбумажных систем документооборота. В частности, в качестве одного из аргументов приводилось следующее утверждение: то, что написано на бумаге, трудно удалить и оно остается навечно; данные же на компьютерных носителях могут быть легко уничтожены, они недолговечны. Но, во-первых, сохранность бумажных документов в значительной мере зависит от качества бумаги и для их длительного хранения необходимо применение специальных мер, а во-вторых, современные носители компьютерных данных позволяют хранить информацию достаточно долго и при осуществлении соответствующих мер безопасности (в том числе и периодическое копирование) их надежность не ниже, чем у традиционных. Кроме того, когда речь идет о деловой информации, обычно существуют определенные сроки хранения такой информации, исчисляемые годами или десятилетиями, а в течение указанных сроков возможна сохранность даже магнитных носителей, не говоря уже о дисках CD-ROM.

Еще один аргумент, приводимый в пользу бумажного документа, заключается в том, что он осязаем (т. е. любой может физически проверить наличие документа), каждый грамотный человек может прочитать такой документ. То, что электронный документ не может быть не посредственно воспринят человеком, не является непреодолимой сложностью. Теоретически, конечно, можно предположить, что создана система ЭДО, в которой один участник вносит в документ Manchester, а другой получает на экране монитора или при распечатке Live rpool. Однако данная проблема легко решается, если предположить, что существует согласованная участниками или определенная нормативным актом уполномоченного органа процедура изготовления по электронному оригиналу традиционной (бумажной) копии документа. (Более подробно об этом мы поговорим, когда будем рассматривать процедуры разрешения конфликтов, связанных с использованием ЭДО.)

И, наконец, пожалуй, самый существенный аргумент. Бумажный документ почти невозможно изменить, в электронный же документ легко внести поправки, и очень трудно потом доказать факт их внесения. Можно, конечно, отметить, что подделка традиционных документов имеет, наверное, не меньшую историю, чем история письменности, но это не снимает проблемы идентификации электронных документов.

Решить приемлемым образом данную задачу удалось только во второй половине 1970-х годов, когда американские математики У. Диффи и М. Э. Хеллмэн предложили использовать цифровую подпись для подтверждения подлинности электронных сообщений.

С учетом изложенного электронный документ можно определить как набор данных, записанных в компьютерочитаемом виде, для которых выполнено следующее условие: существует признанная участниками ЭДО или утвержденная компетентным органом процедура, позволяющая однозначно преобразовать эти данные в документ традиционного режима. Признание указанной процедуры должно быть подтверждено участниками системы ЭДО посредством традиционного (письменного) документа, либо такая процедура должна быть санкционирована уполномоченным государственным органом.

Необходимость традиционного документа или акта уполномоченного органа для признания процедуры преобразования объясняется тем, что в противном случае возможен порочный логический круг, когда вопросы признания или непризнания юридической силы электронного документа будут решаться на основании другого электронного документа, силу которого тоже можно оспорить.

Очевидно, что для создания такой процедуры нужно, чтобы подлинность данных была подтверждена с достаточной степенью надежности (например, с помощью электронно-цифровой подписи).

**Понятие электронно-цифровой подписи**

В 1976 г. американские математики У. Диффи и М.Э. Хеллмэн опубликовали работу под названием "Новые направления в криптографии", которая существенно повлияла на дальнейшее развитие криптографии и, в частности, привела к появлению такого понятия, как "цифровая подпись" (часто используется термин "электронно-цифровая подпись" (ЭЦП), поскольку применяется она в основном для подтверждения подлинности электронных документов).

Мы не будем здесь подробно останавливаться на криптографическом определении цифровой подписи, а лишь представим в самом общем виде математические принципы, положенные в основу использования ЭЦП.

Прежде всего рассмотрим понятие "односторонняя функция с секретом". Функция F(k,s), зависящая от двух числовых аргументов - k (секретный ключ) и s (цифровая подпись) - и устанавливающая соответствие между этими аргументами и документом 9, называется односторонней функцией с секретом. Ей присущи следующие свойства:

1. Для любого секретного ключа k и любой подписи s значение функции F можно вычислить достаточно просто (за приемлемое время)10, причем для вычисления по известному s значения m необязательно знать ключ k. Другими словами, зная саму функцию F и s (цифровую подпись под данным документом), легко вычислить значение m, т.е. проверить подлинность данной подписи s под данным сообщением m.

2. Если секретный ключ k неизвестен, то по известным s (подписи) и m (сообщению) невозможно достаточно просто (за приемлемое время) найти секретный ключ k11.

3. Если секретный ключ k известен, то по известному (заданному) m (сообщению) можно достаточно легко (за приемлемое время) вычислить s (подпись).

Суть использования односторонних функций для цифрового подписывания заключается в следующем. Любой документ, как отмечалось, можно рассматривать как некоторое число m. Документ, подписанный цифровой подписью, по существу, есть пара чисел m и s, где m - сообщение (договор, платежное поручение и т.п.), а s - подпись, которая получена путем решения уравнения F(k,s) = m (для каждого сообщения m вычисляется своя подпись s). Здесь F - известная всем участникам электронного документооборота односторонняя функция, а k - секретный ключ. Из третьего свойства односторонней функции следует, что существует алгоритм, позволяющий отправителю, знающему свой секретный ключ k, за приемлемое время вычислить подпись под документом m. Кто-либо другой (не знающий секретного ключа k) не сможет подписать документ (второе свойство односторонней функции), т. е. цифровую подпись практически невозможно подделать. Поэтому при возникновении спора о подлинности подписи лицо, чей секретный ключ был использован для подписывания документа, не сможет отказаться от исполнения обязательств по такому документу (если только не докажет ненадежность используемых в системе ЭЦП алгоритмов, о чем речь пойдет в следующей статье). Проверить подлинность подписи может любой участник ЭДО, знающий открытый ключ, т. е. саму функцию F (первое свойство односторонней функции).

Еще одним свойством ЭЦП, способствовавшим ее широкому практическому применение, является то, что подписанное сообщение можно, не опасаясь фальсификаций, передавать по любым, в том числе открытым, каналам связи. Если сообщение будет умышленно либо вследствие сбоев канала связи искажено, то подпись под ним окажется недействительной.

Представим схему практического использования ЭЦП на простейшем примере. Пусть несколько участников системы ЭДО договорились использовать ЭЦП для подтверждения подлинности своих электронных документов. Каждый участник i имеет свой открытый ключ Fi и секретный ключ ki, кроме того, каждому из участников известны все открытые ключи Fi. Получив от участника i подписанный документ, любой другой участник, зная соответствующий открытый ключ, может проверить подлинность подписи под документом и, если подпись признана программой проверки подлинной, быть уверенным в том, что документ отправлен именно участником i и в документ не были внесены никакие изменения.

Но, как говорится, было гладко на бумаге, да забыли про овраги. Первая проблема заключается в том, что с момента введения математического понятия односторонней функции (1975 г.) ни для одной функции не удалось строго доказать, что она является односторонней. На практике применяется несколько функций, для которых второе свойство пока строго не доказано, но установлено, что задача нахождения секретного ключа k эквивалентна давно изучаемой трудной математической задаче, т. е. на настоящий момент не найдено достаточно быстрого алгоритма вычисления k. Это не означает, что такой алгоритм не будет построен (если только не удастся подтвердить односторонность функции). Здесь следует сказать, что для некоторых функций, относительно которых предполагалось, что они могут быть односторонними и могут использоваться для систем ЭЦП, были найдены полиномиальные (достаточно быстрые) алгоритмы нахождения секретного ключа k по документу и подписи под ним, т. е. было доказано, что они не являются односторонними. Поэтому выбор функции для реализации системы ЭЦП - один из самых ответственных моментов, ведь если будет построен быстрый алгоритм нахождения секретного ключа, участники ЭДО могут понести значительные убытки, так как станет возможной подделка электронной подписи под документами.

Второй, уже чисто практической является проблема вычислений с большими числами на ЭВМ. Поскольку длина сообщения m, вообще говоря, не ограничена и может быть достаточно большой, то для вычисления подписи, возможно, придется оперировать очень большими числами, что сложно реализовать на ЭВМ. Поэтому в используемых на практике системах ЭЦП подпись вычисляется не для самого сообщения m, а для некоторого числа определенной длины, которое получается из m посредством применения к нему специальной функции, называемой хэш-функцией. Другими словами, хэш-функция задает соответствие между документом произвольной длины и числом заранее заданной длины.

В некоторых странах с целью минимизировать риски, связанные с выбором для систем цифровой подписи хэш-функций и функций подписывания (упомянутых односторонних функций), введены государственные стандарты таких функций. В частности, в России в 1994 г. были приняты стандарты: ГОСТ Р 34.11-94 "Функция хэширования" и ГОСТ Р 34.10-94 "Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма".

Первый из этих ГОСТов определяет функцию преобразования любой конечной последовательности двоичных бит (т. е. любого документа) в бинарное (двоичное) число длины 256 (очевидно, что выбор длины существенно влияет на надежность системы ЭЦП).

Второй стандарт определяет функцию и алгоритм вычисления электронно-цифровой подписи, а также алгоритм проверки подлинности подписи.

Таким образом, система ЭЦП содержит три алгоритма: алгоритм хэширования (преобразования документа в двоичное число определенной длины), алгоритм выработки ЭЦП под документом и алгоритм проверки подписи. Поскольку результаты работы первого алгоритма скрыты от пользователя (они используются как исходные данные для второго алгоритма), то в популярной литературе обычно говорят о двух алгоритмах: подписывания и проверки подписи.

Функция, принятая в описанных стандартах, в качестве односторонней функции с секретом была предложена в 1977 г. американскими специалистами Р. Ривестом, А. Шамиром и Л. Адлеманом. Системы на основе этой функции получили название "RSA систем" (по первым буквам фамилий авторов).

Попытаемся проанализировать сравнительные характеристики различных способов подтверждения подлинности как традиционных документов, так и данных, обрабатываемых с помощью ЭВМ.

Бумажные документы заверяются обычно либо собственноручной подписью компетентного лица с указанием его полного имени и должности, либо мастичной печатью юридического лица (на практике часто используют оба эти способа одновременно; иногда вместо собственноручной подписи должностного лица пользуются штампом с ее факсимильным воспроизведением). В последнее время реже применяется ранее распространенный метод оттиска отпечатка пальца под документом. В случае компьютерных данных используются цифровая (электронно-цифровая) подпись, электронные (магнитные) карты/ключи, пароли.

Подпись требуется для идентификации подписывающего лица и для подтверждения того, что информация, приведенная в документе, достоверна. Традиционно считается, что собственноручная подпись под документом имеет достаточно высокий уровень надежности. За столетия своего развития графология достигла значительных успехов, и с ее помощью можно установить с высокой степенью точности подлинность традиционной подписи. Но тем не менее специалисты по графологии никогда не делают абсолютных заключений. Например, в практике Норвежского судопроизводства используются четыре уровня достоверности заключения о подлинности подписи: возможно, вероятно, очень вероятно, с уверенностью. В российской судебной практике используются аналогичные утверждения: не исключено, с большой степенью вероятности и т. п. Таким образом, собственноручная подпись не дает абсолютной защиты от фальсификации документов. Более надежным способом в этом смысле является оттиск отпечатка пальца под документом, потому что отпечаток пальца неповторим, уникален.

Использование штампов (печатей, факсимиле подписи и т. п.) также не может гарантировать от подделок. Кроме того, в этой ситуации возможен еще один способ фальсификации документов: печать может быть похищена, либо ее оттиск поставлен неуполномоченным лицом. А так как, в отличие от предыдущего случая, здесь нет физической связи между тем, кто заверяет документ, и полученным на бумаге оттиском, выяснить, кто в действительности поставил печать, практически невозможно (аналогичная ситуация складывается и с ЭЦП).

Использование электронных документов породило еще одну проблему, кроме указанных. Если для традиционных документов подпись или штамп всегда были жестко привязаны к самому документу, то, например, указание пароля либо предъявление магнитной карточки открывает вход в некую систему создания документов, и в дальнейшем такие документы не имеют жестко увязанного с ними подтверждения их подлинности. Например, вы вставляете магнитную карточку в банкомат и вводите ваш код, после этого делаете запрос (создаете электронный документ) на получение определенной суммы наличными. Никакого документа, аналогичного расходному ордеру с вашей подписью, который вы заполняете в сбербанке, в данной ситуации не существует. Поэтому для повышения безопасности таких систем часто используются комбинации различных методов (например, при оплате товара или услуги с помощью магнитной карточки приходится подписывать бумажный документ, подтверждающий платеж).

**Таблица**

———————————————————————————————————————————————————————————————————————

| | | | |

| Метод | II | III | IV |

|—————————————————————|——————————————————|———————————————|——————————————|

| Собственноручная |Физическая | Высокий | Высокая |

| подпись |характеристика | | |

|—————————————————————|——————————————————|———————————————|——————————————|

| | | | |

| Отпечаток |Физическая | Низкий | Высокая |

| пальца |характеристика | | |

|—————————————————————|——————————————————|———————————————|——————————————|

| | | | |

| Электронная |Имеет | Низкий | Очень |

| карточка/ключ | | | низкая |

|—————————————————————|——————————————————|———————————————|——————————————|

| | | | |

| Пароль |Знает | Средний | Очень |

| | | | Низкая |

|—————————————————————|——————————————————|———————————————|——————————————|

| Электронно-цифровая |Знает | Средний | Высокая |

| подпись | | | |

| | | | |

———————————————————————————————————————————————————————————————————————

В предлагаемой таблице отображены характеристики различных способов подтверждения подлинности документов. В столбце II указан тип связи между лицом, использующим соответствующий способ, и используемыми средствами; в столбце III - уровень возможности идентификации заверившего документ лица по самому документу; в столбце IV - степень привязки к документу.

Из приведенной таблицы видно, что цифровая подпись служит достаточно надежным способом подтверждения подлинности документов. Она обеспечивает высокий уровень защиты документа от внесения несанкционированных изменений (столбец II), подделать ее практически невозможно. Единственный ее недостаток, по сравнению с обычной подписью, в том, что по ней нельзя с такой же степенью уверенности определить, кто именно подписал документ ( столбец III). Это обусловлено тем, что некоторые физические характеристики человека практически неповторимы (почерк, отпечаток пальца и т. п.), а о секретном ключе человек может умышленно либо случайно кому-то рассказать, ключ могут подсмотреть или украсть, если его записали. Но данное свойство цифровой подписи не является непреодолимым препятствием для ее широкого использования в гражданском обороте. Достаточно, чтобы каждый из участников системы ЭДО объявил о признании своих обязательств по всем документам, заверенным его цифровой подписью, пока в системе не будет официально объявлено о компрометации секретного ключа (подробнее на этом остановимся в следующей статье).

Для того чтобы цифровая подпись широко вошла в гражданский оборот и применялась наряду с традиционной (используемой уже тысячелетиями) подписью, требовалось выполнить несколько условий как правового, так и неправового характера.

1. Субъекты гражданского оборота оценили удобство и выгодность ее использования. Ранее были показаны преимущества использования систем ЭДО. Однако если такие системы не позволят совершать гражданско-правовые сделки, а будут только удобным инструментом для быстрого обмена информацией, то экономический эффект от их использования, очевидно, снизится.

2. Математики-криптологи предложили достаточно надежный способ подтверждения подлинности электронных документов и убедили в его надежности и возможности практического использования потенциальных пользователей, а также законодателя.

3. Наконец, законодатель: а) определил, что (представляет собой цифровая подпись (в отличие от традиционной подписи от руки, которую можно считать объектом очевидным и не нуждающимся в определении); б) закрепил возможность и сферы применения электронных документов и цифровой подписи; в) установил допустимость использования электронных документов в качестве доказательств в суде.

Мы уже обсудили первые две проблемы и рассмотрели стандарты, связанные с использованием цифровой подписи. Очевидно, что без утвержденного государством определения ЭЦП можно было только теоретически рассуждать о том, что некоторая последовательность байт, добавленная к файлу, является аналогом (на самом деле, как было показано, неполным) собственноручной подписи и может быть использована там, где требуется подпись под документом. Но если вспомнить, что даже криптографическое определение ЭЦП вводится через объекты (односторонние функции с секретом), существование которых строго математически не доказано, а с обыденной точки зрения ЭЦП вообще похожа на строку кабалистических символов, то станет ясно: были необходимы нормативные акты, где давалось бы четкое юридическое определение электронно-цифровой подписи под электронным документом. Такими актами и стали упомянутые стандарты. Исходя из вышеизложенного, следует отметить, что цифровой подписью является только последовательность байт, полученная путем применения алгоритмов и функций, описанных в стандарте12. Если будут использованы другие функции или, например, длина числа, в которое хэш-функция преобразовывает документ, отличается от указанной в стандарте, то полученная подобным образом подпись не будет ЭЦП в юридическом смысле (хотя с точки зрения криптографии она ничем не хуже и не лучше "официальной"). И, следовательно, документ, подписанный "нестандартной" ЭЦП, с юридической точки зрения не может рассматриваться как документ, заверенный ЭЦП.

В данной статье мы остановились лишь на самых общих вопросах, связанных с использованием систем ЭДО (участники таких систем, понятие электронного документа, понятие цифровой подписи). В дальнейшем предполагается рассмотреть такие вопросы, как правовой режим электронного документа, распределение риска убытков среди участников системы ЭДО, возможность использования электронных документов в качестве доказательств в суде, лицензирование деятельности, связанной с созданием средств функционирования систем ЭДО и некоторые другие.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**1** Society for Worldwide Interbank Financial Telecommunications - Всемирное общество межбанковских финансовых телекоммуникаций.

**2** Tollvesenets Innforsels/utforsels system med naringslivet i Norge Импортно/экспортная система таможенного управления и норвежских предпринимателей.

**3** The Journal of Business Strategy. 1990. Jan.

**4** Cf Datatid. 1989. N 12.

**5** Dawkins P. The functions required of software packages for EDI // EDI technology / Ed. M. Gifkins. L., 1989.

**6** Palmer D. EDI - The nuts and the bolts // EDI technology / Ed. M. Gifkins. L., 1989.

**7** The TEDIS Interchange Agreement // Final Draft. 1991. May.

**8** См.: Дорохов В.Я. Понятие документа в советском праве // Правоведение. 1982. N 2. С. 55.

**9** Любой документ можно представить себе как некоторое (может быть, очень большое) число. Один из возможных способов кодирования документа числом - обычное представление его в виде компьютерного файла, после чего получившаяся последовательность двоичных битов интерпретируется как число в двоичной системе счисления.

**10** Здесь и далее мы используем словосочетания "можно вычислить достаточно просто", "за приемлемое время"; в строгом математическом определении, естественно, применяется другая терминология: "существует полиномиальный алгоритм вычисления значения функции" и т.п.

**11** Второе свойство, очевидно, свидетельствует о сложности подделки цифровой подписи. Здесь мы опять используем термин "приемлемое время" вместо не очень понятных "полиномиальных алгоритмов". Для большей наглядности криптологи часто приводят такое разъяснение для "неприемлемого времени": если объединить сотню самых быстродействующих современных компьютеров и заставить их искать по известным в настоящее время алгоритмам секретный ключ по имеющимся документу и подписи под ним, то понадобится несколько сотен лет.

**12** В юридической литературе (см. напр.: Право и рынок // N 11, 1996. С. 12) можно встретить определение ЭЦП через следующие характеристики: набор байтов, являющийся результатом работы программы генерации ЭЦП; ЭЦП является аналогом собственноручной подписи; она неразрывно связана с конкретным документом и только с ним; делает невозможным изменение документа без нарушения подлинности подписи. Ни одна из приведенных характеристик не является полностью справедливой для ЭЦП (а некоторые просто не верны). Во-первых, следовало бы уточнить, что программы генерации должны работать на основании алгоритмов, утвержденных ГОСТами. Во-вторых, не является полным аналогом собственноручной подписи (см. таблицу и пояснения к ней). В-третьих, поскольку множество возможных документов шире, чем множество подписей, то одна и та же подпись одного лица может быть связана с различными документами, по этой же причине в четвертой характеристике следует говорить о малой вероятности или практической невозможности подделки ЭЦП (см. сн. 11).