**ТЕМА: ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ В ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ.**

Системы электронного документооборота представляют собой программные комплексы, применимые для решения ряда задач, в том числе и для построения корпоративных систем электронного документооборота. В рамках автоматизации процесса обработки документа в организации с момента его создания или получения до момента отправки корреспонденту или завершения исполнения и списания в дело должно быть обеспечено решение следующих функций:

регистрация входящих в организацию документов, исходящих из организации документов и внутренних документов;

учет резолюций, выданных по документам руководством организации, и постановка документов на контроль;

централизованный контроль исполнения документов;

списание документов в дело;

ведение информационно-справочной работы;

формирование делопроизводственных отчетов по организации в целом.

Использование системы электронного документооборота позволяет организовать передачу данных о ходе исполнения документов в электронном виде, что качественно меняет организацию контроля исполнения документов. Карточки зарегистрированных централизованно документов с резолюциями руководства рассылаются в электронном виде сотрудникам соответствующих подразделений. Они дополняют их резолюциями по исполнению документов, выдаваемыми руководителями структурных подразделений. По мере появления данных о ходе исполнения документов эти данные вносятся в систему. При этом система автоматически отслеживает наступление даты предварительного уведомления о приближении срока исполнения и наступление самого этого срока. Заинтересованные пользователи системы информируются о названных сроках.

Также значительно видоизменяется процесс согласования проектов документов, в рамках которого сотрудники, участвующие в процессе согласования, получают возможность обмениваться электронными версиями согласуемых проектов. Такая технология позволяет сократить время, затрачиваемое на передачу проектов в бумажном виде.

Система электронного документооборота обязательно включает текущий электронный архив, который решает проблемы оперативного доступа к информации и наличия возможности одновременного использования документа несколькими сотрудниками. Такая форма организации хранения значительно снижает вероятность потери информации и повышает оперативность работы за счет сокращения времени поиска нужного документа. Хранение текстов документов в электронном виде позволяет реализовывать полнотекстовый поиск, что открывает принципиально новые возможности при ведении информационно-справочной работы, например, позволяет делать тематические подборки документов по их содержанию. Использование электронного архива избавляет от необходимости создавать фонд пользования архивных документов, так как по запросу в любой момент может быть выдана электронная копия документа.

С юридической точки зрения понятие электронного документооборота отличается от понятия электронного обмена данными. В основе первого лежит легитимность (процессуальная допустимость и доказательственная сила) электронных документов. Поэтому наряду с совершенствованием информационных технологий важную роль в процессе создания инфраструктуры электронного документооборота должна сыграть его законодательная поддержка, суть которой состоит в придании данным, создаваемым и передаваемым электронным способом, юридического статуса документа.

Основной функцией традиционного документа является удостоверение некоторой информации. При составлении и использовании документа присутствуют два аспекта: во-первых, некоторая информация, а во-вторых, сам документ как материальная вещь, которую можно предъявить или передать. Наличие этой материальной вещи позволяет подтвердить истинность информации, содержащейся в документе. Возможно, для подтверждения истинности необходимо проделать некую процедуру - экспертизу по проверке подлинности документа.

Саму информацию, содержащуюся в документе, тоже можно разделить на две части. Первая часть - непосредственно содержание, вторая - вспомогательная информация, которая дает возможность установить его аутентичность (подлинность). К ней относятся реквизиты типа исходящего номера, подписей и печатей.

В состав информации, как содержательной, так и о носителе, могут входить и данные о времени, условиях и месте составления документа.

Необходимо также отметить, что в случае бумажного документа оригинал существует в ограниченном, известном заранее количестве экземпляров. Например, может быть указано, что договор совершен в трех экземплярах, имеющих равную силу. Любой дополнительный экземпляр явится копией, что в принципе может быть проверено путем проведения соответствующей экспертизы.

В ряде случаев существенно наличие именно оригинала документа. Например, продажа акции, выпущенной в документарной форме, вовсе не равносильна продаже копии ее сертификата, даже заверенной нотариально.

Таким образом, документ выполняет следующие функции:

фиксация некоторой (содержательной) информации;

фиксация лица, подписавшего документ;

фиксация условий составления документа;

доказательство в судебном разбирательстве;

функция оригинала, обеспечиваемая его уникальностью.

**2. Электронная цифровая подпись**

Электронная цифровая подпись - это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе (ст. 3 Закона об ЭЦП).

С юридической точки зрения электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при соблюдении определенных условий (ст. 4 Закона об ЭЦП).

Рассмотрим особенности электронной цифровой подписи. В отличие от рукописной подписи электронная цифровая подпись имеет не физическую, а логическую природу - это просто последовательность символов, которая позволяет однозначно связать лицо, подписавшее документ, содержание документа и владельца ЭЦП. Логический характер электронной подписи делает ее независимой от материальной природы документа. С ее помощью можно подписывать документы, имеющие электронную природу (исполненные на магнитных, оптических, кристаллических и иных носителях, распределенные в компьютерных сетях и т.п.).

Согласно Закону ЭЦП должна решать следующие задачи: защиту электронного документа от подделки, установление отсутствия искажений информации в электронном документе, идентификацию владельца сертификата ключа подписи (ст. 3).

Таким образом, ЭЦП должна обеспечить идентификацию (документ подписан определенным лицом) и аутентификацию (содержание не претерпело изменений с момента его подписания) электронного документа.

Однако следует отметить, что сущность же ЭЦП такова, что она не может непосредственно характеризовать владельца ЭЦП как личность. Связь же между ЭЦП и человеком, ее проставившим, носит не биологический, а социальный характер. Возникновение, существование и прекращение данной связи обусловлены совокупностью различных правовых, организационных и технических факторов.

Определение подлинности ЭЦП свидетельствует только о знании лицом, ее проставившим, закрытого ключа ЭЦП. Для того чтобы выяснить, действительно ли владелец сертификата ключа заверил документ ЭЦП, надо установить помимо факта подлинности ЭЦП и идентификацию человека, ее поставившего. Идентификация человека в традиционном понимании, как это происходит по личной подписи, непосредственно по ЭЦП невозможна. Доказать, что именно данное лицо заверило электронный документ ЭЦП, можно в результате процессуальной деятельности по доказыванию в ходе судебного разбирательства в соответствующем виде процесса.

Независимость ЭЦП от носителя позволяет использовать ее в электронном документообороте. При использовании ЭЦП возможны договорные отношения между удаленными юридическими и физическими лицами без прямого или опосредованного физического контакта. Это свойство ЭЦП лежит в основе электронной коммерции.

Логическая природа ЭЦП позволяет не различать копии одного документа и сделать их равнозначными. Снимается естественное различие между оригиналом документа и его копиями, полученными в результате тиражирования (размножения).

Механизм обслуживания ЭЦП основан на программных и аппаратных средствах вычислительной техники, поэтому он хорошо автоматизируется. Все стадии обслуживания (создание, применение, удостоверение и проверка ЭЦП) автоматизированы, что значительно повышает эффективность документооборота. Вместе с тем автоматизация хоть и способствует повышению производительности труда, она выводит механизм подписи из-под контроля естественными методами (например, визуальными) и может создавать иллюзию благополучия. Поэтому для использования ЭЦП необходимо специальное техническое, организационное и правовое обеспечение.

Техническое обеспечение электронной цифровой подписи основано на использовании методов криптографии.

Любой документ можно рассматривать как уникальную последовательность символов. Изменение хотя бы одного символа в последовательности будет означать, что в результате получится уже совсем другой документ, отличный от исходного.

Чтобы последовательность символов, представляющих документ, могла, во-первых, идентифицировать ее отправителя, а во-вторых, подтвердить ее неизменность с момента отправления, она должна обладать уникальными признаками, известными только отправителю и получателю сообщения. Для этого используются различные средства шифрования, создаваемые и изучаемые наукой криптографией.

Для шифрования и дешифрования информации необходимо знать метод и ключ шифрования.

Метод шифрования - это формальный алгоритм, описывающий порядок преобразования исходного сообщения в результирующее. Ключ шифрования - это набор параметров (данных), необходимых для применения метода. Так, например, буквы любой последовательности символов можно заменить на соответствующие комбинации цифр - это метод шифрования. А конкретное указание, какую букву заменить, на какую последовательность цифр, является ключом.

Существуют симметричные и несимметричные методы шифрования.

Симметричный метод шифрования состоит в том, что партнер создает ключ шифрования, который передает другому партнеру. Сообщение шифруется и дешифруется одним ключом. Этот алгоритм трудно напрямую использовать, например, в электронной коммерции, так как возникает проблема идентификации удаленного партнера.

Несимметричная (асимметричная) криптография использует специальные математические методы. В результате применения этих методов создается пара ключей: то, что зашифровано одним ключом, может быть дешифровано другим, и наоборот. Владелец ключей один оставляет у себя, а другой может распространить, например, прямой рассылкой через Интернет. Ключ, оставленный у владельца, называется закрытым или личным, другой - открытым или публичным.

Закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи (ст. 3 Закона об ЭЦП).

Открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе (ст. 3 Закона об ЭЦП).

Закрытый ключ может быть скомпрометирован различными способами:

хищение ключа путем копирования в результате несанкционированного доступа к оборудованию (прямого или удаленного), на котором он хранится;

получение ключа путем ответа на запрос, использованный с признаками мошенничества или подлога;

хищение ключа в результате хищения оборудования, на котором он хранится;

хищение ключа в результате сговора с лицами, имеющими право на его использование (даже рядовой факт увольнения сотрудника, имевшего доступ к закрытому ключу организации, рассматривается как компрометация ключа).

Незаконность данных традиционных методов компрометации обеспечивает законодательство.

Это не относится к нетрадиционным методам реконструкции закрытого ключа по исходным данным, полученным вполне легально, в частности по открытому ключу. Возможность реконструкции определяется тем, что открытый и закрытый ключи связаны определенными математическими соотношениями. Теоретически знание открытого ключа дает возможность восстановить закрытый ключ. Однако на практике это связано с наличием специальных программных и аппаратных средств и огромными затратами вычислительного времени. Существует специальная отрасль науки, называемая криптоанализом, которая позволяет воспроизводить зашифрованную информацию и оценить степень защиты информации.

Поскольку от алгоритмов, на основе которых действует средство ЭЦП, зависит надежность и устойчивость документооборота, к средствам ЭЦП предъявляются специальные требования.

Средства электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

При создании ключей электронных цифровых подписей для использования в информационной системе общего пользования должны применяться только сертифицированные средства электронной цифровой подписи (п. 2 ст. 5). Использование несертифицированных средств электронной цифровой подписи и созданных ими ключей электронных цифровых подписей в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления не допускается (п. 3 ст. 5).

Открытый ключ потому и называется открытым, что он доступен каждому из партнеров владельца закрытого ключа. Есть очень простой прием подмены открытого ключа с целью создания ложного канала связи. Допустим, сторона C желает перехватить чужие данные. В этом случае она может с помощью средств ЭЦП создать себе пару ключей и опубликовать открытый ключ якобы от имени партнера B. Тогда все сообщения от партнера А к партнеру B будут легко перехватываться и читаться стороной C, причем ни A, ни B не будут даже догадываться о том, что C участвует в "договорных" отношениях.

Эта форма злоупотребления основана на том, что хотя в открытом ключе и приводятся данные о его владельце, в нем нет средств, удостоверяющих, что эти данные подлинные. Без разрешения этого вопроса механизм ЭЦП не может быть использован ни в электронной коммерции, ни в электронном документообороте.

Таким образом, одним из основополагающих моментов использования электронной цифровой подписи для установления подлинности, целостности и аутентичности документов, хранимых, обрабатываемых и передаваемых с помощью информационных и телекоммуникационных систем, является подтверждение принадлежности открытого ключа ЭЦП конкретному лицу посредством выдачи сертификата ключа подписи. Поэтому значительная часть Закона об ЭЦП посвящена механизму удостоверения личности владельца открытого ключа.

Во всех случаях этот механизм основан на том, что вводится (назначается) дополнительная сторона, удостоверяющая принадлежность открытого ключа конкретному юридическому или физическому лицу. Вопросы: кто именно имеет право удостоверять открытые ключи, когда и как, - в законодательстве различных государств решаются по-разному. В частности, это может быть государственный орган или организация, уполномоченная государством для ведения данной деятельности. Возможно, что для внутреннего документооборота предприятия эту функцию можно поручить лицу, назначенному руководством, а для документооборота внутри ведомства - уполномоченному подразделению.

На практике сертификация открытых ключей выполняется следующим образом.

1. Лицо (юридическое или физическое), создавшее себе пару ключей (открытый и закрытый) с помощью средства ЭЦП, должно обратиться в орган, уполномоченный выполнить сертификацию. Этот орган называется удостоверяющим центром (Закон об ЭЦП).

2. Удостоверяющий центр проверяет принадлежность открытого ключа заявителю и удостоверяет этот факт добавлением к открытому ключу своей подписи, завизированной собственным закрытым ключом.

3. Любой партнер, желающий вступить в контакт с владельцем открытого ключа, может прочитать удостоверяющую запись с помощью открытого ключа удостоверяющего центра. Если целостность этой записи не нарушена, то он может использовать открытый ключ партнера для связи с ним.

Следует четко понимать, что удостоверяющий центр заверяет только факт принадлежности открытого ключа конкретному лицу или организации. Наличие полноценного сертификата открытого ключа говорит о том, что ключ можно использовать для удостоверения личности партнера в договорных отношениях. Но законность этих отношений удостоверяющим центром не подтверждается.

К удостоверяющим центрам предъявляются особые требования. Это обусловлено тем, что участники электронного документооборота не могут проверить корректность осуществления подобными организациями своих функций.

В настоящее время в соответствии с рекомендациями Европейского Совета национальное законодательство стран Европы в части требований к удостоверяющим центрам должно содержать требования одобрения или лицензирования деятельности удостоверяющих центров, проверку соблюдения этими центрами необходимых для их деятельности условий, а также требование к уровню надежности технических и программных средств, используемых этими центрами, и т.д. В части экономического обоснования возможности удостоверяющего центра нести гражданскую ответственность за ненадлежащее исполнение своих обязанностей необходимо выделить три критерия:

наличие собственного минимально установленного капитала, выраженного в абсолютной сумме;

подтверждение этой суммы банковской гарантией;

наличие страховки.

Значительно более трудной представляется задача практического создания в нашей стране инфраструктуры открытых ключей (PKI - Public Key Infrastructure) в системах электронного документооборота и электронной торговли.

Термин "инфраструктура открытых ключей" включает в себя полный комплекс программно-аппаратных средств, а также организационно-технических мероприятий, необходимых для использования открытых ключей.

Основным компонентом инфраструктуры является собственно система удостоверяющих центров.

Для создания целостной системы удостоверяющих центров необходимо определить модель и общую структуру системы; степень участия в ее построении различных государственных органов и коммерческих структур; используемые при создании информационные технологии.

Иерархический принцип построения государственного управления подразумевает достаточно естественную структуру построения в перспективе системы удостоверяющих центров системы электронного документооборота: от федерального уровня, через региональные центры и до ведомственных структур и конечных пользователей.

В данной модели определяющую роль выполняет совокупность удостоверяющих центров верхнего уровня, которые должны удовлетворять самым высоким требованиям по информационной безопасности. От надежности защиты этого уровня и доверия к нему в большой мере зависит надежность всей системы в целом и степень доверия к ней.

В настоящее время распространение получили две структурные модели системы сертификации - централизованная и децентрализованная.

Централизованная модель имеет иерархический характер и наиболее соответствует потребностям служебного документооборота. Децентрализованная модель имеет сетевой характер и может использоваться, например, в гражданском электронном документообороте.

В основе централизованной модели сертификации находится один уполномоченный орган сертификации. Такой орган называется корневым удостоверяющим центром (корневым центром сертификации).

Если чисто технически корневой центр не может обеспечить все запросы на выдачу и проверку сертификатов, поступающие от юридических и физических лиц, то он может сертифицировать другие дополнительные органы, называемые доверенными удостоверяющими центрами (доверенными центрами сертификации).

Доверенные центры тоже могут удостоверять чужие открытые ключи своими открытыми ключами, но при этом их открытые ключи тоже нуждаются в удостоверении. Их удостоверяет своим закрытым ключом вышестоящий центр сертификации.

Таким образом, участник электронного документооборота, получивший откуда-то открытый ключ неизвестного партнера, может:

установить наличие сертификата, удостоверенного электронной подписью удостоверяющего центра;

проверить действительность подписи центра сертификации в вышестоящем удостоверяющем центре;

если вышестоящий центр тоже является не корневым, а доверенным, то и его подпись можно проверить в вышестоящем центре, и так далее, пока проверка не дойдет до корневого удостоверяющего центра.

Такую проверку надо выполнить только один раз. Убедившись в правомочности корневого удостоверяющего центра, можно настроить свое программное обеспечение так, чтобы в дальнейшем доверие ему выражалось автоматически. И лишь в случаях, когда цепочку сертификатов не удается проследить до ранее проверенного доверенного центра (или до корневого центра), программное oбecпeчение выдаст предупреждение о том, что открытый ключ не имеет удостоверенного сертификата и пользоваться им нельзя.

Сетевая модель сертификации основана на взаимных договоренностях сторон (в последнем случае они будут иметь правовое значение, только если прямо отражены в двусторонних договоpax). Так, например, при отсутствии централизованной структуры доверенных удостоверяющих центров (или параллельно с ней, если законодательство это допускает) могут существовать сетевые модели сертификации. Такие модели охватывают группы юридических и физических лиц, например, по ведомственной принадлежности.

Два юридических или физических лица, вступающих в электронные коммерческие взаимоотношения, могут сами взаимно заверить друг другу открытые ключи, если обменяются ими при личной встрече с предъявлением друг другу учредительных документов или удостоверений личности (для физических лиц). В этом случае у них нет оснований сомневаться в истинной принадлежности открытых ключей.

Однако, например, электронная коммерция строится исходя из того факта, что участники не нуждаются в очной встрече. В этом случае две стороны могут договориться о том, что им взаимно заверит ключи третья сторона, которую они выберут сами. Также могут договориться и прочие участники рынка. В результате возникает сложная структура, в которой все участники связаны, с одной стороны, двусторонними договорными отношениями, а с другой стороны, еще и выполняют функции заверителей для своих традиционных партнеров. С точки зрения отдельного коммерсанта доверие к его открытому ключу будет тем выше, чем большее количество сертификатов он получит от прочих участников рынка.