Информационные технологии, бурное развитие которых началось в 90е годы, радикально изменили нашу жизнь. Темпы информатизации российского общества - одни из самых высоких в мире. Даже сегодня большая часть оборота информации и документов осуществляется в электронном виде. Технология электронной подписи позволяет еще больше расширить возможности электронного документооборота и распространить его на все сферы общественной жизни. Технологии цифровой подписи постепенно завоевывают признание во всем мире. В то же время развитие возможностей электронной коммерции положительно скажется на российском рынке информационных технологий в целом, поскольку все проекты электронной коммерции, такие как электронная коммерция, интернет-банкинг и интернет-провайдеры, являются крупными потребителями прикладного программного обеспечения, а его развитие создаст целую индустрию специализированных программно-технологических предприятий в России.

Прежде всего следует отметить принятие Федерального закона от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»[1] (далее – Федеральный закон). Этот Федеральный закон, по оценкам специалистов, дает значительный стимул развитию всего высокотехнологического бизнеса в России.

Все это характеризует актуальность темы работы.

Целью является: изучение электронной цифровой подписи как инструмента для придания юридической силы электронным документам.

Исходя из поставленной цели, можно выделить следующий круг задач:

- Раскрыть понятие и сущность электронной цифровой подписи как основного реквизита электронного документа. Условия использования электронной цифровой подписи.
- Виды и схемы электронной цифровой подписи.
- Рассмотреть особенности использования электронной цифровой подписи.

При работе над данной темой и решении поставленных задач использовались: нормативно-правовые источники, регулирующие использование электронную цифровую подпись, учебные пособия.

Понятие и сущность электронной цифровой подписи

Развитие систем электронного документооборота, электронных платежей, электронной почты, распространение информационных систем с большим количеством пользователей ставили задачу поиска такого инструмента взаимодействия посредством электронных средств, при котором пользователи, в том числе и посторонние, могли бы достоверно передавать информацию, точно идентифицировать источник любой информации, полученной по электронным каналам, и источник информации не мог бы отрицать своего авторства. Таким инструментом стали реквизиты, идентифицирующие электронный документ, которые во многом определяют его юридическую силу. Существует множество различных способов идентификации информации, записанной в электронном документе, которые отличаются степенью достоверности.

Так, С. Бернет и С. Пейн считают, что электронная подпись "...представляет собой любой знак или процедуру, осуществляемую электронными средствами, то есть выполняемую или принимаемую участвующей стороной с намерением связать запись с обязательством или удостоверить подлинность записи» . Согласно приведенному выше определению, электронная подпись может быть выходным сигналом сложного биометрического устройства, такого как компьютерная система распознавания отпечатков пальцев, или просто вводом имени в конце электронного сообщения, т. е. согласно этому определению, для электронной подписи не имеет значения технология ее создания электронными средствами.

Н. И. Соловьяненко также указывает, что символы, коды, пароли и т. д. связанные с электронным документом могут считаться электронными подписями, если они "исполнены или приняты сторонами по взаимному согласию и с явным намерением подтвердить подлинность письменного документа". В то же время Н. И. Соловьяненко справедливо считает, что доверие к электронной подписи обеспечивается по следующей общей схеме:

- во-первых, реализуется принятый международной практикой принцип функциональной эквивалентности, предполагающий, что во всех случаях, когда правовая система государства требует подписи, электронная подпись отвечает этим требованиям;
- во-вторых, между контрагентами заключается договор, определяющий возможность и условия использования электронной подписи в предпринимательской деятельности. "Стороны соглашаются, что электронные подписи, сопровождающие передаваемый документ, являются достаточными

для подтверждения того, что документ был создан соответствующей стороной."

Цифровая подпись, согласно С. Бернету и С. Пейну, может быть определена как "заданное преобразование записи с использованием асимметричной криптосистемы и хэш-функции таким образом, чтобы лицо, имеющее исходную запись и открытый ключ автора сообщения, могло точно определить, было ли преобразование выполнено с использованием секретного ключа, соответствующего открытому ключу автора, и была ли изменена исходная запись после выполнения ее преобразования" . Значение того, что С. Бернет и С. Термин "цифровая подпись" во многом согласуется с определением электронной цифровой подписи, сформулированным в пункте 3 ФЗ "Об электронной цифровой подписи": "цифровая подпись-это реквизит электронного документа, предназначенный для защиты этого 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", что приводит к выводу о том, что термины "цифровая подпись" и "цифровая подпись" следует рассматривать как синонимы.

Однако есть и другая точка зрения. Е. В. Ильиных и М. Н. Козлова указывают на необходимость разграничения таких смежных категорий, как "электронная цифровая подпись", "цифровая подпись" и "аналоги собственноручной подписи". Помимо цифровой подписи, аналоги цифровой подписи включают пароли, ПИН-коды, факсимильные изображения и т. д.цифровая подпись также является более общим понятием по отношению к электронной цифровой подписи. ЭЦП следует считать цифровой подписью, созданной с использованием системы сертификатов и центров сертификации.

Так, электронная цифровая подпись (ЭЦП) создается с использованием криптографической системы с открытым ключом, тогда как электронная подпись генерируется любым компьютерным методом, в том числе и криптосистемами с открытым ключом. Электронные цифровые подписи (ЭЦП) связаны с определенной технологией, электронные подписи являются более широким понятием и не зависят от технологии.

Российское законодательство знает и другие определения электронной цифровой подписи, и вот лишь некоторые из них

Электронная цифровая подпись (ЭЦП) - это компьютерный аналог подписи, которую мы ставим на документах, или подписи и печати.

Электронная подпись предназначена для идентификации лица, подписавшего электронный документ, и является полноценным аналогом собственноручной подписи в случаях, предусмотренных законом.

Использование электронной подписи позволяет:

- Контроль целостности передаваемого документа: в случае любого случайного или преднамеренного изменения документа подпись станет недействительной, поскольку она рассчитывается на основе исходного состояния документа и соответствует только ему.
- Защита от изменений (подделки) документа: гарантия обнаружения подделки при контроле целостности делает подделку в большинстве случаев нецелесообразной.
- Невозможность отказа от авторства. Поскольку вы можете создать правильную подпись только в том случае, если вам известен закрытый ключ, а он известен только владельцу, владелец не может отказаться подписать документ.
- Доказательство авторства документа: поскольку вы можете создать правильную подпись, Только зная закрытый ключ, а он известен только владельцу, они могут доказать свое авторство подписи под документом. В зависимости от деталей определения документа такие поля, как "автор", "внесенные изменения", "отметка времени" и т. д.

В сочетании с положениями ст. 4 ФЗ «Об электронной цифровой подписи», устанавливающей условия признания равнозначности ЭЦП в электронном документе и собственноручной подписи в документе на бумажном носителе, а именно:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи, - презумпция авторства в

значительной степени гарантировала бы юридическую силу электронного документа, заверенного ЭЦП.

Таким образом, стабильный электронный документооборот субъектов предпринимательской деятельности нуждается, прежде всего, не в разрозненных ведомственных нормативных актах, а в законе, детально регламентирующем порядок использования ЭЦП в электронном документе.

1. Виды и схемы электронной цифровой подписи

Схема электронной подписи обычно включает в себя:

- алгоритм генерации ключевых пар пользователем;
- функция вычисления подписи;
- функция проверки подписи.

Функция вычисления подписи вычисляет саму подпись на основе документа и секретного ключа пользователя. В зависимости от алгоритма функция вычисления сигнатур может быть детерминированной или вероятностной. Детерминированные функции всегда вычисляют одну и ту же сигнатуру из одних и тех же входных данных. Вероятностные функции добавляют в сигнатуру элемент случайности, что повышает криптографическую прочность алгоритмов ЭЦП. Однако вероятностные схемы требуют надежного источника случайности (либо аппаратного генератора шума, либо криптографически надежного генератора псевдослучайных битов), что усложняет реализацию.

В настоящее время детерминированные схемы практически не используются. Даже первоначально детерминированные алгоритмы теперь модифицируются, чтобы превратить их в вероятностные (например, вторая версия стандарта PKCS#1 добавила предварительное преобразование данных (OAEP) к алгоритму подписи RSA, который включает в себя, среди прочего, шум).

Функция проверки подписи проверяет, соответствует ли подпись документу и открытому ключу пользователя. Открытый ключ пользователя доступен каждому, поэтому любой желающий может проверить подпись под этим документом.

Поскольку подписанные документы имеют переменную (и довольно большую) длину, в схемах ЭЦП подпись часто ставится не на самом документе, а на его хэше. Криптографические хэш-функции используются для вычисления хэша, который гарантирует, что изменения документа будут обнаружены во время проверки

подписи. Хэш-функции не являются частью алгоритма ЭЦП, поэтому в схеме может быть использована любая надежная хэш-функция.

Алгоритмы ЭЦП делятся на два больших класса: обычные цифровые подписи и цифровые подписи с восстановлением документов. К подписываемому документу должны быть приложены обычные цифровые подписи. К этому классу относятся, например, алгоритмы, основанные на эллиптических кривых (ECDSA, ГОСТ Р 34.10-2001, ДСТУ 4145-2002). Цифровые подписи с восстановлением документов содержат подписываемый документ: при проверке подписи автоматически вычисляется тело документа. К этому классу относится один из самых популярных алгоритмов-RSA.

Следует различать электронную цифровую подпись и код подлинности сообщения, несмотря на схожесть решаемых задач (обеспечение целостности документа и неотрицание авторства). Алгоритмы ЭЦП относятся к классу асимметричных алгоритмов, в то время как коды подлинности вычисляются с использованием симметричных схем.

Виды электронной цифровой подписи:

Федеральный Закон Российской Федерации от 6 апреля 2011 года № 63-ФЗ. устанавливает следующие виды:

- Простая электронная подпись (ПЭП);
- усиленная электронная подпись (ЭП);
- усиленная квалифицированная электронная подпись (НЭП);
- усиленная квалифицированная электронная подпись (КЭП).

1. Особенности использования электронной цифровой подписи

Электронная цифровая подпись (ЭЦП) имеет не физическую, а логическую природу — это всего лишь последовательность символов (можно сказать кодов), позволяющая однозначно связать автора документа, содержание документа и владельца ЭЦП. Логическая природа электронной подписи делает ее независимой от материальной природы документа. Он может использоваться для маркировки и последующей аутентификации документов, имеющих электронную природу (выполненных на магнитных, оптических, кристаллических и других носителях, распространяемых в компьютерных сетях и т. д.). О том, какими техническими средствами это достигается, мы поговорим ниже, а пока остановимся на ряде положительных свойств ЭЦП, вытекающих из этого.

- Сопоставимость защитных свойств. При использовании сертифицированных средств цифровой подписи защитные свойства электронной подписи выше, чем у ручной. Более того, им можно дать объективную оценку, основанную не на гипотезе уникальности биометрических параметров человека, а на строгом математическом анализе. Отсюда вытекает принципиальная возможность сопоставимости защитных свойств ЭЦП.

Здесь и далее под средствами цифровой подписи понимается программное и / или аппаратное обеспечение ЭВМ, предназначенное для создания электронной цифровой подписи и для работы с ней.

- Масштабируемость. Свойство масштабируемости вытекает из возможности объективной оценки защитных свойств ЭЦП. Например, в гражданском документообороте можно использовать простейшие инструменты ЭЦП, в официальном документообороте — сертифицированные инструменты, а если речь идет о секретной информации, имеющей ограничительные реквизиты, то необходимо использовать специальные инструменты ЭЦП.
- Дематериализация документации. Независимость электронной подписи от носителей информации позволяет использовать ее в электронном документообороте. При использовании ЭЦП договорные отношения между удаленными юридическими и физическими лицами возможны без прямого или косвенного физического контакта между ними. Это свойство ЭЦП лежит в основе электронной коммерции.
- Эквивалентность копий. Логическая природа ЭЦП позволяет не различать копии одного и того же документа и делать их эквивалентными. Естественное различие между оригиналом документа и его копиями, полученными в результате тиражирования (воспроизведения), устраняется.
- Дополнительная функциональность. Механизм работы средств ЭЦП основан на криптографических средствах, и это позволяет расширить функциональные свойства подписи. В отличие от собственноручной подписи, электронная подпись может выступать не только как средство идентификации, но и как средство удостоверения подлинности документа. Вы не можете вносить изменения в электронный документ, подписанный ЭЦП, без нарушения подписи. То, что подпись не соответствует содержанию документа, выявляется программным обеспечением, и участник электронной сделки получает сигнал о несоответствии документа и подписи.
- Автоматизация. Механизм обслуживания ЭЦП основан на компьютерном оборудовании и программном обеспечении, поэтому он хорошо

автоматизирован. Все этапы обслуживания (создание, применение, сертификация и верификация ЭЦП) автоматизированы, что значительно повышает эффективность документооборота. Это свойство ЭЦП широко используется в электронной коммерции.

Однако использование электронной подписи в место рукописной имеет свои недостатки. Хотя автоматизация повышает производительность, она выводит механизм подписи из-под контроля естественными методами (например, визуальными) и может создать иллюзию благополучия. Поэтому использование ЭЦП требует специального технического, организационного и правового обеспечения. Основой для них должен стать "Федеральный закон Об электронной цифровой подписи", который на момент написания данной книги еще не был принят и существует только в виде проекта.

Заключение

В заключение можно сказать, что в настоящее время широкое применение информационных и коммуникационных технологий является глобальной тенденцией мирового развития и научно-технической революции последних десятилетий.

Субъекты предпринимательской деятельности взаимодействуют посредством электронного документооборота, как между собой, так и органами власти.

Основной задачей реформирования российского законодательства является переход к активному использованию электронного документооборота.

Правовой основой регулирования электронной цифровой подписи как инструмента для придания юридической силы регулируется Федеральным законом «Об электронной цифровой подписи».

Для стабилизации и безопасности электронного документооборота является, с одной стороны, прямое закрепление в нормах права презумпции авторства, в соответствии с которой электронная цифровая подпись в электронном документе признается созданной владельцем сертификата ее открытого ключа, если владелец сертификата ключа подписи не докажет обратное, а с другой стороны, установление обязанности удостоверяющих центров непосредственно проверить соответствие данных, изложенных в заявлении на изготовление сертификата ключа электронной цифровой подписи, предоставленным документам.

Правовое регулирование по использованию такого электронного аналога собственноручной подписи, как электронная цифровая подпись (ЭЦП) в действующих нормах права законодательно закреплено равенства как собственноручной и электронной цифровой подписи при условии соблюдения требований закона

ЭЦП позволяет подтвердить ее принадлежность зарегистрированному владельцу и является неотъемлемой частью электронного документа.

В моем понятии считаю, что электронный документ – это информация, которая представлена в электронной форме.

1. ФЗ от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи» (в ред. от 23. 06.2005 г.) // Российская газета. - 12.01.2002. - № 6. ↑