Закон об ЭЦП принят. Что дальше?

С. В. ВИХОРЕВ,
директор Аналитического Департамента
ОАО «ЭЛВИС-ПЛЮС»

Вот уже почти полгода Россия живет в «новую» эпоху, эпоху юридически значимых электронных документов.

Закон об ЭЦП уже принят, первый год уже прошел. Можно подводить некоторые итоги. Что изменилось? Решил ли этот закон все проблемы? Вот некоторые вопросы, которым посвящены эти материалы. Автор относит к их жанру «лирического эссе с юридическо-техническим уклоном».

Развитие человеческого общества на современном этапе нельзя себе представить без информационных технологий. За сравнительно короткую свою историю эти технологии сами прошли бурное развитие. Естественно, что вместе с ними развивались и технологии обеспечения безопасности информации.

Общеизвестно, что любая система безопасности должна строиться комплексно и охватывать все участки защищаемого технологического процесса, на всех этапах его жизненного цикла. Применительно к информационной сфере, решения по обеспечению безопасности информации должны обеспечивать равнопрочность защиты на всех этапах ее обработки и транспортировки. Иначе, наличие хотя бы одного незащищенного или слабо защищенного участка может сделать неэффективным вложения средств во все остальные меры защиты. Одним из таких участков как раз и является процесс обмена информацией, имеющей юридическую значимость.

Немного истории (к вопросу о постановке проблемы)

Еще не так давно, никто не задумывался о проблеме юридической значимости электронных сообщений. Действительно, нет сообщений – нет проблемы. Но вот эти самые сообщения появились (мы еще вернемся к этому). А потом этих сообщений стало много, и они стали нужны в деловых отношениях. А тут, аккурат, перестройка подоспела, все ускорялось, появилась необходимость и быстро совершать сделки, быстро обмениваться сообщениями, в том числе и таким, от которых многое зависит. Но мир не идеален, раз есть отношения, значит, есть и споры, значит, их надо решать. А суды эти «писульки» не принимают, мол, они не подписаны, мы не знаем что это такое, а посему они не имеют силы. Стали слышны голоса: «Караул! Нам не дают работать! Нас зажимают!».

Тогда общество, в лице государства, задумалось: а действительно, можно ли доверять электронным сообщениям, не произошла ли их подмена в автоматизированной системе? Думало оно думало и, наконец, решило: доверять-то можно, но чтобы не было сомнений – сообщение, как положено, надо подписать! Сказано – сделано: «полученный из автоматизированной системы документ приобретает юридическую силу после его подписания должностным лицом в порядке, установленном российским законодательством» –

сказало оно. Потом подумало еще и добавило: «юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью». А чтобы все об этом знали, все это записало в Законе «Об информации, информатизации и защите информации»[1]. Казалось бы, все в порядке – работайте на здоровье!

Но голоса не смолкли, а наоборот, стали еще сильнее: «Нам не сказали, как пользоваться этой самой электронной подписью! Нам мешают общаться, нам мешают торговать!». Хотя, автору кажется, что здесь была доля лукавства – ведь в системе S.W.I.F.T., Reuters юридически значимыми сообщениями (кстати, цена которых иногда очень велика) к этому времени уже обменивались, да и сейчас продолжают обмениваться. Да и действующий в то время Арбитражный кодекс говорил о допустимости представления в суд документов, полученных «посредством факсимильной, электронной или иной связи, либо иным способом». Это еще в августе 1994 года подтвердил Высший Арбитражный Суд[2] РФ. «Изготавливать и подписывать договоры с помощью электронно-вычислительной техники и использованием системы цифровой подписи вполне допустимо. После возникновения конфликта стороны могут представить суду доказательства, заверенные такой подписью». Правда, Суд оговорил, что при разногласиях, необходим договор, определяющий процедуру устранения разногласий сторон и порядок определения достоверности подписи. И еще раз год спустя, тот же уважаемый Суд подтвердил, что «при подтверждении юридической силы документа электронной цифровой подписью, этот документ может признаваться в качестве доказательства по делу, рассматриваемому арбитражным судом»[3].

Государство еще раз задумалось (почти на пять лет), подумало, подумало, и решило по нажимом этих самых голосов в 2001 году выпустить еще один закон – Закон «Об электронной цифровой подписи». Этот закон[4], направленный на определение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых она признается равнозначной собственноручной подписи, с одной стороны, ввел определенный порядок подписи электронных документов государственных учреждений, установил процедуру подтверждения правомочности электронной подписи специальными органами (сертификационными центрами), а с другой стороны, предоставил определенную свободу действий по организации подписи электронных документов в корпоративных сетях.

Да, еще очень немаловажный факт: появилась возможность признать иностранную цифровую подпись, удостоверенную в соответствии с законодательством иностранного государства на территории России при выполнении наших, российских процедур признания юридического значения иностранных документов[5].

Ну, и что изменилось? Да, практически, ничего. Тот же порядок, что действовал раньше (работа на договорной основе) для тех, кто занимался бизнесом – остался, да голоса о том, что не хватает законодательной базы для ведения электронного бизнеса, стали тише. И вот уже прошло почти полгода, а бурного взрыва обменом юридически значимыми электронными документами что-то не отмечается. Где раньше был этот самый обмен – там и сейчас есть, а где его не было – там и нет.

Кто-то, прочитав эти строки, подумает: «Эк, автор загнул! Скоро сказка сказывается, да не скоро дело делается». Может быть и так, а может быть причина в другом? Может быть причина в том, что еще нет надежных средств создания электронной подписи, надежной и простой системы, позволяющей любому применить эту самую электронную

---

[1] Федеральный Закон «Об информации, информатизации и защите информации», 1995 г., ст. 5
[2] Письмо ВАС от 19.08.1994 г. № С1-7 / ОП-578.
[3] Письмо ВАС от 7.06.1995 г. № С1 / ОЗ-316
[4] Федеральный закон «Об электронной цифровой подписи», 2002 г., ст. 1
[5] Федеральный закон «Об электронной цифровой подписи», 2002 г., ст. 18

подпись и которой можно доверять? То есть вся проблема из правовой смещается в техническую сферу.

Еще немного истории (о том с чего же все это началось)

В прошлом веке, когда все это начиналось, вычислительные машины (еще не «компьютеры, а «ЭВМ») были достаточно громоздки и дороги. Они использовались, как правило, в качестве «электронных счетов» для решения расчетных задач и математического моделирования различных процессов в автономном режиме. Потом их стали использовать в системах управления различными процессами. Позже возник момент, когда информация, обрабатываемая такими машинами, оказалась сосредоточена в одном месте, а пользователь этой информации находился в другом месте. Да и математические модели становились все сложнее, и ресурсов одной ЭВМ уже не хватало. Вот и возникла необходимость несколько машин соединить в одну сеть. К этому времени сами ЭВМ стали намного дешевле и более компактными. Но это еще не революция.

А вот когда ЭВМ стали совсем маленькими и доступными достаточно широкому кругу специалистов, и когда родилась идея с их помощью передавать друг другу информацию, вот тогда и произошла революция. Персональный компьютер, как теперь стали называть ЭВМ, превратился из средства моделирования и расчетов в средство общения, средство передачи информации. А потом уже были Интернет-технологии, которые позволили создать глобальные информационные сети. Это было как нельзя кстати, так как на дворе начинался информационный бум. И все бы было хорошо в нашем королевстве, если бы не одно «но». В бочке меда оказалась ложка дегтя. Переход от автономного использования компьютеров к сетевым технологиям породил одну очень существенную проблему, которой раньше даже не могли себе представить. Это и была проблема подтверждения подлинности сообщения.

Для бумаги все просто. Подпись на протяжении веков является обязательным реквизитом любого документа, как служебного, так и личного. Еще при Иване Грозном наиболее важные документы скреплялись Большой государственной печатью и собственноручной подписью, при осуществлении каких либо сделок с неграмотным человеком, требовалось приложение к документу оттиска его пальца или проставление «креста». (Это очень важно! к этому мы вернемся чуть ниже!) Но и раньше и сейчас иногда на документах можно увидеть воспетую классиками «резиновую печать «Отказать. Полыхаев»» – факсимиле. Это очень удобный заменитель, точно копирующий рисунок собственноручной подписи. Безусловно, факсимиле может служить дополнительным признаком, подтверждающим подлинность документа, но ни как не основным.

О чем идет речь (суть проблемы)

С электронными посланиями все немного сложнее. Требуется не только подтверждение юридической значимости полученного сообщения (аутентификация), но и подтверждение личности того, кто отправил сообщение (идентификация)[6]. Да еще надо подумать о том, чтобы само сообщение дошло без искажений. Таким образом, решение одной проблемы выливается в решение трех взаимосвязанных задач:

- подтверждение авторства сообщения (идентификация);
- подтверждение подлинности сообщения (аутентификация);
- обеспечение целостности передаваемой информации.

---

[6] Для справки. Согласно энциклопедическому словарю (изд. 1988 года под редакцией А. М. Прохорова):
Идентификация – установление тождества объекта или личности по совокупности общих и частных признаков, например идентификация личности по почерку, по следам рук.
Аутентификация – официальное признание текста равнозначным другому тексту, составленному на другом языке (в том числе и машинном – ***авт.***) и имеющим одинаковую с ним юридическую силу.

А это уже задачи защиты информации.

Не будем пока трогать проблему целостности, а поговорим о технической возможности подтверждения подлинности сообщения и его авторства.

В настоящее время метод электронной цифровой подписи (ЭЦП) становится доминирующим в процессе идентификации автора и аутентификации самого электронного сообщения. На этой основе построены практически все действующие стандарты и системы электронного документооборота и электронной торговли.

В мировой практике под электронной подписью понимается, вообще говоря, символ или некоторый другой идентификатор, созданный электронными средствами, обрабатываемый или принимаемый другой стороной с намерением подтвердить подлинность электронного сообщения. Принципы и алгоритмы при этом могут применяться самые разнообразные. (Вопрос о надежности того или иного алгоритма здесь не обсуждается).

Сам по себе процесс подтверждения электронного документа ЭЦП достаточно сложен. Его изучение требует знания основ криптографии и выходит за рамки этой статьи. Отметим только, что этот процесс не возможен без наличия так называемого «секретного ключа», который хранится только у отправителя, и тесно связанного с ним «открытого ключа», которым может владеть любой пользователь на другом конце. На основе «секретного ключа» передаваемое сообщение снабжается специальным атрибутом, а математические методы позволяют однозначно определить с использованием на другом конце «открытого ключа», откуда оно было отправлено. От сохранности «секретного ключа» напрямую зависит степень надежности любой системы ЭЦП.

Иными словами мы сталкиваемся с одной из важнейших проблем – проблемой отделимости такой подписи от ее владельца. Собственноручная подпись (то есть автограф) по вполне понятным причинам неотделима от ее обладателя. Совсем другое дело ЭЦП, точнее ее «секретный ключ», который, к сожалению, представляет собой определенный файл, хранимый, как правило, в компьютере автора сообщения и, естественно вполне отделим. Доступ к этому ключу осуществляется на основе пароля, записанным на интеллектуальной карте, токене или другом аналогичном устройстве (идентификаторе). Такой подход нельзя считать надежным и удобным, особенно при массовом использовании. Владелец этой карты может ее передать другому лицу или даже потерять. И, конечно же, новый владелец может воспользоваться этим паролем для подписи фиктивного сообщения.

Таким образом проконтролировать правомерное использование «секретного ключа» является достаточно проблематичной задачей, особенно с доказательной для арбитража точки зрения. Как видно, в данном случае ЭЦП может исполнять роль только факсимиле, но ни как не автографа автора. (Вспомните, как в Государственной думе первых созывов, при голосовании «электронными карточками» число голосов оказывалось больше числа присутствующих в зале депутатов.)

Можно ли сделать электронный цифровой автограф?

Так в чем же собственно существенная разница между собственноручной подписью (автографом) и факсимиле? Самое существенное то, что факсимиле может существовать отдельно от автора, а автограф – нет (это, кстати, и ответ некоторым «оппонентам», уже ратующим за изменение нового закона об ЭЦП и предлагающих закрепить подпись не за физическим, а за юридическим лицом – мол, это удобнее, – может это и удобнее, но вряд ли юридически правильно). Все упирается в то, что при формировании автографа используются биометрические параметры самого человека (нажим, скорость письма, характерные росчерки и пр.), а факсимиле может ставить и автомат. Заметим также, что ЭЦП это результат «математических преобразований», а не оцифрованный образ рукописной подписи. Между тем, существует целый ряд методов, позволяющих с очень высокой степенью достоверности обеспечить привязку ЭЦП к автору сообщения. Примером может служить технология цифровой обработки биометрических параметров: папиллярного узо-

ра отпечатка пальца, радужной оболочки глаза, наконец, самого рукописного автографа. Только в этом случае можно говорить, что электронная цифровая подпись стала аналогом собственноручной подписи (автографа). Проблема отделимости ЭЦП от автора сообщения или, что в принципе, одно и то же, проблема сохранности «секретного ключа», может быть решена путем жесткой привязки процесса формирования и использования «секретного ключа» к какому-либо биометрическому параметру человека. Такая привязка должна обеспечить надежное закрытие собственно «секретного ключа» и включение образа биометрического параметра в состав электронного сообщения.

Вместе с тем, необходимо отметить, что спрос на системы, которые это умеют делать, будет только в случае их достаточной дешевизны. Такая система, на взгляд автора, должна как минимум обеспечивать:

- формирование собственно электронно-цифровой подписи;
- распознавание образа, созданного на основе биометрического параметра;
- включение этого параметра в электронное сообщение;
- закрытие «секретного ключа» на основе образа биометрического параметра;
- обработку сообщения у получателя.

Целесообразно было бы, что бы такие системы дополняли уже существующие системы защиты информации и формирования ЭЦП. Это позволит получить комплексную систему обеспечения безопасности информации корпоративных сетей. Наиболее простым в этом случае может быть использование специальных дактилоскопических датчиков, вырабатывающих парольный код, только при совпадении папиллярного узора (вспомните «приложение к документу оттиска пальца»). При этом сам код должен применяться не только как пароль для входа в систему, но и непосредственно участвовать в процессе генерации «секретного ключа». Плохо, что существующие и международные, и российские стандарты, применяемые в электронном документообороте и электронной торговле, к сожалению, не охватывают эту проблему, утверждая, что она выходит за их рамки. Но с другой стороны это позволяет разработчикам систем ЭЦП активно начать их применение («что не запрещено, то разрешено»).

Кстати, еще одна проблема

Это проблема создания, хранения и управления закрытыми и открытыми ключами или, как говорят специалисты, построение инфраструктуры PKI. Естественно, что сама по себе инфраструктура обеспечения ЭЦП это достаточно сложная автоматизированная система и она сама требует определенных мер защиты (если не сказать больших). Ведь, как ни крути, а именно в этой системе сосредоточена вся наиважнейшая информация об адресатах и их «закрытых ключах». Но и «открытые ключи», как ни странно, тоже требуют усиленной защиты. Ведь сам такой ключ справедлив только в том случае, если сопровождается неким специальным документом – цифровым сертификатом (и, заметьте, этот документ тоже электронный и на него распространяются все правила, применимые к таким документам). Отметим, что, хотя подделать такой цифровой сертификат без «закрытого ключа» практически невозможно, изменить содержимое самого сертификата – реально. А это уже предпосылка к невозможности его аутентификации, то есть сама система отторгнет этот документ. Если это так, то о какой инфраструктуре ЭЦП может идти речь?

Кроме того, надо предусмотреть еще и процедуру аннулирования ЭЦП. Это необходимо на случай, если произойдет какой-нибудь сбой в системе или владелец сертификата перестанет заслуживать доверия.

Несколько слов о роли даты

Обычно документ считается документом, если есть дата его регистрации. В электронных сообщениях дата становится одним из важнейших параметров (реквизитов).

Правда и здесь происходит некоторая трансформация. Наверное, правильнее говорить не столько о дате, сколько о точном времени создания электронного сообщения. Проблема синхронизации действий всех средств относительно единого источника времени – единой точки отсчета – это еще одна большая проблема, которая выходит за рамки этой статьи.

Допустим, что любое электронное сообщение перед передачей его в канал связи регистрируется и маркируется специальным атрибутом, в котором содержится точное время его отправки и сведения о том сервере, откуда он отправлен. Допустим так же, что имеется некий злоумышленник, который смог-таки создать фальшивый электронный образ папиллярного узора автора сообщения. Чтобы внести какие-либо изменения в истинное электронное сообщение, ему нужно время. Время прохождения сигнала электронного документа по каналам связи, в принципе, всегда заранее известно. Поэтому, получив электронное сообщение с временной меткой всегда можно сверить время его прохождения и при различиях во времени (например, задержка в его получении), приемный сервер всегда может запросить у передающего подтверждение отправки документа. Если же повторное сообщение не совпадает с первоначально полученным сообщением, то можно с уверенностью говорить, что произошло несанкционированное вмешательство.

Таким образом, временная метка становится одним из важнейших элементов подтверждения подлинности электронного документа. Она в данном случае играет роль мастичного штампа учреждения с датой и регистрационным номером документа.

Вместо заключения

Итак, что мы имеем? Дата и время создания электронного сообщения – близко к понятию штамп с регистрационным номером. ЭЦП без биометрических параметров – факсимиле. ЭЦП с биометрическими параметрами – собственноручный автограф.

То есть, формируемая ЭЦП должна содержать метку времени, а при ее формировании должны использоваться биометрические параметры человека, которому она принадлежит. Эти вопросы выходят за рамки юриспруденции и, вряд ли, должны быть включены в законы, но они достойны быть включенными в стандарты, определяющие требования к средствам создания ЭЦП (не к алгоритмам «математических преобразований», а именно к техническим средствам).