К вопросу об эквивалентности электронно-цифровой и собственноручной подписей

1. Постановка задачи

То, что такие достижения материальной цивилизации, как электронная почта и интернет, заметно облегчают обмен информацией, бесспорно. Но любое нововведение, как известно, порождает новые проблемы. Когда сведения собственноручно написаны на бумаге (да к тому же еще и скреплены подписью), особых трудностей с определением источника этих сведений не возникает, а вот если это электронный документ?

Нужен какой-то электронный эквивалент собственноручной подписи. Если мы попробуем «буквально» перенести процедуру подписывания с простой бумаги на компьютер (путем дописывания в конец файла определенной последовательности символов), то мою подпись любой человек сможет дописать в конец любого файла. Соответственно, такая подпись имеет смысл только тогда, когда все друг другу полностью доверяют, а подпись нужна исключительно для того, чтобы понять, с кем я разговариваю. В общем же случае (особенно если речь идет о банковских или государственных системах) такой подход, конечно, не применим.

Цель данной статьи – продемонстрировать один из возможных подходов к поиску эквивалентов собственноручной подписи для электронных документов. Я не претендую на полноту и исчерпывающую точность приведенного анализа – это дело специалистов в соответствующей области и требует большой работы. Здесь же я хотел бы только наметить обхий ход такого анализа.

2. Подход функциональной аналогичности

Электронная подпись – это аналог собственноручной подписи для электронных документов. Из этого понятно, каким должен быть ход наших рассуждений. Нужно посмотреть, какие функции выполняет собственноручная подпись в случае бумажных документов и в чем состоят отличия электронного документа от бумажного. После чего мы должны создать такую сущность, которая выполняла бы те же функции, но с учетом выявленных отличий. Этот подход носит название «подхода функциональной аналогичности», он был сформулирован во Введении к Типовому закону ЮНСИТРАЛ о правовых аспектах электронного обмена данными 1995 года.

Итак, какие же функции выполняет подпись? Сформулируем вопрос в более общем виде: какими функциональными признаками обладает подпись под бумажным документом?

a) Однозначное соответствие подписи ее владельцу. Более строго: существуют методы определения принадлежности данной подписи данному человеку. В случае бумажных документов это осуществляется путем сверки подписи с оригиналом, записанным в паспорте. Предполагается также и то, что процедура проверки должна происходить без участия владельца подписи.

b) Привязка подписи к документу. Это означает, во-первых, что подписанный документ невозможно изменить (точнее – существуют методы проверки подлинности документа), и во-вторых, что подпись невозможно перенести на другой документ (с тем же примечанием).

c) Собственно говоря, главное свойство подписи – человек ставит подпись, укрепляя тем самым за собой некоторую ответственность. Это означает, что подпись должна ставиться всегда осознанно. Поэтому, например, в качестве подписи нельзя использовать отпечатки пальцев. Они хотя и удостоверяют личность как нельзя лучше, тем не менее, могут буть поставлены, так сказать, без ведома их владельца. Впрочем, это не снимает ответственности с человека, если он поставил подпись «не подумав» – несмотря на все достижения технологий исуственного интеллекта, думать все-таки приходится.

Теперь разберемся с отличиями электронного документа от бумажно.

a) Строгая математичность. Индивидуума с его бесконечными свойствами для компьютеров не существует. Копия эквивалентна оригиналу.

b) Можно произвольно изменять любые данные, не оставляя физических следов.

c) Существует две формы информации – машинная и человеческая. Все действия производятся в машинной форме, для человека же они остаются невидимыми. Отображение информации в доступной для человека форме требует определенных алгоритмов

преобразования. За счет использования этих алгоритмов (особенно если они не вполне корректны) информация может существенно искажаться.

3. Определения

Итак, введем строгое *функциональное* определение подписи.

Под «подисью» мы будем понимать функциональную целостность, назначением которой является установление ответственности некоторого лица за некоторую информацию.

В соответствии с выявленными функциональными признаками подписи, эта целостность будет включать в себя не только сам процесс подписывания документа, но и методы идентификации владельца подписи, методы проверки подлинности документа и т.д.

Заметим, что в силу принципа функциональной аналогичности, это определение одинаково подходит и для собственноручной, и для электронной подписи.

Мы не ставим цели создать идеально надежную электронную подпись – это попросту невозможно, поскольку в мире не бывает ничего идеального. С другой стороны, оставить все как есть мы тоже не можем. Нужен какой-то разумный критерий надежности электронной подписи. Учитывая все тот же принцип функциональной аналогичности, можно ввести такое определение.

Электронную подпись будем считать надежной, если возможность ее подделки по крайней мере не выше, чем для ее «традиционных» функциональных аналогов.

4. Специфические проблемы элетронной подписи

Мы выявили 3 признака подписи и 3 отличия электронных документов от бумажных. Попробуем теперь построить матрицу 3х3, с помощью которой проследим те проблемы, которые возникают при попытке удовлетворить каждому из признаков подписи в связи с каждым отличием электронных документов от бумажных. На первом месте стоит номер (буква) свойства, на втором – номер отличия.

aa) Проблема обеспечения однозначного соответствия подписи владельцу с учетом того, что копия эквивалентна оригиналу. Если в случае собственноручной подписи повторение ее крайне сложно технически, то для электронной подписи сложность может представлять только “добыча” чужой подписи – если подпись известна, повторить ее сможет любой.

ab) Проблема обеспечения однозначного соответствия подписи владельцу с учетом возможности изменять любые данные. Кто-то может сгенерировать ЭЦП, зарегистрировать ее на мое имя и подписывать ей что угодно, а отвечать мне?

ac) Проблема обеспечения однозначного соответствия подписи владельцу с учетом возможного несоответствия человеческой и машинной информации. Если использовать в качестве подписи образцы голоса, изображения и т.п., злоумышленник может “обмануть” компьютер, вручив ему вместо голоса владельца магнитофонную запись, либо просто скопировав уже оцифрованные данные.

ba) Проблема обеспечения привязки подписи к документу с учетом того, что копия эквивалентна оригиналу. В случае бумажного документа подпись «привязывается» к документу физически – скопировать ее будет крайне трудно. В случае же электронного документа физической привязки будет недостаточно – ее можно будет легко «отвязать» и привязать к чему угодно.

bb) Проблема обеспечения привязки подписи к документу с учетом возможности изменять любые данные. Возможно изменение уже подписанного документа.

bc) Проблема обеспечения привязки подписи к документу владельцу с учетом возможного несоответствия человеческой и машинной информации. В случае электронного документа, вообще говоря, нет гарантий того, что текст, который я вижу на экране, и текст, который я подписываю являются одной и той же сущностью. От меня ведь требуется только подпись, а уже сам процесс подписывания происходит без моего участия.

ca) Проблема гарантии осознанности подписывания документу с учетом того, что копия эквивалентна оригиналу. В отличие от собственноручной подписи, которую приходится каждый раз тщательно “копировать”, электронную подпись можно поставить случайно – особенно в том

случае, когда она ставится (как любят говорить в рекламных лозунгах) “одним щелчком мышки”.

cb) Проблема гарантии осознанности подписывания с учетом возможности изменять любые данные. Такой проблемы, видимо, нет.

cc) Проблема гарантии осознанности подписывания с учетом возможного несоответствия человеческой и машинной информации. Возможно, что из информации, отображенной на экране, будет не вполне понятно, что происходит подписывание. Подпись опять может оказаться на документе без воли ее владельца.

5. Пути решения проблем

Итак, электронную подпись будем считать надежной, если возможность ее подделки по крайней мере не выше, чем для ее «традиционных» функциональных аналогов. Задачу будем считать решенной, если доказана *возможность* обеспечения такой надежности, т.е. задача свелась к чисто технической.

Искать решения этих проблем будем исходя из того же принципа функциональной аналогичности. Но сначала, чтобы лучше понять суть любой аналогии, приведем одну цитату:

«Первый из объектов аналогии - это как бы "пользователь аналогии", а второй - как бы "поставщик нового знания". Ведь обычно, как минимум, делается вывод о том, что в первом интересующем нас предмете, возможно, имеется-таки еще один признак X, который пока в нём ещё не обнаружен, но - точно - есть во втором из предметов. <…>

Идея поиска этого "X" тривиальна: надо посмотреть, чего очень желаемого и полезного нет в данной системе, но есть в другой системе и сделать **что-то** так, чтобы это X стало существовать и в данной системе. А если не известно, как этого добиться, надо ещё внимательнее изучить аналог и понять, как же всё-таки это в нём достигнуто.

Достигнув понимания, будут пытаться, воздействуя на первый (П1) предмет аналогии, как бы то ни было *переделать* его так, чтобы это обнаруженное в П2 свойство X в переделанном объекте (П1') всё-таки обеспечить» [1, стр. 242]

В нашем случае под предметом П1 следует понимать электронную подпись, под П2 – собственноручную.

Заметим, что если бы мы взялись решать поставленную задачу во всем ее объеме, то надо было бы разделить «подпись» как функциональную целостность на 5 видов процессов. Создание подписи, хранение подписи, использование подписи (т.е. не только сам процесс подписывания, но и процессы дальейшего распространения и храниения подписанных документов), изменение подписи (не только изменение моей личной подписи, но и развитие всей функциональной структуры в целом – скажем, как быть в случае, если компания переходит на новую технологию) и утилизация подписи (в случае компрометации или истечения срока годности). Независимо от этого следовало бы провести еще разделение на внутренние функции (т.е. технологии электронной подписи) и внешние функции (т.е. юридическое регулирование использования электронных подписей). Таким образом у нас получится уже не матрица 3х3, а 4-мерная струкрута размером 3х3х5х2=90 ячеек, каждую из которых, по-хорошему, надо бы проанализировать (впрочем, многие ячейки, видимо, оказались бы пустыми – но ведь это надо проверить!). Такой подход, хотя и гарантирует, что мы уже точно ничего не забудем, требует все-таки слишком больших трудозатрат и может быть использован только специалистами при разработке соответствующих вопросов. Я же позволю себе в качестве демонстрации рассмотреть только некоторые проблемы.

Скажем, технический аспект проблемы (aa) в процессе использования подписи. Как технически обеспечить секретность подписи в процессе ее использования? Это достигается с помощью асимметричных систем шифрования – есть секретный ключ, который знает только владелец, и открытый ключ, который знают (или имеют возможность узнать) все. С помощью первого происходит подписывание документа, с помощью второго – проверка. Та же проблема в процессе создания подписи накладывает определенные требования на алгоритмы формирования секретного и открытого ключей – а именно, необходимо, чтобы зная открытый ключ, получить секретный было невозможно (в разумные сроки). Юридический аспект этой проблемы заключается в создании стандарта на алгоритмы электронной подписи. Дело осложняется тем, что существуют разные алгоритмы, и – вдруг на следующий день после принятия закона будет

доказано, что данный алгоритм неустойчив? Поэтому вместо введения единого стандарта, в Законе [2] говорится о сертификации средств ЭЦП (ст. 5). Сертификация также дает некоторую априорную гарантию того, что данная компания использует «правильные» алгоритмы.

Технический аспект проблемы (ba) в процессе использования подписи попробуем исправить по аналогии с собственноручной подписью. Каким образом в бумажных документах достигается привязка подписи к тексту докмента? Дело в том, что подпись и сообщение изменяют сам носитель информации – бумагу, в результате оказываются к ней физически привязанными. Понятно, что электронные документы нельзя подписывать, физически изменяя носитель (впрочем, это возможно, если использовать в качестве носителя ПЗУ, в котором будет просто-напросто прошито и сообщение, и подпись, но ценность такого подхода не просто нулевая, а даже отрицательная – удобнее все-таки использовать бумагу, чем электронные карточки). Нужен какой-то аналог бумаги – нечто, жестко связанное и с документом, и с подписью. Для этого используется хэш-функция – функция, вычисляемая по тексту документа, причем должно выполняться очевидное условие технической сложности подбора документа по известной его хэш-функции. В таком случае сама хэш-функция является аналогом неподписанного листа бумаги, а зашифрованная секретным ключом – подписанному.

Теперь рассмотрим, например, юридический аспект проблемы (ab) в процессе создания подписи. Кто-то может сгенерировать ЭЦП, зарегистировать его на мое имя и подписывать им что угодно.

Здесь существует два решения. Первое заключается в том, что я лично передаю свой открытый ключ всем, с кем я намерен вести переписку. Применимость такого решения весьма ограничена (не со всеми можно встретиться лично, невозможно заранее предусмотреть всех адресатов). Второе решение заключается в создании Удостоверяющего Центра. В качестве такого центра выбирается лицо, которому все доверяют, и с которым хотя бы один раз могут встретиться лично, либо имеют надежный (т.е. не допускающий искажений/подделок) канал связи. После выбора такого лица, все участники обмена генерируют свои пары ключей и, взяв свой открытый ключ, направляются в Удостоверяющий Центр, который на устраивающих всех условиях удостоверяет личность пришедшего, добавляет к его открытому ключу некоторые дополнительные сведения: имя владельца, другие идентифицирующие данные, сроки действия ключа, перечень информационных систем, в которых допустимо его использовать и другая информация и подписывает своим секретным ключом (см. статью 6 Закона [2]). Все это вместе (открытый ключ, блок данных и ЭЦП) называется *сертификатом открытого ключа*.

Технический аспект этой проблемы сводится, таким образом, к созданию Центра Сертификации – а там, в свою очередь, возникают новые проблемы – как технические, так и юридические. Попытку решения юридических проблем, связанных с созданием Центров Сертификации, представляет собой третья глава Закона [2].

И на последок одна проблема, решения которой пока не существует. Рассмотрим технический аспект проблемы (ac) в процессе использования подписи. Здесь существует одна лазейка для злоумышленника. Можно (с помощью вируса) отслеживать, когда происходит подписывание, и «подсовывать» на подпись какой-то другой документ.

Надо заметить, проблемы связанные с тем, что иформация, отображаемая на экране, и информация, с которой работает компьютер – это разные вещи, почему-то упорно игнорируются. Единственное доступное решение – сначала подписывать документы, а потом – уже в другом формате – отправлять их по почте с подписью (отдельно). Это решение, действительно, довольно эффективно, но крайне неудобно. Как же быть, если, например, требуется подписать какой-нибудь документ не у себя дома, а, скажем, в банке? Пока такие ситуации в обыденной жизни не встречаются, но нужно быть готовыми к тому, что в ближайшем будущем это станет вполне реальным. Где гарантии того, что я подписал именно то, что мне показали на каком-то экранчике? И как я потом буду в суде доказывать, что «я-то, знаете, совсем даже не это подписывал»? Можно предложить разве что (как в случае с бумажными документами) хранить копию у себя. В таком случае потребуется, конечно, подпись другой стороны, которую хорошо бы проверить «не отходя от кассы». Словом, здесь возникает целый ряд не столь тривиальных проблем, которые, видимо, делают массовый переход от бумажных документов к электронным пока очень опасным.

6. **Список литературы**

1. И.П. Беляев & В.М. Капустян, «Системный анализ: прикладной аспект», Москва - 1999, 360 стр. Именно использована глава 5: Системная аналогика.
2. Федеральный Закон Российской Федерации от 10 января 2002 г. N 1-ФЗ «Об электронно-цифровой подписи» (http://www.rg.ru/oficial/doc/federal_zak/128_F3.shtm).
3. Владислав Мяснянкин, Андрей Межутков, «Электронная подпись или тернистый путь избавления от бумаги» (http://www.free-unices.org/~cybervlad/ecp/).
4. В.Л. Полещук, «Правовой статус информации размещенной в Интернет: проблемы признания электронных публикаций и обеспечения их доказательственной силы» (http://bilimdon.uz/library/publ.php?s=view&id=77).
5. Виктор Любезный, «Электронная цифровая подпись: законы и реалии» (http://www.crime-research.ru/library/Lubezniy.html).
6. К.ю.н., доц. О.В. Ефремкина, «Электронная цифровая подпись в ЕС (правовой аспект)» (http://www.eulaw.edu.ru/documents/articles/eu13.htm).
7. М.М. Дутов, «Сравнительный анализ европейского законодательства в области электронного документооборота» (http://jur-lib.kharkov.ua/dutov/5.htm). Там же есть ссылки на европейское законодательство.
8. Американское законодательство:

   http://www.uncitral.org/english/workinggroups/wg_ec/wp-84.pdf

   http://www.uncitral.org/english/sessions/unc/unc-34/acn-493e.pdf

   http://www.uncitral.org/english/workinggroups/wg_ec/wp-82.pdf