Технические инструменты обеспечения доверия к электронным документам при их использовании и хранении

Курило А.П. КТН,
Доцент
АО РНТ
Главный эксперт

Постараемся заглянуть в будущее, оно даст ответ

О Риме и истории того времени мы знаем столько много только потому,
что империя была правовым государством и очень многие события, записывались,
а архивы дошли до наших дней.
Бумага как носитель информации обладает свойством обеспечения аутентичности.
Этот вопрос очень важен для историков, та как аутентичность информации об исторических событиях позволяет сформировать точную картину мира.

Что будут знать о нашем времени через 2000 лет,
если мы полностью перейдем на электронные документы?

Как обеспечить аутентичность на протяжении столь длительного времени?

Как ввести ЭД в гражданско- правовой оборот сейчас, когда живет и развивается наше Общество и государство и мы все в этом заинтересованы?

Нужно ли заниматься этим вопросом?

Что и как делать.

О чем говорит статья 6 ФЗ № 63-ФЗ «Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью»

- *Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации.*
- *Электронный документ, подписанный усиленной электронной подписью признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью.*
- *Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов.*

Достаточно ли этого на практике?

- Для обеспечения равнозначности двух форм документов – да, при условии действительности ЭП, но как оказывается, равнозначность может быть установлена и без ЭП;
- Для введения в правовой оборот – в общем случае, недостаточно, нужны дополнительные атрибуты и свидетельства доверия.

  В вырожденном случае – если суд решит, то да, достаточно.

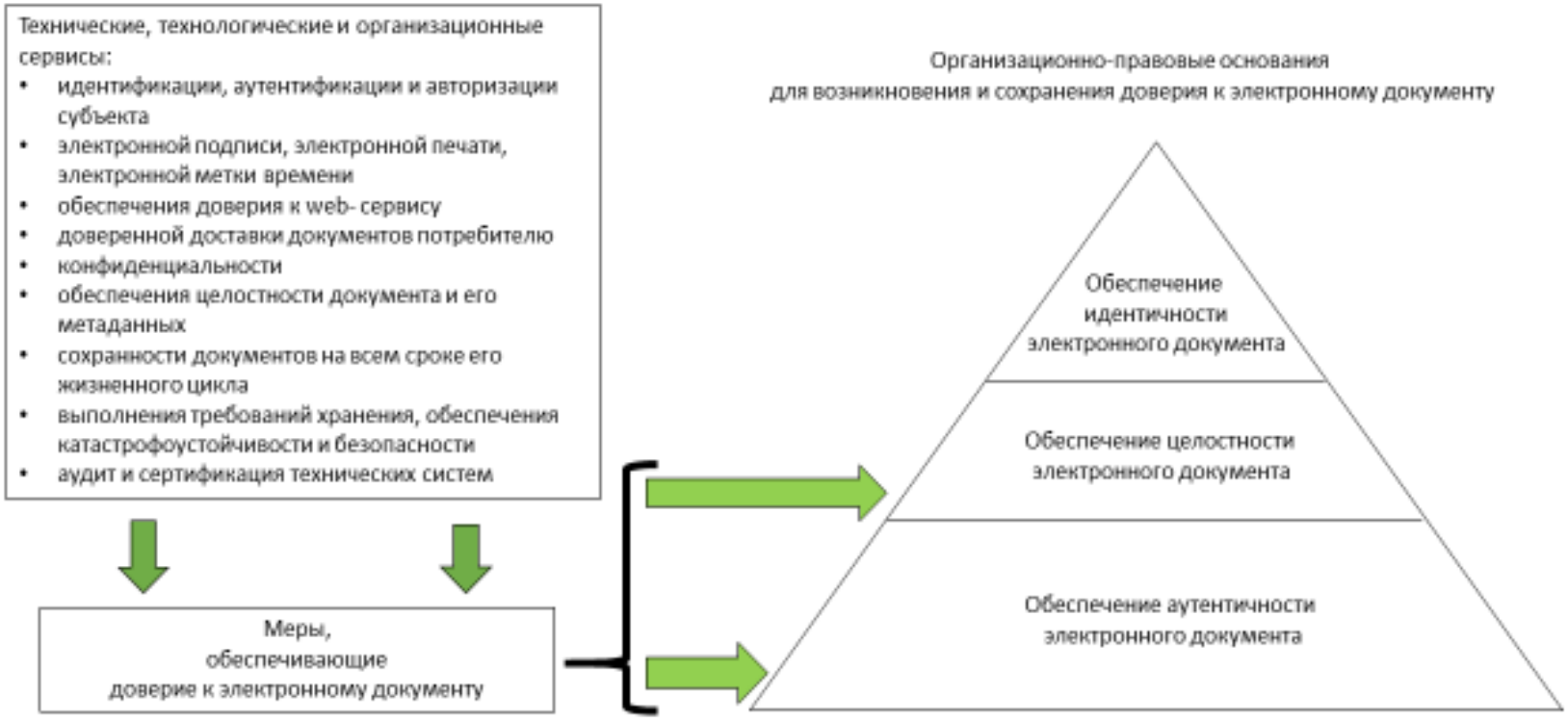
Какой подход избрать для случая массового перехода на ЭП?

1. Снабдить каждый документ необходимым набором атрибутов и свидетельств доверия, достаточных для признания его в суде пригодным для ведения в правовой оборот
2. Каждый раз проводить соответствующую правовую экспертизу.

Основной фактор, позволяющий использовать электронный документ в системе правоотношений - это возможность придания ему в случае необходимости юридической силы на всем протяжении жизненного цикла, или с точки зрения права обеспечить необходимый уровень доверия.

Доверие к документу возникает только в том случае, когда обеспечивается его аутентичность, что подразумевает обеспечение идентичности (идентификации) и целостности электронного документа, естественно также на всем протяжении его жизненного цикла.

Технические, технологические и организационно-правовые основания возникновения и сохранения доверия к электронному документу



Электронный документ - автономный объект защиты

Электронный документ (совместно с его метаданными), являясь самостоятельным юридическим объектом, с точки зрения информационной безопасности также представляет собой самостоятельный, если точнее - автономный объект защиты, для которого должны быть обеспечены следующие приоритеты безопасности и требования сохранности:

- должна быть обеспечена целостность (идентичность, аутентичность документа). Приоритет является абсолютным и должен быть обеспечен на всех этапах жизненного цикла документа;
- должна быть обеспечена доступность документа на всех этапах жизненного цикла документа. Правила предоставления доступа к документу со временем могут изменяться в зависимости от его статуса;
- должна быть обеспечена конфиденциальность документа. Требования к отнесению документа к категории конфиденциальных, могут изменяться со временем;
- должна быть обеспечена сохранность документа на всем жизненном цикле и защищенность от неконтролируемого уничтожения;

В соответствии с обозначенными приоритетами, требованиями государственных регуляторов, государственными стандартами и официальными базами данных угроз, для электронного документа в совокупности с метаданными и для СЭВ выделяются следующие классы угроз:

- несанкционированный доступ к информационным ресурсам;
- компьютерные атаки;
- заражение вредоносным кодом;
- нарушение конфиденциальности данных, идентификационной (аутентификационной) и ключевой информации;
- использование недекларированных возможностей программного обеспечения;
- физическое воздействие на средства и системы хранения электронных документов, системы обработки и передачи данных.

Реализация перечисленных угроз приводит к следующим неприемлемым последствиям:

- утрате электронными документами юридической силы;
- модификации (нарушения целостности) электронных документов и метаданных;
- созданию ложных электронных документов, имеющих юридическую силу;
- уничтожению электронных документов и метаданных;
- нарушению доступа к электронным документам и их хранилищам;
- нарушению функционирования аппаратно-программных комплексов систем обработки и хранения электронных документов;
- разглашению содержания конфиденциальных электронных документов.

Некоторые умозаключения

Таким образом, с точки зрения принципов организации документооборота и электронного взаимодействия последствия реализации перечисленных угроз означают утрату аутентичности, нарушение доступа к документам и нарушение конфиденциальности, что делает невозможным дальнейшее использование их как объектов правовых отношений, так как доверие к ним в этом случае полностью утрачивается.

Очевидно, что в этом случае гарантом доверия к электронному документу, как к полноценному объекту правоотношений и аналогу бумажного документа выступает система безопасности (включая средства электронной подписи, печати, печати, обеспечения подлинности сайтов, средства шифрования каналов связи), в совокупности с традиционными системами сопровождения задействованных автоматизированных систем обработки и хранения этих документов.

При этом гарантии могут быть обеспечены:

- установлением требований по обеспечению информационной безопасности для СЭВ и ее компонент;
- установлением официальных методик контроля выполнения этих требований;
- использованием (по аналогии с системами обеспечения защиты персональных данных и конфиденциальной информации) действующих систем сертификации, аттестации и лицензирования (аккредитации);
- использованием сертифицированных по требованиям ФСТЭК России и ФСБ России средств защиты информации, включая квалифицированные средства электронной подписи и средств шифрования.

Что может быть использовано в качестве свидетельств доверия

При наличии уже действующих гарантий со стороны государства и хорошо налаженной системы контроля со стороны государственных регуляторов (или по их поручению), в качестве свидетельств доверия могут быть использованы имеющиеся документы, подтверждающие заявленные свойства безопасности.

В качестве таких свидетельств, (по аналогии со свидетельствами аудита), могут выступать:

1. Перечень реализованных исходных технических и организационных требований, на основании которых построена система защиты.

2. Положительные заключения о результатах проверки (аудита, контроля) этих требований с указанием сроков проведения контроля и очередных сроков проверки.

3. Сведения об используемых средствах безопасности, согласно заранее сформированному списку разрешенных применению средств и программных продуктов, наличие действующих сертификатов безопасности, сроки их действия.

4. Наличие действующих свидетельств аттестации объектов по требованиям безопасности, сроки их окончания.

5. Наличие соответствующих действующих лицензий (свидетельств по аккредитации) организаций на право обработки и хранения электронных документов, возможно – устанавливающих право на архивное хранение.

Оформление свидетельств доверия.

Опора при подготовке свидетельств доверия к техническим средствам и системам обеспечения безопасности и защиты информации на действующие государственные системы контроля, сертификации аккредитации и лицензирования, позволяет обеспечить достаточное качество контроля и обеспечить наиболее высокий уровень доверия, гарантируемый государством. При этом, вся необходимая информация в отношении отчетов по результатам оценки соответствия требованиям защиты информации, сертификатов средств защиты, лицензий, выданных организациям, сроков их действия, причин отзыва лицензий хранится в централизованных базах данных государственных регуляторов и может быть легко проверена. В случае необходимости, по запросу могут быть предоставлены официальные выписки, в том числе и в форме электронного документа.

Какие документы могут быть использованы в качестве свидетельств доверия

1. Официальный, актуальный по дате отчет по результатам оценки соответствия организации требованиям защиты информации, содержащий заключение о соответствии уровня защиты организации установленным требованиям. Для организаций кредитно-финансовой сферы - не ниже 0,85.

2. Перечень средств защиты информации с действующими сертификатами на них. Сведения о наличии сертификатов на средства электронной подписи включаются в сертификат ключа проверки подписи.

3. Лицензия по технической защите конфиденциальной информации, с указанием установленных для СЭВ видов лицензированной деятельности, выданная организации - участнику электронного взаимодействия на финансовом рынке.

4. Лицензия, по предоставлению телематических услуг связи, выданная организации, как организатору системы доверенной передачи сообщений (требует нормативно-правового оформления).

5. Свидетельство об аккредитации организации на выполнение деятельности, связанной с долговременным хранением электронных документов (требует нормативно-правового оформления).

Где и каким образом хранить эту информацию

- Наиболее целесообразным является присоединение этой информации к самому электронному документу, что позволяет в этом случае наиболее оперативно использовать эту информацию для подтверждения уровня доверия к нему.
- Такая информация может быть помещена в метаданные документа, обработанного в конкретной системе и корректироваться по мере перемещения документа из хранилища в хранилище, а также по мере измерения статус самих свидетельств.
- Однако следует сократить избыточность информации, присоединяемой к документу, так как для признания свидетельства доверия легитимным, следует иметь только его реквизиты и сроки действия. Это существенно уменьшает объем присоединяемых данных, но всегда дает возможность по имеющимся реквизитам обратится к централизованно хранящемуся в базе данных первоисточнику.

Спасибо за внимание!

А.Курило