

## Комментарии к проекту ФЗ "Об электронной подписи"

28 декабря в Госдуму внесен новый законопроект об электронной подписи, который призван заменить действующий ФЗ "Об электронной цифровой подписи" (ФЗ-1).

Изменение действующего законодательства - процесс затратный и затрагивающий различные сферы жизни общества, а также интересы как отдельных юридических и физических лиц, так и профессиональных сообществ. Принятию новых законов, особенно рассматривающих сложные технологические аспекты, должен предшествовать детальный анализ и обсуждение с привлечением специалистов и профессиональных участников рынка основных положений действующего законодательства, особенностей его применения и имеющихся недостатков, как это и принято в мировой практике.

Не затрагивая юридических и правовых аспектов, послуживших толчком к подготовке этого законопроекта, считаем необходимым остановиться на ряде технологических и организационных аспектов, отраженных в Пояснительной записке и самом законопроекте.

Однако, прежде всего, имеет смысл обратиться к европейскому опыту по этой теме, поскольку одной из причин появления проекта нового закона явилось желание привести российское законодательство в соответствие международному.

В Директиве ЕС по применению электронной подписи (1999 г.) и последующих соглашениях между странами-участницами определяются различные типы электронных подписей и механизмы их формирования и проверки.

В частности, в документе [CWA 14365] описываются три типа подписи:

- электронная подпись (Electronic Signature) или простая электронная подпись.  
Данная подпись представляет собой набор данных, которые присоединяются или логически связываются с другими данными и которые используются для аутентификации подписанта. Несмотря на то, что документ оставляет возможность для применения некриптографических подходов к созданию электронной подписи (это сделано с перспективой на будущее развитие технологий), на практике в европейских странах электронная подпись реализуется на основе асимметричной криптографии. Простая электронная подпись обеспечивает контроль целостности электронных сообщений и аутентификацию подписанта в том смысле, что для проверки подписи используется открытый ключ парный секретному, с помощью которого сформирована подпись, но это не дает гарантий, что хранитель (holder) секретного ключа и его владелец (owner) являются одним и тем же лицом. Вместе с тем, простая электронная подпись может использоваться в суде в качестве доказательства, принятие которого (его зачимость) выносится на усмотрение судьи.
- улучшенная электронная подпись (Advanced Electronic Signature).  
Таковой считается электронная подпись с более жесткими требованиями, включающими:
  - наличие уникальной связи подписи с подписантом;

- возможность идентификации подписанта;
  - необходимость использования средств подписи, которые находятся под контролем подписанта
- и
- обеспечение надежного контроля целостности данных за счет использования криптографических алгоритмов с соответствующими параметрами (для улучшенной электронной подписи документ [CWA 14365] прямо рекомендует использование криптографических хеш-функций и алгоритмов с соответствующей длиной ключа)

Для обеспечения первых двух требований рекомендуется использовать сертификаты X.509 в двух видах: квалифицированный сертификат, выпущенный доверенной третьей стороной (например, Удостоверяющим центром), или неквалифицированный сертификат, который может быть выпущен как доверенной третьей стороной, так и самим подписывающим.

Улучшенная электронная подпись обеспечивает контроль целостности сообщений, аутентификацию подписанта и в некоторых случаях (например, при использовании квалифицированного сертификата) неотказуемость его от подписи.

- квалифицированная электронная подпись (Qualified Electronic Signature).

В понятие квалифицированной подписи входит применение улучшенной (Advanced Electronic Signature) подписи при использовании квалифицированного сертификата подписи и одновременном применении SSCD (Secure Signature Creation Device) - устройства для безопасного формирования ключевого материала подписи, к которому предъявлены следующие требования:

- должны быть обеспечены уникальность и секретность ключа;
- сама электронная подпись должна быть защищена от подделки с использованием доступной на сегодняшний день технологии;
- закрытый ключ, используемый для создания подписи законным владельцем, должен быть надежно защищен от использования другими лицами.
- ключевая пара должна генерироваться при личном участии будущего владельца внутри защищенной памяти SSCD (токена, смарт-карты), закрытый ключ не должен иметь технических возможностей экспортирования (копирования) закрытого ключа.

Квалифицированный сертификат должен быть валидным на момент подписания и однозначно идентифицировать подписанта.

Таким образом, подписант полностью контролирует жизненный цикл закрытого ключа подписи, и сам отвечает за его сохранность.

Квалифицированная электронная подпись обеспечивает контроль целостности сообщений, аутентификацию подписанта и неотказуемость его от подписи.

Согласно стандартам ЕС только квалифицированная электронная подпись полностью приравнивается к собственноручной.

Сравнивая положение дел в области технологии электронной подписи в России и Европе можно отметить, что в России (на основании ФЗ-1) используются технологии ЭЦП, соответствующие улучшенной (с применением квалифицированных сертификатов) и квалифицированной электронным подписям.

Причем, последняя появилась на рынке в 2009 году и построена с использованием технологии неизвлекаемых секретных ключей, формирующихся и хранящихся на USB-токенах. Эти технологии реализуют российские криптографические стандарты, что имеет особенное значение, поскольку затрагивает проблемы национальной безопасности. В Европе, кстати, это понимают и созданию собственных криптографических стандартов уделяют достаточное внимание. Например, в 2003 году был запущен проект NESSIE (New European Schemes for Signatures) для определения безопасных шифровальных алгоритмов по результатам которого, в частности, для электронной подписи наряду с американскими стандартами:

- □ □ ECDSA: Certicom Corp., США and Certicom Corp., Канада;
- □ □ RSA-PSS: лаборатории RSA, США;
- был рекомендован к использованию стандарт Франции:
- □ □ SFLASH: Schlumberger.

Заметим, что ФЗ-1 однозначно трактует электронно-цифровую подпись как квалифицированную, поскольку в статье 1 Закона сказано: "Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе".

Таким образом, с позиции основных свойств ЭЦП, обеспечивающих целостность сообщений, аутентификацию подписанта и неотказуемость его от подписи, существующие российские технологии обеспечивают все необходимые условия для приравнивания ЭЦП к собственноручной подписи.

Обратимся теперь к Пояснительной записке к предлагаемому проекту закона, поскольку она содержит ряд предпосылок, вошедших в закон и отражающих мотивы авторов по необходимости его создания.

В Пояснительной записке сказано:

1) « ... вопреки сложившейся мировой практике Федеральный закон «Об электронной цифровой подписи» допускает использование единственной технологии электронной цифровой подписи (основанной на так называемой технологии асимметричных ключей подписи)»;

***Комментарий: да, европейское законодательство, учитывая, в перспективе, развитие технологий, жестко не регламентирует алгоритмические аспекты электронной подписи, хотя, в некоторых случаях (см. выше,) оно все-таки ориентируется на современную криптографию. Вместе с тем, в настоящее время, реальной альтернативы криптографии с открытым распределением ключей для технологии электронной подписи - нет, что и подтверждается существующей практикой в странах Евросоюза.***

2) ФЗ-1 «...делает необходимой единую иерархическую систему удостоверяющих центров»

*Комментарий: это неверно. ФЗ-1 не предусматривает создание иерархической системы Удостоверяющих Центров, а требует лишь депонирования самоподписанного сертификата УЦ в УФО (ст.10 п.1). На практике в России существуют различные схемы объединения УЦ, включая иерархические, мостовые и на основе кросс-сертификации.*

3) ФЗ-1 "...обязывает применять сертифицированные средства электронной цифровой подписи"

*Комментарий: применение сертифицированных средств ЭЦП обеспечивает потребителям гарантии соответствия применяемой технологии ЭЦП требованиям в области средств криптографической защиты информации (СКЗИ) и позволяет значительно упростить разрешение конфликтных ситуаций за счет упрощения процедуры проведения экспертизы. Отсутствие в законопроекте требования сертификации либо аттестации средств электронной подписи (за исключением средств для защиты государственной тайны, а также средств, используемых в составе аккредитованного УЦ) на соответствие хоть каким-то требованиям или критериям создаёт условия для снижения общего уровня безопасности систем, использующих технологии электронной подписи. Без наличия критериев соответствия средств электронной подписи современным требованиям по безопасности конечному потребителю будет довольно трудно убедиться в качестве применяемого средства.*

4) «...не допускается электронная цифровая подпись юридических лиц»;

*Комментарий: в практике электронного документооборота (равно как и в бумажном) понятие подписи юридического лица не предусматривается, поэтому его введение на законодательном уровне вызывает сомнения. В европейском законодательстве, в качестве одного из применений для подписи юридического лица предполагается использование простой электронной подписи при подписании сервером программного обеспечения компании, однако, это можно сделать и с помощью ЭЦП Администратора сервера, тем более, что ФЗ-1 допускает использование псевдонимов в сертификате ключа подписи. Также вызывает сомнение (см. заключение правительства на проект закона) возможность автоматической подписи документов на сервере с последующей их публикацией в сети. Это удобно, но не обеспечивает персональной ответственности подписывающего, и, как следствие, легитимности документов.*

5) «По информации Государственно-правового управления Президента Российской Федерации, по состоянию на февраль 2007 г., количество действующих в России сертификатов ключа подписи составляет 200 тыс. ед., а

число удостоверяющих центров - более 300. Таким образом, процент лиц, использующих ЭЦП в России, не превышает 0,2%, а среднее число сертификатов ключей подписи, выданных удостоверяющим центром – не более 700, что свидетельствует об использовании ЭЦП преимущественно в корпоративных информационных системах.»

**Комментарий:** количественная информация явно не соответствует действительности: например, только одна компания Сигнал-КОМ реализовала в общей сложности более 250 проектов построения Удостоверяющих центров, 5 из которых в настоящее время имеют более 100.000 выпущенных сертификатов. По результатам доклада на РКІ-форуме в 2009 году в УФО зарегистрировано порядка 240 Удостоверяющих центров, позиционирующих себя как публичные, и это не считая корпоративных УЦ, которых значительно больше.

6) «В то же время, по данным Института Фраунхофера по открытым коммуникационным системам, по состоянию на 2005 г. (т.е. через 5 лет после принятия соответствующей Директивы) в Европе использовали усиленные электронные подписи до 70% населения»

**Комментарий:** это не проблемы существующего ФЗ-1, а проблемы неразвитости электронных сервисов для населения с использованием ЭЦП (сфера ответственности государства), что в конечном итоге и определяет применение ЭЦП практически только в корпоративном секторе.

7) "При этом необходимо отметить, что речь идет именно об усиленных электронных подписях, не связанных жестко с технологией асимметричного шифрования и единой иерархической структурой удостоверяющих центров"

**Комментарий:** это неверно (см. выше)

Таким образом, из анализа Пояснительной записки необходимость принятия нового закона не очевидна.

Применительно к законопроекту необходимо отметить:

1. Если ориентироваться на международное (европейское) законодательство, то представляется, что в статье 5 законопроекта содержится концептуальная ошибка в части невозможности отследить за счет простой электронной подписи изменение исходной информации (контроль целостности - это по определению (ISO 7498-2:1989) одно из свойств электронной подписи, а иначе она и не нужна). Эта ошибка приводит к последующим правовым и технологическим нестыковкам в законе, например в ст. 6, где документы, подписанные простой электронной подписью признаются «равнозначными документам на бумажном носителе, подписанным собственноручной подписью и заверенным печатью». Поскольку свойства простой электронной подписи (см. ст.5) не позволяют «установить неизменность подписи и подписанной

*информации после подписания», проект оставляет неясными механизм проверки такой подписи и, как следствие, процедуру разрешения конфликтов в случае её использования.*

- 2. Разница между усиленной и квалифицированной подписями, так как они описаны, представляется слишком незначительной, чтобы включать последнюю в закон. По аналогии с европейским законодательством, для квалифицированной подписи имеет смысл предусмотреть и специальные средства для генерации и хранения ключей (например, неизвлекаемые ключи на USB-токенах).*
- 3. Использование трех типов подписей из которых только одна технологически обеспечивает эквивалентность собственноручной подписи, другая для этого требует наличия дополнительной доказательной базы, а третья вообще никуда не годится - неочевидно. Понятно желание авторов использовать простые и усиленные подписи в системах, где ответственность подписантов за свои действия минимальна, но стоит ли в этих случаях вообще использовать электронные подписи, если доказывать авторство не предполагается, а если потребуется - то доказать будет трудно или вообще не удастся?*
- 4. При использовании квалифицированной подписи предписывается жёсткая иерархическая схема сертификации с одним корневым УЦ (ст. 4, 13). Невозможность организации других схем, например, создания изолированных систем удостоверяющих центров, а также невозможность объединения уже существующих удостоверяющих центров путем кросс-сертификации или по мостовой схеме (более устойчивой, чем иерархическая) – всё это противоречит принципу «технологической нейтральности» законодательства. Действующий ФЗ-1, кстати, лишён этого недостатка.*
- 5. Совмещение функций уполномоченного федерального органа и корневого УЦ представляется ошибочным.*
- 6. Отсутствие аккредитации уполномоченного федерального органа (ст.13, ч.8) делает иерархическую систему УЦ уязвимой - поскольку не существует гарантии выполнения корневым УЦ, например, требований ст.13, ч.3, п.3 и 4.*
- 7. Аккредитация удостоверяющих центров (см. ст.13), безусловно, является прогрессивным нововведением. Однако, в ст.13, ч.1 говорится, что только «главный (корневой) удостоверяющий центр аккредитованной системы удостоверяющих центров должен соответствовать требованиям, установленным для аккредитованных удостоверяющих центров». Вероятно, упомянутые требования должны распространяться на все УЦ, входящие в систему, а не только на корневой.*
- 8. Существует противоречие в части функции УЦ – приостановления сертификатов, а именно, в ст. 4 ч. 2 п. 4 вводится понятие реестра приостановленных сертификатов, а в ст. 9 данная функция отсутствует.*

9. *Некоторые положения законопроекта более уместны в регламенте работы конкретного УЦ или системы УЦ, чем в законе, в частности:*
- *ст.7, ч.7, п.2, предписывающая действия в случае компрометации ключа подписи (при этом не предусмотрено никакой ответственности за нарушение)*
  - *чисто технологическое поле сертификата "номер квалифицированного сертификата удостоверяющего центра" (ст.14, ч.1, п.6) - достаточно было бы "ссылки на сертификат удостоверяющего центра";*
  - *"наименование используемого средства электронной подписи" в сертификате (ст.14, ч.1, п.5). Вопрос: какого средства - используемого в удостоверяющем центре или используемого владельцем сертификата? Но разве он не может пользоваться разными средствами?*
10. *Законопроект не содержит определения или отсылочной нормы термина «электронное сообщение», хотя в тексте данный термин встречается и видимо отличается от термина «электронный документ», что приведет к неоднозначности толкования положений закона.*
11. *Признание электронных подписей, созданных в соответствии с нормами иностранного права (ст.7, ч.6) - например, подписей RSA - создаёт неравные условия для российской криптографии и отечественных производителей ввиду широкого распространения средств зарубежной криптографии на территории РФ (например, в составе операционных систем).*

На самом деле замечаний намного больше, что свидетельствует о крайне низкой проработанности законопроекта.

#### Выводы

1. Анализ представленного законопроекта «Об электронной подписи» показывает, что цель, поставленная разработчиками, в части соблюдения его технологической нейтральности и соответствия международным требованиям - не достигнута.
2. Законопроект подлежит дополнительному всестороннему анализу специалистов на предмет более полного учета в нем технологических и организационных требований международного законодательства и, в случае решения о его принятии, потребует значительной переработки.
3. Необходимость принятия закона на текущий момент не очевидна. Существующий Ф3-1 обеспечивает все необходимые для нормальной работы правовые и технологические возможности, за исключением возможности применения западных криптографических стандартов, использование которых для юридически значимых действий потребует в обязательном порядке:
  - разработки к ним специальных требований и создание системы аттестации или сертификации, проводящей анализ используемых решений на соответствие этим требованиям;

либо

- признания западных систем сертификации (аттестации);
- проведения исследований по оценке специальных свойств западных криптографических стандартов, в частности, по оценке криптографической стойкости.

В противном случае при применении такой электронной подписи на первый план выйдут вопросы безопасности.

#### Литература

1. О задаче защиты закрытого ключа ЭЦП от компрометации.  
<http://www.intertrust.ru/analytics/articles/136/>
2. Mirella Mazzeo. Digital Signatures and European Laws 2004-01-26
3. CEN WORKSHOP AGREEMENT (CWA) 14365-1 March 2004
4. Федеральный закон № 1-ФЗ. "Об электронной цифровой подписи".
5. ФЕДЕРАЛЬНЫЙ ЗАКОН Об электронной подписи. Проект
6. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА к проекту федерального закона «Об электронной подписи»
7. ЗАКЛЮЧЕНИЕ на проект федерального закона "Об электронной подписи", вносимый в Государственную Думу депутатом Государственной Думы О.В.Морозовым

Ген. директор  
ЗАО Сигнал-КОМ

В.А. Смирнов



Ген. директор  
ООО Топ Кросс

С.М. Муругов



Ген. директор  
ОАО Инфотекс

