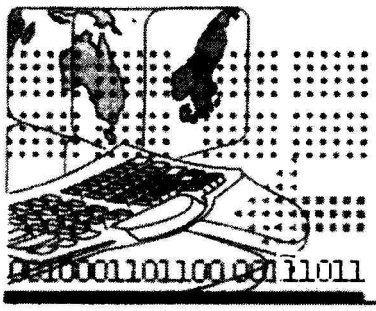
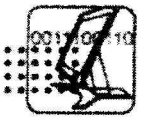


ПРАКТИЧЕСКИЕ АСПЕКТЫ КРИПТОГРАФИИ



УДК 004.056

А.П. Баранов

Центр безопасности ФСБ РФ, Москва

АКТУАЛЬНЫЕ ЮРИДИЧЕСКИЕ АСПЕКТЫ ПРАКТИЧЕСКОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматривается ряд положений закона об электронной подписи (ЭП) с учетом выполнения существующих требований по обеспечению безопасности конфиденциальной информации.

Ключевые слова: закон об электронной цифровой подписи, закон о персональных данных, закон о техническом регулировании.

A.P. Baranov

ACTUAL JURIDICAL ASPECTS OF PRACTICAL IT-SECURITY

Article describes the statements of the law on Electronic Signature from the point of the security of confidential information.

Keywords: the law on the electronic digital signature, the law on the personal data, the law on technical regulation.

Три актуальных направления активно обсуждаются в настоящее время среди юристов и защитников информации.

Защитники информации поняли, что если они не займутся законотворчеством и законодательно, нормативно не закрепят понятные им направления обеспечения безопасного существования общества в определенных направлениях, то юридически подкованные специалисты, некомпетентные в техническом отношении, могут допустить ряд ошибок. К этим направлениям относятся положения, отраженные в следующих документах:

1. "Закон об электронной цифровой подписи (ЭЦП)".
2. "Закон о персональных данных (ПД)".
3. "Закон о техническом регулировании".
4. Проект "Закона об электронной подписи (ЭП)".

Три указанных закона действуют. Внесен в Государственную Думу проект "Закона об электронной подписи (ЭП)", которым предлагается прекратить действие "Закона об электронной цифровой подписи (ЭЦП)". В отношении этих документов ведутся интенсивные обсуждения, вносятся

предложения об их изменении. Актуальность дискуссий в ближайшие год-два не будет утрачена.

1. "Закон о ПД"

Закон в отношении защиты персональных данных предусматривает две нормы:

а) все создаваемые вновь системы обработки ПД должны соответствовать требованиям защиты, т. е. все системы, создаваемые с 2007 г., должны удовлетворять требованиям ФСТЭК и ФСБ РФ, сформулированным в Постановлении Правительства РФ;

б) ранее созданные системы в соответствии со статьей 25, п. 3 должны были быть приведены в соответствие с упомянутыми выше требованиями ФСТЭК и ФСБ России к 01.01.2010 года.

Полемика о дате введения закона (01.01.2010) активно ведется и в настоящее время. Контролирующие по закону органы – "Служба по контролю и надзору в сфере информационных технологий и связи", ФСТЭК и ФСБ России – требовали безусловного выполнения закона. Ряд операторов персональных данных и в первую очередь банки заявляли о невозможности, затратности и обременительности в организационном плане выполнения требований. Закон был принят в июле 2006 г., что означает, что трех с половиной лет не хватило, чтобы его выполнить. Требования банков сводятся к следующим: отложить ввод в действие закона на 2 года и переработать нормативную базу ФСТЭК и ФСБ. К этим требованиям присоединились и другие операторы, не желающие приводить свои системы в надлежащий порядок. В настоящее время эта глубоко эгоистичная (на взгляд автора) позиция частично может быть удовлетворена. Ведомства, ответственные за организацию исполнения закона, согласились на отсрочку в один год, которую должна узаконить Госдума, внеся изменения в закон. Можно предположить, что это паллиативное решение мало что изменит и, если ситуация не изменится кардинально, к концу 2010 г. мы придем с тем же результатом.

В настоящее время появились три альтернативных проекта закона о ПД, и можно надеяться, что они будут исходить из опыта уже существующего более чем 3 года закона, который несмотря ни на что работает. Как показали проведенные в этом году проверки ряда операторов (например, Пенсионного фонда), выполнять требования можно и невыполнимых препятствий не существует.

Тем не менее, работа над требованиями будет продолжена, например ФСБ России планирует открыть горячую линию для приема предложений о внесении поправок в закрепленную за ней нормативную базу Хотелось бы узнать и от читателей этого журнала, что, по их мнению, надо исправлять. Опыт показывает, что требования и законы не читают, а тем более не изучают. Зачастую обсуждение происходит по схеме: "документ не читал, но осуждаю". Впервые опубликовав требования к некоторым видам криптозащиты, ФСБ рассчитывает услышать мнение научной общественности.

Необходимо отметить, что в предполагаемых законодательных инициативах существует и "альтернативный подход" к доведению требований законопроекта до общественности, состоящий в том, что в случае несанкционированного появления ПД необходимо жестко карать оператора ПД, допустившего утечку. Тогда операторы сами затребуют правила как обработки, так и проверки с фиксацией уровней защиты. Это та добавка, которую предполагается вносить в любой следующий вариант закона о ПД. В заключение можно отметить, что отсрочка окончательного ввода в действие закона на один год не избавляет от необходимости его исполнения сейчас, хотя бы для вновь создаваемых систем и при проведении проверок систем, созданных за последние два года.

2. "Закон о техническом регулировании"

В соответствии со ст. 14 п. 8 Федерального Закона (ФЗ) "Об информации, информационных технологиях (ИТ) и о защите информации" программно-технические средства и средства защиты информации должны удовлетворять требованиям технических регламентов, принимаемых в соответствии со ст. 6 п. 1 ФЗ "О техническом регулировании" в следующих целях:

1) защита жизни и здоровья граждан, имущества физических или юридических лиц, государственного имущества или муниципального имущества;

2) охрана окружающей среды, жизни и здоровья животных и растений;

3) предупреждение действий, вводящих в заблуждение приобретателей.

При этом в соответствии со ст. 6 п. 2 этого ФЗ принятие технических регламентов в иных целях не допускается. Из этого следует, что законодательство РФ о техническом регулировании не допускает разработку и принятие технических регламентов, целью которых является установление обязательных требований, определяющих качество защиты информации, обеспечиваемое техническими средствами, устанавливаемыми в системах ПД, криптографическими или иными средствами защиты информации. Регулирующие статьи закона о техническом регулировании не направлены на обеспечение качества информации или ее свойств, а могут касаться лишь средств передачи информации, влияющих на указанные в ст. 6 п. 1 параметры жизнедеятельности.

В связи с изложенным выше можно отметить наблюдающееся противоречие в законодательстве, которое должно быть устранено.

3. "Закон об электронной цифровой подписи (ЭЦП)" и проект Закона об электронной подписи (ЭП)

Масштаб внедрения ЭЦП обусловлен потребностью научно-технического прогресса в сфере информатики и в значительной мере неослабевающим энтузиазмом разработчиков. Критики ЭЦП говорят о том, что применение ЭЦП в соответствии с принятым законом сужает круг возможных потребителей технологии до 1 %. Однако, учитывая, что к настоящему моменту продано около 5 миллионов комплектов СКЗИ с ЭЦП, в соответствии с данной оценкой в России 500 млн. потребителей технологии, чего никак не может быть. Таким образом, можно констатировать, что ЭЦП в России состоялась, что мы находимся на передовых позициях применения электронных средств подтверждения подлинности и что законодательная база (не во всех развитых странах в отношении ЭЦП имеющаяся) достаточно эффективна, хотя и требует совершенствования.

Именно сейчас и накапливается правоприменительная практика, являющаяся главным критерием качества закона. Вместе с тем открываются и возможности для критики и усовершенствований. Мы знаем о ряде недостатков Закона об ЭЦП, которые трудно было предусмотреть на этапе его создания, например, только личная ЭЦП, отсутствие корпоративной ЭЦП и т. д.

Вносить изменения в Закон надо, и для этого есть все возможности. Однако в ряде случаев ЭЦП и Закон об ЭЦП критикуют, не понимая его сути. В чем принципиальное отличие ЭЦП от обыкновенной подписи? Надо заметить, что математики, сделавшие ЭЦП, к сожалению, не удосужились разъяснить его гуманитарную сущность, преимущества и требования для основной массы населения не технического склада ума и образования. Недавно подготовленные и распространенные в ряде министерств три листка описания без единой формулы здорово способствовали пониманию явления ЭЦП среди руководящих работников.

Необходимо отметить, что в ЭЦП есть тайный элемент, доступный только владельцу ЭЦП, разглашение которого недопустимо и который однозначно связан

с ключом проверки ЭЦП. Этим обеспечивается невозможность подделки ЭЦП. Как известно, ЭЦП – надежный механизм, когда он стоит на трех китах:

1) сертифицированном изделии;

2) лицензированном производителе;

3) правильном удостоверяющем центре (УЦ), в котором используется сертифицированное ПО. УЦ хранит образец сертификата ключа подписи и предоставляет его по требованию с собственной ЭЦП.

Не останавливаясь на технических проблемах сертификации и лицензирования, поясним еще раз, зачем они нужны. Для этого сформулируем главное свойства ЭЦП, которое состоит в том, что две взаимодействующие стороны всегда могут привлечь третью сторону для решения спора о подлинности документа и ЭЦП. При этом третья сторона (суд) проблему спора всегда может решить. Конечно, важны все остальные технические и организационные аспекты, но именно вот это гуманитарное свойство наиболее ценно. Назовем его свойством "суда". Для обеспечения этого свойства и разработана вся инфраструктура: УЦ, сертификация и лицензирование.

На этом следует подробно остановиться, потому что именно это свойство ЭЦП, свойство "суда", отличает его от других видов подписей, включая личную. Как известно в суде личная подпись мало что значит, ибо допускает легкую подделку, особенно учитывая возможности средств копирования. Наша рукописная подпись скорее символ.

Вместе с тем Министерством связи активно продвигается проект "Закона об **электронной** подписи", который не менее активно критикуется и не поддерживается. К сожалению, ряд ведомств, не вникая в сущность предложения Министерства связи, согласовали проект этого закона, внесенного теперь уже группой депутатов Госдумы.

При этом проект "Закона об ЭП" вводит другую подпись, отличную от ЭЦП, в которой свойство "суда" отсутствует, или может быть, а может и не быть, с отсутствием описаний и обоснований ситуаций, когда свойство "суда" не обязательно. К видам ЭП в соответствии с данным законом относятся простая ЭП и усиленная ЭП. Простая ЭП является аналогом личной подписи. Усиленная ЭП есть что-то подобное имитовставке, не использующей при проверке механизма УЦ.

Однако криптографы хорошо знают, что не может быть надежного шифрования без тайного ключа. Даже в открытом ключе он есть, и не может быть доказательства правильности имитовставки без ее предварительного депонирования.

Непонимание свойства "суда", заключающееся в использовании подписи для двух сторон, и, следовательно, провоцирование возникновения ситуации, в которой произойдет отказ от подписи или ее фальсификации (невозможность этого есть одно из основных достижений ЭЦП), двигает Министерство связи к отрицанию "Закона об ЭЦП" и замене его на "Закон об ЭП". Таким образом, "Закон об ЭП" предлагает введение в законодательном порядке возможности использования ненадежной подписи, т. е. подписи, подлинность которой (или подлинность подписываемого документа) не подтверждена компетентной экспертизой.

Следует отметить, что, как и "осетрины второй свежести", не бывает малонадежной подписи. Подпись бывает или надежной (не допускающей подделки или изменения подписываемого документа), или ненадежной.

Еще одним из нововведений проекта "Закона об ЭП" является отказ от сертификации средств ЭП. В связи с данным требованием вызывает удивление позиция МВД, которое было завалено делами о фальшивых "АВИЗО" в 1990–1992 годах. Подделки и обманы с помощью "простой ЭП" или "усиленной ЭП" обрушат банковскую и нотариальную сферы. А предпосылки для этого создаются, поскольку приня-

тие проекта "Закона об ЭП" позволит использовать для подписания конфиденциальных документов импортные продукты ЭП без сертификации. Следовательно, для обычных документов эта возможность будет использоваться тем более. Представляется, какую "клиптографическую" (от слов криптография и греческого клепто – краду) услугу можно будет открыть в некоторых сопредельных государствах, где будет хеш-функция с "нужной" дыркой, позволяющей менять несколько знаков. Сделать это крайне просто, достаточно в программе, а не в описании алгоритма, пропустить эти несколько знаков.

Основным тезисом о необходимости принятия ЭП является тезис об обслуживании "малозначительных" услуг в "электронном правительстве" и "малозначительном электронном документообороте". Можно заметить, однако, что если в системе существуют "малозначимые объекты", то для них подпись не нужна. Вместе с тем выпуск в оборот и придание юридической значимости таким "простым" подписям породит массу злоупотреблений и подорвет доверие к законопослушным юридическим и физическим лицам и к электронному правительству. Непонятно, как чиновник будет ставить такую собственную ЭП, если знает, что ее можно легко подделать. Либо будет ставить, чтобы потом от нее отказаться, поскольку в суде можно доказать ее неоднозначность.

Как следствие выполненного анализа, можно прогнозировать появление множественных подписей, а уж афер на этом якобы малозначимом обороте будет построено предостаточно. Криминальный ум настроен на использование подобных "безобидных" ситуаций.

Заключение

В систему ЭЦП в России вложены крупные средства, созданы УЦ, существует пять миллионов инсталляций ПО поддержки ЭЦП, проводятся электронные торги под эгидой казначейства, что обеспечивает стабильное использование и развитие современных электронных технологий. Отечественные средства ЭЦП легко встраиваются в любой электронный документооборот, конечно, если целью не ставить протаскивание любой ценой импортного продукта. В целом сейчас в ФСБ прорабатывается вариант, при котором "Закон об ЭЦП" остается действовать с поправками, а "Закон об ЭП" идет параллельно. Пример подобного решения содержится в Директиве 1999/93/ЕС Европейского Парламента и Совета от 13.12.1999 г., где указано "...она (ЭП) не распространяется на какие-либо аспекты заключения и исполнения договоров или иных обязательств, которые подчиняются требованиям национального законодательства, и также не затрагивает правила и ограничения, содержащиеся в национальном законодательстве, или права сообщества, регулирующие использование документов".

Таким образом, можно констатировать необходимость учета практических аспектов защиты информации при разработке законов об информатизации муниципального и коммерческого документооборота. Это должно достигаться, по мнению автора, за счет интеграции усилий юристов-правоведов и технических экспертов, представляющих, к каким последствиям могут привести недостаточно подготовленные законы.