Эссе по курсу "Защита информации", кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ), http://www.re.mipt.ru/infsec

Юридические аспекты электронной цифровой подписи.

Обухова Ирина,
гр.215

25.04.2006

Развитие современных технологий привело к появлению принципиально нового вида юридических отношений в международной торговле – электронной коммерции. Электронные соглашения постепенно вытесняют традиционные документы на бумажных носителях. Сейчас в мире уже достаточно широко используется обмен электронными документами и электронная подпись, особенно в банковской системе. Долгое время отсутствие правового регулирования использования электронной цифровой подписи и последствий ее применения препятствовало развитию электронной торговли.

Как работает ЭЦП?

Есть сеть участников сделок, которые обмениваются подписанными электронными документами. Для каждого абонента существует два ключа: секретный и открытый. Секретный ключ используется для генерации электронной цифровой подписи и должен храниться в тайне. Открытый ключ распространяется свободно и предназначен для проверки подписи получателем документа. Генерация ключей подписи и самой подписи осуществляется при помощи специальных программных средств (т.н. "средства ЭЦП").

Электронная цифровая подпись обладает следующими важными свойствами:

- удостоверяет, что документ создан лицом, поставившим подпись;
- делает невозможным отказ от авторства после подписания документа;
- гарантирует целостность документа, т.е. невозможность внесения изменений в документ после его подписания;
- гарантирует невозможность генерации подписи без владения секретным ключом.

Использование электронной цифровой подписи включает в себя:

- генерацию ЭЦП;
- проверку ЭЦП с помощью открытого ключа.

Важность юридического регулирования проблемы обусловлена тем, что сегодня, в условиях быстро развивающихся информационных технологий необходимы современные способы заключения сделок, которые будут иметь юридическую силу.
Электронный документооборот все глубже проникает во все сферы деятельности, и, как следствие, появляются новые услуги, связанные с применением электронной цифровой подписи. Таким образом, нельзя ограничиться только сертификацией средств ЭЦП и самой ЭЦП. Законы должны рассматривать также продукты и услуги, каким-либо образом связанные с ней. Обмен электронными документами отличается от обмена традиционными документами на бумажных носителях, что приводит к необходимости специального законодательства на национальном и международном уровне.

Одна из основных проблем, существующих на данный момент - несовершенство законов, регулирующий данный вид отношений, а также противоречивость соответствующих нормативных актов разных стран.
Также существует ряд проблем, связанных с внедрением ЭЦП.
Во-первых, появляется ряд новых понятий, таких как электронная цифровая подпись, электронная сделка и т.д., которые должны быть определены в законодательных актах.
Во-вторых, традиционные сделки на бумажных носителях являются источником формальных требований закона к форме документа (обязательная письменная форма, наличие подписей и т.п.).
Т.е. возникают проблемы, связанные с созданием таких критериев для электронных сделок и процедуры их заключения, а также вопросы соответствия требований, выработанных законодательными органами, возможностям разработчиков ПО.
В-третьих, существует принцип, в соответствии с которым стороны не могут подвергать сомнению законность и сделки только на том основании, что она заключена электронным способом. Но этот принцип может быть не закреплен законодательно, что приводит к юридическим проблемам.
В-четвертых, собственноручная подпись подразумевает, что человек, подписывая документ,
читает его и осознает последствия своей подписи, в то время как электронная цифровая подпись не может непосредственно восприниматься человеком. Поэтому в законодательстве ряда стран существуют требования к обязательной традиционной письменной форме сделки в некоторых случаях.

В 1995 году комиссией по международной торговле ООН был разработан проект закона UNCITRAL.Закон создавался как типовой набор требований к правовому регулированию отношений, возникающих при использовании электронных документов. Предполагалось, что на этой основе страны могут в национальных законах решить основные проблемы по признанию юридической силы электронных записей, электронной подписи, копий электронных данных, а также вопросы по признанию электронных документов в качестве судебных доказательств.

В 1999 году Европейским парламентом была принята “Директива о порядке использования электронных подписей в европейском сообществе”, целью которой было способствовать использованию электронной подписи и ее юридическому признанию.

Далее национальное законодательство в этой области развивалось по трем основным направлениям.

Первый вариант – модель, принятая в США. Суть этой модели в том, что правительство предоставляет гражданам и организациям самостоятельно регулировать отношения в сфере использования электронных документов, выбирать способ заключения сделки и технологии, которые будут при этом использоваться. Любой способ подписи электронного документа считается законным, если он признан всеми участниками сделки, будь то ПИН-код (персональный идентификационный номер), ЭЦП, или, например, биометрические данные (отпечатки пальцев, радужная оболочка глаза, голос и т.д.). Участники сами решают, использовать ли им электронную подпись, сертификация ключей необязательна. Федеральный закон “Об электронной подписи” был принят в США в 2000 году, еще раньше подобные нормативные акты были приняты в отдельных штатах (Юта, Флорида и т.д.).

Вторая модель - жесткое законодательное регулирование отношений, касающихся использования электронной подписи путем обязательного государственного лицензирования сертификационных центров. Такой подход используется, например, в России и Индии.

Перечисленные подходы различаются требованиями (с точки зрения) закона к электронной подписи:

В первом случае к электронной подписи предъявляются самые общие требования, такие как уникальность, возможность проверки подписи, возможность использования только владельцем секретного ключа (т.е. практически те же требования, что и к собственноручной подписи). Такие законы ни к чему не обязывают, поскольку не выполняются требования аутентичности документа, невозможность его изменения и невозможность отказа от авторства.

Второй подход - жесткие, детальные требования к электронной подписи; включает в себя описание информационных технологий, которые используются для ее генерации и проверки.
Именно такая разновидность электронной подписи называется *электронной цифровой подписью*.

Рассмотрим подробнее регулирование использования электронной цифровой подписи в России.
Российское законодательство признает, что кроме традиционной сделки на бумаге, договор может быть заключен с помощью “телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору” (Гражданский кодекс РФ ст.434 п.2).

По ст.160 ГК РФ при совершении сделок разрешено использование электронной цифровой подписи или других аналогов собственноручной подписи “в случаях и порядке предусмотренных законодательными актами или соглашением сторон”.
ЭЦП является подтверждением достоверности содержимого документа и того факта, что документ составлен и подписан должным образом уполномоченным лицом.

В 2002 году в России был принят федеральный закон “Об электронной цифровой подписи”,
в котором перечислены условия использования ЭЦП в электронных документах физическими и юридическими лицами и государственными организациями; права и обязанности владельца сертификата электронной цифровой подписи, статус центров выдачи сертификатов ключей подписи и т.д.

Необходимость принятия такого закона объясняется тем, что при использовании электронных документов и электронной цифровой подписи возникают новые права и обязанности сторон, заключающих соглашения, для сертификации создаются соответствующие организации, деятельность и ответственность которых должны быть оговорены в законе.

По данному закону, электронная цифровая подпись в электронном документе считается равнозначной собственноручной подписи, “если сертификат ключа подписи действителен на момент проверки или на момент подписания, в случае существование доказательств, определяющих момент подписания”. Электронный документ имеет юридическую силу в случаях, перечисленных в сертификате ключа подписи, при этом оговаривается возможность владения сертификатами в любом количестве. Владелец сертификата – физическое лицо, которому выдан сертификат ключа подписи, - имеет закрытый ключ, что позволяет ему подписывать документы. Для проверки подписи используется открытый ключ.

Сертификаты ключей подписи выдаются удостоверяющими центрами – юридическими лицами, несущими гражданскую ответственность перед пользователями сертификатов в случае недостоверных сведений, содержащихся в сертификате.
Основные функции удостоверяющего центра состоят в следующем:
- изготовление сертификатов ключей подписи,
- создание ключей электронных цифровых подписей,
- гарантия сохранения в тайне секретного ключа,
- приостановление, возобновление, аннулирование действия сертификатов,
- выдача сертификатов ключей подписи в форме бумажных и электронных документов,
- проверка уникальности открытых ключей подписи,
- ведение реестра сертификатов ключей и обеспечение свободного доступа к ним.

Средства, которые используются для генерации ключей подписи, должны быть также сертифицированы, иначе они считаются недействительными.
Первый удостоверяющий центр появился в России в сентябре 2002 года.
Вообще говоря, подписывать документы можно и с помощью несертифицированных ключей, но в случае судебного разбирательства такая подпись не может быть рассмотрена в качестве доказательства.

Итак, основные моменты российского закона “об электронной цифровой подписи“ состоят в следующем:
Во-первых, возможность использования несертифицированных средств ЭЦП. Обязательная сертификация требуется только для публично – правовых отношений.
Во-вторых, средства ЭЦП рассматриваются отдельно от средств шифрования.
Далее, требуется обязательное государственное лицензирование центров выдачи сертификатов подписи (в этом одно из отличий российского закона от Директивы СЕ, где предусмотрено добровольное лицензирование).
В корпоративных системах условия использования ЭЦП определяются самими участниками этих систем.
Признание равносильности ЭЦП собственноручной подписи (при выполнении ряда требований) и признание возможности использования ее как доказательства в суде.
Ограниченная ответственность центров выдачи сертификатов.

В заключение нужно сказать, что применение ЭЦП не решает всех проблем по обеспечению безопасности электронных сделок.
Поэтому как в России, так и в мире происходит дальнейшее совершенствование правовой базы в отношении использования ЭЦП и электронного обмена данными в целом.

Литература:

1. http://www.cs.auckland.ac.nz/~pgut001/tutorial/index.html
2. http://www.ekey.ru/lib
3. http://www.cci.ru/infolaws/doctoc.asp?id=32
4. http://www.infolaw.ru/lib/2005-2-e-docs
5. http://eulaw.edu.ru/documents/articles/eu13.htm
6. http://bugtraq.ru/library/crypto/sign.html
7. http://www.ros-expo.com/ecp/ecpporyadoc.html