Министерство общего и профессионального образования в Российской Федерации

Российский Государственный Университет нефти и газа имени И. М. Губкина

**Р Е Ф Е Р А Т**

По дисциплине: Информационное право

На тему:

**«ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В РОССИИ»**

Проверил:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Выполнила:

Пашкевич А. В.

Юридический факультет

IV- ый курс

Гр. ЮР-98-2

Москва

2002

Применение глобальных коммуникаций в коммерческой деятельности и повседневной жизни привело к появлению принципиально новой области юридических отношений, связанных с электронным обменом данными. В таком обмене участвуют производители товаров и услуг, оптовые и розничные торговцы, дистрибьюторы, перевозчики, банки, страхователи, органы государственной власти и их организации, а также физические лица в своих деловых и личных отношениях. Сегодня электронный обмен данными оказывает существенное влияние на экономику и права граждан, то обусловлено равным образом как правом, так и технологией. Поэтому данные отношения требуют особого правового регулирования на уровне как национального законодательства, так и международного права.

Неразвитость существующих правовых норма, относящихся к указанной сфере, а также значительные противоречия между соответствующим законодательством разных стран являются препятствием для развития электронного бизнеса, электронного документооборота в сфере государственного управления, обеспечения информационных прав граждан, а также для успешного международного обмена электронными данными.

Электронные документы способны найти широкое применение в коммерческих и управленческих процессах лишь при условии, что достоверность содержащейся в них информации не вызывает сомнений.

Процесс обмена электронными документами существенным образом отличается от обычной формы обмена документами на бумажных носителях. При широком внедрении в деловую и административную практику обмена электронными документами необходимо решить проблему подтверждения подлинности содержащейся в них информации и ее соответствия смыслу волеизъявления человека. Технически эта проблема решается путем использования средств электронной цифровой подписи (ЭЦП).

*Электронная цифровая подпись* – это криптографическое средство, которое позволяет удостовериться в отсутствие искажений в тексте электронного документа, а в соответствующих случаях – идентифицировать лицо, создавшее такую подпись.

В развитых странах мира, в том числе и в Российской Федерации, электронная цифровая подпись широко используется в хозяйственном обороте. Банк России и другие банки Российской Федерации эффективно используют ЭЦП для осуществления своих операций путем пересылки банковских электронных документов по корпоративным и общедоступным телекоммуникационным сетям.

Для преодоления всех существующих в данной области отношений препятствий необходимо создание унифицированных правил, при помощи которых страны могут в национальном законодательстве решить основные проблемы, связанные с юридической значимостью записей в памяти ЭВМ, письменной формой электронных данных (в том числе и документов), подписью под такими данными, оригиналом и копиями электронных данных, а также признанием в качестве судебных доказательств электронных данных, заверенных электронной подписью.

*10 января 2002 года* был принят *Федеральный Закон «Об электронной цифровой подписи», вступивший в силу с 22 января текущего года*, который закладывает основы решения проблемы обеспечения правовых условий для использования электронной цифровой подписи в процессах обмена электронными документами, при соблюдении которых электронная цифровая подпись признается юридически равнозначной собственноручной подписи человека в документе на бумажном носителе.

Необходимость принятия такого закона обусловлена тем, что при использовании ЭЦП возникают новые права и обязанности субъектов правоотношений, для удостоверения подлинности ЭЦП формируется система специальных организаций, права, обязанности и ответственность которых также должны быть законодательно установлены. Нормативным актом, устанавливающим права, обязанности и ответственность субъектов, может быть только закон. Подзаконные акты вправе конкретизировать правовые механизмы им установленные. С учетом таких актов впоследствии будет сформировано российское законодательство об ЭЦП.

Ряд развитых стран, в частности США, Канада, Германия и другие европейские страны, тоже приняли соответствующие законодательные акты. Например, Закон Германии «Об электронной цифровой подписи» 1997 года, Закон Штата Юта (США) «Об электронной цифровой подписи» 1996 года, Постановления Штата Флорида «Об электронной цифровой подписи» 1996 года. Аналогичные законопроекты существую в Великобритании, Швеции, Франции, Испании, Дании, Австрии, Финляндии и др. Европейским Союзом в июне 1999 года принята Директива «Об общих условиях использования электронных подписей».

Для использования ЭЦП в России частично правовую базу создают отдельные немногочисленные положения, содержащиеся в ГК РФ (ст. 160, 434, 847) и федеральных законах («Об информации, информатизации и защите информации», «Об участии в международном информационном обмене»).

Федеральный Закон «Об электронной цифровой подписи» определяет условия использования ЭЦП в электронных документах органами государственной власти и государственными организациями, а также юридическими и физическими лицами, при соблюдении которых:

Средства создания подписи признаются надежными;

Сама ЭЦП признается достоверной, а ее подделка или фальсификация подписанных данных могут быть точно установлены;

Предоставляются юридические гарантии безопасности передачи информации по открытым телекоммуникационным каналам;

Соблюдаются правовые нормы, содержащие требования к письменной форме документа;

Сохраняются все традиционные процессуальные функции подписи, в том числе удостоверение полномочий подписавшей стороны, установление подписавшего лица и содержания сообщения, а также роль подписи в качестве судебного доказательства;

Обеспечивается охрана персональной информации.

В Законе устанавливаются права и обязанности обладателя электронной цифровой подписи.

В соответствии с законом *владельцем сертификата ключа подписи (обладателем* *электронной цифровой подписи)* является физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись электронных документах (подписывать электронные документы).

Владелец сертификата ключа подписи обязан (статья 12 Закона):

Хранить в тайне закрытый ключ электронной цифровой подписи;

Не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее;

Немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена.

При несоблюдении требований, возмещение причиненных убытков возлагается на владельца сертификата ключа подписи.

 Определены требования к сертификату ключа подписи, выдаваемому удостоверяющим центром для обеспечения возможности подтверждения подлинности ЭЦП. Устанавливается состав сведений, содержащихся в сертификате ключа подписи, срок и порядок его хранения, а также порядок ведения реестров сертификатов.

Согласно ст. 6 данного Закона *сертификат ключа подписи* должен содержать следующие сведения:

Уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;

Фамилия, имя, отчество владельца сертификата ключа подписи или псевдоним владельца;

Открытый ключ электронной цифровой подписи;

Наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;

Сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

В Законе устанавливаются правовой статус *удостоверяющих центров*, их функции. В частности, удостоверяющий центр обязан вести реестр сертификатов ключей подписей и обеспечивать участникам информационной системы свободный доступ к содержащимся в нем сведениям. По обращениям пользователей сертификатов ключей подписей удостоверяющий центр должен подтверждать подлинность электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей. Определяются отношения этих центров с уполномоченным федеральным органом исполнительной власти, который координирует деятельность удостоверяющих центров и также ведет единый государственный реестр сертификатов ключей подписей удостоверяющих центров.

Затраты федеральных органов исполнительной власти по внедрению и использованию ЭЦП будут осуществляться в пределах средств федерального бюджета, предусмотренных для их деятельности.

Закон устанавливает, что удостоверяющим центром для информационных систем общего пользования (для использования неограниченным кругом лиц) может быть организация, обладающая признаками юридического лица и способная нести гражданскую ответственность перед пользователями сертификатов ключей подписи. При этом конкретные требования, предъявляемые к материальным и финансовым возможностям таких центров, будут установлены Правительством Российской Федерации. В корпоративной информационной системе по соглашению участников системы функции удостоверяющего центра могут выполняться одним из участников.

Закон исходит из того, что деятельность удостоверяющего центра по выдаче сертификатов ключей подписи в информационных системах общего пользования подлежит лицензированию. При оформлении лицензии организация, претендующая на ее получение, должна представить обоснование своей способности нести гражданскую ответственность в размере, не менее чем в 1000 раз превышающим предел цены сделки, который данный центр может указывать в сертификате ключа подписи.

Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре определяется договором между удостоверяющим центром и владельцем сертификата ключа подписи. При этом обеспечивается доступ участников информационной системы в удостоверяющий центр для получения сертификата ключа подписи.

По истечении срок хранения сертификат ключа подписи исключается из реестра сертификатов ключей подписей и переводится в режим архивного хранения. Срок архивного хранения составляет не менее чем пять лет. Порядок выдачи копий сертификатов ключей подписей в этот период устанавливается в соответствии с законодательством Российской Федерации.

Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его (статья 14 Федерального закона):

По истечении срока его действия;

При утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационных системах общего пользования;

В случае если удостоверяющему центру стало известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи;

По заявлению в письменной форме владельца сертификата ключа подписи;

В иных установленных нормативными правовыми актами Илии соглашением сторон случаях.

Законом предусматривается защита прав лиц, использующих ЭЦП в процессах электронного обмена документами, и условия приостановления действия и (или) аннулирования сертификата ключа подписи.

Данный закон содержит 5 глав, 21 статью.

В первой главе (3 статьи) определяется цель и сфера применения закона и приводится перечень понятий, используемых в законе.

 Закон распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях; и не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Электронная цифровая подпись документов производится шифром, который называется *ключом.* Фактически ключ – это большой цифровой код (более 1000 цифр), который создается специально для его владельца. Этот персональный, принадлежащий только ему ключ записывается на его ключевую дискету, которую он должен хранить таким образом, чтобы ее никто не мог украсть или скопировать, ведь иначе злоумышленник, обладая таким секретным ключом, сможет подписывать любые документы от его имени. Ключи электронных цифровых подписей используются на основании соответствующих сертификатов. Этим секретным ключом производиться непосредственно электронная цифровая подпись.

Для того, чтобы получатель документа мог проверить электронную подпись лица на полученном документе, ему необходимо иметь Открытый ключ. Открытый ключ – это маленькая часть секретного ключа, достаточная только для проверки подписи (но не для подписания документа от имени владельца электронной цифровой подписи).

Иными словами, электронная цифровая подпись представляет собой код, который содержит в себе в зашифрованном виде:

Идентификацию секретного ключа владельца как лица, подписавшего документ;

Дату и время произведения подписи;

Самое главное – весь исходный текст документа в том виде, в каком он существовал на момент произведения подписи.

Теперь, если исправить хотя бы одну букву в исходном тексте документа, при проверке подписи программа заявит, что «Документ искажен после подписания»!

Подписанный электронной цифровой подписью документ имеет юридическое значение только в пределах тех отношений, которые указаны в сертификате ключа подписи. Участник информационной системы может одновременно владеть любым количеством сертификатов ключей подписей. Однако в отличие от зарубежной практики владельцами сертификатов ключей в соответствии с Законом могут быть только физические лица.

Во второй главе (4 статьи) определены условия, выполнение которых необходимо для юридической равнозначности ЭЦП собственноручной подписи человека в документе на бумажном носителе. Установлены требования к средствам ЭЦП при ее использовании в информационных системах общего пользования, в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления. Установлены порядок выдачи удостоверяющим центром сертификата ключа подписи пользователям, внесения его в реестр сертификатов, а также срок и порядок хранения сертификата.

Сертификаты ключей подписей будут изготавливаться и выдаваться удостоверяющими центрами на основании заявлений участников информационных систем. Заявление должно содержать установленные законом сведения и необходимые для идентификации владельца сертификата ключа подписи и передачи ему сообщений. Заявление подписывается собственноручно владельцем сертификата ключа подписи. Содержащиеся в заявлении сведения подтверждаются предъявлением соответствующих документов.

Третья глава (8 статей) содержит нормы, определяющие особенности правового статуса удостоверяющих центров, отношения удостоверяющих центров с уполномоченным федеральным органом исполнительной власти, обязанности удостоверяющего центра по отношению к обладателю ЭЦП, обязанности обладателя ЭЦП, условия приостановления действия и (или) аннулирования сертификата ключа подписи, порядок прекращения деятельности удостоверяющего центра.

В четвертой главе (4 статьи) содержатся нормы, определяющие порядок использования ЭЦП в сфере государственного управления и корпоративных информационных системах, а также условия признания иностранных сертификатов ключей подписи.

В пятой главе (2 статьи) говорится о приведении нормативных правовых актов в соответствие с этим законом, и содержатся переходные положения.

 Исходя из статьи 160 Гражданского кодекса Российской Федерации на информацию, заверенную электронной цифровой подписью, распространяются все традиционные процессуальные функции собственноручной подписи, в том числе, удостоверение полномочий подписавшей стороны, установление подписавшего лица и содержания сообщения, а также роль подписи в качестве судебного доказательства.

При несоблюдении правил Закона электронная цифровая подпись может быть признана недействительной со всеми вытекающими из этого последствиями.

Применительно к гражданско - правовым сделкам такие последствия регламентированы гражданским кодексом Российской Федерации.

Например, нарушение требований данного закона при заключении сделки, для которой установлена простая письменная форма, по общему правилу не приведет к ее недействительности, но лишит заключивших ее лиц возможности ссылаться на свидетельские показания.

Использование ЭЦП является необходимым, но недостаточным элементом обеспечения безопасности электронных сделок (электронной коммерции). С помощью средств ЭЦП обеспечивается аутентификация сторон сделки при обмене сообщениями и проверяется целостность сообщений. Конфиденциальность же содержания сообщений по сделкам достигается с помощью средств шифрования.

Однако сфера применения ЭЦП не ограничивается электронной коммерцией и охватывает также публично-правовые отношения (внутри государственного сектора), взаимоотношения с государственными органами и организациями и частно-правовые отношения, не связанные с коммерцией.

В заключении я бы хотела выделить несколько основных, принципиальных моментов данного Закона:

*Это возможность использования несертифицированных средств ЭЦП*.

Закон допускает использование средств ЭЦП, не имеющих сертификата. При этом владелец несертифицированных средств ЭЦП (владелец закрытого ключа подписи) обязан заявить об отсутствии сертификата на него всем пользователям открытого ключа, создаваемого этим средством. В этом случае риск убытков от использования несертифицированных средств ЭЦП ложиться на владельца закрытого ключа и пользователя открытого ключа. При желании обеспечить более высокий уровень защиты стороны вправе договориться об обязательном использовании сертифицированных средств ЭЦП.

Закон требует использования сертифицированных средств ЭЦП только в рамках публично-правовых отношений.

Корпоративные системы решают этот вопрос самостоятельно. Обязательная сертификация накладна для больших корпоративных систем, т. к. действие сертификата ограничено во времени, и по окончании срока его действия придется заменить средства ЭЦП всем участникам системы.

Директива СЕ допускает возможность использования несертифицированных средств ЭЦП. Федеральный закон №1 требует обязательную сертификацию, «если иное не установлено соглашением сторон» и сертификация средств ЭЦП рассматривается как условие признания ЭЦП.

*Средства ЭЦП не относятся к средствам шифрования.*

Это положение существенно для российских условий, где нормативными правовыми актами установлены жесткие ограничения (обязательное лицензирование) на создание, распространение и, главное, использование средств шифрования. Кроме того, средства ЭЦП не являются средствами шифрования в общепринятом смысле: использование ЭЦП не защищает подписанную информацию от несанкционированного доступа, кодирования подписанного сообщения не происходит (при создании ЭЦП используется хэш-функция).

Кстати, в Директиве СЕ средства шифрования упоминаются наряду со средствами ЭЦП, что свидетельствует об их различии.

*Государственная аккредитация центров регистрации открытых ключей.*

Центры регистрации открытых ключей создаются для удостоверения ЭЦП и идентификации лица, подписавшего электронный документ. Центры выдают свидетельства на открытый ключ ЭЦП, где указано, кому принадлежит ключ и кто, соответственно, подписал электронное сообщение.

Работа таких центров может осуществляться только в разрешительном (лицензирование) порядке.

В свою очередь, Директива СЕ предусматривает добровольную аккредитацию Центров. Они должны свободно предлагать свои услуги без предварительно полученного разрешения, деятельность их не должна быть связана с получением лицензии. Дополнительные требования могут вводиться отдельными странами, но это не должно препятствовать оказанию трансграничных услуг для граждан и свободному обращению услуг на внутреннем рынке.

*возможность использования открытых ключей ЭЦП, не имеющих свидетельства удостоверяющего центра.*

Требование обязательного наличия сертификата на открытый ключ ЭЦП устанавливается законом только для публично-правовых отношений, но оно может также выводиться по соглашению сторон и в частноправовых отношениях. Органы государственной власти и органы местного самоуправления обязаны иметь сертификат ключа подписи, а также сообщения, направляемые в эти органы и подписанные ЭЦП, принимаются органами при наличии сертификата ключа подписи. Распространение данного требования на все отношения затруднит использование ЭЦП субъектами в ситуациях, когда степень доверия к партнеру не требует дополнительного подтверждения его личности или когда субъекты действуют в доверительной среде (корпоративные системы) либо просто не видят необходимости в использовании сверхнадежных средств ЭЦП. Следовательно, признание ЭЦП не должно связываться с наличием сертификата ключа подписи.

В соответствии с Директивой СЕ отсутствие сертификата на открытый ключ ЭЦП не является основанием для непризнания электронной подписи. Настоящий Федеральный закон одним из условий подлинности ЭЦП является наличие выданного Удостоверяющим центром сертификата ключа подписи.

*Условия использования ЭЦП в корпоративных системах устанавливают участники этих систем.*

Закон предусматривает, что корпоративные (закрытые) системы вправе самостоятельно устанавливать порядок использования ЭЦП.

Согласно Директиве СЕ, общее регулирование не является необходимым для ЭЦП, которое используется исключительно внутри закрытых систем.

*Ограниченная ответственность организаций, удостоверяющих ЭЦП.*

Согласно закону Удостоверяющий центр несет ответственность только в размере прямого реального ущерба (т. е. не включаются штрафные санкции, возмещение упущенной выгоды, компенсация морального вреда и др.). Кроме того, Центр не несет ответственность за ущерб, понесенный лицом не по вине Центра. Для обеспечения ответственности предусмотрено условие деятельности Центра – наличие у него уставного капитала.

Полная ответственность Центра представляется неоправданной, поскольку она, прежде всего, не соответствует степени возможной вины. Например, Центр выдал сертификат, не проверив должным образом данные на владельца закрытого ключа подписи, а потом подтвердил эту подпись по запросу заинтересованного лица. Лицо, доверившись подписи, понесло какие-то убытки. Но Центр может отвечать только за ненадлежащее выполнение своих функций, а не за весь убыток, величина которого зависит от множества иных факторов.

Директива СЕ предусматривает, что пределы ответственности Центра могут быть установлены в сертификате.

*Юридическая сила ЭЦП и признание ее в качестве доказательства в суде.*

Закон предусматривает, что любая ЭЦП, используемая по соглашению сторон или в соответствии с требованиями закона, равнозначна собственноручной подписи лица, если:

Прошла проверку на подлинность при помощи открытого ключа, имеющего сертификат Удостоверяющего центра или в порядке, предусмотренном соглашением сторон;

Подписавшее лицо правомерно владеет закрытым ключом;

ЭЦП является действующей на момент подписания;

В соответствии с этим допускается предоставление в качестве судебных доказательств электронных данных (сообщений), подписанных ЭЦП.

Директива СЕ признает ЭЦП равнозначной собственноручной подписи и при этом предостерегает, что нельзя отрицать юридическую силу электронной подписи или опровергать использование электронной подписи в судебных процедурах только на том основании, что она в электронной форме, не имеет особого сертификата, и не создана надежным 9сертифицированным) устройством электронной цифровой подписи.

Федеральный закон допускает предоставление электронных данных, подписанных ЭЦП, в качестве судебных доказательств только при наличии сертификата ключа подписи, выданного в соответствии с федеральным законом.

*Предмет и сфера действия федерального закона.*

Предмет данного закона – ЭЦП, которая определяется как электронные данные, полученные в результате преобразования исходных электронных данных при помощи закрытого ключа, что позволяет:

Подтвердить неизменность электронных данных;

Установить, что ЭЦП создана с помощью закрытого ключа, соответствующего открытому;

Установить владельца открытого ключа.

Предметом регулирования в законе является только ЭЦП, иные аналоги собственноручной подписи не рассматриваются.

Таким образом, сфера действия закона охватывает только использование ЭЦП.

Директива СЕ распространяется на электронные подписи, что включает ЭЦП, но не ограничивается ею. Также Директива не ограничивает сферу использования электронной подписи, но устанавливает требование, чтобы условия использования были направлены на ее свободное обращение на внутреннем рынке.

В российском законе присутствует технологическое определение ЭЦП, а сфера использования ЭЦП ограничена процессами обмена электронными данными.

**ИСПОЛЬЗУЕМАЯ ЛИТЕРАТУРА:**

Гражданский кодекс Российской Федерации

Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 года №1-ФЗ

Пояснительная записка к проекту федерального закона «Об электронной цифровой подписи» // Кафедра правовой информатики МГЮА, 2001г.

Андрюкин Ю. Федеральный закон «Об электронной цифровой подписи» //Консультант плюс: Важнейшие документы недели, выпуск от 7 февраля 2002 года.

(www.consultant.ru/Online/Review/iw0207)

Некоторые концептуальные вопросы законодательства об электронной цифровой подписи // Журнал «Банки и технологии», №1, 2001г.

Электронная подпись // АКБ «Челиндбанк», 2001г. (www.icb.chel.su/clbank/usr-02-08.shtml)

Электронная подпись и шифрование // МО ПНИЭИ

(www.security.ru/el.wright.html)