ПРИЛОЖЕНИЕ
К ЕЖЕМЕСЯЧНОМУ ЮРИДИЧЕСКОМУ ЖУРНАЛУ
Х·О·З·Я·Й·С·Т·В·О и ПРАВО
Учредители —
Высший Арбитражный Суд Российской Федерации,
Министерство юстиции Российской Федерации
и Некоммерческое партнерство
Журнал "Хозяйство и право"
Издается с июля 1999 года
ПРИЛОЖЕНИЕ к № 5, май 2003 г.

Н. СОЛОВЯНЕНКО

Комментарий к Федеральному закону "Об электронной цифровой подписи"

Комментарий к Федеральному закону " Об электронной цифровой подписи"

1. ЦЕЛИ И СФЕРА ПРИМЕНЕНИЯ ФЕДЕРАЛЬНОГО ЗАКОНА "ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ"

Федеральный закон от 10 января 2002 года № 1-ФЗ "Об электронной цифровой подписи" введен в действие со дня его официального опубликования[1].

Разработка и принятие рамочного регулирования, относящегося к применению информационных и коммуникационных технологий (ИКТ), в том числе реализующих электронные подписи, — одна из глобальных тенденций развития законодательства последних десятилетий.

В конце XX — начале XXI века в Российской Федерации ИКТ стали интенсивно использоваться в сфере государственного управления, коммерческой и иной деловой деятельности, а также в повседневной жизни. Постановлением Правительства РФ от 28 января 2002 года № 65 была утверждена Федеральная целевая программа "Электронная Россия (2002–2010 гг.)"[2].

Программа предусматривает в 2003–2004 годах:

- реализацию проектов, обеспечивающих взаимодействие органов государственной власти и органов местного самоуправления с гражданами и хозяйствующими субъектами в сфере налогообложения, по вопросам оформления таможенной документации, регистрации и ликвидации юридических лиц, выдачи лицензий и сертификатов, подготовки и представления отчетной документации, предусмотренной законодательством Российской Федерации об акционерных обществах, рынке ценных бумаг и поставках продукции для федеральных государственных нужд;
- создание на этом этапе основы единой информационной и телекоммуникационной инфраструктуры для органов государственной власти и органов местного самоуправления, бюджетных и некоммерческих организаций, системы электронной торговли в сфере поставок продукции для федеральных государственных нужд и для общественных пунктов подключения к общедоступным информационным системам.

---

[1] Российская газета, 2002, 12 января, № 6; Собрание законодательства РФ, 2002, № 2, ст. 127.

[2] ": http://www.e-rus.org

К 2010 году планируется:

- внедрить ИКТ во все сферы общественной деятельности на основе единой информационной и телекоммуникационной инфраструктуры и использования системы электронной торговли;
- обеспечить внедрение системы электронной торговли в сфере поставок продукции для государственных нужд на федеральном уровне и уровне субъектов Российской Федерации, стандартизованного электронного документооборота и систем обеспечения информационной безопасности;
- завершить формирование единой информационной и телекоммуникационной инфраструктуры для органов государственной власти и органов местного самоуправления, бюджетных и некоммерческих организаций, общественных пунктов подключения к общедоступным информационным системам.

Как видно из положений программы "Электронная Россия", в Российской Федерации активно формируется комплекс технологических, организационных, экономических и юридических отношений, связанных с применением информационных и коммуникационных технологий.

В правовой сфере утвердились такие новые для традиционной юриспруденции категории как электронный документ, электронные подписи, электронная торговля (или "электронная коммерция"), электронные сделки, электронные платежи и расчеты, электронные деньги и ряд других, объединяемые понятием "электронный обмен данными".

В правовом регулировании электронного обмена данными положения, регламентирующие применение электронных подписей и связанных с ними услуг, позволяющих аутентифицировать данные, принадлежат к числу приоритетов. Обеспечение доверия к электронной подписи и ее правовое признание — обязательный элемент электронной торговли (коммерции); заключения договоров и иных сделок, передачи права собственности и обязательственных прав; а также совершения иных юридически значимых действий посредством электронной связи. Отношения, связанные с применением электронных подписей, становятся предметом специального законодательства, цель которого — предоставить необходимые юридические гарантии участникам электронного обмена данными и обеспечить защиту их прав и законных интересов.

В 1999 году была издана Директива Европарламента и Совета Европейского Союза "Об электронных подписях"[3], в 2000 году принят модельный закон СНГ "Об электронной цифровой подписи"[4], а Рабочая группа по электронной торговле Комиссии Организации Объединенных Наций по праву международной торговли (UNCITRAL) посвятила 31–38-ю сессии подготовке и принятию Типового закона UNCITRAL "Об электронных подписях"[5]. В связи с этим можно положительно оценить намерение российского законодателя в специальном Законе "Об электронной цифровой подписи" (2002 г.) сосредоточить основные положения, относящиеся к применению ЭЦП.

Необходимо отметить, что нормативные правовые акты, регулирующие применение электронных подписей, действуют более чем в 60 странах мира, принадлежащих к различным правовым системам. При разработке и принятии национального законодательства, регламентирующего электронные под-

---

[3] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 013, 19/01/2000, p. 0012–0020.

[4] Принят на 16-м пленарном заседании Межпарламентской Ассамблеи государств — участников СНГ 9 декабря 2000 года // Информационный бюллетень МПА СНГ, 2001, № 26, с. 310.

[5] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment. United Nations, New York, 2002.

писи, зарубежные государства, как правило, воспринимают положения названных нормативных и типовых актов Евросоюза и UNCITRAL[6].

Развитие иностранного законодательства и международного права в данной области идет по пути гармонизации, выработки единой методологии, что позволит создать на мировом уровне универсальную правовую инфраструктуру электронной подписи. Современное правовое регулирование электронных подписей не ограничивается сферой гражданского и торгового права, а включает также вопросы административного права, в том числе юридические нормы и правила "нового поколения", регламентирующие так называемые "услуги информационного общества", а также правовой статус, обязанности и ответственность лиц, предоставляющих подобные услуги, сертификационных (удостоверяющих) центров, которые выпускают сертификаты ключей электронных подписей, и т. д.

Окинавская хартия глобального информационного общества[7] также предусматривает дальнейшее развитие и эффективное функционирование электронной идентификации, электронной подписи, криптографии и других средств обеспечения безопасности и достоверности операций. Окинавская хартия ставит перед правительствами государств задачу создания "предсказуемой, транспарентной и недискриминационной политики и нормативной базы, необходимой для информационного общества". "Нам необходимо позаботиться о том, чтобы правила и процедуры, имеющие отношение к ИТ, соответствовали коренным изменениям в экономических сделках с учетом принципов эффективного партнерства между государственным и частным сектором, а также транспарентности и технологической нейтральности. Такие правила должны быть предсказуемыми и способствовать укреплению делового и потребительского доверия".

Необходимо отметить, что при разработке юридической инфраструктуры электронной цифровой подписи в российском Законе об ЭЦП обнаружились в целом те же проблемы и тенденции, что и в построении правовой базы электронной подписи в зарубежных странах.

Российский Федеральный закон "Об электронной цифровой подписи" (ЭЦП) ставит своей целью обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении

---

[6] Примерами специальных нормативных правовых актов, регулирующих электронные подписи в европейских странах, являются: Закон Германии "Об электронной цифровой подписи" 1997 года (с изм. 2000 года), Закон Эстонии "Об электронной цифровой подписи" 1999 года; Закон Чешской республики 2000 года.

Закон Австрии "Об электронной подписи" вступил в силу 1 января 2000 года. Закон полностью базируется на Директиве Евросоюза "Об электронных подписях". Австрия первой из европейских государств включила положения Директивы в национальное законодательство.

В Бельгии 14 июня 2001 года Парламент одобрил Билль о Центрах сертификации и квалифицированных сертификатах, который реализует положения Директивы Европарламента "Об электронных подписях". В Дании в октябре 2000 года вступил в силу Закон об электронной подписи, который реализует положения Директивы Европарламента "Об электронных подписях". Во Франции 29 февраля 2000 года был принят Закон об электронных подписях, адаптирующий законодательство о доказательствах к информационным технологиям и электронным подписям. Закон вступил в силу 1 апреля 2001 года. Он вводит положения Директивы Европарламента "Об электронных подписях" во французское право. В Венгрии 29 мая 2001 года был принят Закон об электронных подписях, который вступил в силу 1 сентября 2001 года. Закон полностью отвечает принципам европейского законодательства. В Норвегии Парламентом был принят Закон "Об электронной подписи", который вступил в силу 1 июля 2001 года.

В Бразилии 29 июня 2001 года правительство издало нормативный акт, гарантирующий юридическую силу электронным документам и электронным подписям. В Израиле Закон "Об электронной подписи" был принят Парламентом 25 марта 2001 года, вступил в силу 25 сентября 2001 года. В Японии 1 апреля 2001 года вступил в силу Закон "Об электронных подписях и услугах по выдаче сертификатов".

Федеральный закон США 2000 года "Об электронных подписях в международной и внутренней торговле" принадлежит к числу законодательных актов, посвященных общим принципам регулирования электронной торговли, в том числе правовому признанию электронных сделок, кроме того, он включает значительное число норм, регламентирующих применение электронных подписей и выпуск сертификатов электронных подписей.

[7] Пункт 7 Окинавской хартии глобального информационного общества. Принята 22 июля 2000 года лидерами [illegible]

которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе (п. 1 ст. 1).

В данной норме подразумевается юридическая, а не технологическая равнозначность электронных и собственноручных подписей. Физическая подпись не является средством защиты информации и не может замещать печать. В юридическом смысле электронная цифровая подпись представляет собой не только реквизит электронного документа, предназначенный для защиты электронного документа от подделки. Применение ЭЦП прежде всего служит основанием возникновения правового отношения.

В указанной статье Закона идет речь о правовом признании и равной юридической силе электронных документов, подписанных ЭЦП, и документов на бумажном носителе, подписанных собственноручной подписью. Здесь воспроизведен принцип функционального эквивалента, лежащий в основе мировой практики правового регулирования электронного обмена данными.

Названный принцип означает, что в случае, когда национальный закон предписывает, чтобы юридические действия осуществлялись в письменном виде или с использованием письменных документов, данное требование считается выполненным, если указанные действия осуществляются посредством одного или нескольких электронных документов, подписанных электронными подписями, с соблюдением положений законодательства.

Электронная подпись в электронном документе, как правило, выполняет следующие юридические функции:

— указывает, кем подписан электронный документ или иное электронное сообщение;

— гарантирует, что электронный документ подписан уполномоченным лицом;

— обеспечивает подлинность и неизменность подписанного документа;

— обозначает выражение воли стороны по сделке;

— символизирует необходимую письменную форму сделки, заключенной посредством электронной связи.

Сфера применения ФЗ "Об электронной цифровой подписи" не имеет четко установленных границ. Определенно назван только один вид правовых отношений, на которые распространяется его действие, — отношения, возникающие при совершении гражданско-правовых сделок (п. 2 ст. 1). Другие случаи, на которые распространяется Закон об ЭЦП, должны быть специально предусмотрены законодательством Российской Федерации (п. 2 ст. 1).

Таким образом, российский Закон "Об электронной цифровой подписи" не осуществил принципиального признания юридической равнозначности электронной цифровой подписи и собственноручной подписи лица для неопределенного круга юридических действий, которые совершаются посредством электронного обмена данными и оформляются электронными документами. В этом смысле Закон ограничился правовым признанием ЭЦП в связи с заключением гражданско-правовых сделок.

Однако Гражданский кодекс РФ (часть первая) еще в 1994 году обозначил электронную цифровую подпись в качестве аналога собственноручной подписи при совершении договоров и иных сделок (ст. 160).

Гражданский кодекс РФ, во-первых, признал иные варианты заключения договора в письменной форме, нежели составление документов на традици-

онном бумажном носителе и подписание таких документов посредством собственноручных подписей сторон. Так, в п. 2 ст. 434 ГК РФ называются способы заключения договоров и указывается, что договор может быть заключен путем обмена документами посредством "...телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору". Приведенный перечень используемых при заключении договора технических средств включает электронно-вычислительную технику. Во-вторых, ГК РФ (п. 2 ст. 160) устанавливает, что при совершении сделок допускается использование ... электронной цифровой подписи либо иного аналога собственноручной подписи в случаях и порядке, предусмотренных законом, иными правовыми актами или соглашением сторон. Таким образом, основные правовые условия использования электронной цифровой подписи при совершении сделок обеспечены гражданским законодательством, а не Федеральным законом об ЭЦП. В силу названных положений Кодекса сделки, совершенные с использованием электронной цифровой подписи, отвечают формальным требованиям к простой письменной форме.

Указанным нормам гражданского законодательства корреспондируют рекомендации Высшего Арбитражного Суда РФ (информационное письмо от 19 августа 1994 года № С1-7/ОП-587 "Об отдельных рекомендациях, принятых на совещаниях по судебно-арбитражной практике"): "В том случае, когда стороны изготовили и подписали договор с помощью электронно-вычислительной техники, в которой использована система цифровой (электронной) подписи, они могут представлять в арбитражный суд доказательства по спору, вытекающему из этого договора, также заверенные цифровой (электронной) подписью.

Если же между сторонами возник спор о наличии договора и других документов, подписанных цифровой (электронной) подписью, арбитражный суд должен запросить у сторон выписку из договора, в котором указана процедура порядка согласования разногласий, на какой стороне лежит бремя доказывания тех или иных фактов и достоверности подписи.

С учетом этой процедуры арбитражный суд проверяет достоверность представленных сторонами доказательств. При необходимости арбитражный суд вправе назначить экспертизу по спорному вопросу, используя при этом предусмотренную договором процедуру.

В случае отсутствия в таком договоре процедуры согласования разногласий и порядка доказывания подлинности договора и других документов, а одна из сторон оспаривает наличие подписанного договора и других документов, арбитражный суд вправе не принимать в качестве доказательств документы, подписанные цифровой (электронной) подписью"[8].

Необходимо отметить, что разъяснения Высшего Арбитражного Суда РФ обнаруживают преемственность подхода к представлению в качестве судебных доказательств документов, заверенных электронной цифровой подписью, по отношению к инструктивным указаниям Госарбитража СССР от 29 июня 1979 года № И-1-4 "Об использовании в качестве доказательств по арбитражным делам документов, подготовленных с помощью электронно-вычислительной техники".

В данном документе в целях обеспечения единства практики по делам, в которых в качестве доказательств используются документы, подготовлен-

[8] Хозяйство и право. 1994. № 11. с. 148.

ные с помощью электронно-вычислительной техники, Государственный арбитраж СССР предложил органам арбитража руководствоваться следующими указаниями.

■ Стороны по арбитражным делам в обоснование своих требований и возражений вправе представлять арбитражам документы, подготовленные с помощью электронно-вычислительной техники. Эти документы, поскольку они содержат данные об обстоятельствах, имеющих значение для дела, должны приниматься органами арбитража на общих основаниях в качестве письменных доказательств.

■ При решении вопроса, находятся ли стороны в договорных отношениях, исходить из того, что сделкой в письменной форме является также заключенная сторонами сделка, когда ее условия переданы или зафиксированы с помощью средств электронно-вычислительной техники.

■ Органы арбитража должны требовать от сторон, чтобы представляемые ими документы, подготовленные с помощью электронно-вычислительной техники, были надлежащим образом оформлены.

■ Документы, подготовленные с помощью электронно-вычислительной техники и представляемые в арбитраж в качестве доказательств по делу, должны быть представлены в таком виде, который позволял бы уяснить их содержание.

В связи с этим примечателен тот факт, что инструктивные указания Госарбитража СССР об использовании в качестве доказательств по арбитражным делам документов, подготовленных с помощью электронно-вычислительной техники, появились почти за двадцать лет до того, как аналогичные рекомендации были сформулированы в Типовом законе UNCITRAL "Об электронной торговле" и руководстве по его принятию[9]. Речь идет о зафиксированных в названном документе UNCITRAL положениях, определяющих юридическую силу договоров, заключаемых при помощи ЭВМ, письменную форму электронных документов, применение электронных подписей, условия хранения договорной документации в электронном виде, признания в качестве судебных доказательств, а также устанавливающих соотношение между оригиналом и копиями электронных документов.

Тем не менее виды юридических документов, которые можно применять в электронном виде с использованием ЭЦП, значительно разнообразнее электронных документов, оформляющих исключительно гражданско-правовые сделки.

Вопрос о том, насколько Закон об электронной цифровой подписи признал действительность таких электронных документов, остается открытым. Чтобы легализовать электронную цифровую подпись в электронных документах, оформляющих трудовые, налоговые, административные и иные отношения, не относящиеся к категории гражданско-правовых сделок, по-прежнему необходимы соответствующие положения, закрепленные в законодательных актах.

Было бы правильным уже сейчас внести изменения в рассматриваемый Федеральный закон, закрепив в нем, прежде всего, возможность использования ЭЦП в качестве эквивалента собственноручной подписи в случаях, когда это прямо не запрещено законодательством. Наряду с этим следует четко указать в законе, какие документы не могут использоваться в элек-

---

[9] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996), with additional article 5 *bis* as adopted in 1998 (articles 5–8).

тронном виде и, соответственно, подписываться электронной цифровой подписью.

В зарубежном законодательстве об электронной подписи такие запреты относятся к завещанию, процессуальным документам и ряду других. Конечно, принятие аналогичных положений потребует внесения соответствующих изменений и дополнений в действующие российские законы.

Такие нормы в современном российском законодательстве за редким исключением отсутствуют.

К исключениям относится, например, положение ст. 4 Федерального закона от 11 марта 1997 года № 48-ФЗ "О переводном и простом векселе", которое допускает возможность составления простого и переводного векселя только на бумаге (бумажном носителе). В связи с этим постановление Пленума Верховного Суда РФ и Пленума Высшего Арбитражного Суда РФ от 4 декабря 2000 года № 33/14 "О некоторых вопросах практики рассмотрения споров, связанных с обращением векселей" дает судам и арбитражным судам разъяснения, в соответствии с которыми следует учитывать, что нормы вексельного права не могут применяться к обязательствам, оформленным на электронных и магнитных носителях (п. 2).

В настоящее время в Российской Федерации действует значительное число норм специального законодательства, устанавливающих случаи применения ЭЦП на основании комментируемого Федерального закона. Поскольку сфера применения ЭЦП в юридической практике постоянно расширяется, объем специального законодательства увеличивается. Положения, посвященные ЭЦП, закрепляются не только на уровне законов, но в большинстве случаев — в подзаконных нормативных правовых актах.

Федеральный закон от 1 апреля 1996 года № 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования" (с изм. от 25 октября 2001 года, 31 декабря 2002 года) содержит общие правила представления сведений о застрахованных лицах и порядок хранения этих сведений (ст. 8). Указанные сведения могут представляться как в виде документов в письменной форме, так и в электронной форме (на магнитных носителях или по каналам связи) при наличии гарантий их достоверности и защиты от несанкционированного доступа и искажений. В этом случае юридическая сила представленных документов должна подтверждаться электронной цифровой подписью в соответствии с законодательством Российской Федерации. Вопрос о возможности представления информации в электронной форме решается Пенсионным фондом РФ совместно с конкретными плательщиками страховых взносов государственного пенсионного страхования. Постановление ПФР от 26 января 2001 года № 15 "О введении в системе Пенсионного фонда Российской Федерации криптографической защиты информации и электронной цифровой подписи" предусматривает обеспечение защиты информации, представляемой в электронной форме в системе электронного документооборота Пенсионного фонда РФ. Правление ПФР постановляет использовать для защиты информации, передаваемой в электронной форме, средства криптографической защиты информации и электронной цифровой подписи.

В соответствии с п. 2 ст. 80 Налогового кодекса РФ издан приказ МНС РФ от 2 апреля 2002 года № БГ-3-32/169 "Об утверждении Порядка представления налоговой декларации в электронном виде по телекоммуникационным каналам связи". "Представление налоговой декларации в электронном виде допускается при обязательном использовании сертифициро-

ванных Федеральным агентством правительственной связи и информации при Президенте Российской Федерации средств электронной цифровой подписи (далее — ЭЦП), позволяющих идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации, содержащейся в налоговой декларации в электронном виде" (п. 8).

На основании Федерального закона от 22 апреля 1996 года № 39-ФЗ "О рынке ценных бумаг" (с изм. на 28 декабря 2002 года) и Федерального закона от 10 января 2002 года № 1-ФЗ "Об электронной цифровой подписи" было принято постановление Федеральной комиссии по рынку ценных бумаг от 31 октября 2002 года № 43/пс "Об утверждении Положения о порядке предоставления в Федеральную комиссию по рынку ценных бумаг электронных документов". В постановлении устанавливается последовательность действий организаций, представляющих в Федеральную комиссию по рынку ценных бумаг электронные документы, подписанные электронной цифровой подписью. Электронные документы могут быть переданы в ФКЦБ РФ посредством телекоммуникационных каналов связи, в формате и способом, установленными правовыми актами Федеральной комиссии.

Приказом ГТК РФ от 29 июля 2002 года № 801 "Об организации эксперимента по декларированию в электронной форме в Приволжском и Центральном таможенных управлениях" утверждены Временные правила таможенного оформления и таможенного контроля при заявлении сведений в электронной форме о товарах и транспортных средствах (далее — Временные правила). На основании указанного приказа ГТК организовывалось проведение эксперимента по использованию декларирования в электронной форме с применением электронной цифровой подписи в соответствии с Временными правилами при осуществлении таможенного оформления товаров и транспортных средств, перемещаемых через таможенную границу Российской Федерации. Временные правила действовали в течение пяти месяцев со дня вступления в силу приказа (с 22 сентября 2002 года по 22 февраля 2003 года).

Временные правила разработаны на основании ст. 16, 126, 169, 174, 176, 179, 180 Таможенного кодекса РФ, Федерального закона "Об электронной цифровой подписи" в целях ускорения товарооборота, сокращения времени таможенного оформления, а также внедрения безбумажных технологий при таможенном оформлении и таможенном контроле. Временные правила определяют особенности проведения таможенного оформления и таможенного контроля при заявлении сведений в электронной форме о перемещаемых через таможенную границу Российской Федерации товарах и транспортных средствах:

а) при декларировании в соответствии с общеустановленным порядком путем подачи грузовой таможенной декларации в электронной форме (далее — ЭГТД);

б) при применении особого порядка декларирования, установленного Положением о применении временных, неполных и периодических таможенных деклараций, утвержденным приказом ГТК России от 17 апреля 2000 года № 299 (с изм. от 21 ноября 2001 года № 1107), до фактического представления товаров таможенному органу, в котором будет производиться их таможенное оформление, путем подачи предварительной грузовой таможенной декларации в электронном виде (п. 5.1).

Указание ЦБР от 24 октября 1997 года № 7-У "О порядке составления и представления отчетности кредитными организациями в Центральный банк

Российской Федерации" (с изм. на 11 апреля 2002 года) устанавливает обязательные для кредитных организаций правила составления и представления отчетности в Банк России, а также унифицированные требования к оформлению, построению и утверждению форм отчетности (п. 1). Под отчетностью понимается предусмотренная действующим законодательством Российской Федерации и нормативными актами Банка России форма получения информации о деятельности кредитных организаций, при которой Банк России получает информацию в виде установленных отчетных документов (форм отчетности), утвержденных Банком России, подписанных электронной цифровой подписью или собственноручно лицами, ответственными за достоверность представленных сведений. Отчетность представляется кредитными организациями в Банк России на бумажных носителях и/или в электронном виде в форматах, установленных Банком России, содержащих тот же набор показателей, что и документ на бумажном носителе, в соответствии с требованиями нормативных актов Банка России. Формы отчетности являются официальными документами кредитной организации, которая в соответствии с действующим законодательством несет ответственность за их достоверность, правильность оформления и своевременность представления. Проверка подлинности электронного документа включает проверку правильности электронной цифровой подписи и соответствие зарегистрированного владельца этой ЭЦП составителю документа, а также контроль за правильностью и полнотой идентификационных реквизитов электронного документа.

В Федеральном законе об ЭЦП указываются основные нормативные правовые акты, в соответствии с которыми осуществляется правовое регулирование отношений в области использования электронной цифровой подписи. Наряду с названным Федеральным законом и ГК РФ названы также Федеральные законы "Об информации, информатизации и защите информации"[10] и "О связи"[11].

Федеральный закон от 20 февраля 1995 года № 24-ФЗ "Об информации, информатизации и защите информации" (с изм. от 10 января 2003 года) предусматривает, что юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью. Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования (п. 3 ст. 5).

Помимо перечисленных положений непосредственное отношение к применению ЭЦП имеет глава 4 Федерального закона, посвященная информационным системам, технологиям и средствам их обеспечения. В первую очередь представляет интерес определение понятия "информационная система", которое включено в понятийный аппарат Закона об информации (ст. 2). Данное понятие интенсивно используется и в Законе об ЭЦП, однако не имеет в нем собственной дефиниции.

Федеральный закон от 16 февраля 1995 года № 15-ФЗ "О связи" (с изм. от 6 января, 17 июля 1999 года) воздействует на применение электронной циф-

[10] Собрание законодательства РФ, 1995, № 8, ст. 609.

[11] Собрание законодательства РФ, 1995, № 8, ст. 600.

ровой подписи, поскольку "средства связи вместе со средствами вычислительной техники составляют техническую базу обеспечения процесса сбора, обработки, накопления и распространения информации" (ст. 1).

Перечень нормативных правовых актов, регламентирующих отношения в области использования электронной цифровой подписи, не является исчерпывающим: указанное регулирование может осуществляться также другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации. Использование электронной цифровой подписи регламентируется также соглашением сторон (ст. 2).

Базовые нормы российского законодательства, оказывающие непосредственное воздействие на применение электронной цифровой подписи, содержатся также в следующих нормативных правовых актах:

◆ Федеральном законе от 8 августа 2001 года № 128-ФЗ "О лицензировании отдельных видов деятельности", поскольку деятельность удостоверяющего центра подлежит лицензированию в соответствии с законодательством Российской Федерации о лицензировании отдельных видов деятельности (ст. 17).

◆ Кодексе РФ об административных правонарушениях от 30 декабря 2001 года № 195-ФЗ, который устанавливает ответственность за: "Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна)" (ст. 13.13);

◆ Федеральном законе от 27 декабря 2002 года № 184-ФЗ "О техническом регулировании"[12], который регулирует отношения, возникающие при разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, а также разработке, принятии, применении и исполнении указанных требований на добровольной основе;

◆ государственных стандартах, в том числе: ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи" и ГОСТ Р 34.11-94 "Информационная технология. Криптографическая защита информации. Функция хеширования"[13].

Применение электронной цифровой подписи должно подчиняться не только специальным требованиям нормативных правовых актов Российской Федерации, предъявляемым к использованию электронных документов, но, в первую очередь, общим нормам российского законодательства.

Особая роль в правовом регулировании отношений отводится Гражданскому кодексу РФ, поскольку действие Федерального закона об ЭЦП распро-

---

[12] Настоящий Федеральный закон вступает в силу по истечении шести месяцев со дня его официального опубликования (ст. 48).

[13] Необходимо учитывать положения ст. 2 Федерального закона "О техническом регулировании", в соответствии с которым стандарт — документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. К документам в области стандартизации, используемым на территории РФ, Закон относит: национальные стандарты; правила стандартизации, нормы и рекомендации в области стандартизации; применяемые в установленном порядке классификации, общероссийские классификаторы технико-экономической и социальной информации; стандарты организаций (ст. 13).

Со дня вступления в силу Федерального закона "О техническом регулировании" утрачивает силу (ст. 47) Закон РФ от 10 июня 1993 года № 5154-I "О стандартизации".

страняется, прежде всего, на отношения, возникающие при совершении гражданско-правовых сделок.

Не менее значимы нормы Арбитражного процессуального кодекса РФ от 24 июля 2002 года № 95-ФЗ и Гражданского процессуального кодекса РФ от 14 ноября 2002 года № 138-ФЗ, называющие документы, полученные посредством электронной связи, в числе письменных доказательств.

Так, в ч. 3 ст. 75 АПК РФ установлено, что документы, полученные посредством факсимильной, электронной или иной связи, а также документы, подписанные электронной цифровой подписью или иным аналогом собственноручной подписи, допускаются в качестве письменных доказательств в случаях и в порядке, которые установлены федеральным законом, иным нормативным правовым актом или договором.

Часть 1 ст. 71 ГПК РФ признает письменными доказательствами содержащие сведения об обстоятельствах, имеющих значение для рассмотрения и разрешения дела, акты, договоры, справки, деловую корреспонденцию, иные документы и материалы, выполненные в форме цифровой, графической записи, в том числе полученные посредством факсимильной, электронной или другой связи либо иным позволяющим установить достоверность документа способом.

Действие комментируемого Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Закон "Об электронной цифровой подписи" не воспроизводит подход иностранного законодательства и международного права к регулированию электронных подписей. Так, отечественный закон сосредоточил внимание исключительно на технологии электронно-цифровой подписи, которая строится на идеологии асимметричного шифрования (ст. 3). Российский Закон об ЭЦП не регулирует отношения, возникающие при использовании иных аналогов собственноручной подписи.

Между тем общепринятый в мировом сообществе подход — так называемая "технологическая нейтральность" законодательства. Правовое признание любых электронных аналогов собственноручной подписи и юридическая сила последних не ограничиваются в зависимости от реализуемой в них технологии. Электронные подписи должны лишь отвечать требованиям применяемого права.

По этой причине рабочая группа ЮНСИТРАЛ по электронной торговле отказалась внести понятие "криптографический ключ" в проект Типового закона "Об электронных подписях" как не отвечающее принципу нейтральности, лежащему в основе данного проекта[14].

Директивой Евросоюза "Об электронных подписях"[15] также устанавливается равный правовой режим для различных технологий создания электронных подписей. Названной Директивой предусматривается, что юридическая сила электронных подписей и допустимость последних в качестве доказательств не должна отрицаться только на том основании, что подписи являются электронными, или не созданы при помощи надежных средств электронной цифровой подписи, или не имеют соответствующего сертификата (ст. 5).

---

[14] Доклад Комиссии ООН по праву международной торговли о работе ее 34-й сессии 25 июня-13 июля 2001 года. Генеральная Ассамблея. Официальные отчеты. 56-я сессия. Дополнение № 17 (A/56/17).ООН, 2001 г., с. 56.

[15] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 013 , 19/01/2000, p. 0012-0020.

Необходимо отметить, что гражданское законодательство РФ более полно отвечает принятому в мировой практике подходу, поскольку позволяет распространить определение электронной подписи на связанные с электронными документами символы, коды, пароли, персональные идентификационные номера (ПИН), биометрические устройства (системы оперативной идентификации по отпечаткам пальцев) и т. д., не являющиеся электронной цифровой подписью по смыслу федерального закона[16]. Они могут рассматриваться в качестве подписи, если используются участниками информационной системы с явным намерением подтвердить подлинность электронного документа и идентифицировать подписавшую сторону в порядке, установленном для соответствующей информационной системы, в том числе на основании соглашения участников системы.

В силу п. 2 ст. 160 ГК РФ при совершении сделок допустимо использование как электронной цифровой подписи, так и любого иного аналога собственноручной подписи. Таким образом, сделки, совершенные ("подписанные") с применением аналога собственноручной подписи, признаются совершенными в простой письменной форме.

Названный подход характерен также для арбитражного процессуального и гражданского процессуального законодательства.

Как было указано ранее, в соответствии с ч. 3 ст. 75 АПК РФ документы, подписанные ЭЦП либо иным аналогом собственноручной подписи, допускаются в качестве письменных доказательств в случаях и в порядке, которые установлены федеральным законом, иным нормативным правовым актом или договором. К "технологически нейтральным" относится положение ч. 1 ст. 71 ГПК РФ, включающее в число письменных доказательств документы и материалы, выполненные в форме цифровой, графической записи, в том числе полученные посредством факсимильной, электронной или другой связи либо иным позволяющим установить достоверность документа способом. Таким образом, общее законодательство, в отличие от специального, посвященного исключительно ЭЦП, создает правовую среду, нейтральную (без каких-либо предпочтений) по отношению к различным носителям информации и программным средствам.

Использование иных аналогов собственноручной подписи может с большей или меньшей степенью детализации регламентироваться федеральными законами или иными нормативными правовыми актами РФ.

Так, в п. 3 ст. 847 ГК РФ предусмотрена возможность на основании договора удостоверять права распоряжения денежными суммами, находящимися на счете, электронными средствами платежа и другими документами с использованием в них аналогов собственноручной подписи, кодов, паролей и иных средств, подтверждающих, что распоряжение дано уполномоченным на это лицом.

В качестве примера подзаконного нормативного правового акта, регулирующего применение аналогов собственноручной подписи, можно назвать Временное положение ЦБР от 10 февраля 1998 года № 17-П "О порядке приема к исполнению поручений владельцев счетов, подписанных аналога-

[16] Первый для российского здравоохранения проект по созданию системы защищенного электронного документооборота, построенной на биометрических устройствах, проводится в экспериментальном порядке на базе городской больницы г. Тольятти. Проектом предусматривается авторизация доступа врачей к электронным историям болезни и назначениям курса лечения; реализация личных подписей лечащих врачей под записями в истории болезни с последующим контролем прав доступа на основе биометрических характеристик пользователей медицинской информационной системы из числа врачебного и административного персонала больницы.
http://biolink.ru/ru/

ми собственноручной подписи, при проведении безналичных расчетов кредитными организациями". Данный нормативный документ ЦБР устанавливает порядок приема к исполнению поручений владельцев счетов, в том числе составленных на электронных носителях (далее — платежные документы), подписанных аналогами собственноручной подписи, при проведении безналичных расчетов на территории Российской Федерации между кредитными организациями и кредитными организациями и их клиентами. Здесь в качестве аналога собственноручной подписи (АСП) предусмотрен персональный идентификатор кредитной организации либо клиента кредитной организации, являющийся контрольным параметром правильности составления всех обязательных реквизитов платежного документа и неизменности их содержания.

Положение Банка России от 9 апреля 1998 года № 23-П "О порядке эмиссии кредитными организациями банковских карт и осуществления расчетов по операциям, совершаемым с их использованием" (с изм. от 29 ноября 2000 года) устанавливает требования Банка России к кредитным организациям по эмиссии последними банковских карт, правилам осуществления расчетов и порядок учета кредитными организациями операций, совершаемых с использованием банковских карт. Банковские карты могут быть использованы для осуществления операций по счетам юридических и физических лиц. В соответствии с данным нормативным правовым актом Банка России (п. 1) документ, являющийся основанием для осуществления расчетов по операциям с использованием банковских карт и/или служащий подтверждением их совершения, составленный с применением банковских карт или их реквизитов на бумажном носителе и/или в электронной форме, может быть подписан держателем банковской карты собственноручно или аналогом его собственноручной подписи.

2. ВЗАИМОСВЯЗЬ ПОНЯТИЙНОГО АППАРАТА ЗАКОНА И ТЕХНОЛОГИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

В ст. 3 Федерального закона "Об электронной цифровой подписи" представлен значительный понятийный аппарат. Основные понятия, используемые в Законе, неразрывно связаны с технологией ЭЦП.

Как работает технология электронной цифровой подписи? Цифровые подписи создаются и проверяются с помощью криптографии — отрасли прикладной математики, занимающейся преобразованием электронных документов в кажущуюся неразборчивой форму и обратно.

В Федеральном законе об ЭЦП "электронный документ" определен как "документ, в котором информация представлена в электронно-цифровой форме".

Для электронных цифровых подписей обычно используются два различных вида ключей: один — для создания цифровой подписи или преобразования данных в неразборчивую форму, а другой — для проверки цифровой подписи или возвращения электронного документа в его первоначальную форму. Хотя истоки цифровых подписей относятся к криптографии, цифровая подпись как таковая не подразумевает шифрования или обеспечения конфиденциальности подписанного документа. Обычно цифровая подпись является приложением к электронному документу, а преобразования, необходимые для создания цифровой подписи, не влияют на содержание элек-

тронного документа и не делают его конфиденциальным. Конфиденциальность может обеспечиваться дополнительными способами.

Компьютерное оборудование и программное обеспечение, использующие два названных ключа, часто называют "асимметричной криптосистемой".

Ключи асимметричной криптосистемы для электронной цифровой подписи включают закрытые ключи, которые известны только подписывающей стороне и служат для создания подписи, и открытые ключи, которые обычно известны более широко и применяются для проверки подписи. Получатель электронного документа должен обладать соответствующим открытым ключом для того, чтобы проверить, действительно ли электронная цифровая подпись принадлежит лицу, подписавшему документ. Если проверка цифровых подписей проводится большим числом лиц (или неопределенным кругом лиц), открытый ключ должен быть предоставлен всем лицам (или неопределенному кругу лиц), в том числе посредством публикации в информационной системе.

Хотя пара ключей математически связана, расчетным образом вывести один из другого невозможно (если асимметричная криптосистема была разработана и внедрена с учетом требований надежности и безопасности электронных цифровых подписей). Несмотря на то, что открытый ключ конкретной подписывающей стороны будет известен большому числу лиц, они не смогут определить закрытый ключ и воспользоваться им для подделки цифровой подписи.

Для целей Федерального закона используются следующие основные понятия:

электронная цифровая подпись — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

закрытый ключ электронной цифровой подписи — уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;

открытый ключ электронной цифровой подписи — уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;

средства электронной цифровой подписи — аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций — создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;

сертификат средств электронной цифровой подписи — документ на бумажном носителе, выданный в соответствии с правилами системы сертифи-

кации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Использование электронной цифровой подписи состоит из двух видов действий: одни действия выполняются подписывающей стороной, а другие — получателем электронного документа с электронной цифровой подписью.

Создание цифровой подписи — это процесс вычисления кода, выведенного из подписанного электронного документа и конкретного закрытого ключа и являющегося уникальным для них. Чтобы этот код или цифровая подпись были надежно защищены, должна существовать *пренебрегаемо* малая вероятность того, что тот же код или цифровая подпись могут быть созданы для другого сообщения или закрытого ключа.

Подтверждение подлинности электронной цифровой подписи — это процесс проверки подписи путем соотнесения с исходным электронным документом и открытым ключом, что позволяет определить, была ли создана цифровая подпись для этого электронного документа при помощи закрытого ключа, соответствующего данному открытому ключу.

При создании и проверке цифровой подписи используется более общая *процедура,* которая носит название "хэш-функции". Хэш-функция создает цифровой слепок с электронного документа — код, существенно более короткий, чем электронный документ, но неизменно уникальный для него. Если электронный документ изменяется, всегда изменяется и хэш-результат документа. Хэш-функция позволяет программному обеспечению для создания цифровых подписей использовать меньший и более предсказуемый набор данных, обеспечивая в то же время прочную корреляцию с содержимым исходного электронного документа.

Для того чтобы подписать электронный документ или иную информацию, подписывающей стороне нужно сначала точно определить то, что будет подписываться. Затем хэш-функция программного обеспечения подписывающей стороны рассчитывает хэш-результат — уникальный для данного электронного документа. Потом программа подписывающей стороны преобразует полученный хэш-результат в цифровую подпись путем соотнесения с закрытым ключом подписывающей стороны. Это преобразование иногда называют "шифрованием". Полученная таким образом цифровая подпись уникальна как для электронного документа, так и для использованного при ее создании закрытого ключа.

Обычно цифровая подпись "привязана" к электронному документу и хранится или передается вместе с электронным документом. Тем не менее ее можно отослать или хранить в виде отдельного элемента данных при условии, что подпись находится в надежной связи с электронным документом. Поскольку цифровая подпись уникальна для своего электронного документа, она бесполезна, если связь между нею и документом разрывается.

Проверка (или подтверждение подлинности) электронной цифровой подписи достигается путем вычисления нового хэш-результата исходного электронного документа с помощью той же хэш-функции, что была использована при создании цифровой подписи. Таким образом, с помощью открытого ключа сторона, получившая электронный документ с ЭЦП, проверяет, была ли цифровая подпись создана с помощью соответствующего закрытого ключа и соответствует ли вновь вычисленный хэш-результат хэш-результату, выведенному из цифровой подписи.

Если закрытый ключ подписывающей стороны и хэш-результат идентичны, процедура подтверждения подлинности цифровой подписи закончена.

Результат проверки показывает, что (1) цифровая подпись была создана при помощи закрытого ключа подписывающей стороны, потому что только открытый ключ подписывающей стороны может проверить цифровую подпись, созданную с помощью закрытого ключа подписывающей стороны, и (2) электронный документ с момента подписания не был изменен, потому что хэш-результат, вычисленный при проверке, совпадает с хэш-результатом цифровой подписи, рассчитанным при создании цифровой подписи в электронном документе.

Вследствие создания электронной цифровой подписи и подтверждения ее подлинности достигаются основные требуемые от цифровой подписи результаты:

✓ аутентификация подписывающей стороны: если пара открытого и закрытого ключей связана, как описано ранее, с указанной подписывающей стороной, цифровая подпись при помощи закрытого ключа действительно идентифицирует подписывающую сторону с электронным документом. Цифровая подпись не может быть использована никем, кроме самой подписывающей стороны, кроме случаев, когда подписывающая сторона утеряла контроль над закрытым ключом;

✓ аутентификация электронного документа: процесс цифрового подписывания опознает подписываемый документ с гораздо большей определенностью и точностью, чем это делают подписи на бумаге. Проверка также выявляет наличие подделок документа, поскольку обработка хэш-результатов (одного при подписывании и другого при проверке) показывает, остался ли документ неизменным со времени подписания;

✓ скрепление подписью: создание цифровой подписи требует от подписывающей стороны использования закрытого ключа и запуска той функции программного обеспечения, которая ответственна за создание цифровой подписи. Это действие может стать основанием для возникновения правового отношения, например, при совершении сделки;

✓ эффективность: процессы создания и проверки цифровой подписи обеспечивают высокий уровень гарантии того, что цифровая подпись действительно принадлежит подписывавшей стороне, при этом данные процессы практически полностью автоматизированы либо поддаются автоматизации.

Для проверки (подтверждения подлинности) электронной цифровой подписи проверяющая сторона должна получить открытый ключ и удостовериться в том, что открытый ключ соответствует закрытому ключу подписавшей стороны. Однако пара открытого и закрытого ключей не имеет внутренне обусловленной связи с каким-либо лицом (владельцем ключей ЭЦП) — это просто пара чисел. Связь между конкретным лицом и парой ключей должна быть установлена на правовой основе.

Например, при совершении двусторонней сделки оба контрагента могут идентифицировать друг друга при помощи открытых ключей, которые есть у обеих сторон в результате взаимного обмена. Взаимное признание и подтверждение подлинности электронной цифровой подписи участниками электронной сделки происходит на основе заключенного ими соответствующего двустороннего договора. Подобные договоры могут заключаться также между участниками корпоративных информационных систем.

Однако проведение такой идентификации представляет значительные сложности, когда обе стороны географически удалены друг от друга, взаимодействуют друг с другом в открытой, незащищенной информационной сети и являются не физическими, а юридическими лицами (хозяйственными обще-

ствами, государственными предприятиями, некоммерческими организациями и др.) и, соответственно, действуют через представителей, чьи личности и полномочия требуют подтверждения.

Например, важнейшая особенность электронной торговли в открытых сетях типа Интернет состоит в том, что участники большинства таких отношений (в том числе электронные магазины и их клиенты) не устанавливают предварительных договорных отношений и не знают друг друга.

Поскольку надежная идентификация отдаленного контрагента требует значительных усилий, создание возможностей цифровой подписи для каждой из многочисленных сделок неэффективно. Вместо этого сторона с цифровой подписью идентифицирует себя при помощи пары ключей и использует это опознавание во множестве сделок в течение какого-то периода времени.

Для этой цели подписывающая сторона может сделать заявление типа: "Подписи, проверяемые следующим открытым ключом, принадлежат мне". Однако контрагенты такой подписывающей стороны могут быть не готовы принять на слово опознавание подписывающей стороны парой ключей. Особенно в случае электронных сделок в глобальных, а не в корпоративных информационных системах. Участник такой информационной системы сталкивается с риском заключить сделку с призраком или самозванцем либо рискует получить отказ от цифровой подписи на основе утверждения, что подпись была создана неуполномоченным лицом — в особенности если сделка оказывается невыгодной для подписывавшей стороны. Для того чтобы обеспечить действительные гарантии идентификации каждой стороны при помощи конкретной пары ключей, одно или несколько третьих лиц, которым обе стороны доверяют, должны связать опознаваемое лицо одного контрагента по сделке с парой ключей, которые создают цифровую подпись в электронном документе, получаемом другим контрагентом, и наоборот.

Это доверенное третье лицо в Федеральном законе "Об электронной цифровой подписи" называется удостоверяющим центром (ст. 8).

К сожалению, последний не имеет собственной дефиниции в Федеральном законе, несмотря на то, что "удостоверяющий центр" — одно из основных используемых в Законе понятий. Фактически удостоверяющий центр получает определение в п. 1 ст. 9 Закона посредством перечисления видов деятельности, которые он осуществляет. Важнейшие из видов деятельности, составляющие признаки удостоверяющего центра, заключаются в:

- ♦ изготовлении сертификатов ключей подписей,
- ♦ ведении реестра сертификатов ключей подписей,
- ♦ обеспечении актуальности реестра и возможности свободного доступа к реестру участников информационных систем,
- ♦ выдаче пользователям сертификатов ключей подписей с информацией об их действии.

Для соотнесения пары ключей с будущей подписывающей стороной удостоверяющий центр выпускает сертификат ключа подписи — документ, в котором содержатся открытый ключ и подтверждение того, что данная подписывающая сторона, указанная в сертификате, имеет соответствующий закрытый ключ.

В Законе об ЭЦП сертификат ключа подписи определен как "документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выда-

ются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи".

Лицо (или сторона), подписывающее(ая) электронный документ, в Законе называется "владельцем сертификата ключа подписи" и определяется как "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 в электронных документах (подписывать электронные документы)".

Лицо, осуществляющее проверку (подтверждение подлинности) цифровой подписи в электронном документе, называется в Законе "пользователем сертификата ключа подписи". Это физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Подтверждение подлинности электронной цифровой подписи в электронном документе определяется в Законе как "положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе".

Таким образом, основная функция сертификата — соотнесение пары ключей и подписывающей стороны — владельца сертификата ключа подписи, что позволяет пользователю соответствующего сертификата — лицу, проверяющему цифровую подпись при помощи открытого ключа, указанного в сертификате, быть уверенным в том, что соответствующий закрытый ключ также принадлежит подписывающей стороне, указанной в сертификате.

Для подтверждения подлинности сертификата подписывающей стороны удостоверяющий центр прилагает к нему собственную электронную цифровую подпись, то есть данный сертификат должен быть подписан электронной цифровой подписью уполномоченного лица удостоверяющего центра (п. 4 ст. 6 Закона об ЭЦП).

Цифровая подпись удостоверяющего центра на выдаваемом им сертификате может быть проверена при помощи открытого ключа, указанного в другом сертификате, а этот другой сертификат может быть проверен при помощи открытого ключа, указанного еще в одном сертификате, и так далее, до тех пор, пока лицо, полагающееся на цифровую подпись, не убедится достаточным образом в подлинности подписи.

По смыслу ст. 10 Закона подтверждение подлинности электронных цифровых подписей удостоверяющих центров в выданных ими сертификатах должен осуществлять уполномоченный федеральный орган исполнительной власти.

Для того чтобы открытым ключом и его идентификацией с конкретным владельцем сертификата можно было без затруднений воспользоваться при проверке цифровой подписи, сертификат ключа подписи публикуется в реестре сертификатов ключей подписей. Реестры сертификатов — это соответствующие электронные базы данных, доступные в режиме "он-лайн". Удостоверяющий центр обеспечивает ведение реестров, их актуализацию и выдачу сертификатов ключей подписи обратившимся к нему участникам информа-

ционных систем (п. 1 ст. 9). Нередко эти данные можно извлечь автоматически при помощи прямого запроса, адресованного реестру и производимого программой проверки с целью получения требуемых сертификатов.

Уполномоченный федеральный орган исполнительной власти, в свою очередь, должен вести единый государственный реестр сертификатов ключей подписи удостоверяющих центров, функционирующих в информационных системах общего пользования, обеспечивать пользователям возможность свободного доступа к этому реестру и выдавать им указанные сертификаты в виде электронных документов (п. 2 ст. 10).

После того, как сертификат изготовлен, он может утратить надежность, если владелец сертификата предоставил центру недостоверную информацию о своей личности.

В других ситуациях сертификат может быть надежным в момент выдачи, но утрачивает надежность позднее. Например, если подписывающее лицо утратило контроль над закрытым ключом, сертификат становится ненадежным, поскольку цифровые подписи, созданные с помощью утерянного закрытого ключа, могут на основании сертификата восприниматься как принадлежащие подписывающему лицу.

Такую ситуацию участники информационных систем, использующие электронную цифровую подпись, называют "компрометацией ключа ЭЦП", то есть констатацией лицом, владеющим закрытым ключом ЭЦП, обстоятельств, при которых возможно использование данного ключа неуполномоченными лицами. Подобным обстоятельством может стать увольнение сотрудников, имевших доступ к ключевым носителям; нарушение правил хранения ключевых носителей и ряд других. Порядок действий участников информационных систем при компрометации ключей ЭЦП, как правило, устанавливается на основании соглашения.

В случаях, когда подпись "скомпрометирована", сертификат ключа подписи становится ненадежным. Удостоверяющий центр, в том числе по письменному заявлению владельца сертификата ключа подписи, должен приостановить действие сертификата (ст. 11, 13) или окончательно аннулировать сертификат (ст. 14).

Сразу после приостановления действия или аннулирования сертификата удостоверяющий центр должен опубликовать в реестре сертификатов информацию о приостановлении действия или аннулировании сертификата, чтобы известить тех лиц, которые делали запрос или о которых известно, что они получили цифровую подпись, подлинность которой удостоверяется путем отсылки к ненадежному сертификату.

3. ВИДЫ ИНФОРМАЦИОННЫХ СИСТЕМ, ПРИМЕНЯЮЩИХ ЭЛЕКТРОННУЮ ЦИФРОВУЮ ПОДПИСЬ

В Федеральном законе об ЭЦП информационные системы, в которых используются электронные документы с электронными цифровыми подписями, подразделяются на два вида:

1) корпоративные информационные системы;

2) информационные системы общего пользования.

В Законе предусмотрен целый ряд особенностей применения электронной цифровой подписи и сертификатов ключей ЭЦП в зависимости от того, в какой из названных систем осуществляется электронный документооборот.

Вид информационной системы имеет значение при решении следующих вопросов:

- о порядке создания ключей ЭЦП;
- о применении сертифицированных средств ЭЦП;
- о выпуске и использовании сертификатов ключей ЭЦП, в том числе о содержании информации в сертификатах; порядке ведения реестра сертификатов, приостановлении действия, аннулировании и хранении сертификатов;
- о статусе удостоверяющего центра, обеспечивающего функционирование информационной системы;
- о взаимодействии информационных систем различных видов при предоставлении услуг удостоверяющего центра неограниченному кругу лиц;
- о порядке прекращения деятельности удостоверяющего центра и ряде других.

Здесь целесообразно вспомнить о том, что само понятие "информационная система" не получило определения в Законе "Об электронной цифровой подписи".

Определение данного понятия содержится в Федеральном законе "Об информации, информатизации и защите информации": информационная система — организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы (ст. 2). В соответствии с п. 2 ст. 16 Закона об информации государственные и негосударственные организации, а также граждане имеют равные права на разработку и производство информационных систем, технологий и средств их обеспечения.

Следует обратить внимание на тот факт, что Закон об информации и Закон об электронной цифровой подписи наделяют понятие "информационная система" различным содержанием.

Так, в соответствии со ст. 17 Закона об информации информационные системы, технологии и средства их обеспечения могут быть объектами собственности физических и юридических лиц, государства. Собственником информационной системы, технологии и средств их обеспечения признается физическое или юридическое лицо, на средства которого эти объекты произведены, приобретены или получены ... иным законным способом. Информационные системы, технологии и средства их обеспечения включаются в состав имущества субъекта, осуществляющего права собственника или владельца этих объектов. Информационные системы, технологии и средства их обеспечения выступают в качестве товара (продукции)... Собственник информационной системы, технологии и средств их обеспечения определяет условия использования этой продукции.

Текст ст. 17 Закона об информации в целом свидетельствует о том, что данный Закон рассматривает информационные системы исключительно в качестве совокупности объектов гражданских прав. Из перечня объектов гражданских прав, предусмотренных ст. 128 ГК РФ, в состав информационной системы, по-видимому, могут входить: вещи; иное имущество, в том числе имущественные права; информация; результаты интеллектуальной деятельности.

Закон об электронной цифровой подписи, напротив, исходит из того, что информационная система — это, прежде всего, совокупность юридических взаимоотношений физических и юридических лиц — участников системы.

Участники информационных систем наряду с удостоверяющими центрами — главные действующие лица Закона об ЭЦП, поскольку именно они вступают в юридические отношения, которые регламентируются данным Законом.

По смыслу Закона об ЭЦП участники информационной системы:

— пользуются электронной цифровой подписью (ст. 3);

— создают ключи электронных цифровых подписей (п. 1 ст. 5);

— являются владельцами сертификатов ключей подписей (п. 2 ст. 6);

— взаимодействуют с удостоверяющим центром по поводу сертификатов ключей ЭЦП и реестра сертификатов (ст. 9);

— являются пользователями сертификатов ключей подписей (п. 4 ст. 6, п. 1 ст. 9);

— взаимодействуют с уполномоченным федеральным органом исполнительной власти по поводу сертификатов ключей подписей уполномоченных лиц удостоверяющих центров (п. 2 ст. 10) и др.

В соответствии с Законом об ЭЦП корпоративная информационная система — информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы (ст. 3).

Юридические отношения участников корпоративной информационной системы могут строиться как на основе соглашения, то есть иметь договорную природу, так и на основе нормативного правового акта.

В корпоративной информационной системе на основании решения владельца системы или соглашения ее участников могут определяться: статус удостоверяющего центра, обеспечивающего функционирование данной информационной системы (п. 1 ст. 8); порядок создания ключей электронных цифровых подписей для использования в корпоративной информационной системе (п. 1 ст. 5); содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов ключей подписей, порядок хранения аннулированных сертификатов ключей подписей, случаи утраты указанными сертификатами юридической силы в корпоративной информационной системе (п. 1 ст. 13, п. 3 ст. 17); прекращение деятельности удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, в связи с передачей обязательств данного удостоверяющего центра другому удостоверяющему центру или в связи с ликвидацией корпоративной информационной системы (п. 3 ст. 15).

Как следует из положений Закона об ЭЦП, в корпоративной информационной системе устанавливаются специальный "порядок" (п. 1 ст. 5) или "правила использования" (ст. 17) электронной цифровой подписи и сертификатов ключей ЭЦП. Исходя из определения корпоративной информационной системы, названные "порядок" или "правила" должны приниматься решением владельца этой информационной системы или соглашением участников системы.

К числу корпоративных можно отнести следующие действующие информационные системы.

Системы "Клиент-Банк"[17] — автоматизированные компьютерные системы, позволяющие обеспечить проведение расчетных операций по банковскому счету (счетам) Клиента, открытому (открытым) в Банке на основании электронных платежных документов, а также доставку электронных служеб-

[17] http://banking.guta.ru/clientbank/

но-информационных документов между Клиентом и Банком дистанционно в режиме удаленного доступа по каналам электрической связи. Договор на обслуживание в электронной системе "Клиент–Банк" является неотъемлемой частью договоров банковского счета, заключенных между клиентами и банками.

Корпоративная система электронного документооборота (ЭДО) Некоммерческого партнерства "Фондовая биржа РТС"[18]. Система представляет собой совокупность программного обеспечения, обслуживаемого Партнерством, а также вычислительных средств и баз данных, принадлежащих или подконтрольных Партнерству, предназначенную для передачи подписанных ЭЦП электронных документов. Партнерство предоставляет Клиенту доступ к Системе ЭДО, обеспечивает Клиенту возможность эксплуатации клиентской части Системы ЭДО и оказывает иные сопутствующие услуги. Доступ к системе ЭДО предоставляется Клиенту при условии присоединения последнего к Соглашению об использовании электронной цифровой подписи в системе электронного документооборота РТС.

Система электронного документооборота Московской межбанковской валютной биржи (СЭД) ММВБ[19], которая позволяет организовать использование электронных документов (ЭД) при совершении сделок или иных юридически значимых действий. Нормативный документ, регламентирующий использование электронных документов при организации информационного взаимодействия сторон в Системе электронного документооборота, — Правила электронного документооборота. Правила вступают в силу в отношении Участника СЭД в результате заключения между Участником СЭД и Организатором СЭД Договора о присоединении к Правилам электронного документооборота.

Система Автоматизации Предварительной Обработки Документов ОАО "Мосжилрегистрация" (АО МЖР), осуществляющего подготовку в электронном виде документов к регистрации прав на жилые и нежилые помещения, земельные участки и сделок с ними как на первичном, так и на вторичном рынке с использованием Удостоверяющего центра электронной цифровой подписи[20].

Договор об участии в корпоративной информационной системе — это, как правило, договор присоединения и регламентируется Гражданским кодексом РФ. В соответствии с п. 1 ст. 428 Кодекса договором присоединения признается договор, условия которого определены одной из сторон в формулярах или иных стандартных формах и могли быть приняты другой стороной не иначе как путем присоединения к предложенному договору в целом.

В связи с этим необходимо учитывать положение п. 2 ст. 428 ГК РФ. В названной норме Кодекса установлено, что присоединившаяся к договору сторона вправе потребовать расторжения или изменения договора, если договор присоединения хотя и не противоречит закону и иным правовым актам, но лишает эту сторону прав, обычно предоставляемых по договорам такого вида, исключает или ограничивает ответственность другой стороны за нарушение обязательств либо содержит другие явно обременительные для присоединившейся стороны условия, которые она исходя из своих разумно по-

[18] http://www.rts.ru

[19] http://www.micex.ru/sed/

[20] www.mgr.ru

нимаемых интересов не приняла бы при наличии у нее возможности участвовать в определении условий договора.

В комментируемом Федеральном законе особо выделяются корпоративные информационные системы федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления. Правовая основа функционирования названных корпоративных информационных систем — нормативный правовой акт.

Федеральный закон об ЭЦП установил особые условия функционирования подобных корпоративных информационных систем: использование несертифицированных средств ЭЦП и созданных ими ключей электронных цифровых подписей в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления не допускается (п. 3 ст. 5).

Необходимо подчеркнуть, что по смыслу Закона об ЭЦП любые другие корпоративные информационные системы вправе использовать средства электронной цифровой подписи (как сертифицированные, так и несертифицированные) на основании решения владельца системы или соглашения участников системы. Выбор средств ЭЦП обычно фиксируется в "правилах" системы.

Таким образом, Закон об ЭЦП распространяет запрет использовать несертифицированные средства электронной цифровой подписи только на одну категорию корпоративных информационных систем — федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления.

К названным системам можно отнести Автоматизированную информационную систему (АИС) "Налог". МНС РФ 28 декабря 2001 года утвердил Систему передачи данных бухгалтерской и налоговой отчетности (Список форм и состав показателей форм бухгалтерской и налоговой отчетности в электронном виде. Формат и порядок представления бухгалтерской и налоговой отчетности в электронном виде). Версия 1.00. Система передачи данных бухгалтерской и налоговой отчетности в электронном виде предназначена для обмена данными между налогоплательщиками и налоговыми органами — инспекциями Министерства РФ по налогам и сборам (ИМНС) — в электронном виде на магнитных носителях или по каналам связи.

Кроме того, система может использоваться для обмена данными о налогоплательщиках и их налоговой отчетности между налоговыми органами. Установленный Системой регламент электронного документооборота при сдаче отчетности в электронном виде по каналам связи (п. 3.2.2) предусматривает, что данные бухгалтерской и налоговой отчетности формируются на рабочем месте налогоплательщика в виде текстовых файлов стандартного формата. Файлы отчетности подписываются электронной цифровой подписью (ЭЦП) налогоплательщика, закрываются использованием сертифицированных ФАПСИ средств шифрования с гарантированной стойкостью.

Можно также назвать Единую автоматизированную информационную систему ГТК России[21], системы государственных электронных закупок, автоматизированную систему ведения государственного земельного кадастра и государственного учета объектов недвижимости, создание которой преду-

[21] www.customs.ru

смотрено соответствующей Федеральной целевой программой (2002–2007 годы)[22].

В Москве созданы "Единая автоматизированная система обработки документированной информации в Управлениях Комплекса перспективного развития города"; ИС "Государственный градостроительный кадастр"; "Автоматизированная система пообъектного учета выполненных и оплаченных работ на строительстве объектов городского заказа"[23].

Образованы также территориальная сеть Мэрии, Система обработки финансовой информации Департамента финансов, сеть Государственной городской инспекции по контролю за использованием объектов нежилого фонда г. Москвы, сеть Московской лицензионной палаты, Единая городская автоматизированная система для предупреждения и ликвидации чрезвычайных ситуаций ГУ ГО ЧС и МЧС по г. Москве, сеть Московского комитета образования, сеть Комитета социальной защиты населения г. Москвы, система контроля энергопотребления Управления топливно-энергетического хозяйства, система диспетчеризации станций скорой и неотложной помощи, сеть Милиции общественной безопасности, общегородская автоматизированная система управления дорожным движением "СТАРТ", корпоративная телесеть Комплекса архитектуры, строительства, развития и реконструкции города и ряд других[24].

Использованию электронной цифровой подписи в сфере государственного управления посвящена ст. 16 Закона об ЭЦП.

Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, а также организации, участвующие в документообороте с указанными органами, используют для подписания своих электронных документов электронные цифровые подписи уполномоченных лиц указанных органов, организаций (п. 1 ст. 16).

Сертификаты ключей подписей уполномоченных лиц федеральных органов государственной власти включаются в реестр сертификатов ключей подписей, который ведется уполномоченным федеральным органом исполнительной власти, и выдаются пользователям сертификатов ключей подписей из этого реестра в порядке, установленном Федеральным законом для удостоверяющих центров (п. 2 ст. 16).

Порядок организации выдачи сертификатов ключей подписей уполномоченных лиц органов государственной власти субъектов Российской Федерации и уполномоченных лиц органов местного самоуправления устанавливается нормативными правовыми актами соответствующих органов (п. 3 ст. 16).

Информационная система общего пользования определяется в Федеральном законе об ЭЦП как "информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано".

Условия функционирования информационных систем общего пользования и юридические отношения участников с подобными системами близки к гражданско-правовой конструкции публичного договора в случае, если информационная система общего пользования или ее владелец — юридиче-

[22] http://www.economy.gov.ru/fcp_kadastr.html

[23] Городская целевая программа "Электронная Москва". Проект от 2003-02-05 http://www.el-mos.ru/

[24] Городская целевая программа "Электронная Москва". Проект от 2003-02-05 http://www.el-mos.ru/

ское лицо — коммерческая организация. По смыслу данного определения информационная система общего пользования не может действовать в рамках некоммерческой организации.

В соответствии со ст. 426 ГК РФ публичным договором признается договор, заключенный коммерческой организацией и устанавливающий ее обязанности по продаже товаров, выполнению работ или оказанию услуг, которые такая организация по характеру своей деятельности должна осуществлять в отношении каждого, кто к ней обратится.

Коммерческая организация не вправе оказывать предпочтение одному лицу перед другим в отношении заключения публичного договора, кроме случаев, предусмотренных законом и иными правовыми актами. Цена товаров, работ и услуг, а также иные условия публичного договора устанавливаются одинаковыми для всех потребителей, за исключением случаев, когда законом и иными правовыми актами допускается предоставление льгот для отдельных категорий потребителей. Отказ коммерческой организации от заключения публичного договора при наличии возможности предоставить потребителю соответствующие товары, услуги, выполнить для него работы не допускается.

При необоснованном уклонении коммерческой организации от заключения публичного договора применяются положения, предусмотренные п. 4 ст. 445 Кодекса: если сторона, для которой в соответствии с Гражданским кодексом РФ или иными законами заключение договора обязательно, уклоняется от его заключения, другая сторона вправе обратиться в суд с требованием о понуждении заключить договор. Сторона, необоснованно уклоняющаяся от заключения договора, должна возместить другой стороне причиненные этим убытки.

В построении юридических отношений участников с информационными системами общего пользования применяется положение Гражданского кодекса РФ о публичной оферте (ст. 437): "Содержащее все существенные условия договора предложение, из которого усматривается воля лица, делающего предложение, заключить договор на указанных в предложении условиях с любым, кто отзовется, признается офертой (публичная оферта)".

Примером заключения договора путем акцепта публичной оферты может служить порядок принятия участником информационной системы общего пользования Правил использования электронной цифровой подписи при дистанционном финансовом обслуживании юридических лиц в ЗАО "КБ "ГУТА-БАНК".

Настоящие Правила являются типовым формуляром Банка, распространение текста которого Банком по открытым каналам должно рассматриваться Клиентами как публичное предложение (оферта) Банка заключить договор присоединения на условиях, определенных Правилами. Заключение договора присоединения на условиях Правил осуществляется Клиентом в соответствии со ст. 428 ГК РФ путем представления в Банк письменного заявления о присоединении к Правилам использования электронной цифровой подписи при дистанционном финансовом обслуживании юридических лиц в ЗАО "КБ "ГУТА-БАНК" (акцепта условий Правил), оформленного в соответствии с требованиями Банка[25].

Федеральный закон об ЭЦП установил ряд особых требований к порядку создания ключей электронных цифровых подписей, выпуску и аннулирова-

[25] http://banking.guta.ru/clientbank/request/documents.htm

нию сертификатов ключей ЭЦП, а также к деятельности удостоверяющих центров в информационных системах общего пользования:

- применение исключительно сертифицированных средств электронной цифровой подписи при создании ключей электронных цифровых подписей для использования в информационной системе общего пользования (п. 2 ст. 5);
- обязательное аннулирование сертификата ключа подписи при утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационных системах общего пользования (ст. 14);
- прекращение деятельности удостоверяющего центра, выдающего сертификаты ключей подписей для использования в информационных системах общего пользования, в порядке, установленном гражданским законодательством (п. 1 ст. 15);
- обязанность удостоверяющего центра представить в уполномоченный федеральный орган исполнительной власти сертификат ключа подписи уполномоченного лица удостоверяющего центра до начала использования ЭЦП уполномоченного лица удостоверяющего центра (п. 1 ст. 10);
- наличие единого государственного реестра сертификатов ключей подписей удостоверяющих центров, работающих с участниками информационных систем общего пользования (п. 2 ст. 10);
- обязанности уполномоченного федерального органа исполнительной власти по ведению указанного единого государственного реестра, по обеспечению свободного доступа к этому реестру и выдаче сертификатов ключей подписей уполномоченных лиц удостоверяющих центров (п. 2 ст. 10).
- обязательное приведение в соответствие с Федеральным законом об ЭЦП в течение шести месяцев со дня вступления его в силу учредительных документов удостоверяющих центров, выдающих сертификаты ключей подписей для использования в информационных системах общего пользования (п. 2 ст. 20).

Необходимо отметить, что в Законе об ЭЦП не проведено четкое разграничение между корпоративной информационной системой и общедоступной информационной системой.

Отсутствие четкости в разграничении — следствие положений п. 1 ст. 17 Закона: корпоративная информационная система, предоставляющая участникам информационной системы общего пользования услуги удостоверяющего центра корпоративной информационной системы, должна соответствовать требованиям, закрепленным Федеральным законом для информационных систем общего пользования.

Закон, вопреки положениям п. 1 ст. 17, не устанавливает требования для систем общего пользования. Он определяет требования к ключам электронных цифровых подписей (п. 2 ст. 5) и к удостоверяющим центрам (ст. 8) указанных систем.

Кроме того, в Законе об ЭЦП не сформулированы принципиальные различия между участниками корпоративной информационной системы (ст. 3) и участниками информационной системы общего пользования (п. 1 ст. 5, п. 1 ст. 17), как не определено само понятие "участник информационной системы". Такая неопределенность в значительной степени затрудняет реализацию ряда положений Закона, например, в ситуациях, когда одно и то же лицо использует и корпоративную и общедоступную информационные системы.

4. УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Закон об электронной цифровой подписи предусматривает обязательные юридические условия, которые должны соблюдаться при использовании ЭЦП.

Данные условия относятся к следующим аспектам применения электронной цифровой подписи:

1. признанию равнозначности электронной цифровой подписи и собственноручной подписи (ст. 4);
2. замещению печатей, то есть признанию равнозначности электронных документов, подписанных ЭЦП, и документов на бумаге, подписанных собственноручной подписью и скрепленных печатью (ст. 19);
3. применению средств электронной цифровой подписи при создании ключей электронных цифровых подписей (п. 2 ст. 5);
4. использованию сертификатов ключей электронных цифровых подписей: изготовлению, выдаче, хранению; сведениям, составляющим содержание указанных сертификатов (ст. 6, 7).

1. Условия равнозначности электронной цифровой подписи и собственноручной подписи

Статья 4 Закона об ЭЦП, по сравнению с другими положениями данного Федерального закона, в наибольшей степени корреспондирует продекларированным в ст. 1 целям Закона, поскольку здесь в концентрированном виде сформулированы правовые условия 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.

В п. 1 ст. 4 установлено, что электронная цифровая подпись в электронном документе считается юридически равнозначной "собственноручной подписи в документе на бумажном носителе" при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи, предусмотренными в ст. 6 Федерального закона.

Таким образом, Закон установил жесткую взаимосвязь, в соответствии с которой действительность подписи зависит:

- от положительного результата проверки соответствующим средством ЭЦП принадлежности электронной цифровой подписи владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе (ст. 3);
- от надлежащего создания и применения такого документа как сертификат ключа ЭЦП. Сертификат ключа ЭЦП, в свою очередь, имеет юридическую силу при условии правомерных действий не только владельца серти-

фиката, но и удостоверяющего центра, который изготовил данный сертификат (ст. 9).

Данная зависимость свидетельствует о том, что Закон об ЭЦП вовсе не упростил, а, наоборот, значительно усложнил правовые отношения, возникающие в связи с применением электронной цифровой подписи, и тем самым увеличил юридические риски последних. Большая часть таких рисков связана с тем, что Закон принудительно вводит в число участников электронного документооборота нового субъекта — удостоверяющий центр.

Не только положение п. 1 ст. 4, но и понятийный аппарат Федерального закона неразрывно связывают электронную цифровую подпись с сертификатом ключа ЭЦП, выдаваемым удостоверяющим центром (ст. 3). Удостоверяющий центр не является участником гражданско-правовой сделки, при совершении которой используется электронный документ, подписываемый ЭЦП. Вместе с тем действительность сделки и ее правовые последствия могут зависеть: от правомерных и добросовестных действий центра по изготовлению сертификатов ключей подписей; выдаче сертификатов ключей ЭЦП, приостановлению и возобновлению действия; аннулированию сертификатов ключей ЭЦП; ведению реестра сертификатов, обеспечению его актуальности и возможности свободного доступа к нему участников информационных систем и т. д.

Если центр не исполнит любую из своих обязанностей, предусмотренных Законом или договором с владельцем сертификата ключа ЭЦП, либо исполнит ненадлежащим образом, сделка между участниками информационных систем может быть признана недействительной в силу недействительности ЭЦП.

Аналогичные последствия могут наступить, если удостоверяющий центр осуществляет свою деятельность не в соответствии с положениями Закона. В силу ст. 168 ГК РФ сделка, не соответствующая требованиям закона или иных правовых актов, ничтожна, если закон не устанавливает, что такая сделка оспорима, или не предусматривает иных последствий нарушения.

Участник информационной системы может быть одновременно владельцем любого количества сертификатов ключей подписей. При этом в Законе об ЭЦП неоднократно подчеркивается, что электронный документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи (п. 2 ст. 4, п. 1 ст. 6).

Представляется, что сформулированная таким образом правовая норма неопределенна по своему содержанию, практически нереализуема и в итоге вносит непредсказуемость в возникающие в результате использования ЭЦП правоотношения. Термин "отношения", используемый в Федеральном законе, может иметь разное толкование. Отношения (в том числе правоотношения) могут быть гражданскими, административными, обязательственными, абсолютными, относительными. Речь может идти о конкретной сделке, категории сделок или отношениях между конкретными лицами и т. д. Поскольку характеристики таких отношений нет в понятийном аппарате (ст. 3), соответственно нет и точного указания Закона, что в этом смысле указывать в сертификате. Вместе с тем содержащаяся в п. 2 ст. 4 норма сформулирована весьма жестко, ее несоблюдение может означать недействительность электронной цифровой подписи и, соответственно, невозможность правового признания юридических действий, совершенных с применением данной ЭЦП.

Необходимо остановиться еще на одной проблеме, связанной с использованием электронной цифровой подписи при совершении юридических действий. Во всех ли случаях достаточно просто соблюдать указанные условия, предусмотренные Законом об ЭЦП, чтобы электронная цифровая подпись и подписанный с ее помощью электронный документ считались юридически равнозначными документу на бумаге, подписанному собственноручной подписью?

В связи с этим представляется, что универсальная равнозначность бумажного и электронного документа при условии, что последний отвечает всем без исключения требованиям Закона об ЭЦП, сильно преувеличена в обсуждаемом Федеральном законе.

Во-первых, как уже отмечалось, российское законодательство содержит ряд норм, прямо указывающих, что тот или иной документ не может использоваться в виде электронного сообщения, подписанного электронной подписью.

Например, ст. 4 Федерального закона от 11 марта 1997 года № 48-ФЗ "О переводном и простом векселе" (ст. 4) допускает возможность составления простого и переводного векселя только на бумаге (бумажном носителе). Федеральный закон от 22 апреля 1996 года № 39-ФЗ "О рынке ценных бумаг" (ст. 16) предусматривает, что эмиссионные ценные бумаги на предъявителя могут выпускаться только в документарной форме. Невыполнение эмитентом указанных требований — основание для отказа в регистрации выпуска ценных бумаг. В случае хранения сертификатов документарных эмиссионных ценных бумаг в депозитариях права, закрепленные ценными бумагами, осуществляются на основании предъявленных этими депозитариями сертификатов по поручению, предоставляемому депозитарными договорами владельцев, с приложением списка этих владельцев. Эмитент в этом случае обеспечивает реализацию прав по предъявительским ценным бумагам лица, указанного в этом списке.

Во-вторых, в российских законодательных актах также содержатся положения хотя и не запрещающие применять электронный документ, подписанный ЭЦП, при построении регламентируемых ими отношений, однако сформулированные таким образом, что исполнение данных положений возможно только при использовании традиционных бумажных документов, подписанных собственноручной подписью.

Например, в соответствии с п. 2 ст. 907 ГК РФ письменная форма договора складского хранения считается соблюденной, если его заключение и принятие товара на склад удостоверены складским документом. Товарный склад выдает в подтверждение принятия товара на хранение один из следующих складских документов: двойное складское свидетельство; простое складское свидетельство; складскую квитанцию (ст. 912 ГК РФ). Двойное складское свидетельство состоит из двух частей — складского свидетельства и залогового свидетельства (варранта), которые могут быть отделены одно от другого. Двойное складское свидетельство, каждая из двух его частей, и простое складское свидетельство — ценные бумаги. Обе части двойного складского свидетельства должны иметь идентичные подписи уполномоченного лица и печати товарного склада.

Документ, не соответствующий настоящим требованиям, не является двойным складским свидетельством (ст. 913 ГК РФ). Складское свидетельство и залоговое свидетельство могут передаваться вместе или порознь по передаточным надписям (ст. 915 ГК РФ).

Таким образом, чтобы реализовать правовую конструкцию складского свидетельства в электронной форме с применением ЭЦП, недостаточно применить положение ст. 4 Закона об ЭЦП. Следует также ввести электронные складские документы в правовой оборот посредством норм гражданского законодательства.

Аналогичная проблема возникает в связи с совершением в электронной форме и подписанием при помощи электронной цифровой подписи сделок, требующих нотариального удостоверения, или в связи с необходимостью совершения иных нотариальных действий: свидетельствования подлинности подписи на документах, верности копий документов и выписок из них, удостоверения времени предъявления документов.

Безусловно, совершение перечисленных нотариальных действий применительно к электронному документообороту с использованием ЭЦП возможно только в результате внесения соответствующих положений в Основы законодательства РФ о нотариате от 11 февраля 1993 года № 4462-I. В настоящее время Основы законодательства о нотариате ориентированы на традиционные бумажные документы, подписанные собственноручной подписью, и не охватывают специфику электронного обмена данными.

Так, в соответствии со ст. 42 Основ законодательства о нотариате при совершении нотариального действия нотариус устанавливает личность обратившегося за совершением нотариального действия гражданина, его представителя или представителя юридического лица. Установление личности должно производиться на основании паспорта или других документов, исключающих любые сомнения относительно личности гражданина, обратившегося за совершением нотариального действия. Установленный в ст. 44 Основ порядок подписи нотариально удостоверяемой сделки, заявления и иных документов предписывает, что содержание нотариально удостоверяемой сделки, а также заявления и иных документов должно быть зачитано вслух участникам.

Документы, оформляемые в нотариальном порядке, подписываются в присутствии нотариуса. В соответствии со ст. 11 Основ нотариус имеет личную печать с изображением Государственного герба Российской Федерации, указанием фамилии, инициалов, должности нотариуса и места его нахождения или наименования государственной нотариальной конторы, штампы удостоверительных надписей, личные бланки или бланки государственной нотариальной конторы.

2. Условия замещения печатей

Федеральный закон "Об электронной цифровой подписи" содержит два положения, регламентирующие так называемые "случаи замещения печатей" (ст. 19).

В силу п. 1 ст. 19 Закона содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, в соответствии с нормативными правовыми актами или соглашением сторон может заверяться электронной цифровой подписью уполномоченного лица.

Примером названного нормативного правового акта служит Положение ЦБР от 3 октября 2002 года № 2-П "О безналичных расчетах в Российской Федерации". Пункт 2.2 главы 2 части I Положения дает определение расчетного документа, который представляет собой оформленное в виде документа на бумажном носителе или, в установленных случаях, электронного платежного документа:

— распоряжение плательщика (клиента или банка) о списании денежных средств со своего счета и их перечислении на счет получателя средств;

— распоряжение получателя средств (взыскателя) на списание денежных средств со счета плательщика и перечисление на счет, указанный получателем средств (взыскателем). На основании п. 2.10 в состав реквизитов расчетных документов должны входить подписи (подпись) уполномоченных лиц (лица) и оттиск печати (в установленных случаях).

Глава 3 "Порядок представления кредитной организацией (филиалом) электронных платежных документов" части II Положения "Порядок осуществления расчетных операций через корреспондентские счета (субсчета) кредитных организаций (филиалов), открытые в Банке России" предусматривает, что сформированный электронный платежный документ (ЭПД), или пакет ЭПД, кредитная организация (филиал) направляет в подразделение расчетной сети Банка России с использованием средств телекоммуникаций или представляет на магнитном носителе курьером либо спецсвязью. В зависимости от принятого в подразделении расчетной сети Банка России способа обмена информацией кредитная организация (филиал) направляет ЭПД (пакет ЭПД) в виде полноформатных ЭПД или ЭПД сокращенного формата, которые формируются в соответствии с требованиями Банка России. Полноформатный электронный платежный документ (ЭПД) содержит все реквизиты платежного поручения (включая текстовые реквизиты) и имеет равную юридическую силу с платежным поручением на бумажном носителе, оформленным печатью и подписями распорядителя счета в соответствии с заявленными кредитной организацией (филиалом) образцами.

На основании п. 2 ст. 19 Закона об ЭЦП в случаях, установленных законами и иными нормативными правовыми актами РФ или соглашением сторон, электронная цифровая подпись в электронном документе, сертификат которой содержит необходимые при осуществлении данных отношений сведения о правомочиях его владельца, признается равнозначной собственноручной подписи лица в документе на бумажном носителе, заверенном печатью.

Данная норма Закона об ЭЦП реализована в постановлении Федеральной комиссии по рынку ценных бумаг от 31 октября 2002 года № 43/пс "Об утверждении Положения о порядке предоставления в Федеральную комиссию по рынку ценных бумаг электронных документов" (п. 2). Указанное Положение применяется к следующим электронным документам:

отчетность эмитентов эмиссионных ценных бумаг, профессиональных участников рынка ценных бумаг, управляющих компаний инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, специализированных депозитариев инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов;

документы, предоставляемые в Федеральную комиссию для получения лицензии профессионального участника рынка ценных бумаг, лицензии на осуществление деятельности по ведению реестра, лицензии фондовой биржи, лицензии на осуществление деятельности инвестиционных фондов, лицензии на осуществление деятельности по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами, лицензии на осуществление деятельности специализированного депозитария инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов (далее — организации);

иные документы.

Электронные документы по содержанию должны соответствовать документам, составленным на бумажном носителе, требования к которым установлены федеральными законами, правовыми актами Федеральной комиссии, иными правовыми актами.

В случае, если правовыми актами Федеральной комиссии установлено, что организации передают документы на бумажных носителях в организации, уполномоченные Федеральной комиссией на сбор таких документов, информация в виде электронных документов также должна предоставляться в упомянутые уполномоченные организации.

При предоставлении электронных документов предоставление информации на бумажном носителе не требуется.

Электронные документы должны быть подписаны электронной цифровой подписью. Сертификат ключа подписи выдается удостоверяющим центром. Правовые отношения между Федеральной комиссией и удостоверяющим центром регулируются соответствующим договором.

3. Условия применения средств электронной цифровой подписи при создании ключей электронных цифровых подписей

В п. 1 ст. 5 комментируемого Федерального закона предусмотрено несколько способов создания ключей электронных цифровых подписей. Ключи ЭЦП могут создаваться участниками информационных систем общего пользования, либо удостоверяющими центрами по обращению участников информационных систем общего пользования, либо в ином порядке, который установлен в корпоративной информационной системе.

В пп. 2, 3, 4 ст. 5 Закона об ЭЦП содержится одно из принципиальных положений российского нормативного правового регулирования использования электронной цифровой подписи. Для подтверждения подлинности электронных документов подразумевается применение преимущественно сертифицированных средств ЭЦП.

Здесь необходимо обратить внимание на то, что такой элемент, как "защита информации", встроен в определение электронной цифровой подписи, в соответствии с которым последняя предназначена для защиты электронного документа от подделки.

Обязательная сертификация средств защиты информации предусмотрена Указом Президента РФ от 3 апреля 1995 года № 334 "О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации" (с изм. от 25 июля 2000 года).

Указом устанавливается запрет на:

— использование государственными организациями и предприятиями в информационно-телекоммуникационных системах шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись), и защищенных технических средств хранения, обработки и передачи информации, не имеющих сертификата Федерального агентства правительственной связи и информации при Президенте РФ;

— размещение государственных заказов на предприятиях, в организациях, использующих указанные технические и шифровальные средства, не имеющие сертификата ФАПСИ.

Таким образом, данный Указ предусматривает необходимость сертификации шифровальных средств и средств технической защиты информации,

используемых государственными организациями и предприятиями, а также предприятиями, выполняющими госзаказ.

В отношении средств, предназначенных для защиты сведений, составляющих государственную тайну, введено требование их обязательной сертификации.

При этом шифровальные средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных Федеральным агентством правительственной связи и информации при Президенте РФ.

В отношении средств защиты информации, не содержащей государственную тайну, сертификация осуществляется в общем порядке.

Федеральный закон "Об электронной цифровой подписи" предусматривает, что при создании ключей электронных цифровых подписей должны применяться исключительно сертифицированные средства электронной цифровой подписи в следующих случаях:

— в информационных системах общего пользования (п. 2 ст. 5);

— в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления (п. 3 ст. 5);

— в иных корпоративных информационных системах при предоставлении участникам информационной системы общего пользования услуг удостоверяющего центра корпоративной информационной системы (по смыслу п. 1 ст. 17).

Федеральный закон об ЭЦП предусматривает, что сертификация средств электронной цифровой подписи осуществляется в соответствии с законодательством Российской Федерации о сертификации продукции и услуг. В настоящее время действуют нормы, установленные Законом РФ от 10 июня 1993 года № 5151-I "О сертификации продукции и услуг" (с изм. и доп. на 10 января 2003 года) и издаваемыми в соответствии с ним актами законодательства РФ — Правилами по проведению сертификации в Российской Федерации, утвержденными постановлением Госстандарта РФ от 10 мая 2000 года № 26 (с изм. от 5 июля 2002 года).

В соответствии с названными нормативными правовыми актами для подтверждения соответствия средств электронной цифровой подписи установленным требованиям должен выдаваться документ на бумажном носителе — сертификат средств электронной цифровой подписи. В настоящее время система сертификации средств ЭЦП отсутствует.

Более того, со дня вступления в силу Федерального закона от 27 декабря 2002 года № 184-ФЗ "О техническом регулировании" Закон РФ "О сертификации продукции и услуг" признается утратившим силу (ст. 47).

В Законе "О техническом регулировании" сертификация определена как форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов или условиям договоров.

Сертификат соответствия — это документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров (ст. 2). В ст. 20 названного Федерального закона установлено, что подтверждение соответствия на территории Российской Федерации может носить добровольный или обязательный характер. Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации.

Обязательное подтверждение соответствия осуществляется в формах:

- ✔ принятия декларации о соответствии (далее — декларирование соответствия);
- ✔ обязательной сертификации.

Порядок применения форм обязательного подтверждения соответствия устанавливается настоящим Федеральным законом.

Обязательное подтверждение соответствия проводится только в случаях, установленных соответствующим техническим регламентом, и исключительно на соответствие требованиям технического регламента (п. 1 ст. 23).

В Законе об электронной цифровой подписи предусматривается, что при возникновении убытков в связи с созданием ключей электронных цифровых подписей несертифицированными средствами электронной цифровой подписи убытки должны возмещаться создателями или распространителями этих средств (п. 2 ст. 5). Однако Закон не указывает, кто возмещает такие убытки в связи с созданием ключей ЭЦП несертифицированными средствами ЭЦП. Нет также ясности в том, как невыполнение требования об обязательной сертификации технических и программных средств, реализующих ЭЦП, в случаях, когда это предусмотрено нормативными правовыми актами РФ, влияет на юридическую силу электронного документа, в котором ЭЦП используется.

4. Условия изготовления и использования сертификатов ключей электронных цифровых подписей

При помощи сертификата ключа ЭЦП, выдаваемого удостоверяющим центром, участник информационной системы подтверждает подлинность электронной цифровой подписи и идентифицирует владельца сертификата — лицо, которое подписывает электронный документ данным ключом ЭЦП. На основании Закона об ЭЦП идентифицирующими признаками подписывающего лица являются сведения, указанные в сертификате ключа подписи (п. 1 ст. 6). Использование ЭЦП в точном соответствии со сведениями, указанными в сертификате ключа подписи, рассматривается в Законе в качестве важнейшего условия действительности подписи в электронном документе (п. 1 ст. 4).

В соответствии с п. 1 ст. 6 Закона об ЭЦП 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 и отчество владельца сертификата ключа подписи или псевдоним владельца. При использовании псевдонима удостоверяющим центром вносится об этом запись в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный 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 число сведений, содержащихся в сертификате, могут также включаться:

- должность (с указанием наименования и места нахождения организации, в которой установлена эта должность) и квалификация владельца сертификата ключа подписи (указываются в случае необходимости и на основании подтверждающих документов) (п. 2 ст. 6);
- иные сведения (указываются по письменному заявлению владельца и подтверждаются соответствующими документами) (п. 2 ст. 6).

Как следует из указанных норм Закона об ЭЦП, сведения об отношениях, в которых может быть использован сертификат, определяет сам владелец сертификата. В связи с этим нет ясности для ситуации, когда участник информационной системы предпочтет владеть одним сертификатом "на все случаи жизни", по аналогии с его собственноручной подписью, которую он использует во всех отношениях одинаково.

Представляется целесообразным вариант, когда в сертификате круг отношений, в которых используется электронно-цифровая подпись (ЭЦП), конкретно не определяется, а указываются лишь ограничения его применения. Так, в Директиве Европейского Союза об электронной подписи допускается установление удостоверяющим центром предельного объема сделок, гарантию на совершение которых дает выдаваемый им сертификат.

Изготовление сертификатов ключей подписей осуществляется на основании заявления участника информационной системы, которое содержит сведения, указанные в ст. 6 обсуждаемого Федерального закона 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 (п. 2 ст. 9).

При изготовлении сертификатов ключей подписей удостоверяющим центром оформляются в форме документов на бумажных носителях два экземпляра сертификата, которые заверяются собственноручными подписями владельца сертификата и уполномоченного лица удостоверяющего центра, а также печатью удостоверяющего центра. Один экземпляр сертификата ключа подписи выдается владельцу сертификата, второй остается в удостоверяющем центре (п. 3 ст. 9).

Сертификат ключа подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи (п. 3 ст. 6).

Для проверки принадлежности электронной цифровой подписи соответствующему владельцу сертификат ключа подписи выдается пользователям с указанием даты и времени его выдачи, сведений о действии сертификата ключа подписи (действует, действие приостановлено, сроки приостановления его действия, аннулирован, дата и время аннулирования сертификата ключа подписи) и сведений о реестре сертификатов ключей подписей. В случае выдачи сертификата ключа подписи в форме документа на бумажном носителе этот сертификат оформляется на бланке удостоверяющего центра и заверяется собственноручной подписью уполномоченного лица и печатью удостоверяющего центра. В случае выдачи сертификата ключа подписи и указанных дополнительных данных в форме электронного документа этот сертификат должен быть подписан электронной цифровой подписью уполномоченного лица удостоверяющего центра (п. 4 ст. 6).

В Законе об ЭЦП (ст. 12) предусмотрены следующие обязательства владельца сертификата ключа подписи:

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

• хранить в тайне закрытый ключ электронной цифровой подписи;

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

При несоблюдении требований, изложенных в настоящей статье, возмещение причиненных вследствие этого убытков Закон возлагает на владельца сертификата ключа подписи.

Ответственность владельца сертификата (в силу определения — физического лица) наступает при наличии вины, за исключением случаев, когда сертификат использует в своей деятельности индивидуальный предприниматель (п. 3 ст. 401 ГК РФ).

В соответствии с п. 1 ст. 401 Гражданского кодекса РФ лицо, не исполнившее обязательства либо исполнившее его ненадлежащим образом, несет ответственность при наличии вины (умысла или неосторожности), кроме случаев, когда законом или договором предусмотрены иные основания ответственности. Лицо признается невиновным, если при той степени заботливости и осмотрительности, какая от него требовалась по характеру обязательства и условиям оборота, оно приняло все меры для надлежащего исполнения обязательства.

Закон об электронной цифровой подписи содержит ряд относящихся к применению сертификатов ключей ЭЦП норм, которые далеко не всегда гармонично сочетаются с иными положениями российского законодательства. Так, последовательно проведенная в Законе мысль о том, что электронная цифровая подпись (и, соответственно, сертификат ключа ЭЦП) может принадлежать только физическому лицу, привела к следующим правовым результатам.

Во-первых, Закон об электронной цифровой подписи не допускает возникновения гражданско-правовых отношений по поводу сертификата ключа подписи между удостоверяющим центром и юридическим лицом. В связи с этим центр не гарантирует аннулирование сертификата ключа подписи, например, при досрочном прекращении полномочий единоличного исполнительного органа общества с ограниченной ответственностью или его управляющего, до тех пор, пока названные лица, получившие сертификат на свое имя и являющиеся его законными владельцами (п. 1 ст. 6), не направят центру соответствующее письменное заявление. По смыслу Закона удостоверяющий центр связан обязательствами, предусмотренными ст. 11, только по отношению к физическому лицу (владельцу сертификата ключа подписи), а именно: вносить сертификат ключа подписи в реестр; обеспечивать выдачу сертификата ключа подписи обратившимся к нему участникам информационных систем; приостанавливать действие сертификата ключа подписи; уведомлять владельца сертификата ключа подписи о фактах, которые стали известны удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи и т. д. Таким образом, реестр сертификатов ключей подписей, который ведет удостоверяющий центр, может потерять достоверность и привести к значительным убыткам для юридических лиц, действующих вне корпоративных систем.

Во-вторых, аналогичная проблема может возникнуть и при наличии убытков, понесенных юридическим лицом в результате доверия к тем данным, которые содержатся в сертификате, а также к результатам проверки ЭЦП, выполненной центром. Дело в том, что только физическим лицом может быть и пользователь сертификата ключа подписи, использующий полученные в удостоверяющем центре сведения о сертификате с целью проверки ЭЦП (ст. 3).

В ст. 7 Закона об ЭЦП предусмотрены положения, регламентирующие сроки и порядок хранения сертификата ключа подписи в удостоверяющем центре.

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 (п. 1 ст. 7).

Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре после аннулирования сертификата ключа подписи должен быть не менее установленного федеральным законом срока исковой давности для отношений, указанных в сертификате ключа подписи (п. 2 ст. 7).

Необходимо учитывать, что в целях неукоснительного соблюдения приведенной нормы Закона об ЭЦП хранение сертификатов ключей электронных цифровых подписей в удостоверяющем центре должно осуществляться вечно. В ст. 208 ГК РФ установлен перечень требований, на которые исковая давность не распространяется (иск может быть предъявлен в любое время), в том числе: о защите личных неимущественных прав и других нематериальных благ; вкладчиков к банку о выдаче вкладов; собственника или иного владельца об устранении всяких нарушений его права, хотя бы эти нарушения не были соединены с лишением владения. Помимо этого личные неимущественные права и другие нематериальные блага, принадлежавшие умершему, могут осуществляться и защищаться другими лицами, в том числе наследниками правообладателя (ст. 150).

Следует принимать во внимание и то, что в соответствии со ст. 199 Кодекса требование о защите нарушенного права принимается к рассмотрению судом независимо от истечения срока исковой давности и исковая давность применяется судом только по заявлению стороны в споре, сделанному до вынесения судом решения.

Кроме того, существуют иные сроки, применяемые в юридических отношениях, не имеющих гражданско-правового характера: например, ЭЦП может использоваться для подписания налоговой декларации. Учитывая изложенное, следует установить в Законе точный срок хранения сертификата ключа ЭЦП, например три года.

На основании п. 2 ст. 7 Закона об ЭЦП по истечении срока хранения сертификат ключа подписи исключается из реестра сертификатов ключей подписей и переводится в режим архивного хранения. Срок архивного хранения составляет не менее пяти лет. Порядок выдачи копий сертификатов ключей подписей в этот период устанавливается в соответствии с законодательством РФ. Сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательством РФ об архивах и архивном деле (Основы законодательства РФ об Архивном фонде Российской Федерации и архивах от 7 июля 1993 года № 5341-I).

5. УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ

1. Правовой статус и деятельность удостоверяющего центра

Удостоверяющим центром, выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, должно быть юридическое лицо, выполняющее функции, предусмотренные комментируемым Федеральным законом (п. 1 ст. 8). Указанные функции перечислены в п. 1 ст. 9 Закона об ЭЦП, посвященном деятельности удостоверяющих центров.

Удостоверяющий центр:

- изготавливает сертификаты ключей подписей;
- создает ключи электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;
- приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;
- ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;
- проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;
- выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии (услуги по выдаче участникам информационных систем сертификатов ключей ЭЦП, зарегистрированных удостоверяющим центром, а также информации об их действии в форме электронных документов оказываются безвозмездно);
- осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей;
- может предоставлять участникам информационных систем иные связанные с использованием электронных цифровых подписей услуги.

Удостоверяющим центром может быть коммерческая организация, преследующая извлечение прибыли в качестве основной цели своей деятельности, либо некоммерческая организация, не имеющая извлечение прибыли в качестве такой цели и не распределяющая полученную прибыль между участниками (ст. 50 ГК РФ).

В ст. 8 Закона, посвященной правовому статусу удостоверяющего центра, не указывается, является ли деятельность удостоверяющего центра исключительной, требующей создания специализированного юридического лица, или может осуществляться наряду с другими видами деятельности иного юридического лица.

Возможно, косвенным образом в пользу создания специализированного юридического лица говорит п. 2 ст. 20 Закона об ЭЦП. В соответствии с данным пунктом ст. 20 учредительные документы удостоверяющих центров, выдающих сертификаты ключей подписей для использования в информационных системах общего пользования, подлежат приведению в соответствие с настоящим Федеральным законом в течение шести месяцев со дня вступления его в силу.

В связи с этим необходимо уточнить, что корпоративным информационным системам предоставлено право самостоятельно определять статус собственных удостоверяющих центров по усмотрению владельца или по соглашению участников этой системы.

Остается ряд неясностей относительно статуса удостоверяющих центров в общедоступных информационных системах, а также регистрации, ликвидации и реорганизации таких центров. В частности, требуется более точный законодательный ответ на следующие вопросы:

- подлежат ли названные в п. 1 ст. 8 Закона об ЭЦП удостоверяющие центры государственной регистрации в уполномоченном государственном органе в порядке, определяемом законом о государственной регистрации юридических лиц (ст. 51 ГК РФ);
- включаются ли данные о государственной регистрации удостоверяющих центров в единый государственный реестр юридических лиц, открытый для всеобщего ознакомления [в соответствии с Правилами ведения Единого государственного реестра юридических лиц и предоставления содержащихся в нем сведений, утвержденными постановлением Правительства РФ от 19 июня 2002 года № 438 (с изм. и доп. от 13 ноября 2002 года)];
- может ли коммерческая организация, обладающая общей правоспособностью, институциализировать себя в качестве удостоверяющего центра только посредством получения лицензии на один или несколько видов деятельности, названных в п. 1 ст. 9 Закона об ЭЦП.

В п. 2 ст. 8 Закона об ЭЦП установлено, что деятельность удостоверяющего центра подлежит лицензированию в соответствии с законодательством Российской Федерации о лицензировании отдельных видов деятельности. На основании ст. 49 ГК РФ право удостоверяющего центра осуществлять деятельность, на занятие которой необходимо получение лицензии, возникает с момента получения такой лицензии или в указанный в ней срок и прекращается по истечении срока ее действия, если иное не установлено законом или иными правовыми актами.

Необходимо подчеркнуть, что вопреки положению п. 2 ст. 8 Закона об ЭЦП законодательство РФ о лицензировании предписывает получение лицензии не на деятельность определенного субъекта, а на конкретные виды деятельности.

Так, Федеральным законом от 8 августа 2001 года № 128-ФЗ "О лицензировании отдельных видов деятельности" (ст. 17) предусматривается, что лицензированию подлежит деятельность:

- по выдаче сертификатов ключей электронных цифровых подписей;
- по регистрации владельцев электронных цифровых подписей;
- по оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей.

На основании ст. 5 Федерального закона "О лицензировании отдельных видов деятельности" Правительство РФ в соответствии с определенными Президентом РФ основными направлениями внутренней политики государства утверждает положения о лицензировании конкретных видов деятельности. В настоящее время положение о лицензировании перечисленных видов деятельности Правительством РФ не утверждено.

Тем не менее Кодекс РФ об административных правонарушениях от 30 декабря 2001 года № 195-ФЗ устанавливает ответственность за: "Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установ-

ленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна).

Ответственность заключается в наложении административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на должностных лиц — от двадцати до тридцати минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на юридических лиц — от ста до двухсот минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой" (ст. 13.13 "Незаконная деятельность в области защиты информации").

Закон об ЭЦП не раскрывает юридическую задачу лицензирования деятельности удостоверяющих центров, связанной с выпуском сертификата и подтверждением подлинности электронной цифровой подписи. Остается без ответа вопрос, какое фундаментальное обеспечение прав и интересов лиц, доверяющих сертификату, предоставляет центр при наличии лицензии по сравнению с ее отсутствием; каким образом такое обеспечение гарантируется со стороны выдавшего лицензию уполномоченного государственного органа.

В отличие от российского Закона признание электронных подписей в зарубежном и международном праве не связано с получением разрешения (лицензии) для ведения деятельности по выпуску сертификатов ключей электронных подписей.

Для современной мировой практики характерен отказ от обязательного лицензирования деятельности удостоверяющих центров. Директива Европейского Союза "Об электронных подписях", к примеру, предусматривает на всей территории Евросоюза право удостоверяющих центров свободно предлагать свои услуги без предварительного получения разрешения.

В соответствии с п. 1 ст. 8 Закона об ЭЦП удостоверяющий центр должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

Требования, предъявляемые к материальным и финансовым возможностям удостоверяющих центров, определяются Правительством Российской Федерации по представлению уполномоченного федерального органа исполнительной власти.

К настоящему времени требования, предъявляемые к материальным и финансовым возможностям удостоверяющих центров, в законодательстве не сформулированы. Предполагается, что указанные требования будут включены в перечень лицензионных условий, установленных в положении о лицензировании перечисленных видов деятельности.

Невозможна также реализация положений ст. 10 Закона об электронной цифровой подписи, устанавливающей отношения между удостоверяющим центром и уполномоченным федеральным органом исполнительной власти, который осуществляет в соответствии с положением об уполномоченном федеральном органе исполнительной власти полномочия по обеспечению действия данного Федерального закона. Указанное в ст. 10 положение об уполномоченном федеральном органе исполнительной власти к настоящему времени не издано.

По смыслу названной статьи Закона об ЭЦП удостоверяющий центр до начала использования электронной цифровой подписи удостоверяющего центра для заверения от имени удостоверяющего центра сертификатов ключей подписей обязан представить в уполномоченный федеральный орган исполнительной власти сертификат ключа подписи уполномоченного лица удостоверяющего центра в форме электронного документа, а также этот сертификат в форме документа на бумажном носителе с собственноручной подписью указанного уполномоченного лица, заверенный подписью руководителя и печатью удостоверяющего центра.

Уполномоченный федеральный орган исполнительной власти ведет единый государственный реестр сертификатов ключей подписей, которыми удостоверяющие центры, работающие с участниками информационных систем общего пользования, заверяют выдаваемые ими сертификаты ключей подписей, обеспечивает возможность свободного доступа к этому реестру и выдает сертификаты ключей подписей соответствующих уполномоченных лиц удостоверяющих центров.

Уполномоченный федеральный орган исполнительной власти осуществляет по обращениям физических лиц, организаций, федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей.

По указанной причине (отсутствие положения об уполномоченном федеральном органе исполнительной власти) невозможна также реализация ст. 21 "Переходные положения" Закона об ЭЦП. В соответствии с данной статьей Закона удостоверяющие центры, создаваемые после вступления в силу настоящего Федерального закона до начала ведения уполномоченным федеральным органом исполнительной власти реестра сертификатов ключей подписей, должны отвечать требованиям Федерального закона, за исключением требования предварительно представлять сертификаты ключей подписей своих уполномоченных лиц уполномоченному федеральному органу исполнительной власти. Соответствующие сертификаты должны быть представлены указанному органу не позднее чем через три месяца со дня вступления в силу настоящего Федерального закона.

2. Обязательства и ответственность удостоверяющего центра

Перечисленным в п. 1 ст. 9 Закона об ЭЦП функциям удостоверяющих центров корреспондируют положения ст. 11 данного Закона, посвященные обязательствам удостоверяющего центра.

Удостоверяющий центр при изготовлении сертификата ключа подписи принимает на себя следующие обязательства по отношению к владельцу сертификата ключа подписи:

- вносить сертификат ключа подписи в реестр сертификатов ключей подписей;
- обеспечивать выдачу сертификата ключа подписи обратившимся к нему участникам информационных систем;
- приостанавливать действие сертификата ключа подписи по обращению его владельца;
- уведомлять владельца сертификата ключа подписи о фактах, которые стали известны удостоверяющему центру и которые существенным образом

могут сказаться на возможности дальнейшего использования сертификата ключа подписи;

• иные установленные нормативными правовыми актами или соглашением сторон обязательства.

Помимо обязательств, перечисленных в данной статье, Федеральный закон прямо называет и иные обязательства удостоверяющего центра по отношению к владельцам сертификатов, например:

• использовать электронные цифровые подписи уполномоченных лиц удостоверяющих центров только после включения их в единый государственный реестр сертификатов ключей подписей, не допускать использования этих электронных цифровых подписей для целей, не связанных с заверением сертификатов ключей подписей и сведений об их действии (п. 3 ст. 10);

• оказывать безвозмездно услуги по выдаче участникам информационных систем сертификатов ключей подписей, зарегистрированных удостоверяющим центром, одновременно с информацией об их действии в форме электронных документов (п. 4 ст. 9);

• хранить сертификат ключа подписи в форме электронного документа в удостоверяющем центре после аннулирования сертификата ключа подписи не менее установленного федеральным законом срока исковой давности для отношений, указанных в сертификате, по истечении указанного срока перевести сертификат в режим архивного хранения (п. 2 ст. 7);

• при прекращении деятельности удостоверяющего центра аннулировать и передать на хранение уполномоченному федеральному органу исполнительной власти сертификаты ключей подписей, не переданные в другой удостоверяющий центр (п. 2 ст. 15).

Следует обратить внимание на тот факт, что Закон не предусматривает необходимых положений об ответственности удостоверяющих центров перед теми лицами, которые доверяют сертификату (пользователями).

Одними из наиболее значительных положений Закона об электронных подписях должны были бы стать нормы об ответственности удостоверяющих центров, подтверждающих подлинность электронной подписи посредством выдачи соответствующих сертификатов. На основании подобных положений должны выполняться специфические требования, предъявляемые к процедуре электронной подписи, и обеспечиваться доверие к последней. Механизм ответственности удостоверяющих центров является объектом особого внимания в Директиве Европейского Союза "Об электронных подписях". Следуя традициям иностранного законодательства об электронных подписях, для удостоверяющих центров должна предусматриваться правовая схема ограниченной ответственности, которая раскрывается следующим образом: удостоверяющий центр несет ответственность за убытки в объеме реального ущерба, понесенного лицом в результате доверия к представленным в сертификате данным, которые удостоверяющий центр обязан проверить и подтвердить.

Ответственность удостоверяющего центра не включает: штрафные санкции, возмещение упущенной выгоды, возмещение морального вреда.

Если иное не предусмотрено законом или договором, удостоверяющий центр несет ответственность, если не докажет, что надлежащее исполнение его обязанностей оказалось невозможным вследствие непреодолимой силы, то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств.

Удостоверяющий центр не несет ответственности:

— за ущерб, понесенный в результате доверия к недействительной или подделанной подписи, если удостоверяющий центр выполнил все требования Закона или договора в отношении недействительной или скомпрометированной электронной цифровой подписи;

— за ущерб свыше суммы, указанной в сертификате в качестве установленного предела имущественной ответственности удостоверяющего центра, понесенный в результате доверия к представленным в сертификате сведениям, которые центр обязан проверить и подтвердить.

3. Приостановление действия и аннулирование сертификата ключа подписи

Удостоверяющий центр может приостановить действие сертификата ключа подписи на основании указания лиц или органов, имеющих такое право в силу закона или договора, а в корпоративной информационной системе также в силу установленных для нее правил пользования (ст. 13 Закона об ЭЦП).

Действие сертификата ключа подписи по указанию полномочного лица (органа) приостанавливается на исчисляемый в днях срок, если иное не установлено нормативными правовыми актами или договором. Удостоверяющий центр возобновляет действие сертификата ключа подписи по указанию полномочного лица (органа). Если по истечении указанного срока не поступает указание о возобновлении действия сертификата, последний подлежит аннулированию.

В соответствии с указанием полномочного лица (органа) о приостановлении действия сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов соответствующей информации с указанием даты, времени и срока приостановления действия сертификата, а также извещает об этом владельца сертификата и полномочное лицо (орган), от которого получено указание о приостановлении действия сертификата ключа подписи.

Период от поступления в удостоверяющий центр указания о приостановлении действия сертификата ключа подписи до внесения соответствующей информации в реестр сертификатов ключей подписей должен устанавливаться в соответствии с общим для всех владельцев сертификатов ключей подписей правилом. По договоренности между удостоверяющим центром и владельцем сертификата ключа подписи этот период может быть сокращен.

Согласно ст. 14 Закона об ЭЦП удостоверяющий центр обязан аннулировать выданный им сертификат ключа подписи в следующих случаях:

— по истечении срока его действия;

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

— если удостоверяющему центру стало достоверно 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 или соглашением сторон ситуациях.

При аннулировании сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты и времени аннулирования сертификата ключа подписи, за исключением случаев аннулирования сертификата ключа подписи по истечении срока его действия, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание об аннулировании сертификата ключа подписи.

4. Прекращение деятельности удостоверяющего центра

В соответствии со ст. 15 Закона об электронной цифровой подписи деятельность удостоверяющего центра, выдающего сертификаты ключей подписей для использования в информационных системах общего пользования, может быть прекращена в порядке, установленном гражданским законодательством.

При прекращении деятельности удостоверяющего центра сертификаты ключей подписей, выданные этим удостоверяющим центром, могут быть переданы другому удостоверяющему центру по согласованию с владельцами сертификатов ключей подписей.

Сертификаты ключей подписей, не переданные в другой удостоверяющий центр, аннулируются и передаются на хранение уполномоченному федеральному органу исполнительной власти.

Следует заметить, что Законом об ЭЦП фактически не определен порядок прекращения деятельности удостоверяющего центра, действующего в информационных системах общего пользования, поскольку гражданское законодательство Российской Федерации не устанавливает порядок прекращения какой бы то ни было деятельности. Речь может идти о предусмотренной ст. 61 ГК РФ ликвидации юридического лица, которая влечет его прекращение без перехода прав и обязанностей в порядке правопреемства к другим лицам.

Нуждается также в уточнении норма, разрешающая подлежащему ликвидации удостоверяющему центру передавать другому удостоверяющему центру сертификаты ключей.

При этом не определен порядок сохранения неизменности такого сертификата, которая, вероятно, невозможна ввиду того, что сертификат всегда содержит наименование и местонахождение удостоверяющего центра, выдавшего сертификат (п. 1 ст. 6 Закона). Соответственно изменение реквизитов центра ведет к изменению сертификата.

Деятельность удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, прекращается по решению владельца этой системы, а также по договоренности участников системы в связи с передачей обязательств данного удостоверяющего центра другому удостоверяющему центру или в связи с ликвидацией корпоративной информационной системы (п. 3 ст. 15).

Установленный в п. 3 ст. 15 Закона порядок прекращения деятельности удостоверяющего центра в корпоративных информационных системах свидетельствует о том, что подобные системы могут ликвидировать такой центр без перехода прав и обязанностей последнего к его правопреемнику, только ликвидировавшись сами. Полного прекращения функций удостоверяющего центра в рамках действующей корпоративной системы Закон об ЭЦП не предусматривает.

6. ПРИЗНАНИЕ ИНОСТРАННОГО СЕРТИФИКАТА КЛЮЧА ПОДПИСИ

В силу ст. 18 Федерального закона об ЭЦП иностранный сертификат ключа подписи, удостоверенный в соответствии с законодательством иностранного государства, в котором этот сертификат ключа подписи зарегистрирован, признается на территории Российской Федерации в случае выполнения установленных законодательством РФ процедур признания юридического значения иностранных документов.

Подобное признание может быть осуществлено, если иностранный сертификат ключа подписи является документом на бумажном носителе. На сертификаты ключей ЭЦП в виде электронных документов Инструкция о консульской легализации (утв. МИД СССР 6 июля 1984 года) и Конвенция, отменяющая требование легализации иностранных официальных документов (Гаага, 5 октября 1961 года)[26] не распространяется.

7. ВМЕСТО ЗАКЛЮЧЕНИЯ

В связи со сложностями применения ряда положений Закона, относящихся к деятельности удостоверяющих центров, требуется законодательный ответ на вопросы, возникающие в правоприменительной практике: насколько обязательно обращение к услугам такого центра? И возможно ли в отсутствие более обстоятельного подзаконного регулирования сохранить прежние двусторонние договоренности по взаимному предоставлению ключей ЭЦП участниками сделки и не использовать в электронном документообороте удостоверяющий центр?

Представляется, что применение в электронном документообороте средств криптографической защиты информации (СКЗИ), в которых реализована возможность использования электронной цифровой подписи, может иметь и договорный статус, то есть основываться на соглашении сторон.

Такое соглашение реализуется, как правило, в виде приложения к договору, устанавливающего порядок использования электронной цифровой подписи в электронном документообороте. В соглашении предусматриваются программно-технические средства, обеспечивающие идентификацию подписи, и устанавливается режим их использования.

Договорная основа использования аналога собственноручной подписи соответствует п. 2 "Положения о порядке разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну" (приложение к приказу ФАПСИ от 23 сентября 1999 года № 158): "При организации информационного обмена конфиденциальной информацией, не подлежащей обязательной защите, необходимость ее криптографической защиты и тип применяемых СКЗИ (в случае принятия решения о криптографической защите информации) определяются соглашениями между участниками обмена".

Как видно из приведенных положений действующего законодательства РФ, допускается установление прямых договорных отношений по применению СКЗИ в электронном документообороте. При подобных отношениях стороны договора вправе признавать аналоги собственноручной подписи друг

[26] О присоединении СССР к Конвенции см. постановление ВС СССР от 17 апреля 1991 года № 2119-I.

друга без использования сертификата ключа подписи, который выдается участнику информационной системы удостоверяющим центром на основе Закона "Об электронной цифровой подписи".

Использование СКЗИ в электронном документообороте на основе предусмотренных законодательством РФ договорных отношений позволяет сделать вывод о том, что на них не распространяется действие Федерального закона "Об электронной цифровой подписи".

По смыслу ст. 3 Закона последний может распространяться только на случаи применения участниками информационных систем единственной технологии подтверждения подлинности электронной цифровой подписи в электронном документе: с использованием сертификата ключа подписи, который выдается удостоверяющим центром участнику информационной системы для подтверждения подлинности ЭЦП и идентификации владельца сертификата.

Вместе с тем Закон не содержит императивной нормы (прямого предписания) частным физическим или юридическим лицам — участникам электронного документооборота — использовать исключительно регулируемую им технологию. В Законе также нет нормы, запрещающей указанным лицам использовать иные технологии подтверждения подлинности электронной цифровой подписи, широко применяемые в практике обмена электронными документами.

К иным технологиям относится взаимное признание и подтверждение подлинности ЭЦП участниками электронного документооборота на основе заключенного ими двустороннего договора без обращения к услугам третьего лица — удостоверяющего центра и, соответственно, без использования выдаваемого таким центром сертификата. Поскольку ни Гражданский кодекс РФ, ни Закон "Об электронной цифровой подписи" не включают императивную норму, обязывающую стороны электронного документооборота заключать договоры с удостоверяющим центром по выдаче им сертификатов ключей подписей, на указанные отношения распространяется положение п. 1 ст. 421 ГК РФ "Свобода договора": "Граждане и юридические лица свободны в заключении договора. Понуждение к заключению договора не допускается...".

Н. СОЛОВЯНЕНКО,
старший научный сотрудник Института государства и права РАН,
кандидат юридических наук,
член рабочих групп по подготовке проекта
Федерального закона "Об электронной цифровой подписи"
и проекта Федерального закона "Об электронной торговле",
эксперт Государственной Думы Федерального Собрания РФ