ГРАЖДАНСКОЕ ПРАВО

*В. И. Квашнин**

ОТВЕТСТВЕННОСТЬ ПРИ ЗАКЛЮЧЕНИИ СДЕЛОК С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

На практике при заключении сделок с использованием электронной цифровой подписи (далее — ЭЦП) ответственность может наступить, прежде всего, у следующих субъектов: в связи с использованием несертифицированных средств при создании ЭЦП у распространителей и создателей; у владельца и пользователя ЭЦП (предпринимательские и не предпринимательские риски); у удостоверяющих центров (далее — УЦ).

Ответственность в связи с использованием несертифицированных средств при создании ЭЦП (распространителей и создателей)

Согласно п. 2 ст. 5 ФЗ «Об электронной цифровой подписи»[1] (далее — ФЗ «Об ЭЦП») при создании ключей электронных цифровых подписей для использования в информационной системе общего пользования должны применяться только сертифицированные средства ЭЦП. Возмещение убытков, причиненных в связи с созданием ключей ЭЦП несертифицированными средствами ЭЦП, может быть возложено на создателей и распространителей этих средств в соответствии с законодательством Российской Федерации.

До настоящего времени создание средств ЭЦП относится к лицензируемым видам деятельности. В соответствии с Федеральным законом от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности» лицензированию подлежит деятельность по разработке и производству, распространению, техническому обслуживанию шифровальных (криптографических) средств, а также предоставление услуг в области шифрования информации.[2] Пунктом 2 ст. 14.1 Кодекса об административных

* Квашнин Владислав Игоревич — аспирант кафедры коммерческого права СПбГУ.

E-mail: contact@digesta.ru

[1] *Федеральный* закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» // СЗ РФ. 2002. № 2. Ст. 127.

[2] Подпункты 5–8 п. 1 ст. 17 Федерального закона «О лицензировании отдельных видов деятельности» (в редакции федеральных законов № 28-ФЗ от 13 марта 2002 г., № 31-ФЗ от 21 марта 2002 г., № 164-ФЗ от 9 декабря 2002 г., № 17-ФЗ от 10 января 2003 г., № 29-ФЗ от 27 февраля 2003 г., № 32-ФЗ от 11 марта 2003 г., № 36-ФЗ от 26 марта 2003 г., № 185-ФЗ от 23 декабря 2003 г., № 127-ФЗ от 2 ноября 2004 г., № 20-ФЗ от 21 марта 2005 г., № 80-ФЗ от 2 июля 2005 г.) // Российская газета. 2001. 10 авг.

правонарушениях РФ[3] (далее — КоАП РФ) предусмотрено наказание за осуществление предпринимательской деятельности без специального разрешения (лицензии), если такое разрешение (такая лицензия) обязательно (обязательна), которое влечет наложение административного штрафа на граждан в размере от двадцати до двадцати пяти минимальных размеров оплаты труда с конфискацией изготовленной продукции, орудий производства и сырья или без таковой; на должностных лиц — от сорока до пятидесяти минимальных размеров оплаты труда с конфискацией изготовленной продукции, орудий производства и сырья или без таковой; на юридических лиц — от четырехсот до пятисот минимальных размеров оплаты труда с конфискацией изготовленной продукции, орудий производства и сырья или без таковой.

Также согласно п. 1 ст. 13.12 КоАП РФ существует наказание за нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), которое влечет наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц — от пяти до десяти минимальных размеров оплаты труда; на юридических лиц — от пятидесяти до ста минимальных размеров оплаты труда.

Рассмотрим пример, когда банк предлагает своим клиентам использовать систему «Банк-Клиент», основанную на применении ЭЦП. Согласно вышеперечисленному по смыслу ФЗ «Об ЭЦП» это использование будет происходить в рамках корпоративной системы, и необходимости в использовании сертифицированных средств ЭЦП здесь как бы не возникает, но к числу видов лицензируемой деятельности в сфере защиты информации относятся помимо всего прочего: деятельность по распространению шифровальных (криптографических) средств, следовательно, банку, если он передает своему клиенту такие средства, необходимо обладать соответствующей лицензией. А согласно Положению по лицензированию деятельности по распространению шифровальных (криптографических) средств, утвержденному Постановлением Правительства Российской Федерации от 29 декабря 2007 г. № 957,[4] средства ЭЦП относятся к шифровальным (криптографическим) средствам. Все это порождает проблему лицензирования: распространение криптографических (шифровальных) средств или предоставление услуг в области шифрования информации может являться одновременно и оказанием услуг, связанных с использованием ЭЦП, что потребует получения лицензии даже в корпоративных системах.

Однако законодатель в ФЗ «Об ЭЦП» не указывает, кому должны быть возмещены убытки. Думается, что императивные требования сертификации средств ЭЦП в данном случае установлены, прежде всего, в интересах участников информационной системы общего пользования.

Обязанности по доказыванию недобросовестности изготовителя или распространителя в таких случаях будут лежать на приобретателе ключа ЭЦП, который обязан удостовериться в сертификации прав и средств изготовителя и распространителя. ФЗ «Об ЭЦП» не устанавливает какой-либо ответственности по возмещению убытков на

---

[3] *Кодекс* Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Там же. 2001. 31 дек.

[4] *Положение* по лицензированию деятельности по распространению шифровальных (криптографических) средств, утв. Постановлением Правительства Российской Федерации от 29 декабря 2007 г. № 957 // СЗ РФ. 2008. № 2. Ст. 86.

создателей и распространителей сертифицированных средств ЭЦП в связи с использованием таких сертифицированных средств по созданию и применению ключей электронной цифровой подписи. Если государственная сертификация средств подписи имеет какой-то смысл, то он может заключаться именно в том, чтобы дать гарантии и снять риски убытков пользователям.

На наш взгляд, было бы правильнее возложить ответственность на владельца закрытого ключа ЭЦП, использующего несертифицированные средства для ее создания, в том случае, если он не обеспечил уведомление пользователей сертификата ключа подписи об отсутствии сертификата на средство ЭЦП. Подобные положения содержал п. 3 ст. 4 проекта Федерального закона «Об электронной цифровой подписи» В. А. Тарачева и А. Н. Шохина,[5] аналогичной позиции придерживается В. А. Копылов.[6]

А последний законопроект «Об электронной подписи»,[7] внесенный депутатами Государственной Думы ФС РФ О. В. Морозовым, В. А. Васильевым, В. В. Володиным, В. Я. Комиссаровым, П. В. Крашенинниковым, В. М. Резником, В. Н. Плигиным, К. Б. Шипуновым 25 декабря 2009 г. и принятый ГД ФС РФ в первом чтении 22 января 2010 г., в п. 4 ст. 8 вовсе предлагает оставить обязательную сертификацию только для средств ЭЦП, предназначенных для подписания электронных документов, которые содержат сведения, составляющие государственную тайну, или предназначенных для использования в информационной системе, которая обрабатывает информацию, содержащую сведения, составляющие государственную тайну.

Следует напомнить, что запрет на создание, распространение и использование несертифицированных средств ЭЦП в корпоративной информационной системе отсутствует. Производители и распространители несертифицированных средств ЭЦП не обязаны выяснять, для использования в какой информационной системе такие средства приобретаются. Вышесказанное позволяет сделать вывод о том, что правовые основания для возложения ответственности на создателей и распространителей несертифицированных средств ЭЦП отсутствуют.

Ответственность владельцев и пользователей ЭЦП

ФЗ «Об ЭЦП» не упоминает, что существует также административная ответственность и пользователей несертифицированными средствами по п. 2 ст. 13.12 КоАП, согласно которой использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц — от десяти до двадцати минимальных размеров оплаты труда; на

---

[5] *Проект* Федерального закона «Об электронной цифровой подписи» В. А. Тарачева и А. Н. Шохина № 33842-3 // http://www.duma.gov.ru.

[6] *Копылов В. А.* О применении Федерального закона «Об электронной цифровой подписи» для регулирования отношений в административном и гражданском электронном документообороте // http://ilaw.nm.ru/publication/skecprags.htm.

[7] *Проект* Федерального закона «Об электронной подписи» О. В. Морозова, В. А. Васильева, В. В. Володина, В. Я. Комиссарова, П. В. Крашенинникова, В. М. Резника, В. Н. Плигина, К. Б. Шипунова № 305592-5 // http://www.duma.gov.ru.

юридических лиц — от ста до двухсот минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой.

Согласно положению о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации, утвержденному Приказом ФСБ от 9 февраля 2005 г. № 66,[8] которое регулирует отношения, возникающие при разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее — информация конфиденциального характера), шифровальные (криптографические) средства защиты информации конфиденциального характера в этом положении именуются средствами криптографической защиты информации (далее — СКЗИ), и к ним прямо отнесены средства электронной цифровой подписи.

Согласно п. 3 данным положением необходимо руководствоваться при разработке, производстве, реализации и эксплуатации средств криптографической защиты информации конфиденциального характера в следующих случаях:

— если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;

— при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации (далее — государственные органы);

— при организации криптографической защиты информации конфиденциального характера в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд (далее — организации, выполняющие государственные заказы);

— если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации;

— при обрабатывании информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путем использования средств криптографической защиты;

— при обрабатывании информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации.

В связи с этим можно сделать вывод, что ясность в сфере обязательной сертификации криптографических средств (средств ЭЦП) отсутствует. Вместе с тем, если в случае взаимодействия по заключению контракта между предпринимателем и государственным органом будет использовано несертифицированное средство ЭЦП, наступит ответственность по п. 2 ст. 13.12 КоАП. Также ответственность может наступить, если информация, которая передается посредством несерцифицированных средств, носит

[8] Приказ ФСБ от 9 февраля 2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» // Российская газета. 2005. 19 марта.

конфиденциальный характер и подлежит защите в соответствии с законодательством Российской Федерации.

Требования Положения ПКЗ-2005 носят рекомендательный характер при разработке, производстве, реализации и эксплуатации:

— средств криптографической защиты информации, доступ к которой ограничивается по решению обладателя, пользователя (потребителя) данной информации, собственника (владельца) информационных ресурсов (информационных систем) или уполномоченных ими лиц, не являющихся государственными органами или организациями, выполняющими государственные заказы;

— средств электронной цифровой подписи, предназначаемых для использования в электронном документообороте, информация которого не относится к информации конфиденциального характера.

СКЗИ должны удовлетворять требованиям технических регламентов, оценка выполнения которых осуществляется в порядке, определяемом Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».[9]

Также согласно ст. 12 ФЗ «Об ЭЦП» владелец сертификата несет следующие обязательства:

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

— хранить в тайне закрытый ключ ЭЦП;

— немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа ЭЦП нарушена.

Ответственность владельцев сертификатов ключей подписей за неисполнение или ненадлежащее исполнение вышеперечисленных обязательств предусматривается комментируемым Законом в виде возмещения причиненных убытков. При этом убытки причиняются, как правило, не УЦ, а иным участникам информационной системы.

ФЗ «Об ЭЦП» не предусматривает положений, которые бы ставили наступление ответственности в зависимость от наличия или отсутствия вины владельца сертификата ключа подписи. В соответствии с п. 1 ст. 401 Гражданского кодекса РФ[10] (далее — ГК РФ) лицо, не исполнившее обязательство или исполнившее его ненадлежащим образом, несет ответственность только при наличии вины. Надлежащее исполнение предусмотренных ФЗ «Об ЭЦП» обязанностей продиктовано, в первую очередь, требованиями по обеспечению безопасности электронных взаимоотношений между контрагентами по той или иной сделке, а не в отношениях с УЦ. Поэтому представляется обоснованным несение владельцем сертификата ключа подписи ответственности на началах предпринимательского риска (п. 3 ст. 401 ГК РФ).

Перечисленные в ст. 12 ФЗ «Об ЭЦП» случаи — это случаи так называемой «компрометации закрытого ключа ЭЦП». Этот термин обозначает утрату владельцем ЭЦП по каким-либо причинам доверия к ЭЦП, появление у владельца сомнений в сохранении тайны закрытого ключа ЭЦП. Достаточность оснований для предъявления владельцем ЭЦП требования о приостановлении действия сертификата ключа подписи определяется

---

[9] *Федеральный* закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» // СЗ РФ. 2002. № 52 (ч. I). Ст. 5140.

[10] *Гражданский* кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ (часть вторая) от 26 января 1996 г. № 14-ФЗ и (часть третья) от 26 ноября 2001 г. № 146-ФЗ // Российская газета. 1994. 8 дек.; 1996. 6, 7, 8 февр.; 2001. 28 ноября.

самим владельцем ЭЦП. УЦ в соответствии с положениями ст. 11 ФЗ «Об ЭЦП» не вправе отказать владельцу ЭЦП в приостановлении действия сертификата ключа подписи.

По нашему мнению, закрепленные на законодательном уровне меры не могут гарантировать безопасности закрытого ключа. Так, например, и К. Б. Леонтьев считает, что при доказывании наличия вины в действиях или бездействии владельца ЭЦП, приведших к несанкционированному использованию закрытого ключа ЭЦП и причинению убытков другим лицам, в случае возникновения спора большую роль будут играть конкретные обстоятельства дела и субъективные факторы. «Например, закрытый ключ может быть похищен, даже если приняты все разумные меры безопасности. При этом "кражу" закрытого ключа чаще всего сразу заметить трудно. Таким образом, положения данной статьи (ст. 12 ФЗ "Об ЭЦП". — *В. К.*) дают основания предполагать появление довольно противоречивой судебной практики. Во многих случаях решения судов будут основываться, прежде всего, на признаниях и объяснениях самого владельца ЭЦП».[11]

Как мы уже знаем, на уровне подзаконных актов имеет место и более жесткий подход, в соответствии с которым предполагается, что ЭЦП была применена в электронном документе лицом, являющимся владельцем сертификата ключа подписи, до тех пор, пока это лицо не заявило обратное.

Так, например, Методические рекомендации об организации и функционировании системы представления налоговых деклараций и бухгалтерской отчетности в электронном виде по телекоммуникационным каналам связи устанавливают, что электронный документ считается исходящим от участника информационного обмена, если он подписан ЭЦП, принадлежащей уполномоченному лицу данного участника. При этом риск неправомерного подписания электронного документа ЭЦП несет участник информационного обмена, на уполномоченное лицо которого зарегистрирован сертификат соответствующего ключа подписи. Открытый ключ считается действующим, если до момента получения адресатом электронного документа, подписанного ЭЦП, лицом, на чье имя зарегистрирован сертификат ключа данной ЭЦП, не было заявлено о его недействительности.[12]

По нашему мнению, проблема закрытого ключа может быть решена путем прямого закрепления в законе презумпции, которая заключается в предположении, что ЭЦП в электронном документе создана владельцем сертификата ее открытого ключа, если владелец сертификата ключа подписи не докажет обратное, условно назовем ее «презумпция авторства». Презумпция авторства в значительной степени гарантировала бы юридическую силу электронного документа, заверенного ЭЦП. В настоящее время данный принцип действует при договорном установлении основания ответственности и распределения рисков убытков. В качестве примера можно привести положения разд. 9 «Ответственность Сторон и риски убытков» Договора об обмене электронными

---

[11] *Леонтьев К. Б.* Комментарий к Федеральному закону «Об электронной цифровой подписи» (постатейный). М., 2003. С. 43.

[12] См.: п. 6.2, 6.3, 6.4 Методических рекомендаций об организации и функционировании системы представления налоговых деклараций и бухгалтерской отчетности в электронном виде по телекоммуникационным каналам связи, утв. Приказом МНС РФ от 10 декабря 2002 г. № БГ-3-32/705@ (в ред. Приказа ФНС РФ от 04.03.2010 № ММ-7-6/96@, с изм., внесенными Приказом МНС РФ от 08.08.2003 № БГ-3-32/443@) // Учет. Налоги. Право — Официальные документы. 2003. № 2.

документами при осуществлении расчетов через расчетную сеть Банка России (Приложение I к Положению № 20-П).[13]

В российском законе отсутствует ответственность владельцев за предоставление заведомо ложной информации, тогда как, к примеру, в пункте 4 (a) ст. 46-3-304 Закона штата Юта о цифровой подписи 1995 г. закрепляется, что, соглашаясь с данными, предоставляемыми им для включения в сертификат цифровой подписи, владелец такого сертификата обязан компенсировать все убытки сертифицирующего органа (в том числе понесенные в связи с возмещением ущерба лицам, положившимся на соответствующий сертификат), возникшие в результате выпуска или публикации сертификата, основанного на недостоверной информации, предоставленной владельцем сертификата, при наличии вины последнего. В свою очередь согласно ст. 46-3-304 рассматриваемого акта получатель сообщения, удостоверенного цифровой подписью, принимает на себя риск того, что цифровая подпись является поддельной, если с учетом конкретных обстоятельств доверие к подписи было необоснованным.

Работодатели также могут столкнуться с проблемой привлечения к ответственности своих должностных лиц, использующих ЭЦП, так как в ФЗ «Об ЭЦП» наименее подробно регламентированы вопросы правового режима хранения ЭЦП ее владельцем. Представляется, что участники электронного документооборота должны самостоятельно разработать и установить режим тайны закрытого ключа электронной цифровой подписи (далее — тайны ключа). Мы полагаем возможным определить режим данной тайны как служебной. «Служебная тайна» широко используется в праве при установлении режима защиты информации. Именно в таком значении используется данное понятие в Трудовом кодексе РФ (далее — ТК РФ).[14] В ФЗ «О государственной гражданской службе Российской Федерации»[15] используется разновидность понятия «служебная тайна» — «служебная информация».

При определении режима тайны ключа надо учитывать, что работодатель, в конечном счете, в значительно большей степени, чем его работник — владелец сертификата ключа подписи ЭЦП, заинтересован в сохранении тайны ключа. Это вполне понятно, так как в соответствии с действующим гражданским и трудовым законодательством права и обязанности в результате деятельности работника будут возникать у работодателя. Вся проблема заключается в том, что такое регулирование должно учитывать требования ст. 12 Закона, согласно которой именно владелец сертификата ключа подписи обязан хранить в тайне закрытый ключ ЭЦП. Следовательно, владелец сертификата ключа подписи либо должен принимать участие в установлении режима тайны ключа, либо им должно быть прямо выражено согласие присоединиться к данному режиму, разработанному работодателем. Видимо, для большинства работодателей потребуется использовать два вида нормативных актов: трудовой договор (контракт) и инструкцию (положение, и т. п.). Также надо согласиться с правильным замечанием А. Ткачева, что необходимо отметить наличие противоречий между обязанностью владельца сертификата ключа подписи возместить убытки (включая упущенную выгоду) в слу-

---

[13] *Положение* Банка России от 12 марта 1998 г. № 20-П «О правилах обмена электронными документами между Банком России, кредитными организациями (филиалами) и другими клиентами Банка России при осуществлении расчетов через расчетную сеть Банка России» (в редакции указаний Банка России № 551-У от 28 апреля 1999 г., № 774-У от 11 апреля 2000 г.) // Вестник Банка России. 1998. № 20.

[14] *Трудовой* кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ // Российская газета. 2001. 31 дек.

[15] *Федеральный* закон от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» // Там же. 2004. 31 июля.

чае несоблюдения требований Закона и ограничением ответственности работника по ТК РФ только возмещением прямого действительного ущерба. Данная норма Закона в полном объеме может быть распространена только на владельцев сертификата ключа подписи, связанных с лицом, которому они причинили убытки гражданско-правовыми отношениями.[16]

Возвращаясь к вопросу ответственности на началах предпринимательского риска в сделках, заключаемых в электронно-цифровой форме, стоит упомянуть о риске, который существует в результате технических сбоев, а также в результате действий третьих лиц (информационных провайдеров). Если же утрата информации происходит в результате умышленных действий самих сторон, то это уже можно признать нарушением права и применить (по аналогии) норму п. 3 ст. 157 ГК РФ: «Если наступлению условия недобросовестно воспрепятствовала сторона, которой наступление условия невыгодно, то условие признается наступившим. Если наступлению условия недобросовестно содействовала сторона, которой наступление условия выгодно, то условие признается ненаступившим». Об этом писали еще И. Б. Новицкий и Л. А. Лунц: «Если предложивший договор умышленно помешал получению ответа, содержащего принятие предложения, то нужно применить по аналогии норму, установленную для условных сделок: если наступлению условия недобросовестно воспрепятствовала сторона, которой выгодно ненаступление условия, то условие считается наступившим».[17] В обоих случаях последствием будет пропуск срока, в течение которого договор мог быть заключен, что, возможно, повлечет незаключение договора: если была утрачена оферта, то она не приобретет юридического значения, так как и не была получена акцептантом (п. 2 ст. 435 ГК РФ); если был утрачен ответ на оферту, то неполучение оферентом в течение нормально необходимого или прямо установленного срока акцепта приводит к утрате офертой юридического значения. В случае утраты акцепта могут возникнуть серьезные убытки, обусловленные тем, что акцептант, считая себя связанным своим акцептом, может начать приготовления для исполнения договора. В то же время договор не будет считаться заключенным, так как лицо, направившее оферту, акцепта не получило (п. 1 ст. 433 ГК РФ).

Распределение убытков, связанных с возможностью случайной утраты информации, необходимо связывать с требованием нормальной разумности и осмотрительности участников оборота. Н. А. Дмитрик в своей работе «Осуществление субъективных гражданских прав с использованием сети Интернет» пишет: «Выбирая средства доставки, лицо должно предполагать, что в нормальных условиях функционирования сетей информация должна с высокой степенью вероятности достигнуть адресата. Тем более что существуют и весьма распространены методы повышения надежности доставки: подтверждение получения (прочтения), отчет о доставке письма (либо информации, передаваемой иным способом). По аналогии: заказное письмо с уведомлением о вручении может считаться более надежным способом доставки корреспонденции, нежели обычное письмо. Следовательно, если сторона не проявила достаточной разумности и осмотрительности в выборе средств и методов доставки информации адресату, к ней может быть предъявлено требование о возмещении возникших в результате этого имущественных потерь. Если же действия сторон отвечали требованиям нормальной

---

[16] *Ткачев А.* Электронная подпись: право на жизнь // Бизнес-адвокат. 2005. № 9.

[17] *Новицкий И. Б., Лунц Л. А.* Общее учение об обязательстве. М., 1950. С. 163.

разумности и осмотрительности, то возложение на какую-либо из сторон всех понесенных потерь недопустимо».[18] И это разумно. Что же касается влияния третьих лиц (информационных посредников), то к ним также применяются общие нормы об ответственности: они отвечают при наличии вины.

Ответственность удостоверяющих центров

Согласно п. 1 ст. 8 ФЗ «Об ЭЦП» УЦ 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 УЦ, определяются Правительством Российской Федерации по представлению уполномоченного федерального органа исполнительной власти.

Материальные и финансовые возможности удостоверяющего центра призваны обеспечить гарантии интересам пользователей информационных систем общего пользования.

Директива Европейского парламента и Совета 1999.93.ЕС от 13 декабря 1999 г. «О правовых основах Сообщества для электронных подписей»[19] также предусматривает, что УЦ должен располагать финансовыми ресурсами, достаточными для осуществления деятельности, включая возможную имущественную ответственность перед лицами, понесшими убытки вследствие недостоверности содержания сертификатов, выдаваемых УЦ.

В законодательстве других государств предусматривается возможность ограничения ответственности УЦ. Так, разрешается УЦ устанавливать предельный объем сделок, в отношении которых действует электронная цифровая подпись. И в случае превышения этого максимального предела участниками информационной системы УЦ не несет ответственность за их убытки.

ФЗ «Об ЭЦП» не предусматривает какого-либо ограничения ответственности УЦ. Более того, в настоящее время до сих пор отсутствует четкое определение этих требований к материальным и финансовым возможностям УЦ. В соответствии с ФЗ «Об ЭЦП» ответственность УЦ наступает в случае причинения убытков пользователям сертификатов ключей подписей вследствие недостоверности представленных в сертификатах ключей подписей сведений. В соответствии с ГК РФ (п. 3 ст. 401) УЦ будет нести ответственность на началах предпринимательского риска, т. е. в любом случае вне зависимости от наличия его вины, если не докажет, что не выполнил свои обязанности только в силу непреодолимой силы (чрезвычайных и непредотвратимых при данных условиях обстоятельств).

Корпоративная информационная система, так же, как и статус их УЦ, регулируется внутренними нормативными актами, а именно: соглашением всех участников этой системы либо решением владельца такой системы, являющегося обязательным для остальных участников-пользователей. Таким образом, требования, указанные в п. 1 ст. 8 ФЗ «Об ЭЦП», не распространяются на УЦ корпоративных информационных систем.

---

[18] *Дмитрик Н. А.* Осуществление субъективных гражданских прав с использованием сети Интернет. М., 2006. С. 84.

[19] http://www.ict.etsi.org/EESSI/Documents/e-sign-directive.pdf.

Проблема определения достаточности материальных и финансовых средств разрешается в абзаце втором ст. 8 ФЗ «Об ЭЦП». Уровень достаточности «необходимых средств» оценивается уполномоченным федеральным органом исполнительной власти, который делает представление Правительству РФ, и последнее обязано вынести соответствующее решение. Выбор термина «материальные средства» и постановка его рядом с термином «финансовые» дают основание считать, что под материальными средствами можно понимать как защищенные помещения, так и технологические возможности центра.

Разумно выглядит определение финансового обеспечения для УЦ, имеющих право выдавать квалификационные сертификаты для ЭЦП (по тексту проекта закона «для квалифицированной электронной подписи») при их аккредитации в п. 3 ст. 13 проекта Федерального закона «Об электронной подписи» № 305592-5 не менее полутора миллионов рублей.

Согласно ст. 11 ФЗ «Об ЭЦП» УЦ 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.

Следовательно, в случае нарушения вышеуказанных обязательств, которые привели к убыткам владельца сертификата, УЦ должен нести ответственность.

На основании вышеизложенного можно сделать следующие выводы:

1. Необходимо внести изменения в ФЗ «Об ЭЦП», связанные с:

— закреплением норм, устанавливающих презумпцию того, что ЭЦП в электронном документе создана владельцем сертификата ее открытого ключа, если владелец сертификата ключа подписи не докажет обратное — презумпцию авторства;

— возложением ответственности на владельца закрытого ключа ЭЦП, использующего несертифицированные средства для ее создания, в том случае, если он не обеспечил уведомление пользователей сертификата ключа подписи об отсутствии сертификата на средство ЭЦП. Подобные положения содержал п. 3 ст. 4 проекта Федерального закона «Об электронной цифровой подписи» В. А. Тарачева и А. Н. Шохина,[20] аналогичной позиции придерживается В. А. Копылов.[21]

2. Неопределенная позиция законодателя в отношении возможности использования несертифицированных средств ЭЦП является существенным фактором, сдерживающим распространение использования электронного документооборота в предпринимательской

[20] *Проект* Федерального закона «Об электронной цифровой подписи»» В. А. Тарачева и А. Н. Шохина № 33842-3 // http://www.duma.gov.ru.

[21] *Копылов В. А.* О применении Федерального закона «Об электронной цифровой подписи» для регулирования отношений в административном и гражданском электронном документообороте.

деятельности. В связи с этим мы предлагаем внести следующие коррективы в ФЗ «Об ЭЦП»:

— установить обязательное использование сертифицированных средств ЭЦП только в информационных системах, в которых принимают участие федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации и органы местного самоуправления, а также при ситуации, если информация подлежит защите в соответствии с законодательством Российской Федерации. В остальных случаях вопрос об используемых средствах ЭЦП должен решаться в договорном порядке;

— предлагается исключить положение п. 2 ст. 5 ФЗ «Об ЭЦП», предусматривающее возможность возложения на создателей и распространителей несертифицированных средств ЭЦП возмещения убытков, причиненных в связи с созданием данными средствами ключей электронных цифровых подписей. Создатели и распространители несертифицированных средств ЭЦП не обязаны выяснять, для использования в какой информационной системе такие средства приобретаются. Отмеченное позволяет сделать вывод о том, что правовые основания для возложения ответственности на создателей и распространителей несертифицированных средств ЭЦП отсутствуют. В связи с этим предлагается изменить п. 2 ст. 5 ФЗ «Об ЭЦП», изложив его в следующей редакции: «При создании ключей электронных цифровых подписей для использования в информационной системе общего пользования должны применяться только сертифицированные средства электронной цифровой подписи»;

— установить обязанность организатора информационной системы электронного документооборота (ее участников) уведомлять контрагентов об использовании несертифицированных средств электронной цифровой подписи, а также возместить убытки, причиненные вследствие использования несертифицированных средств ЭЦП при отсутствии такого уведомления.

3. Представляется, что участники электронного документооборота должны самостоятельно разработать и установить режим тайны закрытого ключа электронной цифровой подписи. Мы полагаем возможным определить режим данной тайны как служебной. «Служебная тайна» широко используется в праве при установлении режима защиты информации. Именно в таком значении используется данное понятие в Трудовом кодексе РФ. В ФЗ «О государственной гражданской службе Российской Федерации» используется разновидность понятия «служебная тайна» — «служебная информация».