

ЭЛЕКТРОННЫЕ РЕСУРСЫ

Степанов О.А.¹

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА



В XXI веке практически все сферы жизни и государственной деятельности зависят от качества и безопасности информационных технологий (ресурсов), связанных с ними. Развитие информационных технологий все в большей степени ассоциируется с понятиями «электронный документооборот», «информационный терроризм», «электронно-цифровая подпись», то есть с возникновением принципиально новой среды общения — информационно-электронной.

Возможность использования систем электронного документооборота в настоящее время обусловлена действием части первой Гражданского кодекса РФ. Так, согласно ст.160 («Письменная форма сделки») при совершении сделок допустимо применение электронной цифровой подписи (а, следовательно, допустим и обмен документами в электронной форме). В соответствии со ст. 434 ГК РФ («Форма договора») договор в письменной форме может быть заключен путем обмена документами электронной связи, позволяющей достоверно установить, что документ исходит от стороны по договору. Статья 847 ГК РФ («Удостоверение права распоряжения денежными средствами, находящимися на счете») устанавливает, что договором может быть предусмотрено удостоверение прав распоряжения денежными суммами, находящимися на счете, электронными средствами платежа и другими документами с использованием в них аналогов собственноручной подписи. Кроме того, согласно ст. 4 и ст. 19 Федерального закона «Об электронной цифровой подписи» электронная цифровая подпись в электронном документе является не просто равнозначной собственноручной подписи на бумажном носителе, но и в ряде случаев признается равнозначной подписи личности, заверенной печатью.

Реализация положений российской доктрины информационной безопасности (утвержденной Президентом России 9 сентября 2000 г.) предполагает подготовку порядка 30-50 нормативных правовых актов, в их числе должны быть законы, определяющие организацию следствия, процедуру судебного разбирательства по фактам противоправных действий в информационной сфере и разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисцип-

линарной ответственности, в том числе в сфере электронного документооборота.

В этой связи следует заметить, что решение проблемы безопасного использования электронного документооборота предполагает не только соответствующий уровень квалификации человека, но и осуществление определенных процедур безопасности, общих на всей территории Российской Федерации. Такие процедуры должны стать опорой для формирования конкретного содержания договоров, а также для экспертов и для судебных органов. Это предполагает, в частности, необходимость разработки законопроекта «О безопасности электронного документооборота». Этот нормативный правовой акт должен определять не только правовые основы обеспечения безопасности электронного документооборота, и обеспечивать защиту прав и законных интересов граждан, но защиту интересов общества и государства путем предупреждения противоправных действий в информационно-электронном пространстве.

Если под безопасностью электронного документооборота понимать состояние данного процесса, отражающее степень защищенности его участников от противоправных действий и их последствий, то в качестве основных правовых принципов обеспечения безопасности электронного документооборота могут быть названы:

соблюдение интересов граждан, общества и государства при создании условий безопасности электронного документооборота, реализация которых предполагает обеспечение безопасности электронных транзакций при максимально допустимом учете и удовлетворении интересов личности, а также реализацию угрозы ее наказания при использовании личностью опасных для общества методов и информационных технологий;

программно-целевой подход к деятельности по обеспечению безопасности электронного документооборота, предполагающий осуществление единой информационно-правовой политики на федеральном и региональном уровнях.

В качестве главных направлений развития законодательства в сфере обеспечения безопасности рассматриваемого процесса могут быть названы:

В XXI веке практически все сферы жизни и государственной деятельности зависят от качества и безопасности информационных технологий.

¹ Степанов Олег Анатольевич — кандидат юридических наук, доцент, сотрудник Академии управления МВД России, автор многих публикаций, связанных с правовым регулированием развития новых информационных технологий.

координация деятельности федеральных органов власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, юридических и физических лиц в целях предупреждения противоправных действий и снижения тяжести их последствий;

разработка и утверждение в установленном порядке подзаконных ведомственных нормативных правовых актов по вопросам обеспечения безопасности электронного документооборота;

осуществление сертификации средств электронного документооборота;

осуществление государственного надзора и контроля за выполнением законодательства Российской Федерации, правил, стандартов, технических норм в области обеспечения безопасности электронного документооборота.

разработка федеральных, региональных и местных программ, направленных на предупреждение противоправных действий в сфере электронного документооборота, а также материальное и финансовое обеспечение мероприятий по безопасности электронного документооборота.

В настоящее время согласно Уголовному кодексу Российской Федерации (далее — УК РФ) преступными, в частности, считаются такие действия, как неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ персоналом.

При этом неправомерный доступ к компьютерной информации квалифицируется как преступление при следующих условиях:

если компьютерная информация охраняется законом, то есть представлена на машинном носителе, в ЭВМ или их сети;

если неправомерный доступ к компьютерной информации повлек за собой уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Эти действия наказываются штрафом, либо исправительными работами, либо лишением свободы на срок до двух лет. Те же действия, совершенные с использованием служебного положения, влекут за собой наказание в более крупном размере (ст. 272 ч. 2 УК РФ). Эта норма означает, что посторонние лица несут меньшую уголовную ответственность, чем сотрудники организации, допущенные к компьютерной информации.

Под вредоносными программами для ЭВМ (оказывающими в том числе влияние на реализацию электронного документооборота) понимаются программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, а также приводящие к нарушению работы ЭВМ, системы ЭВМ или их сети (ст. 273 УК РФ).

Применительно к проблеме электронного документооборота опасность создания, использования, распространения вредоносных программ определяется тем, что такие программы способны в самый неожиданный момент парализовать работу компьютерной системы. Уголовному наказанию подлежат действия, связанные не только с созданием вредоносных программ, но и с переделкой уже существующих программ во вредоносные посредством заражения вирусом, а также использование и распростра-

нение вредоносных программ или их машинных носителей. В зависимости от тяжести последствий такие преступления наказываются лишением свободы на срок до трех лет либо до семи лет (ст. 273 ч. 2 УК РФ).

К разряду преступлений отнесено также нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее за собой уничтожение, блокирование или модификацию компьютерной информации в случае, если причинен существенный вред или, по неосторожности, причинены тяжкие последствия (ст. 274).

В рамках реализации обязательств, взятых на себя Россией в соответствии с Окинавской Хартией Глобального Информационного Общества (2000г.) в апреле 2003 г. Государственной Думой были внесены изменения в текст статьи 146 УК РФ («Нарушение авторских и смежных прав»), предусматривающие определение конкретного

денежного выражения «крупного» и «особо крупного» размера ущерба (имущественного вреда), нанесенного пиратской деятельностью (составляющего соответственно 100 и 500 минимальных размеров оплаты труда). При этом правообладатель нового продукта в информационно-электронном виде (независимо от привлечения лица к уголовной ответственности) вправе требовать и возмещения причиненного ущерба в гражданском порядке, направив соответствующий иск в суд по месту жительства ответчика или месту нахождения организации.

Кроме того Арбитражным процессуальным кодексом РФ с сентября 2002 г. предусматривается возможность принятия судом по заявлению правообладателя предварительных обеспечительных мер, которые могут быть применены еще до подачи искового заявления без уведомления ответчика, в целях предотвращения сокрытия или уничтожения им доказательств, в том числе в электронном виде.

Важно заметить, что решение проблемы правового обеспечения электронного документооборота в России предполагает и международно-правовое регулирование информационно-электронных отношений в рамках развития глобальной информационной структуры.

Речь может идти о таких аспектах, связанных с электронным документооборотом, как регламентация трансграничных обменов информацией и предупреждение действий хакеров, нарушающих права интеллектуальной собственности, в том числе в Интернете.

В настоящее время еще недостаточно развиты связи России с другими государствами, прежде всего по процессуальной линии в части ее интеграции в международное правовое пространство. Установление соответствующего порядка по делам, попадающим под действие юрисдикции нескольких государств, приведет к устранению дублирования при расследовании высокотехнологичных преступлений и повышению возможностей привлечения виновных к ответственности.

Существенную роль в обеспечении гарантий безопасности электронного документооборота могут сыграть и несудебные международные органы, деятельность которых создает основу для совместных консультаций (согласительных процедур) по наиболее важным вопросам. При этом большое значение может иметь создание в рамках ООН специального органа, уполномоченного осуществлять контроль за применением тех или иных мер

Установление соответствующего порядка по делам, попадающим под действие юрисдикции нескольких государств, приведет к устранению дублирования при расследовании высокотехнологичных преступлений и повышению возможностей привлечения виновных к ответственности.

воздействия и давать рекомендации об усилении их действенности.

Вместе с тем следует иметь в виду, что, например, юридическая природа электронного документооборота, приводит к невозможности для любой отдельно взятой страны решить проблему преступлений в сфере высоких технологий. Для сокращения до минимума выгоды от преступной деятельности и увеличения до максимума риска наказания за участие в этой деятельности различные государства должны осуществлять сбор и обмен информацией в глобальных масштабах. Только это позволит им противодействовать транснациональным преступлениям с применением Интернета.

В декабре 1997 г. на встрече министров юстиции и внутренних дел стран «восьмерки» в городе Вашингтоне были одобрены следующие принципиальные положения о борьбе с преступлениями в сфере высоких технологий, а именно: для тех, кто злоупотребляет информационными технологиями, не должно быть «тихих гаваней»; расследования международных высокотехнологических преступлений и наказания за них должны координироваться всеми заинтересованными странами независимо от того, где был нанесен ущерб; сотрудники охраны правопорядка должны быть подготовлены и оснащены для борьбы с преступлениями, использующими современные технологии; юридические системы должны защищать конфиденциальность, целостность и доступность данных систем, а также гарантировать их защиту от несанкционированного вмешательства при одновременном обеспечении наказания за серьезные злоупотребления; юридические системы должны разрешать сохранение и быстрый доступ к данным в электронной форме (не требующий разрешений государств, на территориях которых они находятся) представителей охраны правопорядка для проведения более успешного расследования преступлений; режимы оказания взаимной помощи должны способствовать своевременному сбору и обмену уликами по делам, относящимся к международным преступлениям с применением современных информационных технологий; необходимо разработать и применять судебные стандарты получения и определения подлинности электронных данных для использования при расследовании уголовных преступлений и судебном преследовании; информационные телекоммуникационные системы должны по возможности разрабатываться в целях оказания помощи в обеспечении защиты и определении случаев злоупотреблений, а также способствовать выявлению преступников и сбору улик; работа в данной области должна быть скоординирована с деятельностью других родственных международных организаций для предотвращения дублирования их усилий.

В соответствии с указанными принципами ключевым положением борьбы с преступностью в сфере высоких технологий (с учетом скорости электронных коммуникаций и недолговечности электронных доказательств) является наличие возможности международного доступа к национальной компьютерной информации.

Ключевым положением борьбы с преступностью в сфере высоких технологий (с учетом скорости электронных коммуникаций и недолговечности электронных доказательств) является наличие возможности международного доступа к национальной компьютерной информации.

Примером взаимоприемлемого сотрудничества правоохранительных органов различных стран (связанного по сути дела с вопросами электронного документооборота) является Соглашение о сотрудничестве государств-участников Содружества Независимых государств в борьбе с преступлениями в сфере высоких технологий, которое было подписано в Минске 1 июня 2001 г.

Согласно положениям этого Соглашения стороны должны обмениваться информацией о готовящихся или совершенных преступлениях и причастных к ним физических и юридических лицах, о формах и методах предупреждения, выявления, пресечения, раскрытия и расследования преступлений, о способах их совершения, о национальном законодательстве и международных договорах, регулирующих вопросы предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере компьютерной информации, исполняют запросы о проведении соответствующих оперативно-розыскных мероприятий, а также процессуальных действий согласно международным договорам о правовой помощи, проводят скоординированные операции по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере компьютерной информации, оказывают друг другу содействие в подготовке квалифицированных кадров, а также в создании соответствующих информационных систем, проведении совместных научных исследований по представляющим взаимный интерес проблемам борьбы с преступлениями в сфере компьютерной информации и другое.

К указанному выше следует добавить, что в законодательном порядке должны также получить развитие национальные нормы, которые создают возможность проведения совместных с зарубежными службами расследований в информационно-электронном пространстве, охватывающем территорию данного государства. Так, в некоторых случаях проведение трансграничного розыска вполне допустимо осуществлять без официального разрешения соответствующей стороны, но с последующим уведомлением по каналам национального контактного пункта государства, в котором он проводится. Такие случаи могут касаться работы с общедоступными данными, находящимися в открытых источниках (базах), либо законного согласия лица, которое имеет полномочия на разрешение доступа к конкретным данным. В качестве официальных оснований для представления конкретной (ограниченной по времени) возможности действовать в национальном информационно-электронном пространстве следует рассматривать решение судебного или иного правоприменительного органа в запрашиваемого государства в соответствии с традиционными процедурами оказания правовой помощи. При этом важно, чтобы национальные правовые системы были адаптированы к функционированию в условиях развития информационно-электронной среды.

Представляется, что учет этих положений на начальном этапе развития электронного документооборота в России является весьма актуальным.