ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ СРЕДСТВ СВЯЗИ ПРИ СОВЕРШЕНИИ БАНКОВСКИХ СДЕЛОК

А.Г. Фабричнов

Кафедра гражданского и трудового права
Российский университет дружбы народов
ул. Миклухо-Маклая, 6, Москва, Россия, 117198

В статье рассматриваются вопросы нормативного определения термина «электронные средства связи», а также особенности применения этих средств при совершении банковских сделок в контексте информационной безопасности. Анализируя содержание нормативно-правовых актов, автор выделяет уровни информационной безопасности и предлагает способы их обеспечения.

Реалии современной жизни таковы, что ее невозможно представить без электронных средств передачи информации. Информационно-коммуникационные технологии играют все большую роль в жизни человека. В настоящее время в средствах массовой информации и научных изданиях чаще стали упоминаться сделки, совершение которых происходит при помощи электронных средств связи. Повсеместное развитие получил институт «электронной торговли», но и не только он, посредством электронных средств связи совершается множество сделок в различных сферах экономики, в том числе банковской, биржевой и других, что требует определенного нормативно-правового регулирования. Предметом данного исследования является процесс использования электронных средств связи при совершении банковских сделок, а так как эти сделки требуют особых условий, в том числе определенной безопасности, то встает необходимость освещения рассматриваемого вопроса в контексте информационной безопасности.

Практика показывает, что большинство банковских договоров заключается в письменной форме. Договор в письменной форме может быть заключен путем составления одного документа, подписанного сторонами, а также путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору [1]. В Гражданском кодексе Российской Федерации (далее — ГК РФ) не установлен исчерпывающий перечень видов связи, посредством которых могут быть переданы документы для заключения договора в письменной форме. Становится понятным, что электронный вид связи может быть использован в качестве такового. Но необходимо указать на то, что документы передаются ни только и ни за счет определенного вида связи, а путем использования определенных средств. Следовательно, анализ возможности использования какой-либо связи в гражданских правоотношениях, в том числе и банковских, необходимо проводить в ракурсе изучения средств этой связи. Рассмотре-

ние средств осуществления электронной связи предполагает собственно рассмотрение электронных средств связи.

Для определения условий использования электронных средств связи при совершении банковских сделок необходимо определить понятие термина «электронные средства связи» и попытаться очертить круг данных средств.

Понятие «электронное средство связи» встречается в большей степени в технической литературе, и оно является обширным. Но для достижений целей работы необходимо обратиться к нормативно-правому определению данных средств.

В переводах современных иностранных и международных нормативно-правовых актов, регламентирующих «электронную торговлю», часто используется термин «электронные средства связи».

Рассматривая отечественное законодательство, отметим, что в Законе о связи [4] не содержится определения термина «электронные средства связи», но присутствуют два термина — «средства связи» и «электросвязь».

В технической литературе под электронными средствами связи понимается техника передачи информации из одного места в другое в виде электрических сигналов, посылаемых по проводам, кабелю, оптоволоконным линиям или вообще без направляющих линий.

Исходя из вышеуказанных определений, можно сделать вывод, по мнению автора, что телефон, телеграф, телетайп, факс являются электронными средствами связи, но дальнейший анализ нормативных актов показывает, что это спорный вопрос. Возвращаясь к ст. 434 ГК РФ, видно, что законодатель обособил телеграфную, телетайпную, телефонную, электронную связь. Данное разграничение содержится еще в ряде актов, например в ч. 1 ст. 4 Соглашения стран Содружества Независимых Государств от 22.01.1993 «Об учреждении Межгосударственного Банка» [2] указано, что передача всей информации по платежам между центральными (национальными) банками и Банком производится по телефону, телексу, телеграфу или через электронные средства связи.

Типовой закон ЮНСИТРАЛ об электронной торговле указывает, что электронные средства включают в себя электронный обмен данными, электронную почту, телеграф, телекс, телефакс и другие электронные средства, предназначенные для подготовки, отправки, получения и хранения сообщений данных. К электронным средствам согласно Директиве Европейского парламента 98/34/ЕС относится электронное оборудование, предназначенное для обработки (включая цифровое сжатие), хранения, отправки, передачи и получения данных посредством кабельных и радиолиний связи, оптических и других электромагнитных средств.

Приведенные примеры говорят о том, что в современной правовой доктрине нет однозначного суждения, что понимать под электронными средствами связи. Ориентируясь на нормы ГК РФ и других нормативно-правовых актов, можно классифицировать электронные средства по признаку функциональности:

- электронные средства связи, посредством которых создаются, хранятся, передаются электронные документы;
- электронные средства связи, посредством которых создаются, хранятся, передаются электронные сообщения.

На основе полученных результатов возможно определить электронные средства связи как технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений в виде электрических (электронных) сигналов, посылаемых по проводам, кабелю, оптоволоконным линиям или вообще без направляющих линий.

Возвращаясь к теме работы, нельзя не сказать, что главным условием использования электронных средств связи при заключении договоров в письменной форме является то, что с помощью этих средств должны передаваться не просто сообщения, а документы, точнее, электронные документы.

Понятие «документ» несет в себе правовую направленность, существуют определенные критерии документов. Можно сделать вывод, что электронный документ должен обладать определенными свойствами: защищенность от искажения информации, защищенность от доступа третьих лиц, наличие определенного перечня реквизитов и другие. И в этой связи необходимо рассмотреть электронную цифровую подпись как неотъемлемый реквизит электронного документа, защищающего его от несанкционированного доступа с целью предотвращения искажения информации и позволяющего идентифицировать автора официального письменного документа. В ст. 11 Федерального закона «Об информации, информационных технологиях и о защите информации» есть прямое указание на это: «В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами» [5].

Определив допустимость использования электронных документов в гражданско-правовых отношениях, можно охарактеризовать электронные средства связи, с помощью которых происходит формирование, прием, обработка, хранение, передача, доставка электронных документов.

Итак, электронные средства связи, в частности электронно-вычислительные машины и электронные сети, для нужд гражданского оборота должны иметь функциональную многогранность, соответствующее программное обеспечение, защищенность от воздействия третьих лиц, защищенность от сбоев в работе, высокую производительность и другие признаки, исчерпывающий перечень которых невозможно дать в рамках работы в сфере права.

Внедрение электронных средств связи в гражданско-правовые отношения имеет множество положительных тенденций, но не стоит забывать и об угрозах такого внедрения. К положительным качествам использования электронных средств связи при заключении договоров следует отнести: экономию времени, отсутствие человеческого фактора (т.е. некоторых ошибок), увеличение скорости оборота капитала, развитие новых договорных отношений, снижение расходов по заключению сделок. К отрицательным качествам можно отнести: ненадежность используемых средств, неустойчивость электронной информации к искажению, отсутствие доверия к использованию электронных средств связи при решении крупных вопросов, определенные правовые пробелы и неточности. На фоне этого вопросы информационной безопасности приобретают первостепенное значение.

Под информационной безопасностью понимается состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. Информационная безопасность организации банковской системы Российской Федерации в ряде случаев понимается как состояние защищенности интересов (целей) организации банковской системы Российской Федерации в условиях угроз в информационной сфере.

В стандарте Банка России [3] приводится совокупность свойств информационной безопасности: конфиденциальность, целостность, доступность информационных активов и инфраструктуры.

Состояние защищенности информации достигается путем проведения конкретных мер по ее защите. В соответствии с законом об информации, информационных технологиях и о защите информации [5] защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

Банковские сделки занимают большую часть в гражданском обороте по объему денежной массы. Поэтому они всегда являлись объектом для различных «мошеннических» действий, а с приходом новых технологий в процесс совершения таких действий в отношении банковских сделок стало еще больше, и защита сделок от преступных посягательств является достаточно актуальной проблемой в банковском бизнесе.

Применение электронных средств связи в процессе совершения банковских сделок носит двусмысленный характер с точки зрения защиты информации. С одной стороны, применение современных технологий имеет положительные черты: минимизирует риски, связанные с человеческим фактором (исключает ошибки, которые может допустить человек); ускоряет процессы передачи информации, уменьшая количество звеньев в цепи передачи информации; позволяет шифровать важную информацию и т.д. С другой стороны, применение современных информационно-коммуникационных технологий несет ослабления в систему защиты информации: ненадежность электронных средств связи, возможность стороннего несанкционированного доступа, возможность искажения информации и т.д.

Рассматривая процесс применения электронных средств связи при совершении банковских сделок, можно говорить о двух технологических проблемах (уровнях, задачах) информационной безопасности (защиты информации):

- непосредственная защита процесса совершения сделки;
- защита информации о сделке, ее субъектах, в частности персональных данных, предмете, объекте и т.д.

Защита информации (сведений) о проводимой сделке и непосредственная защита совершения самой сделки — два разных процесса. Хотя ряд мер по защите

информации могут применяться в обоих случаях, но проблемы правового регулирования будут несколько расходиться.

В сфере защиты информации о сделке, ее субъектах необходимо сказать о защите персональных данных: операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением некоторых случаев.

Для надлежащего совершения банковской сделки с помощью электронных средств связи необходимо обеспечить защиту от следующих угроз:

- умышленное несанкционированное раскрытие, модификация или уничтожение информации;
- неумышленная модификация или уничтожение информации;
- недоставка или ошибочная доставка информации;
- отказ в обслуживании или ухудшение обслуживания электронных средств связи;
- отказ от авторства сообщения;
- внесение изменений в функционирование электронных средств связи.

Защита от перечисленных угроз может обеспечиваться с помощью: идентификации, аутентификации, авторизации, управления доступом, контроля целостности, регистрации. Также стандарт Банка России содержит комплекс мер по обеспечению информационной безопасности банковского платежного технологического процесса, который предусматривает:

- защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации платежных документов;
- минимально необходимый, гарантированный доступ сотрудника организации банковской системы Российской Федерации только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения служебных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;
- контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации;
- аутентификацию обрабатываемой платежной информации;
- двустороннюю аутентификацию автоматизированных рабочих мест, участников обмена платежной информацией;
- восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
- авторизованный ввод платежной информации в автоматизированные банковские системы двумя сотрудниками с последующей программной сверкой результатов ввода на совпадение (dual control);
- сверку выходных платежных сообщений с соответствующими поступившими платежными сообщениями;
- гарантированную доставку платежных сообщений участникам обмена.

Банковская организация должна выполнять рекомендуемые нормы, так как в некоторых случаях она может понести ответственность за несоблюдение и непроведение мер информационной безопасности в соответствии с российским законодательством. Организация банковской системы Российской Федерации несет ответственность за:

- достоверность информации, официально предоставляемой внешним организациям и гражданам;

- достоверность и выполнение регламента предоставления внешним организациям и гражданам информации, обязательность и порядок предоставления которой определены законодательством Российской Федерации и/или нормативными документами Банка России;

- обеспечение соответствующего законодательству Российской Федерации уровня защиты как собственной информации, так и информации, официально полученной из внешних организаций и от граждан.

В приведенном перечне действий организации банковской системы Российской Федерации, влекущих за собой ответственность, все действия относятся к одному «уровню» информационной безопасности относительно темы данного исследования, — защите информации о сделке, ее субъектах, в частности персональных данных, предмете, объекте и т.д.

Что же касается другого уровня — непосредственной защиты совершения самой сделки, то в данном случае банковская организация будет нести в основном гражданско-правовую ответственность, соизмеримую с ущербом, поэтому у организации есть хорошая финансовая мотивация для обеспечения информационной безопасности в соответствии с нормативными правовыми актами.

Правовые основы информационной безопасности и защиты информации в банковской системе определяют соответствующие положения Конституции Российской Федерации, Гражданского кодекса Российской Федерации, Федеральных законов «Об информации, информационных технологиях и о защите информации», «О коммерческой тайне», «О Центральном банке Российской Федерации», «О банках и банковской деятельности», «О техническом регулировании» и др. Кроме того, банковская организация должна руководствоваться нормативными документами ФСБ России, ФСО России, Министерства информационных технологий и связи России, Банка России и других министерств и ведомств, действующими стандартами в области защиты информации.

Кроме того, ключевой особенностью использования электронных средств связи при совершении банковских сделок является то, что правила и способы использования этих средств, корреспондирующиеся с мероприятиями по обеспечению информационной безопасности, помимо вышеназванных актов должны быть надлежащим образом закреплены во внутренних документах конкретной банковской организации: инструкциях, положениях, правилах, регламентах и т.д.

ЛИТЕРАТУРА

1. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 №51-ФЗ (ред. от 01.12.2007) // Собрание законодательства Российской Федерации. — 1994. — № 32. — Ст. 3301.

2. Соглашение стран Содружества Независимых Государств от 22.01.1993 «Об учреждении Межгосударственного банка» // Вестник Банка России. — 1999. — № 64.

3. Стандарт Банка России СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» / Принят и введен в действие распоряжением Центрального банка Российской Федерации от 26.01.2006 №Р-27 // Вестник Банка России. — 2006. — № 6.

4. Федеральный закон от 07.07.2003 №126-ФЗ (ред. от 29.12.2006) «О связи» // Собрание законодательства Российской Федерации. — 2003. — № 28. — Ст. 2895.

5. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. — 2006. — № 31 (ч. 1). — Ст. 3448.

6. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. — 2006. — № 31 (ч. 1). — Ст. 3451.

FEATURES OF USE OF AN ELECTRONIC COMMUNICATION FACILITY AT MODERN BANK TRANSACTIONS

A.G. Fabrichnov

The Department of Civil and Labor Law
Peoples' Friendship University of Russia
Mikluho-Maklaya st., 6, Moscow, Russia, *117198*

In article are considered questions of normative definition of the term «an electronic communication facility», and also features of application of these means are considered at fulfillment of bank transactions in a context of information safety. Analyzing the maintenance of legal certificates, the author allocates levels of information safety and offers ways of their maintenance.