# Актуальные вопросы предварительного расследования уголовных дел о мошенничестве

К.О. Семенов
*Помощник прокурора ЗАТО г. Саров Нижегородской области, юрист 3 класса*

Федеральным законом от 29.11.2012 N 207–ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» общий состав мошенничества законодателем был дополнен шестью специальными составами мошенничества.

Несмотря на то, что новые составы преступлений в Уголовном кодексе Российской Федерации (далее – УК РФ) действуют уже более четырех лет, при осуществлении предварительного расследования органами дознания и предварительного следствия в правоприменительной практике возникают некоторые проблемы.

По мнению отдельных специалистов, специальные составы мошенничества являются квалифицированными[1].

Вместе с тем, анализ санкции, указанной в статье 159.6 УК РФ, позволяет сделать вывод о том, что мошенничество в сфере компьютерной информации является привилегированным составом преступления по отношению к общему составу мошенничества.

Например, частью 1 статьи 159 УК РФ предусмотрено наказание в виде лишения свободы, тогда как санкция части 1 статьи 159.6 УК РФ такого наказания не предусматривает вообще.

Кроме того, необходимо учитывать, что примечанием к статье 159.1 УК РФ установлены иные квалифицирующие признаки размера хищения. Так, крупным размером в настоящей статье, а также в статьях 159.3, 159.5, 159.6 признается стоимость имущества, превышающая один миллион пятьсот тысяч рублей, а особо крупным – шесть миллионов рублей.

Таким образом, законодатель, выделяя специальные составы преступления, связанные с мошенничеством, по всей вероятности руководствовался тем, что общественная опасность указанных преступлений ниже, чем общественная опасность общего состава мошенничества, поскольку, в соответствии с уголовно–правовым принципом справедливости, предусмотренным статьей 6 УК РФ, наказание, при–

меняемое к лицу должно быть справедливым, то есть соответствовать характеру и степени общественной опасности преступления.

Более подробно хотелось бы остановиться на составе преступления, предусмотренном ст.159.6 УК РФ – мошенничестве в сфере компьютерной информации.

Данный состав преступления отличается от общего состава мошенничества вследствие различий в объективной стороне преступления, а именно в способе совершения преступления.

Если в мошенничестве способом завладения имущества или приобретения права на чужое имущество служат обман или злоупотребление доверием, то в мошенничестве в сфере компьютерной информации таким способом являются: ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно–телекоммуникационных сетей, то есть фактически употребляется терминология составов преступлений, предусмотренных статьями 272–274 УК РФ.

По мнению профессора В.И. Гладких, под вводом компьютерной информации понимается размещение сведений в устройствах ЭВМ для их последующей обработки и (или) хранения.

Удаление компьютерной информации представляет собой совершение действий, в результате которых становится невозможным восстановить содержание компьютерной информации и (или) в результате которых уничтожаются носители компьютерной информации.

Под блокированием компьютерной информации понимается совершение действий, приводящих к ограничению или закрытию доступа к компьютерной информации, но не связанных с ее удалением.

Модификацией компьютерной информации является совершение любых изменений сведений (сообщений, данных), представленных в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Наконец, вмешательство в функционирование средств хранения, средств обработки, средств передачи компьютерной информации, информационно–телекоммуникационные сети  это осуществление неправомерных действий, нарушающих установленный процесс обработки, хранения, использования, передачи и иного обращения с компьютерной информацией[2].

Согласно правовой позиции, изложенной в пункте 12 Постановления Пленума Верховного Суда РФ от 27 декабря 2007 г. N 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» как мошенничество квалифицируется безвозмездное обращение лицом в свою пользу или в пользу других лиц денежных средств, находящихся на счетах в банках, совершенное с корыстной целью путем обмана или злоупотребления доверием (например, путем представления в банк поддельных платежных поручений, заключения кредитного договора под условием возврата кредита, которое лицо не намерено выполнять).

Вместе с тем, само по себе мошенничество отграничивается от кражи за счет различий в объективной стороне преступления, а именно характерного способа совершения хищения в мошенничестве – путем обмана или злоупотребления доверием.

Так, диспозицией статьи 159.6 УК РФ данный элемент объективной стороны общего состава мошенничества нивелируется, от чего произвести разграничение мошенничества и кражи с использованием ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно–телекоммуникационных сетей не представляется возможным.

Совершение данного преступного деяния возможно исключительно посредством использования современных компьютерных технологий. Компьютерная информация – это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ. Особенность компьютерной информации заключается в следующем: она относительно просто пересылается, преобразовывается, размножается; при изъятии информации, в отличие от изъятия вещи, она легко сохраняется в первоисточнике; доступ к одному и тому же файлу, содержащему информацию, могут одновременно иметь несколько пользователей.

Согласно ст. 6 Федерального закона от 27.07.2006 N 149–ФЗ «Об информации, информатизации и о защите информации» информационные ресурсы находятся в собственности юридических и физических лиц, включаются в состав их имущества, на них распространяется действие гражданского законодательства.

Преступления в сфере информационных технологий включают взлом паролей, кражу номеров кре–

дитных карточек и других банковских реквизитов. В последнее время распространен способ завладения денежными средствами на банковской карте через системы удаленного доступа к управлению счетом (например, систему «Мобильный банк» в ОАО «Сбербанк России»)

Так, например Чекунов И.Г. утверждает, что наиболее привлекательной мишенью киберпреступников является «интернет–банкинг». При этом он выделяет основную цель злоумышленников по отношению к банковским учреждениям – незаконное обогащение путем несанкционированного снятия денежных средств[3].

Стоит отметить, что в конце прошлого века многим государствам пришлось столкнуться с новыми видами преступлений, такими как манипуляции с компьютерными системами и компьютерный шпионаж, которые трудно «подвести» под действующее уголовное законодательство.

Зачастую, сложно установить и тем более доказать как сам факт такого уголовного деяния, так и государственно–географическое место и лицо, его совершившее, отсюда возникают проблемы, касающиеся экстерриториальности и юрисдикционности.

Действительно, на практике возникает множество проблем еще на стадии разрешения сообщения о преступлении. Так, во многих случаях при проведении процессуальной проверки по сообщению о преступлении, в соответствии со ст. 144 Уголовно–процессуального кодекса Российской Федерации (далее – УПК РФ), определить либо установить место совершения противоправного деяния в рамках проверки затруднительно, а подчас и невозможно.

В связи с этим, должностными лицами органов внутренних дел данные сообщения зачастую направляются по территориальности в иные органы внутренних дел, которые могут находиться в других субъектах Российской Федерации, что, однако, не препятствует их возвращению обратно.

Вместе с тем, неоднократное направление сообщений о преступлении по территориальности в иные органы, в частности, при наличии достаточных данных, указывающих на признаки преступления, нарушает требования статьи 6.1 УПК РФ о разумности сроков уголовного судопроизводства, а также права потерпевших в результате преступного посягательства на имущество либо имущественные права, что требует немедленного принятия мер прокурорского реагирования и разрешения прокурором вопроса о территориальной подследственности.

Серьезной проблемой, по–прежнему, является отсутствие скоординированного взаимодействия между правоохранительными органами. Так, довольно часто поручения о проведении следственных или розыскных действий в других субъектах выполняются несвоевременно либо не выполняются вообще, несмотря на установленный частью 1 статьи 152 УПК РФ срок в 10 суток для выполнения поручений.

Стоит отметить, что зачастую мошенничество, в частности совершаемое в сфере компьютерной информации, связано с хищением средств с текущих счетов граждан и организаций, являющихся их банковскими счетами в кредитных организациях.

Часть 1 ст. 857 Гражданского кодекса Российской Федерации указывает, что банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте.

В соответствии со статьей 26 Федерального закона от 02.12.1990 N 395–1 «О банках и банковской деятельности» информация об операциях, о счетах и вкладах клиентов и корреспондентов кредитных организаций представляет банковскую тайну.

Следует отметить, что справки по счетам и вкладам физических лиц, по операциям и счетам юридических лиц и индивидуальных предпринимателей, выдаются кредитной организацией им самим, а при наличии согласия руководителя следственного органа – органам предварительного следствия по делам, находящимся в их производстве.

Таким образом, для органов предварительного следствия предусмотрена возможность внесудебного порядка принятия решения о получении информации, содержащей банковскую тайну.

Кроме того, для получения информации, на которую распространяется режим конфиденциальности, положениями УПК РФ предусмотрен судебный порядок.

В силу части 3 статьи 183 УПК РФ выемка предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, предметов и документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях, производится на основании судебного решения, принимаемого в порядке, установленном статьей 165 УПК РФ.

Вместе с тем, следует учитывать, что предварительное расследование преступлений, связанных с мошенничеством без квалифицирующих признаков (например, ч. 1 ст. 159 УК РФ), проводится, в силу п.1 ч. 3 ст. 150 УПК РФ, в форме дознания.

Такое положение вещей ставит в неравное положение дознавателя и следователя при проведении

предварительного расследования уголовных дел, в частности по хищению денежных средств с банковского счета.

Представляется, что в данном законодательном положении обосновывается стремление законодателя обеспечить конфиденциальность информации в случаях, когда инициатором запроса являлись органы дознания, в связи с рассмотрением сообщений о преступлениях в порядке, предусмотренном ст. ст. 144 и 145 УПК РФ.

Однако установленная законом возможность отказа в предоставлении указанных сведений дознавателю в рамках возбужденного уголовного дела является нормой, влекущей препятствия в проведении эффективного дознания, что влечет впоследствии нарушение разумных сроков уголовного судопроизводства, а также принятие дознавателями незаконного либо необоснованного решения по результатам предварительного расследования.

Вместе с тем, представляется, что возможность получения указанной информации путем выемки, в соответствии с ч.3 ст.183 УПК РФ требующей принятия судебного решения, значительно снижает эффективность проведения предварительного расследования, ставит необходимостью сбор дополнительных данных, подтверждающих обоснованность выемки, что сопровождается значительными потерями времени, что является критичным при расследовании преступлений, связанных с мошенничеством, особенно в сфере компьютерной информации.

Кроме того, причинами отказа в предоставлении органам внутренних дел сведений, составляющих банковскую тайну, являются:

– отсутствие в запросах исчерпывающих данных, позволяющих установить его обоснованность, в частности сведений о возбужденном уголовном деле, о материалах проверки сообщений о преступлениях и документах, на основании которых проводится проверка, и т.д.;

– отсутствие в запросах органов предварительного следствия по делам, находящимся в их производстве, сведений о согласии руководителя следственного органа;

– подписание запросов неуполномоченными должностными лицами;

– наличие технических ошибок, в частности неточное указание реквизитов организаций, отсутствие гербовой печати в запросах;

– требование кредитной организации представить копию обращения, в связи с которым запрашиваются сведения[4].

Не стоит забывать, что, хотя дознаватели не обладают такой процессуальной самостоятельностью как следователи, однако состоят, в силу положений УПК РФ, в отношениях процессуальной подчиненности перед начальником подразделения дознания и прокурором.

Более того, Федеральным законом от 30.12.2015 N 440–ФЗ «О внесении изменений в Уголовно–процессуальный кодекс Российской Федерации в части уточнения полномочий начальника органа дознания и дознавателя» УПК РФ был дополнен статьей 40.2, в соответствии с которой в уголовном судопроизводстве появилась новая фигура, наделенная полномочиями по осуществлению контроля по отношению к дознавателям начальник органа дознания.

Начальник органа дознания имеет сходные с руководителем следственного органа (в части контроля за действиями дознавателей) полномочия, указанные в статье 40.2 УПК РФ.

Представляется необходимым, по аналогии с предоставленной следователям в рамках предварительного следствия возможностью получения по согласию руководителя следственного органа информации, содержащей банковскую тайну, внести изменения в статью 26 Федерального закона от 02.12.1990 N 395–1 «О банках и банковской деятельности» в части наделения дознавателя в рамках дознания полномочиями по получению сведений по счетам и вкладам физических лиц и организаций с согласия начальника органа дознания.

Данные изменения позволят правоохранительным органам эффективнее противодействовать развивающимся с каждым днем методам и средствам совершения хищений денежных средств со счетов граждан и организаций.

---

1. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Г.Н. Борзенков, А.В. Бриллиантов, А.В. Галахова и др.; отв. ред. В.М. Лебедев. 13–е изд., перераб. и доп. М.: Юрайт, 2013.

2. Гладких В.И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. 2014. N 22. С. 25–31.

3. Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. 2012. N 2. С. 37–44.

4. Сидоркин А.И. Практика применения органами внутренних дел законодательства в сфере охраняемой законом тайны // Российский следователь. 2015. N 21. С. 37–43.