1.7. КОМПЬЮТЕРНОЕ МОШЕННИЧЕСТВО

Рагулина Анастасия Вячеславовна, канд. юрид. наук. Должность: доцент. Место работы: Московский государственный юридический Университет имени О.Е. Кутафина. Подразделение: кафедра уголовного права. Должность: заместитель директора по научной работе. Место работы: юридическая группа «Яковлев и партнеры».

Аннотация: В работе рассмотрены проблемы квалификации мошенничества в сфере компьютерной информации. В правоприменительной деятельности возникает ряд вопросов, связанных с уяснением понятий, содержащихся в ст. 159.6 УК РФ. Это связано с тем, что используемые в ней термины не имеют законодательной дефиниции и не разъясняются Верховным Судом. Предлагается внести соответствующие изменения в действующий уголовный закон, предусмотрев в нем статью о хищении чужого имущества путем использования электронной информации.

Ключевые слова: право на имущество, компьютерная информация, доступ к компьютерной информации, блокирование, модификация, удаление компьютерной информации, иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

COMPUTER FRAUDULENCE

Ragulina Anastasia Vyacheslavovna, PhD at law. Position: associate professor. Place of employment: Moscow statre law university named after O.E.Kutafin. Department: Criminal law chair. Position: Deputy director on scientific work. Place of employment: Yakovlev and Partners Legal advisors group.

Annotation: The article examines the problems of qualification of fraudulence in the sphere of computer information. There is a set of questions connected with understanding the concepts contained in the article 159.6 of the Criminal Code of the RF. The reason for it is absence of legal definitions and interpretations of the Supreme Court of used in this article concepts. The author proposes to amend the active law by adding the article about stealing another's property with the use of electronic information.

Keywords: title of property, computer information, access to computer information, blocking, modifying, clear-up of computer information, other interference in functioning of devices for storage, processing or transfer of information.

В последние несколько лет мошенничество в сфере компьютерной информации получило большое распространение. Это связано с развитием информационного общества, в котором информация становится главным ресурсом. Все больше преступлений совершается в интернет пространстве. Если раньше такие деяния встречались крайне редко, то теперь они постоянный компонент современной преступности.

В 2012 году была введена ст. 159.6 УК РФ, в которой предусмотрена ответственность за мошенничество с использованием компьютерной информации. Рассматриваемое преступление заключается в хищении чужого имущества или приобретении права на чужое имущество путем ввода, копирования, удаления, блокирования, модификации компьютерной информации. Пожалуй, данный вид мошенничества, на сегодняшний день, вызывает самое большое количество вопросов, связанных с пониманием признаков, описанных в диспозиции компьютерного мошенничества, что приводит к неправильной уголовно-правовой квалификации содеянного.

Так, например, у следователя или судьи возникает проблема при уяснении отдельных понятий, содержащихся в ст. 159.6 УК РФ. Это связано с тем, что используемые в ней термины не имеют законодательной дефиниции и не разъясняются Верховным Судом. Поэтому судья, прокурор и следователь вынуждены обращаться к доктринальному их толкованию, которое носит авторский, персонифицированный и, как следствие, противоречивый характер. Таким образом, считаем целесообразным рассмотреть наиболее дискуссионные вопросы, связанные с пониманием признаков компьютерного мошенничества.

Первый вопрос касается соотношения ст. 159 УК РФ и ст. 159.6 УК РФ. Считается ли, что компьютерное мошенничество является привилегированным по отношению к простому мошенничеству? По всей видимости, ответ на этот вопрос будет положительным, поскольку об этом свидетельствуют их санкции.

Предметом преступления, ответственность за которое предусмотрена в ст. 159.6 УК РФ выступает чужое имущество. Что касается права на чужое имущество, то здесь хотелось бы отметить, что само по себе рассматриваемое право невозможно присвоить в отрыве от материального носителя, его закрепляющего. Таким образом, похищается материальное выражение этого права. Конечно, можно совершить хищение материального носителя права, воздействуя определенным образом на компьютерную информацию. Но как потом получить это имущество в натуре? Нельзя забывать о том, что хищение считается оконченным с момента, когда собственнику или иному владельцу имуществу причинен ущерб.

Как говорится в «Справке-обобщении изучения судебной практике» [1], компьютерная информация с помощью которой виновный осуществляет обманные действия и завладевает имуществом, является дополнительным предметом компьютерного мошенничества. Однако, то, с помощью чего совершается преступление, именуется в уголовном праве средством, а не предметом.

Представляется, что преступление, ответственность за которое предусмотрена в ст. 159.6 УК РФ, посягает одновременно на два объекта – собственность и безопасность в сфере компьютерной информации. Таким образом, компьютерная информация, наряду с чужим имуществом выступает предметом преступления, поскольку виновные воздействуя на нее, получают доступ к чужому имуществу.

Далее необходимо отметить, что совершение деяния, ответственность за которое установлена в ст. 159.6 УК РФ, возможно исключительно посредством использования современных компьютерных технологий, однако, как уже говорилось ранее, в диспозиции компьютерного мошенничества не содержится разъяснений специальных терминов в этой сфере. Поэтому, в случаях квалификации содеянного по ст. 159.6 УК РФ, целесообразным будет обращение к нормам Главы 28 УК РФ, предусматривающей ответственность за преступления в сфере компьютерной информации. Так, в примечании 1 к ст. 272 УК РФ раскрывается понятие компьютерной информации, под которой понимаются сведения (сообщения, данные), представлен-

ные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В прежней редакции норм главы 28 УК РФ компьютерная информация находилась в неразрывной связи с машинным носителем, в электронно-вычислительной машиной (ЭВМ), системой ЭВМ или их сетью и именно поэтому она получила такое название. До 7 декабря 2011 г. [2] понятие «компьютер» или «ЭВМ» являлось базовым для определения других понятий.

В настоящее время законодатель пошел по иному пути. В переводе с английского «computer» означает вычислитель. Первоначально в английском языке это слово обозначало человека, производящего арифметические вычисления. Затем этот термин стал использоваться для обозначения автоматических устройств, предназначенных для проведения вычислений, сбора, хранения и передачи информации. Усовершенствование и появление новой техники, которая используется для передачи, хранения и обработки информации - процесс динамичный [3 С. 50-52]. В настоящее время компьютерная информация может содержаться в устройствах, которые внешне не напоминают компьютер. Правоприменительная практика признает компьютерами мобильные телефоны, банкоматы, платежные терминалы. Поэтому логичнее было бы говорить о компьютерных системах. Так, Конвенция о киберпреступности [4] (в российском переводе Конвенция о преступности в сфере компьютерной информации) раскрывает содержание такого понятия как компьютерная система - любое устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных.

Использование термина «компьютерная информация» также выглядит не совсем логичным и корректным. Представляется, что его следует заменить на понятие «электронная информация», так как компьютерная информация является одним из ее видов. Кроме того, ввиду недостаточной ясности термина «электрический сигнал», используемый для раскрытия понятия «компьютерной информации», представляется необходимым изъять его из законодательного определения. Тогда под электронной информацией можно было бы понимать сведения (сообщения, данные), представленные в электронно-цифровой форме, независимо от средств их хранения, обработки и передачи».

Анализируя состав преступления, ответственность за которое установлена в ст. 159.6 УК РФ, необходимо отметить, что в основном составе мошенничества дается его понятие, предусматривающее два альтернативных способа, а именно – обман или злоупотребление доверием.

В диспозиции нормы о мошенничестве в сфере компьютерной информации указаны еще и такие способы, как: ввод, удаление, блокирование, модификация компьютерной информации или иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Таким образом, мошенничество в сфере компьютерной информации должно характеризоваться как минимум двумя обязательными способами, один из которых предусмотрен в ч. 1 ст. 159 УК РФ, а второй в ч. 1 ст. 159.6 УК РФ.

Специфика второго способа состоит, прежде всего, в различных видах вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. К ним можно отнести:

- хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации;

- хищение чужого имущества или приобретение права на чужое имущество путем иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно - телекоммуникационных сетей.

Ввод компьютерной информации – это взаимодействие двух и более объектов компьютерной информации (один из которых является «агрессором») без изменения структуры программного кода атакуемого объекта. При вводе используется любой алгоритм действий по набору и электронной обработке сведений (сообщений, данных) для их дальнейшего распознания и использования компьютерной техникой. Здесь необходимо заметить, что «ввод» компьютерной информации целесообразно заменить на термин «доступ» к ней, поскольку он в большей мере отражает то воздействие на информацию, которое необходимо при совершении компьютерного мошенничества и является более широким по объему. Ведь невозможно совершать действия с тем, к чему не имеешь доступа. В п. 6 ст. 2 Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" [5] дается определение доступа к информации. Под ним понимается возможность получения информации и ее использование.

Как показывает судебная практика совершение хищения чужого имущества путем доступа к компьютерной информации возможно без ее модификации, удаления, блокирования.

Нофенко Л.С. была осуждена по ст. 159.6 УК РФ совершила хищение чужого имущества путем ввода компьютерной информации посредством информационно-телекоммуникационных сетей при следующих обстоятельствах. Нофенко Л.С., посредством услуги "Мобильный банк", получив на мобильный телефон электронное сообщение о доступном лимите денежных средств в сумме... на не принадлежащем ей банковском счете, открытом на имя Ш., имея умысел на хищение указанной суммы и реализуя его, используя принадлежащий ей мобильный телефон "Samsung" и сим-карту с абонентским номером, зарегистрированным на имя Д., к которой ошибочно подключена услуга "Мобильный банк" Сбербанка России, предоставляющая право распоряжаться денежными средствами, находящимися на расчетном счету на имя Ш. путем ввода компьютерной информации в форме электронных сигналов - "смс-сообщения" на номер "900", посредством телекоммуникационной сети оператора сотовой связи "Билайн", в несколько приемов перечислила (похитила) денежные средства в сумме..., находившиеся на расчетном счете... и принадлежащие Ш., на счет сим-карты с абонентским номером..., причинив Ш. имущественный ущерб на общую сумму... рублей [6].

Приведенный пример как раз является ярким свидетельством того факта, что уголовная ответственность наступила не за ввод информации, а в целом за ее использование.

Настоящее дело вызывает вопросы, которые не нашли ответа в ходе проведенного следствия. Каким образом данные о лимите денежных средств поступили осужденной? Может это была лишь малая часть хорошо продуманной операции? Хакеры, завладев информацией, решили воспользоваться ей в корыстных целях. Однако, понимая, что могут быть обнаружены службой безопасности банка, решили проверить, мож-

но ли отследить движение денежных средств, которыми они пытались завладеть. Для этих целей воспользовались третьим лицом - Нофенко Л.С. Иначе как объяснить возникшую в данном случае цепь случайностей с подключением услуги "Мобильный банк", с наличием сим-карты на имя Д и т.д. Поэтому, скорей всего, до того, как «смс–сообщение» поступило обвиняемой, были произведены соответствующие манипуляции с компьютерной информацией.

Далее, необходимо рассмотреть удаление компьютерной информации, которое представляет собой приведение информации или ее части в непригодное для использования состояние независимо от возможности ее установления [7].

Под блокированием компьютерной информации понимаются преднамеренные действия, заведомо приводящие к кратковременному или длительному затруднению доступа к разрешенным данным. Представляет интерес тот факт, что заблокированные данные не уничтожаются и не изменяются, но доступ к управлению ими имеет лишь лицо (лица), которое изъяло их из обращения.

Модификация компьютерной информации - добавление, изменение, удаление данных с целью получения доступа к компьютерной информации и управления ею. Анализируя модификацию компьютерной информации необходимо отметить, что существует две ее разновидности:

шумовая модификация – удаление информации и замена файла или его части хаотичной последовательностью данных;

смысловая модификация – замена части команд или данных с целью обхода парольной защиты, внесение изменений в финансовые счета с целью извлечения прибыли. Например, фрагмент программы, запрашивающий у пользователя его пароль.

В любом случае, удаление, блокирование, модификация компьютерной информации являются результатом поучения доступа к ней, например, путем введения пароля, кода или идентификационного номера. Это было учтено законодателем при создании ст. 272 УК РФ, согласно которой преступлением является неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Таким образом, из всех перечисленных способов совершения компьютерного мошенничества, только доступ к информации может являться таковым, поскольку остальные выступают его последствием.

Далее необходимо подробнее остановиться на определении иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Как показывает содержания ст. ст. 159.6 УК РФ, иное вмешательство не должно быть связано с действиями по вводу, удалению, блокированию, модификации компьютерной информации.

Пример "иного вмешательства" приводится в Апелляционном определении Московского городского суда от 6 мая 2013 г. N 10-2076. Обстоятельства дела таковы: Д. признан виновным в совершении девяти мошенничеств в сфере компьютерной информации, т.е. хищении чужого имущества путем иного вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации и информативно-телекоммуникационных сетей, группой лиц по предварительному сговору, с причинением значительного ущерба гражданину. А именно, в том, что вступил в сговор с лицами, дело в отношении которых выделено в отдельное производство, на хищение денежных средств со счетов граждан.

Получив информацию о счетах граждан, Д. изготавливал поддельные доверенности и получал дубликаты сим-карт и пароли. Далее, в период времени с 24 октября по 10 декабря 2011 г. Д., используя сим-карты и пароли через электронную систему "*-Онлайн", путем перечисления на счета и банковские карты различных лиц завладевал денежными средствами. Д. был осужден по ч.2 ст. 159.6 УК РФ и по ч. 2 ст. 325 УК РФ [8].

Изложенное позволяет сформулировать вывод, что существует только два способа компьютерного мошенничества. Это получение доступа к компьютерной информации, повлекшее ее удаление, блокирование, модификацию и иное вмешательство, которое, напротив, не должно быть связано с действиями по вводу, удалению, блокированию, модификации компьютерной информации.

Совершая мошенничество в сфере компьютерной информации, преступники могут использовать сразу два способа, так как одного из них будет недостаточно для реализации сложных схем совершения хищения денежных средств из банка. Они могут одновременно получать доступ к компьютерной информации и совершать иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно - телекоммуникационных сетей.

Так, по делу № 1-100/2013 Хамовнический районный суд города Москвы, рассмотрев в открытом судебном заседании материалы уголовного дела в отношении Ливадного А.А., Босс В.И., установил, что:

Ливадный А.А. совместно с ранее знакомой Босс В.И.и другими лицами, из корыстных побуждений, вступил в организованную неустановленным лицом (организатором), устойчивую преступную группу лиц, заранее объединившихся для совершения преступлений: хищений чужого имущества - денежных средств с банковских счетов различных юридических лиц, путем ввода компьютерной информации и иного вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации.

Осуществляя преступный умысел, Ливадный А.А., Босс В.И. и другие участников организованной группы, используя компьютерную технику и различное, в том числе, вредоносное программное обеспечение, технические познания в сфере компьютерной информации, с компьютера, удаленно, посредством сети Интернет, неправомерно, то есть, не имея законного доступа, осуществляли вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации, а именно, входили в компьютерные информационные системы клиентов различных коммерческих банков, обслуживающихся кредитными организациями по системе «Клиент-Банк», «Интернет-Банкинг» и иных аналогичных систем, содержащих информацию обо всех финансовых операциях по счету, включая перечисления и остатки денежных средств, находящихся на расчетом счете клиентов, после чего копировали информацию в электронной цифровой форме о клиентах банков, а именно: название и банковские реквизиты клиентов, пароли, логины и электронные цифровые подписи клиентов банков (или аналоги собственноручной подписи), являющиеся обязательным реквизитом электронного платежного

документа, предназначенного для его защиты от подделки.

Ливадный А.А. и Босс В.И., используя скопированную в электронной цифровой форме компьютерную информацию о клиентах банков, компьютерную технику и различное, в том числе, вредоносное программное обеспечение, дистанционно, посредством сети Интернет, формировали от имени клиентов банков – юридических лиц, подложные электронные платежные поручения о перечислении денежных средств с банковских счетов клиентов банков на счета своих соучастников, открытых в различных коммерческих банках. Другие соучастники осуществляли получение в наличной форме похищенных денежных средств и их дальнейшую передачу неустановленным лицам. Подложные платежные электронные поручения о перечислении денежных средств заверялись скопированной ранее электронной цифровой подписью (или аналогом собственноручной подписи) клиентов банков, данная компьютерная информация вводилась в систему дистанционного банковского обслуживания с использованием систем «Клиент-Банк», «Интернет-Банкинг» и иных аналогичных систем, направлялись в банки для исполнения, где в результате программной обработки и проверки соответствия электронной цифровой подписи клиента в электронном документе, по системе дистанционного банковского обслуживания осуществлялись финансовые операции по счетам клиентов [9].

Как видится, приведенный пример свидетельствует о неполной квалификации содеянного, поскольку копирование компьютерной информации и использование вредоносных программ не нашло своего отражения при квалификации содеянного, в виду чего отсутствует вменение ст.ст. 272 и 273 УК РФ.

Далее необходимо решить вопрос о том, включает ли объективная сторона компьютерного мошенничества в себя действия, образующие состав преступлений, ответственность за которые предусмотрена ст. ст. 272, 273, 274 УК РФ.

На основании анализа судебной практики, следует сделать вывод, что по этому вопросу имеются противоречия и отсутствует единая позиция правоприменителя.

Ранее приводилось несколько примеров, где содеянное охватывалось только ст. 159.6 УК РФ.

Примером подобной квалификации является приговор по делу 1-226/2013 от 03 июня 2013 года в отношении Колонщаков А.В. и Гасанов Р.Р., обвиняемых в совершении преступления, предусмотренного ч. 3 ст. 159.6 УКРФ.

Как было установлено, Колонщаков А.В. и Гасанов Р.Р., имея специальные познания в области компьютерной техники и программного обеспечения, а также обладая опытом работы в сети Интернет и совершенствуя его в процессе ежедневного использования персонального компьютера, применили приобретенные ими навыки для незаконного обогащения.

Изучив информацию, содержащуюся на Интернет-форумах, посвященных хищению денежных средств со счетов агентов систем электронных платежей путём незаконного (без ведома и согласия владельцев) доступа к принадлежащим им, охраняемой законом компьютерной информации об аутентификационных данных, принципы работы системы электронных платежей, конкретные способы хищения денежных средств и сокрытия преступлений, они решили участвовать совместно с другими пользователями сети Интернет – посетителями тематических форумов и сайтов «хакерской» направленности в хищении путём обмана денежных средств со счетов агентов.

С указанной целью Колонщаков, посещая под псевдонимом «Iladium» Интернет форумы «хакерской» направленности - «www.forum.zloy.bz», познакомился там с пользователями, также обладающими специальными познаниями в области компьютерной техники и опытом работы в сети Интернет, в частности неустановленным лицом, выходящим в сеть Интернет под псевдонимами «Den Adel» и «Robusto», с которым предварительно договорился о хищении денежных средств с расчетных счетов агентов.

Далее Колонщаков А.В. привлек к совершению указанного преступления своего знакомого Гасанова Р.Р., который вступил с Колонщаковым и указанным выше не установленным следствием лицом в преступный сговор на хищение денежных средств с расчетных счетов агентов.

Затем, во исполнение задуманного и согласно распределению преступных ролей, неустановленное лицо, выходящее в сеть Интернет под псевдонимами «DenAdel» и «Robusto», владея языками программирования, создавал на неустановленных электронных ресурсах, распространял в сети Интернет и использовал сам вредоносные программы для ЭВМ, предназначенные для осуществления неправомерного доступа к охраняемой законом компьютерной информации об аутентификационных данных агентов, с целью последующего хищения находящихся на их расчетных счетах денежных средств. В последующем, оно же, полученные неправомерно сведения об аутентификационных данных агентов платёжных систем, использовало для совершения хищения денежных средств. Неустановленное лицо посредством сети Интернет сообщало Колонщакову А.В. и Гасанову Р.Р. номера электронных кошельков в сети Интернет, куда необходимо было перечислить в качестве вознаграждения за участие в хищениях денежные средства его долю от суммы похищенного.

Колонщаков А.В. и Гасанов Р.Р., исполняя отведенную им роль в совершении преступления и действуя в рамках заранее достигнутой преступной договоренности, для собственного использования в преступных целях в сети Интернет открывали анонимно счета (кошельки) в электронных платежных системах и приобрели неустановленным способом абонентские номера телефонов (сим-карты) оператора сотовой связи, зарегистрированные на недостоверные анкетные данные абонентов, либо утраченные абонентами, которые посредством сети Интернет, через систему обмена короткими сообщениями (ICQ) предоставляли неустановленному соучастнику, выходящему в сеть Интернет под псевдонимами «DenAdel» и «Robusto» для последующего зачисления на них похищенных денежных средств с расчетных счетов агентов. После зачисления на лицевые счета абонентских номеров телефонов (сим-карт) похищенных денежных средств, они (Колонщаков А.В. и Гасанов Р.Р.) обналичивали их и 25% от общей суммы, переводили на неустановленный кошелек электронной платежной системы «WebMoney Transfer», предоставленный неустановленным соучастником. Оставшимися денежными средствами они (Колонщаков А.В. и Гасанов Р.Р.) распоряжались по собственному усмотрению.

Так, исполняя преступный план, неустановленное лицо, выходящее в сеть Интернет под псевдонимами «Den Adel» и «Robusto», и имеющее в личном пользовании персональный компьютер (ЭВМ), находясь в не

установленном следствием месте, действуя в рамках ранее достигнутой преступной договоренности с Колонщаковым А.В. и Гасановым Р.Р., используя неустановленную вредоносную программу, похитило охраняемую законом компьютерную информацию: аутентификационные данные, а именно электронно-цифровую подпись (далее ЭЦП), которая использовалась агентом для доступа к собственному расчетному счёту, открытому в Обществе с ограниченной ответственностью, и сохранило их на магнитном носителе своего персонального компьютера в форме, воспринимаемой ЭВМ, намереваясь в дальнейшем использовать полученную информацию в корыстных целях, осознавая при этом, что данная информация в силу своего назначения является конфиденциальной и подлежит защите в соответствии с законодательством Российской Федерации.

Затем неустановленный соучастник, проверив баланс расчетного счета агента и выяснив наличие на нем денежных средств, сообщил посредством сети Интернет данную информацию КолонщаковуА.В. и Гасанову Р.Р. и договорился с ними об осуществлении неправомерных перечислений денежных средств с расчетного счета данного агента на лицевые счета абонентских номеров телефонов оператора сотовой связи подысканных Колонщаковым и Гасановым для совершения преступления, определил себе вознаграждение в размере 25 % от общей суммы перечисленных денежных средств.

Колонщаков А.В. с помощью личного персонального компьютера (ЭВМ), посредством сети Интернет, через систему обмена короткими сообщениями (ICQ), предоставил неустановленному соучастнику, выходящему в сеть Интернет под псевдонимами «DenAdel» и «Robusto», приобретенные им и Гасановым Р.Р. абонентские номера телефонов (сим-карты) оператора сотовой связи<данные изъяты>зарегистрированные на недостоверные анкетные данные абонентов, либо утраченные абонентами, для зачисления на них похищенных денежных средств.

Неустановленный соучастник, используя свой персональный компьютер, запустив установленное на нем программное обеспечение ЗАО , создало неустановленным способом виртуальный терминал. После этого с целью дальнейшей реализации своего преступного умысла, не имея согласия представителя, направило от его имени запрос на сервер компании ЗАО на проверку номеров предоставленных Колонщаковым А.В. и Гасановым Р.Р., заверив данные запросы похищенной у ООО ЭЦП, совершив тем самым ввод и модификацию компьютерной информации.

Сервер компании, идентифицировав ЭЦП агента и проверив наличие необходимых для осуществления платежа средств на его расчетном счете, направил запрос в биллинговую систему оператора на разрешение платежей. Получив подтверждение о снятии денежных средств с расчетного счета, отправил данные платежи в биллинг оператора сотовой связи, то есть произвел пополнение лицевых счетов абонентов [10].

Примером другой квалификации может служить следующее дело. Московский городской суд в Постановлении от 19 мая 2015 г. N 4у/10-2543/15 «Об отказе в передаче кассационной жалобы для рассмотрения в судебном заседании кассационной жалобы для рассмотрения в судебном заседании суда кассационной инстанции», изучив поступившую кассационную жалобу адвоката К., поданную в интересах осужденного Ш., о пересмотре приговора Замоскворецкого районного суда города Москвы от 09 февраля 2015 года и апелляционного определения судебной коллегии по уголовным делам Московского городского суда от 01 апреля 2015 года, установил, что: Приговором Замоскворецкого районного суда города Москвы от 09 февраля 2015 года Ш. признан виновным в участии в преступном сообществе (преступной организации) в целях совместного совершения тяжких преступлений; в совершении в составе преступного сообщества неправомерного доступа к охраняемой законом компьютерной информации, повлекшего копирование компьютерной информации, организованной группой (в четырех преступлениях); а также в совершении мошенничества (4 преступления) в сфере компьютерной информации, то есть хищение чужого имущества путем ввода, блокирования, модификации компьютерной информации, организованной группой, в крупном размере.

На основании установленных фактических обстоятельств дела суд правильно квалифицировал действия Ш. по ч. 2 ст. 210 УК РФ (в редакции Федерального закона N 377-ФЗ от 27.12.2009); ч. 3 ст. 272 УК РФ (в редакции Федерального закона N 420-ФЗ от 07.12.2011) - 4 преступления; ч. 4 ст. 159.6 УК РФ - 4 преступления [11].

В свете рассматриваемого вопроса представляет интерес Апелляционное постановление Московского городского суда от 6 июля 2015 г. N 10-9255/2015 говорится о П. ранее судимом, подозреваемом в совершении преступлений, предусмотренных ч. 2 ст. 273 (271 эпизод), ч. 3 ст. 272 (271 эпизод) и ч. 4 ст. 159.6 (271 эпизод) УК РФ [12].

Показательным также является следующее дело. Чертановским районным судом по делу было установлено, что два родных брата - уроженцы г. Санкт- Петербурга совершали хищения денежных средств со счетов клиентов одного из крупных российских банков. Братья Евгений и Дмитрий Попелыши были признаны виновными в совершении преступлений, предусмотренных ч. 2 ст. 272, ч. 1 ст. 273 и ч. 4 ст. 159 УК РФ [13].

Таким образом, как показывает судебная практика, в одних случаях, достаточно квалификации содеянного только по ст. 159.6 УК РФ, а в других необходима дополнительная по ст.ст. 272, 273 УК РФ.

Как правило, если совершение одного преступления является способом другого, то дополнительная квалификация требуется только в случае, если санкция основного преступления менее строгая, чем санкция того, что выступает способом. Сравнивая между собой санкции ст. 159.6 УК РФ и ст.ст. 272,273 УК РФ, становится очевидным, что санкции компьютерных преступлений строже.

Обобщенная судебная практика свидетельствует о том, что в случаях, когда указанные деяния сопряжены с неправомерным внедрением в чужую информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для электронно-вычислительных машин, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ, содеянное подлежит квалификации по статье 159 УК РФ, а также, в зависимости от обстоятельств дела, по статьям 272 или 273 УК РФ, если в результате неправомерного доступа к компьютерной информации произошло уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или

их сети (п. 12 постановления Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» [14]). Здесь следует заметить, что рассматриваемое постановление было принято в 2007 году, когда ст. 159.6 УК РФ еще не было в уголовном законе.

Представляется, что при квалификации следует учитывать тот факт, что:

если хищение осуществляется путем доступа к компьютерной информации, то содеянное полностью охватывается ст. 159.6 УК РФ;

если хищение осуществляется путем доступа к компьютерной информации, повлекший уничтожение, блокирование, модификацию либо копирование компьютерной информации, то содеянное помимо ст. 159.6 УК РФ должно квалифицироваться по ст. 272 УК РФ;

если хищению путем доступа к компьютерной информации предшествовало создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, то содеянное помимо ст. 159.6 УК РФ должно квалифицироваться по ст. 273 УК РФ;

Далее представляется целесообразным обратиться к разновидностям компьютерного мошенничества, которые в последнее время получили широкое распространение.

Например, хищение денежных средств может осуществляться на пути от платежного терминала (POS-терминал) к банку. Здесь следует отметить, что процесс оплаты через платежный терминал называется эквайринг. В том случае, если платежный терминал соединяется с банком посредством Wi-Fi, то сначала сканером сетей определяется к какой точке доступа он подключен для отправки отчетов по денежным операциям в банк. После этого данная сеть взламывается и образуется своя точка доступа. Если POS-терминал соединен с банком посредством GSM связи, то злоумышленники перебивают сигнал GSM точки (устройство, предоставляющее доступ в интернет посредством цифровой сотовой сети), своим собственным сигналом. Таким образом, злоумышленникам становятся известны все данные по производимым транзакциям (процесс перевода денежных средств между банковскими счетами).

Хищение денежных средств может происходить следующим образом: приобретаются платежные терминалы, имеющие прошивку, отличающуюся от заводской. Это позволяет злоумышленникам изменять данные, внесенные при проведении транзакций. Так, например, подходит официант и дает для проведения оплаты «усовершенствованный» платежный терминал, клиент производит оплату, после чего официант говорит, что в банке проводятся технические работы и уведомления о произведенном платеже придет позднее. Посетитель оплачивает счет и уходит. Позднее клиент узнает, что его деньги полностью или частично списаны. Таким образом, владелец лишается своих денежных средств, находящихся на карте.

В последнее время «стали популярны» случаи хищения денежных средств в общественных местах путем использования мощных NFC- считывателей (считывающие и записывающие устройства, взаимодействующее и изменяющее данные на расстоянии, находящиеся на других электронных устройствах) с клоном POS-терминала. Если положить такой считыватель в карман, то, проходя мимо лиц, имеющих с собой карты поддерживающие функцию PayPass (технология бесконтактной оплаты платежей посредством банковской карты), можно списывать с них небольшие суммы денег.

Большая часть атак на компьютерную информацию с целью хищения денежных средств осуществляется с помощью социальной инженерии либо через «своего человека» в банке.

Социальная инженерия представляет собой атаку не на сервер и не на компьютер банка, а на сознание его клиента. Например, преступникам необходимо получить пароль, для чего они высылают письмо от имени сервиса, который сходен с официальным, с уведомлением о том, что с аккаунта клиента был осуществлен несанкционированный вход, в связи с чем предлагается указать старый пароль, для того что бы заменить его на новый. Возможны и другие варианты, такие как: исследование информации, содержащейся в социальных сетях, общение в чате, предложения заполнения анкет в целях выявления ответа на секретный вопрос клиента банка, необходимый для замены пароля.

«Свой человек» в банке может просто предоставить доступ к компьютеру, на котором он работает. Доступ осуществляется с помощью различных способов. В числе которых, например, установка GSM передатчика – промежуточного звена между компьютером и кабелем интернета. Таким образом, отпадает необходимость использовать Фишинг.

Более сложные атаки происходят с помощью внедрения вирусов через провайдера интернета либо подключения к сети банка через коммуникационные коробки. Существует несколько вредоносных программ, среди них можно отметить:

«Carbank» - создана для обмана клиентов банка. С помощью нее происходит замена движка сайта, после чего возможно будет видеть личные данные по тем банковским карточкам, по которым были произведены транзакции.

«Zeus», «SpyEye», «Carber» были созданы для анализа и сбора информации и взлома банковских систем.

В 2014 году появился банковский троян «Zber» , который мог собирать данные о компьютере, перехватывать данные и SSL-сертификаты (с помощью которых происходит передача шифрованных данных) и предоставлять удаленный доступ к компьютеру жертвы по протоколам RDP и VC (с помощью которых происходит удаленное подключение к рабочему столу). А после банковский троян «Kronos», который закрывал все порты и стирал пути произведенных транзакций.

Взлом банковской системы может осуществляться такими методами как:

убедительный фишинг (получение доступа к конфиденциальным данным неопределенного круга лиц);

эксплойты (вид компьютерной программы, использующей уязвимость в программном обеспечении и применяемая для проведении атак на вычислительные системы);

удаленное подключение к уязвимым компьютерам для установки вредного программного обеспечения.

В настоящее время появились команды, способные проводить сложные многомесячные таргетированные атаки (целенаправленная атака против определенного объекта). Они находят брешь в защите банков и уста-

навливают контроль над компьютером в его сети. Далее в банк приходит зараженное письмо:

от имени Банка России;

в банк по системе интернет-банкинга (технология дистанционного банковского обслуживания, а также доступ к счетам и операциям (по ним), предоставляющийся в любое время и с любого компьютера, имеющего доступ в Интернет);

от имени Налогового органа;

письмо в службу поддержки от недовольного клиента, написанного в формате Word или PDF.

При открытии вложенного файла в компьютер внедряется вирус backdoor. Он позволяет беспрепятственно заходить в систему, не взламывая ее. Затем от зараженного компьютера вирус по локальной сети передается остальным. После заражения компьютеров всей системы, начинается поиск компьютера-администратора, который определяется по максимальному уровню доступа к серверам банка. Далее в действие вступают специалисты, которые, получив информацию из различных источников, включая и соцсети, сайты, глубинный интернет, сканирование сети банка, какая автоматическая банковская система (АБС) используется в банке, какие там системы денежных переводов и где находятся серверы АБС и рабочие места сотрудников, осуществляющих переводы денег. Это необходимо для изучения схемы движения средств в банке, с помощью которой будут разработаны схемы вывода средств. Затем обеспечивается вывод средств через открытые специально на этот случай счета в других банках, с последующим обналичиванием средств через дропперов (лицо, обналичивающее денежные средства), которые снимают наличные или регистрируют на себя банковские карты.

Также, существует специально разработана шпионская программа для получения ключей системы дистанционного управления банковскими счетами. Если на компьютере хранятся электронные ключи, то ни в коем случае нельзя использовать его для сторонних целей.

Можно осуществить проникновение в один компьютер банка посредством фишинговых приемов. После заражения машины вредоносным программным обеспечением преступники получали доступ к внутренней сети банков, находили компьютеры администраторов систем денежных транзакций и разворачивали видеонаблюдение за их экранами. Так преступники знали каждую деталь в работе персонала банка и могли имитировать привычные действия сотрудников при переводе денег на мошеннические счета. В описанной ситуации хакерам не пришлось взламывать банковские серверы. Однако, если им необходимо установить контроль над банкоматами, либо уничтожить следы по проведенным транзакциям, то необходим взлом серверов через компьютер администратора.

Представляет интерес тот факт, что вредоносное программное обеспечение, как правило, имеет механизм самоуничтожения, так что обнаружить его после «операции» не возможно.

Примером мошенничества в сфере компьютерной информации могут выступать ситуации, при которых злоумышленник проникает в систему бухгалтерского учета при помощи мошеннических транзакций и увеличивает баланс средств на счете. Поскольку затрагивается внутренняя система банка, то действия преступника остаются незамеченными для его сотрудников. Он заходит на сервер, получает доступ к банкоматам и отправляет от имени банкомата ложную команду о внесении денежных средств на тот или иной счет, пополнение которого на самом деле не производилось. Так, на счете хранится 1 тысяча долларов, однако баланс искусственно увеличивается до 10 тысяч, а затем осуществляется перевод 9 тысяч. В этом случае владелец счета ничего не узнаёт, поскольку его деньги остаются на месте. Ущерб причиняется банку.

Также хотелось бы отметить такую особенность работы службы информационной безопасности банков, которая, тщательно проверяя транзакции клиентов, тем самым слишком много внимания уделяет внешним операциям, оставляя без должного внимания внутренний контроль операций в самом банке.

В свете рассматриваемой темы, представляет интерес тот факт, что перечисленным в ст. 159.6 УК РФ, компьютерным операциям: «вводу», «удалению», «блокированию», «модификации» компьютерной информации, может предшествовать совершение других действий, как с собственной, так и чужой платежной картой с согласия ее владельца. Так Н. приговором Алтайского краевого суда от 17 января 2013 г. (с учетом изменений приговора суда и кассационного определения судебной коллегии по уголовным делам) был признан виновным в совершении преступления, предусмотренного ст. 159.6 УК РФ.

Фактические обстоятельства содеянного заключались в том, что Н., находясь в торгово-развлекательном центре... обратился с просьбой к С. воспользоваться его банковской картой... с целью установления интернет-обслуживания, тем самым дезинформировав С. С., не догадываясь о преступных намерениях Н., выполнил при помощи карты и банкомата операции, указанные Н., тем самым предоставил ему на двух выданных банкоматом квитанциях полную информацию о банковской карте и о находящихся на ней денежных средствах. Затем в тот же день Н., находясь в комнате... общежития, расположенного по адресу... при помощи компьютера и автоматизированной системы... перевел денежные средства, находящиеся на банковской карте С., на банковскую карту своего знакомого З. в размере 12000 руб. Далее Н., находясь в здании... расположенного... через банкомат по банковской карте З. снял данные денежные средства, тем самым причинив потерпевшему С. значительный ущерб в размере 12000 руб [15].

В приведенном случае вмешательство в функционирование средств хранения, обработки, передачи компьютерной информации стало возможным благодаря получению информации о реквизитах банковской карты потерпевшего. Затем в осуществлении виновным лицом операции ввода компьютерной информации - перевод денежных средств с одного банковского счета на другой. То есть, преступление стало возможным «благодаря» действиям потерпевшего по предоставлению реквизитов своей банковской карты виновному лицу.

В этой связи, следует обратиться к ч.11,12 ст. 9 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» [16], в которых установлено, что в случае утраты электронного средства платежа и (или) его использования без согласия клиента клиент обязан направить соответствующее уведомление оператору по переводу денежных средств в предусмотренной договором форме незамедлительно после обнаружения факта утраты электронного средства платежа и (или) его использования без согласия клиента, но не позднее дня, следующего за днем по-

лучения от оператора по переводу денежных средств уведомления о совершенной операции. После получения оператором по переводу денежных средств уведомления клиента в соответствии с ч. 11 ст. 9 настоящего закона оператор по переводу денежных средств обязан возместить клиенту сумму операции, совершенной без согласия клиента после получения указанного уведомления. Приведенные изменения в законодательстве направлены с одной стороны на защиту интересов клиентов, хранящих денежные средства на банковских счетах, от преступных посягательств с использованием лицом чужой или поддельной платежной карты, а с другой стороны - являются обстоятельством, способствующим совершению мошеннических действий с собственной банковской картой. Например, держатель карты сам снимает деньги со своего счета, а в банк посылает уведомление об изъятии (краже) собственных денежных средств, чтобы получить компенсацию от банка.

Таким образом, изучив различные варианты компьютерного мошенничества, можно прийти к выводу, что хищение денежных средств с использованием компьютерной информации не всегда сопровождается обманом или злоупотреблением доверия, в том классическом понимании, которое обычно используется для целей применения ст. 159 УК РФ.

Чаще совершение таких хищений связано не с обманом собственника или иного владельца имущества, а с воздействием на компьютерную информацию. В таких случаях в заблуждение вводится компьютерная система. В п. 13 постановления Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» [17] сказано, что хищение чужих денежных средств путем использования заранее похищенной или поддельной кредитной (расчетной) карты, если выдача наличных денежных средств осуществляется посредством банкомата без участия уполномоченного работника кредитной организации, необходимо квалифицировать по ст. 158 УК РФ.

Таким образом, представляется необходимым внести соответствующие изменения в действующий уголовный закон, предусмотрев в нем статью о хищении чужого имущества путем использования электронной информации. В этом случае ст. 159.6 УК РФ должна будет утратить силу.

Можно предложить следующую редакцию новой статьи:

«Хищение чужого имущества путем доступа к электронной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи электронной информации». Что же касается модификации, блокирования, удаления, копирования и других действий, то все они должны дополнительно квалифицироваться по ст. ст. 272, 273 УК РФ.

Список литературы:

1. Справка-обобщение изучения судебной практики рассмотрения судами Самарской области уголовных дел о преступлениях, предусмотренных ст.ст. 159.1 – 159.6 УК РФ, отграничение от смежных составов. Практика назначения наказания
http://kuibyshevsky.sam.sudrf.ru/modules.php?name=docum_sud&id=1387

2. Федеральный закон от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» (ред. от 30.12.2012) // СЗ РФ. 2011. № 50. Ст. 7362

3. Ефремова М.А. К вопросу о понятии компьютерной информации // Российская юстиция. 2012. № 7. С. 50-52.

4. «Конвенция о преступности в сфере компьютерной информации ETS N 185», 2001.
http://base.garant.ru/4089723/

5. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 13.07.2015) "Об информации, информационных технологиях и о защите информации"(с изм. и доп., вступ. в силу с 10.01.2016) https://www.consultant.ru/document/cons_doc_LAW_61798/

6. Приговор Грачевского районного суда Ставропольского края от 13 июня 2013 г. по уголовному делу N 1-82/2013 // Судебные решения РФ. Единая база данных решений судов общей юрисдикции Российской Федерации. http://online-zakon.ru/%D0%BF%D1%80%D0%B8%D0%B3%D0%BE%D0%B2%D0%BE%D1%80-%D1%87-1-%D1%87-2-%D1%81%D1%82-159-6-%D1%83%D0%BA-%D1%80%D1%84/

7. "Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации" (утв. Генпрокуратурой России), 2013.http://www.consultant.ru/document/cons_doc_LAW_161817/

8. Апелляционное определение Московского городского суда от 6 мая 2013 г. N 10-2076 // СПС "КонсультантПлюс".
http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=SOJ;n=592329

9. Приговор Хамовнического районного суда города Москвы по делу № 1-100/2013 от 01 августа 2013 https://rospravosudie.com/court-xamovnicheskij-rajonnyj-sud-gorod-moskva-s/act-453358666/

10. Приговор Савельевского районного суда города Москвы по делу № 1-226/2013от 03 июня 2013 https://rospravosudie.com/court-savelovskij-rajonnyj-sud-gorod-moskva-s/act-422449046/

11. Постановление Московского городского суда N 4у/10-2543/15 от 19 мая 2015 г.
http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=SOJ;n=1227232

12. Апелляционное постановление Московского городского суда от 6 июля 2015 г. N 10-9255/2015
http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=SOJ;n=1310049

13. Приговор Чертановского районного суда г. Москвы от 30 октября 2013 г. по уголовному делу № 1-486/2012 // Единая база данных решений судов общей юрисдикции Российской Федерации.
http://судебныерешения.рф/bsr/case/6315701

14. Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. N 51 г. Москва "О судебной практике по делам о мошенничестве, присвоении и растрате»
http://rg.ru/2008/01/12/sud-voprosy-dok.html

15. Постановление Президиума Алтайского краевого суда от 3 сентября 2013 г. по делу № 44у-224/13 http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=SOJ;n=789007

16. Федеральный закон от 27.06.2011 N 161-ФЗ (ред. от 29.12.2014) "О национальной платежной системе" (с изм. и доп., вступ. в силу с 01.03.2015)

http://www.consultant.ru/document/cons_doc_LAW_115625/

17. Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. N 51 г. Москва "О судебной практике по делам о мошенничестве, присвоении и растрате" http://rg.ru/2008/01/12/sud-voprosy-dok.html

18. Ефремова М.А. К вопросу о понятии компьютерной информации // Российская юстиция. 2012. № 7. С. 50-52.

19. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 13.07.2015) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 10.01.2016)

20. Федеральный закон от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» (ред. от 30.12.2012) // СЗ РФ. 2011. № 50. Ст. 7362.

21. Федеральный закон от 27.06.2011 N 161-ФЗ (ред. от 29.12.2014) "О национальной платежной системе" (с изм. и доп., вступ. в силу с 01.03.2015) http://www.consultant.ru/document/cons_doc_LAW_115625/

22. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) http://base.garant.ru/4089723/

23. Справка-обобщение изучения судебной практики рассмотрения судами Самарской области уголовных дел о преступлениях, предусмотренных ст.ст. 159.1 – 159.6 УК РФ, отграничение от смежных составов. Практика назначения наказания http://kuibyshevsky.sam.sudrf.ru/modules.php?name=doc um_sud&id=1387 https://www.consultant.ru/document/cons_doc_LAW_61798/

24. "Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации" (утв. Генпрокуратурой России) http://www.consultant.ru/document/cons_doc_LAW_161817/

25. Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. N 51 г. Москва "О судебной практике по делам о мошенничестве, присвоении и растрате" http://rg.ru/2008/01/12/sud-voprosy-dok.html

26. Приговор Грачевского районного суда Ставропольского края от 13 июня 2013 г. по уголовному делу N 1-82/2013 // Судебные решения РФ. Единая база данных решений судов общей юрисдикции Российской Федерации. http://online-zakon.ru/%D0%BF%D1%80%D0%B8%D0%B3%D0%BE%D0%B2%D0%BE%D1%80-%D1%87-1-%D1%87-2-%D1%81%D1%82-159-6-%D1%83%D0%BA-%D1%80%D1%84/

27. Апелляционное определение Московского городского суда от 6 мая 2013 г. N 10-2076 // СПС "Консультант Плюс". http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=SOJ;n=592329

28. Приговор Хамовнического районного суда города Москвы по делу № 1-100/2013 от 01 августа 2013 https://rospravosudie.com/court-xamovnicheskij-rajonnyj-sud-gorod-moskva-s/act-453358666/

29. Приговор Савельевского районного суда города Москвы по делу № 1-226/2013от 03 июня 2013 https://rospravosudie.com/court-savelovskij-rajonnyj-sud-gorod-moskva-s/act-422449046/

30. Постановление Московского городского суда N 4у/10-2543/15 от 19 мая 2015 г. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=SOJ;n=1227232

31. Апелляционное постановление Московского городского суда от 6 июля 2015 г. N 10-9255/2015 http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=SOJ;n=1310049

32. Приговор Чертановского районного суда г. Москвы по уголовному делу № 1- 486/2012 // Единая база данных решений судов общей юрисдикции Российской Федерации. http://судебныерешения.рф/bsr/case/6315701 (опубликовано 30 октября 2013 г.)

33. Постановление Президиума Алтайского краевого суда от 3 сентября 2013 г. по делу № 44у-224/13 http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=SOJ;n=789007