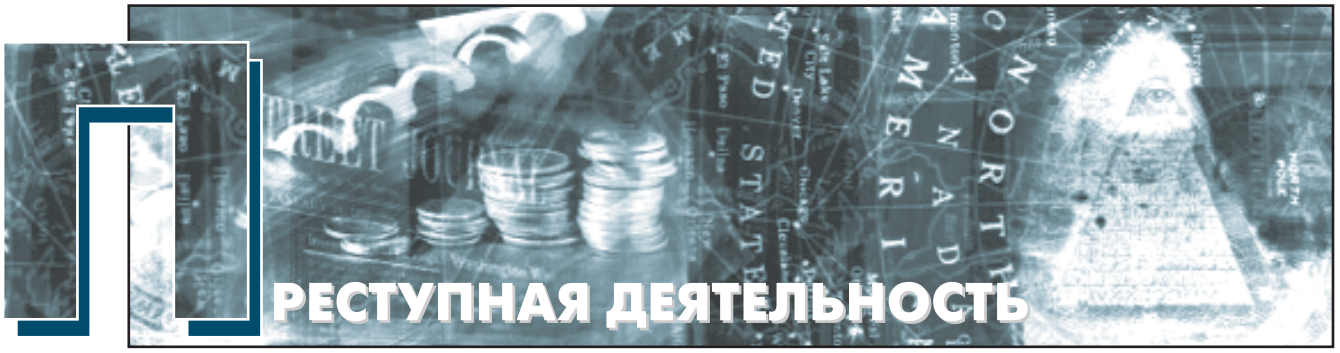

ПО ПОЛЬЗОВАНИЮ РЕСУРСАМИ СОТОВОЙ СВЯЗИ В РОССИЙСКОЙ ФЕДЕРАЦИИ: ВВЕДЕНИЕ В ПРОБЛЕМУ

Семенов Г.В.,
аспирант кафедры криминалистики Воронежского государственного университета

С появлением сотовой связи в нашей стране ее услуги стали привлекательным объектом уголовно-релевантной деятельности, в частности прослушивание переговоров, определение местоположения абонента и его передвижений в пространстве (характерно для убийств, совершенных по заказу), блокирование соединений преднамеренно создаваемыми помехами. Однако наиболее ярким примером использования сотовой подвижной связи в преступных целях явились действия по доступу и пользованию ее ресурсами[1] без намерения их надлежащей оплаты.

Перед науками криминального спектра встала задача разработки средств и методов борьбы с преступной деятельностью по доступу к системам сотовой связи и пользованию их ресурсами и, в первую очередь, правового и криминалистического анализа указанной преступной деятельности.

Используемые в отечественной, в том числе криминалистической, литературе термины "сотовое мошенничество" и "мошенничество в сотовой связи" применительно к действиям по доступу и пользованию ресурсами сотовой связи, с позиции отечественного уголовного закона, строго говоря, являются не совсем корректными, поскольку:

- они заимствованы из зарубежного законодательства. Исходя из анализа норм законодательства ряда Европейских государств действия по доступу к сотовой связи и пользованию ее ресурсами без цели надлежащей оплаты/регистрации в большинстве случаев квалифицируются именно как мошенничество (Нидерланды, Австрия, Финляндия, Германия и др.), телекоммуникационное мошенничество (Испания, Италия и др.)[2].
- ни одна из существующих в Уголовном Кодексе РФ (далее УК РФ) норм не отражает в полной мере той специфики общественных отношений, которые подвергаются общественно опасным посягательствам, совершаемым в целях пользования ресурсами (услугами) сотовой связи без надлежащей оплаты.

В ранее действовавшем отечественном уголовном законодательстве выделялся ряд действий с использованием радиоаппаратуры, за которые предусматривалась уголовная ответственность. В частности, пленум Верховного Суда СССР в Постановлении от 03.07.1963 г. № 12 обратил внимание судов на повышенную общественную опасность действий лиц, использующих радиопередающие устройства. В указанном постановлении было установлено, что "умышленные действия, выразившиеся в ведении по радио передач, связанных с проявлением явного неуважения к обществу, из озорства, грубо нарушающих общественный порядок либо создающих помехи радиовещанию и служебной радиосвязи, должны квалифицироваться в зависимости от их характера по ч. 2 или 1 ст. 206 УК РСФСР и соответствующим статьям УК союзных республик".

В случае использования радиопередающих устройств для передач иного характера содеянное должно квалифицироваться по соответствующим статьям УК союзных республик, то есть так же, как эти действия квалифицируются при совершении их без использования радиопередающих устройств"[3].

В настоящий момент анализ преступных действий, совершаемых в целях пользования ресурсами (услугами) сотовой связи без надлежащей оплаты, и конструкций статей УК РФ, содержащихся в гл. 21, 28 и в отдельных статьях некоторых других глав (например, статьи 272, 327), позволяет сделать вывод о многообъектности указанных преступных посягательств и, следовательно, о сложности их квалификации.

Термин "мошенничество в сотовой связи" обычно рассматривают как криминальную деятельность, включающую:

1) Преступные действия, направленные на получение доступа к системе сотовой связи.

Данные преступления квалифицируются как:

· ***Кража абонентских подвижных станций сотовой связи (ч. 1, 2, 3 ст. 158 УК РФ).***

Так, СО Кировского РОВД г. Ярославля было возбуждено уголовное дело № 00031255 по ч. 2 ст. 158 УК РФ. Расследование установило, что в ходе проведения оперативно-розыскных мероприятий сотрудниками отдела по борьбе с преступлениями в сфере высоких технологий (БПСВТ) задержаны гр. С. и гр. В., которые из корыстных побуждений осуществили кражи личных вещей (в том числе сотового телефона с целью криминального доступа к сотовой связи и пользования ее ресурсами) путем взлома входной двери, нанеся материальный ущерб владельцу в размере 8000 рублей[4].

· ***Иные криминальные способы завладения подвижными станциями сотовой связи (статьи 159, 161, 162 УК РФ и др.).***

Так, СО при УВД Западного АО г. Краснодара 22 июня 2000 г. было возбуждено уголовное дело № 201078 по ч. 2 ст. 162, ст. 175 по следующим обстоятельствам.

В ходе проведения оперативно-розыскных мероприятий, по заявлению потерпевшего, сотрудниками БПСВТ установлены и задержаны г-не Павинов, Сенов, Коровин, Саликов и Вергинин (инициалы изменены), которые, угрожая потерпевшим огнестрельным оружием, завладели 13-ю сотовыми телефонами с целью криминального доступа к сотовой связи и пользования ее ресурсами, а также дальнейшей их реализации[5].

· ***Преднамеренное указание неверных данных путем представления поддельных документов при заключении контракта на пользование услугами сотовой связи (части 1, 2, 3 ст. 327 УК РФ).***

По сообщению информационного агентства "Коминфо Консалтинг" от 09 апреля 2001 г., Управлением по борьбе с преступлениями в сфере высоких технологий ГУВД Санкт-Петербурга было возбуждено уголовное дело по факту мошенничества (ст. 159 УК РФ) и подделки документов (ст. 327 УК РФ) в отношении студента Института бизнеса и права.

Преступник обманным путем устанавливал данные о VIP-клиентах сотовой связи FORA Communications, владельцем которой является ОАО "Санкт-Петербург Телеком", и впоследствии реализовал с помощью поддельных доверенностей возможность пользования ресурсами сотовой связи указанного оператора.

Обычно такие клиенты резервируют так называемые "золотые" и "серебряные" номера, в которых набор цифр легко запоминаем. Затем мошенник звонил владельцам таких номеров, представлялся сотрудником отдела обслуживания FORA Communications и просил предоставить паспортные данные и другие конфиденциальные сведения, объясняя эту необходимость неполадками в базе данных. В ряде случаев излишне доверчивые клиенты такую информацию ему сообщили.

Получив сведения, преступник (опять же под видом представителя компании "Санкт-Петербург Телеком") занимался распространением услуг сотовой связи. Мошенник оформил нотариально заверенные доверенности на свое имя и с ними обратился в отдел обслуживания компании.

В результате оперативных действий мошенник был задержан с поличным и арестован. В настоящий момент у следствия есть заявления от трех клиентов сотового оператора, чьи номера и данные мошенник продал третьим лицам.[6]

Это единственный известный нам случай возбуждения уголовного дела по факту преднамеренного указания неверных данных при заключении контракта с целью криминального пользования ресурсами сотовой связи. Несмотря на это, мы склонны предположить, что подобные действия достаточно распространены в отношении российских операторов сотовой связи, однако из-за нежелания использовать долгий и сложный механизм уголовного преследования, операторы стараются противостоять ему своими силами.

· ***Неправомерный доступ к охраняемой законом компьютерной информации системы сотовой связи, повлекший уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети (ч. 1, 2 ст. 272 УК РФ).***

В качестве примера можно привести фактические обстоятельства, установленные приговором Федерального суда Ленинского района г. Воронежа.

Данным приговором было установлено, что в мае 1997 г. гр. М. и гр. Л, согласно разработанному плану, приобрели в Москве восемь сотовых аппаратов фирмы "МОТОРОЛА" и восемь микропроцессоров со специальной программой, позволяющих при монтаже в данные телефоны получить аппараты с возможностями неправомерного доступа к компьютерной информации компаний сотовой связи, копирования личных и абонентских идентификационных номеров законных пользователей компании, а также осуществления с данных аппаратов телефонных переговоров, оплата которых должна была осуществляться пользователями компании. Для исполнения своего преступного плана эти граждане с помощью переоборудованных аппаратов фирмы "МОТОРОЛА" в период с июля по ноябрь 1997 г. осуществляли неправомерный доступ к охраняемой законом компьютерной информации компании сотовой телефонной связи "ВОТЕК МОБАЙЛ" (стандарт AMPS) и скопировали в Воронеже при помощи имеющихся у них переоборудованных аппаратов 60 номеров законных пользователей данной компании. После этого, желая извлечь незаконную выгоду, неоднократно неправомерно получали доступ к компьютерной информации компании "ВОТЕК МОБАЙЛ", без оплаты осуществляли переговоры лично и предоставляли такую возможность третьим лицам[7].

Подобное уголовное дело рассматривалось Федеральным судом Советского района Нижнего Новгорода. Обвинительным приговором от 21 июня 1999 г. по данному делу было установлено следующее.

В ноябре 1997 г. гр. Н. приобрел у не установленных лиц сотовый телефонный аппарат Motorola. Используя имевшиеся у него в квартире два персональных компьютера и полученные из Интернета специальные компьютерные программы и описания, гр. Н. изменил мобильный идентификационный номер (абонентский номер) указанного аппарата на номер 91-18-86 (владелец ООО "Агентство Альтаир"), с которого впоследствии производил звонки и предоставлял такую возможность третьим лицам.

В январе 1998 г., находясь в Москве, гр. Н. у не установленного лица приобрел сотовый телефонный аппарат Motorola micro TAC ultra Lite, который обладал возможностью использовать при производстве телефонных звонков абонентские номера легальных владельцев сотовых телефонных аппаратов сотовой сети ТОО ПССР.

Впоследствии гр. Н. наряду с другими лицами неоднократно сканировал (перехватывал) идентификационные номера легальных пользователей и вносил в память аппарата, а затем производил телефонные звонки за счет легальных абонентов ТОО ПССР.

В первом случае Федеральный суд Ленинского района г. Воронежа квалифицировал действия злоумышленников по сканированию идентификационных номеров легальных пользователей (ESN и MIN) как неправомерный доступ к компьютерной информации системы сотовой связи (ст. 272 УК РФ, соответствующая часть). Во втором случае Федеральный суд Советского района Нижнего Новгорода установил, что действия по установлению соединений за счет легальных абонентов являются неправомерным доступом к компьютерной информации системы сотовой связи, хранящейся в ЭВМ телефонных коммутаторов, о времени, продолжительности, месте и стоимости телефонного соединения (ст. 272 УК РФ, соответствующая часть).

Для правильного установления объекта и объективной стороны при квалификации деяния по статье 272 УК РФ необходимо четко представлять, что является машинным носителем, ЭВМ, системой ЭВМ или сетью ЭВМ, а также уничтожением, блокированием, модификацией либо копированием компьютерной информации применительно к специфике сетей сотовой связи.

Раскрытие и расследование неправомерного доступа к охраняемой законом компьютерной информации системы сотовой связи предполагает следующие вопросы:

1. Являются ли абонентские подвижные станции той или иной модификации электронно-вычислительными машинами, либо машинными носителями информации компьютерной сети оператора сотовой связи?

2. Является ли совокупность абонентских подвижных станций, базовых станций и коммутационного оборудования оператора сотовой связи сетью ЭВМ?

3. Являются ли идентификационные данные пользователя (MIN, ESN и т.д.) компьютерной информацией?

4. Является ли перенос идентификационных данных абонента с одной абонентской подвижной станции (либо другого устройства) на другую абонентскую подвижную станцию (либо другое устройство), а также модификация, блокирование идентификационных данных абонента доступом к компьютерной информации сети оператора сотовой связи?

На основании анализа материалов ряда уголовных дел, раскрытых и расследованных по фактам криминального пользования ресурсами сотовой связи без надлежащей оплаты, при производстве экспертиз указанные вопросы решались положительно[8].

Однако проблемы квалификации действий, связанных с неправомерным доступом к компьютерной информации системы сотовой связи, по статье 272 УК РФ на этом не заканчиваются.

Так, проводя уголовно-правовой анализ преступлений в сфере компьютерной информации, В.А. Мещеряков подчеркивает, что "серьезные проблемы возникают с квалификацией действий, связанных с неправомочным использованием чужих идентификационных номеров в системах сотовой связи. Особенность данной ситуации заключается в том, что эти идентификационные номера свободно передаются через эфир и могут быть получены практически любым лицом, имеющим необходимый набор технических средств, причем этот набор может быть приобретен на вполне законных основаниях и за умеренную плату"[9].

Действия квалифицируются как неправомерный доступ к компьютерной информации по ст. 272 УК РФ в том случае, если указанная информация охраняется законом. Идентификационные номера пользователей услуг сотовой связи потенциально являются конфиденциальной информацией, а точнее, ее разновидностью - коммерческой тайной. Так, в соответствии со ст. 139 ГК РФ[10] коммерческой тайной является информация, имеющая действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам. К ней нет свободного доступа на законном основании, и обладатель информации принимает меры по охране ее конфиденциальности.

Именно два последних условия вызывают сомнения применительно к описываемым случаям.

Действительно, и с точки зрения существующего законодательства, и с позиции технических особенностей построения сетей сотовой связи эфир открыт для сканирования. В этом случае актуален вопрос: является ли доступ к идентификационным номерам пользователей, находящихся в эфире, свободным?

Предоставление информационным ресурсам статуса коммерческой тайны (информации с ограниченным доступом) осуществляется собственником (в рассматриваемой ситуации - компании сотовой связи) изданием внутренних актов и обеспечением ее реальной охраны (использование алгоритмов шифрования, ключей защиты и т.д.). Однако именно последний тезис нельзя отнести к некоторым операторам аналоговых (NMT-450 без SIS-кода и AMPS без AKey) и цифровых (D-AMPS без AKey) стандартов сотовой связи, так как эти стандарты не обеспечивают шифрование идентификационных данных пользователей. Соответственно не принимаются меры по охране конфиденциальности, что влечет невозможность квалификации по ст. 272 УК РФ. Несмотря на это, по большинству проанализированных нами уголовных дел неправомерный доступ к идентификационным номерам пользователей был квалифицирован по ст. 272 УК РФ.

- ***Незаконное производство, сбыт или приобретение в целях сбыта специальных технических средств (сканеров, абонентских подвижных станций сотовой связи с возможностями сканирования, модифицированных абонентских подвижных станций и их программного обеспечения и т.д.), предназначенных для негласного получения информации (ч. 3 ст. 138 УК РФ).***

Диспозиция ч. 3 ст. 138 УК РФ предполагает уголовную ответственность только за незаконные производство, сбыт и приобретение в целях сбыта специальных технических средств (СТС) и только применительно к тайне переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан.

Так, в Комментариях к Уголовному Кодексу Россий-

ской Федерации под ред. Ю.И. Скуратова, В.М. Лебедева указывается, что "хранение чужих специальных технических средств, предназначенных для негласного получения информации, не является преступлением, а их использование должно квалифицироваться по ч. 2 ст. 138 УК"[11].

Однако, по нашему мнению, приобретение, хранение, а также использование СТС применительно к иным, защищаемым законом видам информации, несет такую же общественную опасность, как и действия, предусмотренные статьей 138 УК РФ. Более того, данные действия чаще всего являются приготовительными к неправомерному пользованию ресурсами операторов сотовой связи без цели их надлежащей оплаты. Так как действия по приобретению в целях сбыта СТС трудно доказуемы, то на практике подобные действия квалифицируются только относительно продавца СТС.

Так, 29 сентября 1999 г. прокуратурой Ленинского р-на г. Ульяновска было возбуждено уголовное дело № 1749, на основе материалов которого было установлено, что в ходе реализации оперативных мероприятий сотрудниками БПСВТ выявлен гр. В. 1977 г.р., который с целью наживы реализовывал сканирующий сотовый телефон. Совместно с УФСБ Ульяновской области гр. В. был задержан. В последствии ему было предъявлено обвинение по ч. 3 ст. 138 УК РФ[12].

Подобные факты, но уже в отношении действий по реализации сотового телефона "двойника" были зафиксированы в материалах уголовного дела № 30632/99, возбужденного прокуратурой г. Кирова 31 мая 1999 г. по ч. 3 ст. 138 УК РФ[13].

Отдельно необходимо выделить действия по доступу к системе сотовой связи, которые не являются наказуемыми с позиции отечественного уголовного закона (приобретение клонированных абонентских подвижных станций, заключение контракта на основании подлинных документов, впоследствии неоплата произведенных переговоров и изменение места пребывания и др.).

Постановлением о прекращении уголовного дела по п. 4 ст. 5 УПК РСФСР установлено, что гр. С. приобрел устройство для незаконного подключения к сотовой сети. (Согласно заключению эксперта данное устройство представляет собой сотовый телефон Micro Tac Ultra Lite стандарта D-AMPS промышленного изготовления. Оно доработано на аппаратном уровне для получения возможности считывания идентификационных номеров активных сотовых телефонных трубок с целью последующего подключения для работы в качестве "двойника".) Устройство было подключено к сотовой сети ЗАО "Акос" без уведомления последнего. Гр. С. пользовался устройством в личных целях в период с 25.02.2000 г. до 18.04.2000 г., чем нанес ЗАО "Акос" материальный ущерб в размере 6721 рублей.

Действия гр. С. по пользованию "двойником" были квалифицированы по ч. 1 ст. 165 УК РФ, а действия по приобретению были признаны правомерными с позиции уголовного законодательства[14].

Как видно, указанные выше уголовно-релевантные и правомерные действия представляют собой не пользование ресурсами (услугами) сотовой связи без цели надлежащей оплаты, а направлены на получение и предоставление различной степени доступа к данным услугам.

2) Преступные действия, представляющие собой получение обманным путем ресурсов (услуг) сотовой связи без цели их надлежащей оплаты (криминальное пользование ресурсами (услугами) сотовой связи) (ст. 159 УК РФ/165 УК РФ).

Ответственность за преступные действия по пользованию ресурсами (услугами) сотовой связи наступает, в зависимости от тех или иных обстоятельств, установленных по уголовному делу, по ч. 1, 2, 3 ст. 159 УК РФ (мошенничество) - или ч. 1, 2, 3 ст. 165 УК РФ (причинение имущественного ущерба путем обмана или злоупотребления доверием).

Подобный дифференцированный подход заключается в следующем.

Данные составы отличаются, прежде всего, механизмом извлечения виновным незаконной имущественной выгоды. Если при мошенничестве, как и при любой форме хищения, происходит изъятие имущества из обладания (фондов) собственника или иного владельца и его незаконное обращение в пользу виновного или других лиц, то при причинении имущественного ущерба путем обмана или злоупотребления доверием такого изъятия не происходит. В этом преступлении отсутствует такой присущий хищению признак, как изъятие имущества из наличных фондов того или иного собственника, то есть не происходит уменьшения наличной массы имущества, принадлежащего собственнику или находящегося у иного законного владельца. Имущественный ущерб, причиняемый при совершении такого преступления, заключается не в прямых убытках, как при хищениях, а в неполучении должного, в упущенной выгоде[15].

Во-первых, использование идентификационных данных легального пользователя, преднамеренное указание неверных данных путем представления поддельных документов при заключении контракта на пользование услугами сотовой связи, хищение абонентских подвижных станций для осуществления пользования ресурсами сотовой связи без надлежащей оплаты является определенной формой обмана в смысле ст. 165 УК РФ и ст. 159 УК РФ[16].

Во-вторых, ст. 159 УК РФ говорит о преступности приобретения права на имущество путем обмана либо злоупотребления доверием (то же самое предполагает и ст. 165 УК РФ), а примечание к ст. 158 УК РФ (кража) определяет хищение лишь как изъятие и/или обращение чужого имущества в свою пользу или пользу других лиц.

Статья 128 Гражданского Кодекса РФ содержит формулировку "иное имущество, в том числе имущественные права", из которой следует, что обратить в свою пользу при хищении можно и имущественные права.

По своему правовому содержанию, в состав отношений, возникающих в сфере деятельности по предоставлению услуг сотовой связи, входят в большинстве своем имущественные права обязательственного характера - право требования компании-оператора к абоненту об уплате соответствующих сумм по договору на оказание услуг сотовой связи, право требования контрагентов компании-оператора по оплате, используемых ее абонентами каналов связи, право требования абонентом оказания в соответствии с договором ресурсов (услуг) сотовой связи и др.

Использование идентификационных номеров легальных пользователей для осуществления пользования

ресурсами сотовой связи без цели надлежащей оплаты является не чем иным, как приобретением права пользования указанными ресурсами, в том числе и счетом легального абонента.

Резюме. По нашему мнению, уголовная ответственность за получение обманным путем ресурсов сотовой связи без цели их надлежащей оплаты должна наступать по ст. 159 в том случае, если преступником осуществляется использование сетей других операторов, в связи с чем оператор, к которому он подключен, оплачивает произведенные преступником соединения другим операторам, по сетям которых данные соединения производились.

Привлечение к уголовной ответственности по ст. 165 УК РФ наступает в случае использования преступником сетей оператора, к которому он подключен. Сюда же следует отнести и преступные действия, включающие предоставление возможности пользования ресурсами сотовой связи без надлежащей оплаты третьим лицам[18].

Тем самым в зависимости от механизма извлечения виновным незаконной имущественной выгоды данные преступные действия могут квалифицироваться по ст. 159 УК РФ или 165 УК РФ. Однако, в рамках расследования конкретного уголовного дела установление пункта назначения каждого исходящего и входящего звонка, для разграничения квалификации по ст. 159 УК РФ или 165 УК РФ - это достаточно долгий и трудоемкий труд[17].

Для разрешения указанной проблемы, на наш взгляд, необходимо создание нового уголовно-правового запрета.

Так, сотрудниками Управления по борьбе в преступлениями в сфере высоких технологий МВД России был представлен в Государственную Думу Федерального Собрания РФ законопроект о видоизменении ст. 159 УК РФ в том плане, чтобы диспозиция данной нормы предусматривала уголовную ответственность за действия по получению обманным путем ресурсов (услуг) различных систем связи без цели их надлежащей оплаты и исключала неоднозначное понимание квалификации[19].

Очевидно, что речь идет о преступной деятельности, в которую включаются не только криминальные действия по пользованию ресурсами (услугами) системы сотовой связи, но и криминальные действия по доступу к данной системе, предусмотренные самостоятельными составами Уголовного Кодекса РФ.

Однако, с криминалистической точки зрения, не всегда правильно говорить о наличии именно преступной деятельности как совокупности целенаправленных действий, предусмотренных различными нормами уголовного законодательства.

Из вышеуказанного следует, что речь идет о преступной деятельности, в которую включаются не только криминальные действия по пользованию ресурсами (услугами) системы сотовой связи, но и криминальные действия по доступу к данной системе, предусмотренные самостоятельными составами Уголовного Кодекса РФ.

Безусловно, значение уголовно-правовых характеристик преступления при изучении той или иной уголовно-релевантной деятельности сейчас считается основополагающим. Однако руководство лишь подобными критериями означает сознательное сужение гносеологических возможностей криминалистики как самостоятельной науки, снижение практической значимости разрабатываемых ею рекомендаций.

Существует достаточное количество доводов для выделения среди преступлений, предусмотренных различными статьями Уголовного Кодекса РФ, определенных систем и классификации, на комбинированных основаниях, то есть руководствуясь при этом не только уголовно-правовыми, но и криминалистическими критериями. Сходство криминалистических признаков различных видов преступлений позволяет группировать эти преступления как криминалистически сходные и впоследствии создавать с учетом названных условий методики их раскрытия и расследования, оптимизировать процесс расследования, определить и применить превентивные и нейтрализующие меры.

Данные положения в полной мере относятся к криминалистическому анализу рассматриваемой преступной деятельности, так как существует достаточно оснований для выделения среди перечисленных выше преступлений определенной системы, используя криминалистические основания.

При выделении общих свойств, позволяющих отнести преступные действия по доступу к системе сотовой связи и, как следствие, криминальное пользование ее ресурсами к одной классификационной группе, следует учитывать следующие категории признаков.

1. Рассматривая методические основы расследования преступлений, О.Я. Баев справедливо считает, что для достижения преступных целей "...лицу, независимо от его субъективных качеств, а зачастую и от складывающейся криминальной ситуации, необходимо совершить ряд типовых действий"[20].

В другой своей работе О.Я. Баев подчеркивает, что "следы не только закономерно возникают в результате совершения любого преступления, но и являются типовыми для преступлений того или иного вида, остаются на определенных объектах, в определенных местах, состоят в определенных изменениях материальной обстановки, содержатся в памяти определенного контингента лиц. Это, в свою очередь, связано с тем, что для совершения преступления определенного вида лицо должно решить ряд типовых задач, для их решения осуществить ряд типовых действий"[21].

Сам по себе механизм рассматриваемой криминальной деятельности заключается в пользовании ресурсами системы сотовой связи. Ресурсы системы сотовой связи не являются чем-то самостоятельным и абсолютным, в связи с чем существует комплекс их аппаратного обеспечения - физические носители ресурса. Общие технические принципы и архитектура построения сети сотовой связи требуют, чтобы на обязательной основе ей был присущ радиоинтерфейс (между абонентской станцией и базовой станцией). С позиции аппаратного обеспечения абонентская станция и базовая станция также перманентно присущи сети сотовой связи. При этом включение нового элемента в систему возможно только в том случае, если он обладает характеристиками, совпадающими с характеристиками самой системы в рамках ее целевой направленности, то есть приемо-передающего устройства и антенно-фидерного устройства - подвижной станцией, обладающей теми признаками, которые присущи стандарту оператора.

Соответственно, пользование ресурсами сотовой связи невозможно без подключения к ее системе (полу-

чения доступа к системе) и абонентской активности (телефонные звонки, переадресация вызова, пользование Интернета, передача данных и др.).

Итак, типичными для совершения рассматриваемой преступной деятельности будут следующие действия:

1) Действия преступника, направленные на получение различной степени доступа к системе сотовой связи (ее функциональным и процедурным элементам). Для осуществления доступа к сети (системе) сотовой связи необходимо иметь абонентскую подвижную станцию, аппаратное и программное обеспечение, а также идентификационные данные, которые позволяют работать в данной системе, то есть быть подключенным к системе.

2) Пользование услугами сотовой связи (абонентская активность) и/или предоставление такой возможности третьим лицам.

Таким образом, сталкиваясь с преступной деятельностью по пользованию услугами сотовой связи без их надлежащей оплаты, в большинстве случаев мы имеем дело с двумя самостоятельными преступлениями. При этом криминальные действия по получению доступа к системе сотовой связи будут являться подготовительным этапом преступных действий по пользованию ресурсами сотовой связи, то есть способом приготовления к совершению преступления[22].

Однако возникает вопрос: во всех ли случаях необходимо рассматривать указанные выше действия в составе преступной деятельности по пользованию ресурсами сотовой связи? На этот вопрос нужно дать отрицательный ответ.

2. А.В. Бондар, исследуя криминалистические средства и методы пресечения и расследования приготовления к преступлению, приходит к справедливому выводу, что "приготовление к преступлению никогда не является самоцелью: оно всегда совершается для осуществления последующей преступной деятельности - для совершения преступления. Поскольку его содержание целиком определяется содержанием того способа совершения преступления, который избран субъектом, его и формально и фактически можно рассматривать как начальный этап формирования этого способа, без которого сам способ совершения преступления будет "недееспособным", неэффективным. Именно поэтому на вопрос о том, может ли в принципе существовать самостоятельный способ приготовления к преступлению, следует дать отрицательный ответ"[23].

Применительно к рассматриваемой преступной деятельности можно добавить, что действия по доступу к системе сотовой связи и пользованию ее ресурсами могут совершаться разными субъектами при условии, что их действия осуществлялись без ведома друг друга. Также действия по доступу к системе сотовой связи и пользованию ее ресурсами могут быть не связаны единым замыслом, если цель пользования ресурсами системы первоначально не преследовалась, а возникла позже, после получения доступа (по аналогии с взглядами Р.С. Белкина на проблему определения содержания понятия способа совершения преступления и его соотношения с действиями по сокрытию преступления[24]).

Поэтому мы полагаем, что в рассматриваемую преступную деятельность входят действия по доступу к данной системе (подготовительные действия) только в случае подчиненности их общей цели - пользованию ресурсами системы сотовой связи без их надлежащей оплаты и/или регистрации.

Тем самым при выделении общих свойств, позволяющих отнести все названные преступления к одной классификационной группе, следует учитывать две категории взаимосвязанных признаков. С одной стороны, типовые действия преступника, с другой - цель совершения преступления.

Резюмируя указанное выше, мы полагаем, что под преступной деятельностью по пользованию ресурсами сотовой связи следует понимать целенаправленную совокупность (комплекс) последовательных действий по доступу к системе сотовой связи, пользованию ее ресурсами без их надлежащей оплаты и/или предоставлению такой возможности третьим лицам, подпадающих под признаки отдельного состава преступления или их совокупности.

Полагаем также, что представленный выше подход к рассматриваемой преступной деятельности станет основой для дальнейших правовых и криминалистических исследований.

1. Необходимо подчеркнуть, что конечной целью рассматриваемой преступной деятельности является пользование услугами системы сотовой связи без их надлежащей оплаты и/или регистрации. В связи с этим напрашивается вывод, что предметом посягательства в криминалистическом смысле являются именно услуги. С учетом особенностей построения системы сотовой связи данный вывод был бы недостаточно точен.

Функциональные возможности системы сотовой связи позволяют осуществлять следующие виды услуг: услуги телефонной связи; переадресация вызова; удержание, или сохранение вызова; ожидание вызова; конференц-связь; автодозвон; голосовая почта; роуминг; передача коротких сообщений; факсимильная связь; доступ к сети Интернет и передача данных и др.

Однако мы полагаем, что услуги сотовой связи нельзя свести к перечисленному набору. Услуги как элемент функционирования сотовой связи - это не только результат. Результатом любой деятельности являются изменения и преобразования окружающей среды. К услугам следует относить и процесс по достижению этого результата.

В связи с этим под услугами следует понимать не только функциональные возможности сотовой связи, но и весь комплекс их программного и процедурного обеспечения (объем внешней и оперативной памяти, время работы процессора базовых станций, коммутаторов, средств компьютерной техники центров технического и клиентского обслуживания и др.).

Поэтому мы полагаем, что применение понятия "ресурс" (фр. ressources - средства, запасы, возможности, источники чего-либо) наиболее удачно для обозначения комплекса услуг сотовой связи и обеспечивающих их технологических и процедурных процессов.

2. Bill Clede. Dealing with cellular phone fraud // Law and order. May 1993, P. 20 - 23; Carlos Singh. Was Cellular Telephone Cloning a Crime Before October 1994? // USABulletin. Electronic Investigative Techniques II.

November 1997, Volume 45, Number 6, P. 24-29; John T. O, Brien. Telecommunications fraud // Published by the Federal Bureau of Investigation, U.S. Department of Justice Reprinted from the FBI Law Enforcement Bulletin. May 1998, Volume 67, Number 5, P. 20-26; Navarrete J. The crime of illegally cloned cellular telephones // Published by the Federal Bureau of Investigation, U.S. Department of Justice Reprinted from the FBI Law Enforcement Bulletin. October 1997, Volume 43, Number 5, P. 17-21; United States v. Brady. 13 F.3d 334 (10th Cir. 1993), United States v. Morris, 81 F. 3d 131 (11th Cir. 1996), United States v. Ashe, 47 F.3d (770 6th Cir.) United States v. Brewer, 835 F.2d 550 (5th Cir. 1987), United States v. Clayton, 108 F.3d 1114 (9th Cir. 1997) // Electronic Investigative Techniques II / Published by the Federal Bureau of Investigation, U.S. Department of Justice Reprinted from the FBI Law Enforcement Bulletin. November 1997, Volume 45, Number 6, P. 29.; Phil Gosset, Mark Hyland Classification, Detection and Prosecution of Fraud on Mobile Networks // MOBILE Communications International, 2000, № 1, P. 14-18; Jos Dumortier, Mark Hyland, Diana Alonso Blas. Legal aspects of fraud detection. - Leuven, 1998. - 53 p. - Информационные ресурсы Интернет: http://www.law.kuleuven.ac.be/icri.

3. Постановление Пленума Верховного Суда СССР "О квалификации действий, связанных с использованием радиопередающих устройств в преступных целях" от 3 июля 1963 г. № 12 // Бюллетень Верховного Суда СССР. 1963. № 4.

4. По материалам уголовного дела № 00031255, находившегося в производстве СО Кировского РОВД г. Ярославля.

5. По материалам уголовного дела № 201078, находившегося в производстве СО при УВД Западного АО г. Краснодара.

6. Информационные ресурсы Интернета: http://www.telecominfo.ru.

7. Архив Федерального суда Ленинского района г. Воронежа. Дело №1-318.

8. Заключение эксперта № б/н от 19.02.2001 г. по уголовному делу № 00124132, находившемуся в производстве СО при Коминтерновском РОВД г. Воронежа, заключение радиотехнической экспертизы № б/н от 4.09.98 г. по уголовному делу № 140, находившемуся в производстве СО УФСБ РФ по Нижегородской области и др.

9. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. - Воронеж, 2001. - С. 25.

10. Гражданский кодекс Российской Федерации // Комментарий к Гражданскому кодексу части первой. Под ред. Садикова О.Н., - М., 1997. - С. 448.

11 Уголовный кодекс Российской Федерации // Комментарий к Уголовному Кодексу Российской Федерации (издание третье, измененное и дополненное). Под ред. Ю.И. Скуратова, В.М. Лебедева. - М., 2000. - С. 311.

12. По материалам уголовного дела № 1749, находившегося в производстве прокуратуры Ленинского р-на г. Ульяновска.

13. По материалам уголовного дела № 30632/99, находившегося в производстве прокуратуры г. Кирова.

14. Постановление о прекращении уголовного дела по п. 4 ст. 5 УПК РСФСР (амнистия) от 29 мая 2000 г. По материалам уголовного дела № 723331, находившегося в производстве Фрунзенский РОВД г. Владивостока.

15. Уголовный кодекс Российской Федерации // Комментарий к Уголовному Кодексу Российской Федерации. Под ред. Ю.И. Скуратова, В.М. Лебедева. - М., 1999. - С 367.

16. "Обман - умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество, и таким образом добиться от него добровольной передачи имущества, а также сообщение с этой целью заведомо ложных сведений". Бюллетень Верховного Суда РСФСР, 1982, N 2. С. 14.

17. Вслед за С.И. Мурзаковым мы полагаем, что привлечение к уголовной ответственности по ст. 165 УК РФ должно наступать в том случае, если сумма ущерба (упущенной выгоды) достигает границ, характеризующих значительный размер для потерпевшего, соответственно, общественную опасность действия, которая требует именно применения мер уголовной ответственности. Тем самым существует необходимость законодательного установления и формального закрепления в ст. 165 УК РФ нижней границы имущественного ущерба, причиняемого данного рода действиями. Мурзаков С.И. Структура материального ущерба преступлений, совершаемых в сфере экономики, и его стоимостные критерии // Сб. научных статей по материалам Всероссийского научно-практического семинара 15-18 декабря 1998 г. "Вопросы квалификации и расследования преступлений в сфере экономики" / Под. ред. Н.А. Лопашенко, В.М. Юрина, А.Б. Нехорошева. - Саратов, 1999. - С. 57-58.

18. Это подтверждается анализом практики применения ст. 165 и ст. 159 УК РФ к рассматриваемым случаям. По всем исследованным нами уголовным делам конечная квалификация действий по пользованию ресурсами сотовой связи проводилась по ст. 165 УК РФ.

19. Завидов Б.Д. Обычное мошенничество и мошенничество в сфере высоких технологий. - М., 2002, - С. 18.

20. Расследование преступлений против личности: Учеб. Пособие. Под ред. О.Я. Баева. - Воронеж, 1998. - С. 6.

21. Баев О.Я. Методические основы расследования отдельных видов преступлений // Расследование отдельных видов преступлений. Под ред. Баева О.Я. - Воронеж, 1986. - С. 5.

22. На основании анализа материалов 25-и уголовных дел, раскрытых и расследованных по фактам криминального пользования ресурсами сотовой связи без надлежащей оплаты, справедливо было бы подчеркнуть, что к действиям по доступу к сотовой связи могут относиться и правомерные действия с позиции уголовного закона. Однако в большинстве случаев подготовительными являлись именно криминальные действия либо действия, не наказуемые с позиции уголовного закона, но по степени своей общественной опасности и ряда других факторов необходимые для закрепления в качестве уголовно-правового запрета (квазикриминальные действия).

23. Бондар А.В. Криминалистические средства и методы пресечения и расследования приготовления к преступлению. Диссертация к.ю.н. - Краснодар, 2001. - С. 30.

24. Р.С. Белкин. Курс криминалистики в 3 тт. Том 3: Криминалистические средства, приемы и рекомендации. - М.,1997. - С. 359-360.