Чертов Андрей Игоревич

Магистрант

Направление: Юриспруденция

Магистерская программа: Уголовный процесс, криминалистика, судебная экспертиза; теория оперативно-розыскной деятельности

Особенности проведения оперативно-розыскных мероприятий при расследовании мошенничества с использованием сети интернет

Аннотация. В статье рассматриваются особенности проведения оперативно-розыскных мероприятий при расследовании мошенничества с использованием сети интернет, проанализированы оперативно – розыскные мероприятия и выявлены проблемы возникающие при снятии информации с технических каналов связи.

Ключевые слова: методика расследования, мошенничество, криминалистическая характеристика, следственные действия.

В работах по теории оперативно-розыскной деятельности термин оперативно-розыскные мероприятия (ОРМ), в отличие от актов законодательства, используется достаточно давно и широко. Попытки определить понятие ОРМ встречаются в работах таких учёных как Ю.Ф. Кваша, В.Г. Бобров, В.В. Дюков, В.И. Елинский, Н.С. Железняк А.М. Ефремов, Д.В. Ривман, А.Г. Лекарь, А.Ю. Шумилов, К.В. Сурков и других.

Представляется что отсутствие в советском уголовно-процессуальном законодательстве определения «оперативно-розыскного мероприятия», а также приоритет теории ОРД на решение более общих методологических задач не способствовало росту интереса в среде исследователей к определению понятия ОРМ и, как следствие, не порождало серьёзных научных дискуссий по этой проблеме. Поэтому заметных попыток сформулировать понятие ОРМ в

общедоступной юридической литературе до середины 90-х гг. почти не встречается.

Более серьёзный интерес к затронутой проблеме возник с зарождением законодательства об оперативно-розыскной деятельности, так как понятие ОРМ приобрело правовой статус. Под ОРМ предлагалось понимать составной структурный элемент оперативно-розыскной деятельности, представляющий собой систему взаимосвязанных действий, главным направлением которых является решение конкретных тактических задач.

В теории ОРД идёт активный процесс конструирования этого системообразующего понятия. Тем не менее, большинство имеющихся определений не способны в полной мере отразить основные, сущностные признаки оперативно-розыскных мероприятий. Причинами этого, на наш взгляд, является отсутствие преемственности и, порой, недостаточное использование логических методов в решении этой проблемы [1].

Интернет как глобальную компьютерную сеть можно рассматривать с двух подходов: технологический подход (Интернет как информационно-телекоммуникационная среда, обеспечивающая обработку и хранение информации); социальный подход (Интернет как социально-культурное образование, влияющее на многие стороны жизни общества и образующее специфическую среду реализации некоторых видов деятельности и проявления общественных отношений).

В качестве нового вида социального пространства Интернет накладывает отпечаток на стратегию и тактику форм ОРД, применяемых в расследованиях преступлений, совершаемых в сети Интернет, а также создаёт особые условия для осуществления ОРМ.

В литературе указывается, что, оперируя понятием «сетевое информационное пространство» (иногда можно встретить термин «киберпространство») можно рассматривать сеть Интернет не только как систему телекоммуникаций, но и как место осуществления ОРД.

Представляется необходимым отметить, что при расследовании мошенничества в сети Интернет оперативно-розыскные мероприятия могут проводиться в самом Интернете. Специфику таких мероприятий обусловливают три фактора: особенности киберпространства, особенности Интернета как особого пространства и особенности мошенничества в Интернете как преступления.

Снятие информации с технических каналов связи представляется одним из перспективных с точки зрения развития оперативно-розыскных мероприятий. В настоящее время технические способы связи, например, Интернет, приобретают всё более распространённый характер. При этом активно развиваются и другие виды технической связи. Поэтому в литературе высказываются предположения о том, что в будущем возможно разделение на законодательном уровне снятия информации с технических каналов связи на несколько – в зависимости от вида связи.

Однако, на наш взгляд, подобное разделение будет излишним, во всяком случае, если речь идёт о дополнении классификации. Представляется, что наиболее рациональным будет выделение различных видов рассматриваемого оперативно-розыскного мероприятия через описание особенностей их проведения в статье 8 закона об ОРД («Условия проведения оперативно-розыскных мероприятий») [2].

В конкретный момент времени информация может находиться в одной из двух форм: статической форме (хранение на машинном носителе) и динамической форме (передача по каналу связи). Снятие информации с технических каналов связи осуществляется в отношении информации, находящейся в процессе передачи, через её сбор в масштабе реального времени путём перехвата за счёт использования специального оборудования и программного обеспечения.

С учётом особенностей данного ОРМ информация, подлежащая съёму, находится в электронно-цифровой форме. Полученная информация

записывается или копируется на различные физические носители информации (лазерные, жесткие диски и др.)

Как правило, снятие информации с технических каналов связи, осуществляется тремя основными способами: внедрение программных, аппаратных, аппаратно-программных устройств для перехвата информации в технические средства хранения, обработки и передачи информации по техническим каналам связи; перехват информации на линиях связи и в сетях передачи данных, а также последующее дешифрование этой информации; внедрение программных средств, нарушающих нормальное функционирование систем защиты информации, компрометирующих ключи и средства криптографической защиты информации в целях получения доступа к защищаемой информации.

Снятие информации с технических каналов связи может осуществляться в пассивной и активной форме. Рассмотрим эти формы подробнее.

Пассивный перехват предполагает слежение за передаваемыми сообщениями без вмешательства в их поток. Это достигается путём копирования сообщений, которые продолжают своё движение по каналам интернет-связи к пункту назначения. Главным достоинством пассивного перехвата является высокий уровень конспирации, поскольку вызванная копированием задержка при передаче сообщения крайне мала и, таким образом, отправитель и получатель не замечают признаков перехвата.

Активный перехват подразумевает производство определённых действий с передаваемой информацией, например, изменение содержания, задержание и т.д. [3]. Также, учитывая ч. 1 ст. 15 закона об ОРД, можно говорить о полной блокировке передачи сообщений в отношении конкретных лиц с целью недопущения получения ими определённой информации. Поскольку активный перехват связан с воздействием на передаваемую информацию, имеет смысл говорить о низкой степени конспирации и, как следствие, снятие информации с технических каналов связи в данной форме не всегда оправдано, поскольку

мошенники часто действуют осторожно и при первых признаках серьёзной опасности могут прекратить свою деятельность.

Представляется, что в таком случае дальнейшее расследование будет существенно затруднено, поскольку может быть утеряна часть следов, указывающих на преступников и их деятельность (например, закрытие денежных счетов, удаление сайтов, попытки исчезновения мошенников из поля зрения правоохранительных органов и т. д.).

Снятие информации с технических каналов связи возможно не только по каналам передачи данных, но также по электромагнитным и другим полям, излучаемым устройствами, сопряжёнными с компьютером (роутеры, устройства, использующие технологию Bluetooth для связи с компьютером и т. д.). Однако в этом случае требуется техническое обеспечение субъектов расследования специальными инструментами. В качестве примера считаем уместным привести разработанное швейцарской компанией Dreamlab Technologies устройство под названием Keykeriki 2, обладающее функцией перехвата данных с беспроводных устройств и систем [4].

Представляется, что применение таких технических средств уместно, в основном, в тех случаях, когда мошенник, или один из соучастников мошенничества использует компьютеры внутри компании, потерпевшей от мошенничества (либо способной потерпеть, если речь идёт о деятельности по предотвращению готовящегося преступления).

При этом возникают определённые проблемы. Дело в том, что при снятии информации с технических каналов связи представляет некоторую сложность выделение из общего потока полученных данных тех сообщений, которые относятся к предполагаемым мошенникам. Данная проблема особенно актуальна, если речь идёт о многопользовательской системе, поскольку одно и то же идентификационное имя может быть доступно разным пользователям.

Таким образом, исходя из сказанного выше, представляется возможным дать следующее определение рассматриваемому оперативно- розыскному мероприятию. Снятие информации с технических каналов связи – это

регламентированное законом об ОРД оперативно-розыскное мероприятие, проводимое на основании судебного решения, заключающееся в негласном съёме информации, передаваемой по сетям электрической связи, компьютерным и иным сетям.

Несмотря на то, что правоохранительные органы, как отмечалось выше, могут привлекать к сотрудничеству компании, предоставляющие услуги связи, мы настаиваем на только негласном характере снятия информации как оперативно-розыскного мероприятия. На это есть несколько причин. Во-первых, не всегда компании-провайдеры ставятся в известность о проводимом оперативно-розыскном мероприятии. Во-вторых, даже если эти компании привлечены к сотрудничеству в расследовании мошенничества, они не располагают всей информацией о том, какие именно действия будут производить субъекты расследования в ходе проведения мероприятия. В-третьих, ст. 17 Закона об ОРД чётко предписывает всем лицам, привлечённым к подготовке или проведению оперативно-розыскных мероприятий, держать в тайне сведения, ставшие им известными в ходе подготовки или проведения оперативно-розыскных мероприятий.

На сегодняшний день большой популярностью пользуется так называемая IP-телефония. Причём нередки случаи, когда такой вид связи комбинируется с обычной и/или мобильной телефонной связью. В этом случае необходимо говорить не только о снятии информации с технических каналов связи, но и о таком оперативно-розыскном мероприятии, как прослушивание телефонных разговоров.

Прослушиваться может связь как односторонняя (общение по очереди), двусторонняя, так и многосторонняя (конференцсвязь); как средство связи, принадлежащее определённому лицу (стационарный, сотовый телефон), так и средство связи, установленное в определённом месте, где бывает интересующее лицо (например, телефон в каком-либо заведении). Прослушиванию подлежит разговор всех абонентов, поскольку прослушивание только одного из них будет

являться не прослушиванием, а наблюдением с использованием специальных технических средств.

В тех случаях, когда для расследования интернет-мошенничества необходима дополнительная помощь, правоохранительные органы вправе привлечь для проведения оперативно-розыскного мероприятия лиц, напрямую не связанных с правоохранительной деятельностью, например, операторов связи.

Для повышения степени защищённости добытой информации и недопущения её искажения, представляется возможным рекомендовать сотрудникам правоохранительных органов использовать, по возможности, одноразовые носители информации, например, диски формата CD-R или DVD-R. Хотя данные носители до сих пор используются, их популярность отходит на второй план (предполагаем, из-за физических размеров, вместимости и относительно невысокой скорости записи/чтения). В этой связи имеет смысл обратить внимание на последние разработки в области производства карт памяти.

Обследование помещений, зданий, сооружений, участков местности и транспортных средств. При расследовании некоторых интернет-мошенничеств может возникнуть необходимость получения доступа к определённой информации, хранящейся в компьютере мошенника, подключённого к сети Интернет. На первый взгляд, подобное исследование можно отнести к снятию информации с технических каналов связи, однако, в силу следующих обстоятельств, такое утверждение будет не верным:

Снятие информации с технических каналов связи производится в отношении информации, находящейся в динамическом состоянии в каналах связи. Доступ к компьютерной системе мошенника осуществляется дистанционно. В случае же со снятием информации с каналов связи существует возможность более близкого контакта с исследуемым объектом.

Рассматриваемое оперативно-розыскное мероприятие, в контексте расследования мошенничества в сети Интернет, как компьютерного

преступления, задаёт специфику разыскиваемой информации. Дело в том, что речь идёт об информации, содержащейся в специфических материальных носителях, которые, являясь продуктом высоких технологий (жёсткие диски, карты памяти, лазерные диски и т. д.), далеко не всегда приспособлены для нахождения в незащищённой либо плохо защищенной среде. Поэтому, на наш взгляд, целесообразно ограничить круг обследуемых объектов. Можно опустить открытые участки местности, поскольку под воздействием природных явлений вероятность порчи носителей информации (даже если создать тайник) велика. К тому же речь может идти и об оборудовании, используемом мошенниками, приобрести которое достаточно проблематично (сканеры и устройства для создания поддельных кредитных карт, например).

Представляется возможным, также, исключить сооружения, поскольку мошенничество в сети Интернет, в отличие от традиционного мошенничества, часто не требует активных передвижений со стороны преступника. То же частично относится и к транспортным средствам, хотя здесь считаем, необходимым отметить, что в некоторых случаях обследование транспортного средства, которым пользовался мошенник, может принести пользу.

Сбор образцов для сравнительного исследования представляет собой оперативно-розыскное мероприятие, заключающееся в изъятии, получении предметов с целью их последующего оперативно-розыскного распознавания или идентификации. Данное мероприятие имеет сходство с получением образцов для сравнительного исследования (ст. 202 УПК РФ), однако к нему (сбору образцов для сравнительного исследования) не применяются процессуальные требования, и оно может осуществляться негласно.

К собираемым образцам принято относить традиционные криминалистические объекты: отпечатки пальцев рук, волосы, обувь и её следы, одежда, запаховые следы и т. п. Могут собираться образцы почерка, подписи (в том числе и цифровой), набранного на компьютере текста (для автороведческой экспертизы), образцы продукции, полуфабрикатов и т. д.

(например, заготовки кредитных карт или носители информации с дампами памяти этих карт, поддельные ценные бумаги и др.).

К проведению мероприятия могут привлекаться эксперты и лица, обладающие соответствующими специальными знаниями, а также применяться технические средства.

Достаточно большая часть учёных-криминалистов связывают сбор образцов для сравнительного исследования с материальными предметами. Однако с развитием преступности в сфере высоких технологий стал актуальным сбор образцов компьютерных программ. Компьютерные программы, в том числе, различные вредоносные программы, не являются материальными предметами. Тем не менее, закон об ОРД перечень собираемых образцов оставляет открытым. Сбор компьютерных программ для их исследования в настоящее время достаточно распространён.

Представляется необходимым отметить, что, поскольку количество вредоносных программ каждый день увеличивается, возникает логичная потребность в специальном учёте этих программ. С этой целью, на наш взгляд, успешно справляются компании производители антивирусных программ. Для целей своей деятельности они располагают специальными лабораториями, в которых, независимо от наличия возбуждённого уголовного дела, изучают все обнаруженные в Интернете вредоносные программы. Поэтому при расследовании мошенничества в сети Интернет, если известно, что мошенники использовали вредоносные программы, мы рекомендуем привлекать к расследованию специалистов антивирусных лабораторий. Вполне возможно, что выявленные вирусы или троянские программы уже исследованы этими специалистами. В этом случае можно исследовать и установить принцип действия конкретной программы, используемой мошенниками, примерное количество заражённых данной вредоносной программой объектов, а также, в некоторых случаях, установить её автора и распространителя.

Литература

1. Илюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: Дис. … канд. юрид. наук. Волгоград, 2008.

2. Коровин Н.К. Криминалистика: Учебное пособие. Новосибирск: НГТУ, 2016.

3. Яблоков Н.П. Криминалистика. М.: Юрайт, 2017.

4. Коровин Н.К. Особенности криминалистической идентификации несовершеннолетних // Сборники конференций НИЦ Социосфера. 2018. № 5.