УДК 343.985.7

Б.В. Ковалик

АКТУАЛЬНОСТЬ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ ПРИ ПРОВЕДЕНИИ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ

Развитие современных информационных технологий идет очень быстрыми темпами, обусловливая постоянное появление новых, весьма специфических возможностей для различных областей общественной жизни.

Глобальная сеть Интернет, связывающая большое число пользователей, представляет собой огромное хранилище информации, единую среду социального общения, а также площадку для различной деятельности людей. Информация, размещенная в интернете, в большей части носит позитивный и созидательный характер, реже – негативный, и, конечно, в интернете содержится информация, в той или иной степени представляющая интерес для правоохранительных органов, в частности для подразделений, осуществляющих ОРД. При наличии определенных навыков и (или) вспомогательных средств в виде программного обеспечения сотрудники подразделений, осуществляющих ОРД, грамотно используя сеть Интернет, могут получить огромное подспорье в раскрытии преступлений, совершенных как в интернет-пространстве, так и за его пределами.

Возможности интернета используются правоохранителями не в полном объеме и не имеют соответствующей регламентации в нормативных правовых и подзаконных актах. Также остро стоит вопрос научного определения и обоснования тактических аспектов проведения ОРМ в сети Интернет.

ОРД в нашей стране не задействует все возможности глобальной сети. По этой причине интернет представляет для правоохранительных органов среду, несущую в себе огромный потенциал для ОРД в части проведения и совершенствования мероприятий, уже закрепленных в Законе Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» (далее – Закон об ОРД). В то же время одной из первоочередных задач является осуществление научно-исследовательской деятельности в целях совершенствования законодательства для приведения его в соответствие с современными тенденциями и, соответственно, более эффективного противодействия преступности.

Как было сказано ранее, глобальная сеть может использоваться сотрудниками подразделений, осуществляющих ОРД, как один из инструментов при проведении ОРМ. При этом она не требует каких-либо вспомогательных средств и специализированной материальной базы. Так, например, имея только мобильный телефон с доступом в интернет, сотрудник ОВД может проводить оперативный опрос не только непосредственно либо посредством сети электросвязи, но и в ходе переписки при помощи мессенджеров, аккаунтов в социальных сетях и т. д. При этом результаты данного опроса сразу же фиксируются в памяти устройства, с которого осуществлялась отправка сообщений.

В настоящее время многие пользователи глобальной сети размещают на различных интернет-ресурсах большое количество сведений о себе. Грамотный подход к изучению учетных записей лиц, представляющих интерес для подразделений, осуществляющих ОРД, может послужить серьезным подспорьем для получения информации об образе жизни, связях и даже местоположении фигуранта. Ввиду того, что особо активные пользователи социальных сетей нередко оставляют достаточно большое количество публикаций с фиксацией времени и привязкой к месту посредством GPS, подобная тактическая последовательность может тесно граничить с наблюдением.

Регулярно посещая различные тематические группы и форумы, на которых общаются пользователи, осуществляющие противоправную деятельность (например, ресурсы так называемой теневой сети), а также принимая участие в ведущихся там обсуждениях и получая при этом сведения, представляющие интерес, сотрудники в широком смысле осуществляют не что иное, как оперативное внедрение.

Однако данные примеры по большому счету являются лишь формами проведения уже закрепленных в Законе об ОРД мероприятий.

Изучение опыта зарубежных правоохранителей, а также оценка тенденций развития преступности обусловливают постановку вопроса о необходимости наличия возможности проведения негласных ОРМ, связанных с удаленным контролем аппаратных компонентов цифровых устройств, находящихся в пользовании лиц, представляющих интерес для решения задач ОРД. Появление подобных ОРМ позволит упростить копирование и перехват информации, содержащейся и передаваемой на средства компьютерной техники, находящейся в пользовании у лиц, осуществляющих противоправную деятельность.

Опыт западных коллег показывает, что проведение подобных ОРМ вполне реально. Так, в ФРГ Законом от 17 августа 2017 г. «О повышении эффективности и практикоориентированности осуществления уголовного судопроизводства» перечень негласных следственных действий дополнен онлайновым обыском, предусматривающим возможность негласного доступа к персональному компьютеру и подобным ему устройствам затрагиваемого лица с целью ознакомления с содержанием находящихся на них файлов, а также предусмотрена возможность осуществления контроля телекоммуникаций путем такого проникновения. Подобные мероприятия проводятся и в других европейских странах (Австрия, Франция, Швейцария), не стоят на месте и законодатели в Российской Федерации. Перечень ОРМ Федерального закона об ОРД был дополнен новым мероприятием – «получение компьютерной информации».

Наличие подобных возможностей у правоохранителей сможет существенно облегчить решение стоящих перед ОРД задач, что повлечет более эффективное раскрытие преступлений. Грамотный подход к анализу существующей оперативной обстановки и изучению опыта зарубежных коллег при разработке и применении законодательства в данной сфере в перспективе позволит внести необходимые изменения в действующий Закон об ОРД.

Подводя итоги, следует отметить, что проведение ОРМ в сети Интернет является не только возможным или оправданным с точки зрения практики, но и необходимым, поскольку сама виртуальная среда представляет собой неотъемлемую часть жизнедеятельности человека. В связи с этим видится необходимым законодательно регламентировать право органов, осуществляющих ОРД, разрабатывать и использовать программное обеспечение, предназначенное для удаленного негласного сбора информации на средствах компьютерной техники.

УДК 343.985

А.А. Ковальчук

СЛЕДЫ КАК ЭЛЕМЕНТ ИНФОРМАЦИОННОЙ МОДЕЛИ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ РЕКВИЗИТОВ БАНКОВСКИХ ПЛАТЕЖНЫХ КАРТОЧЕК

Преступление, являясь междисциплинарной категорией, изучаемой с позиции всех наук уголовно-правового цикла, находится в центре внимания многих ученых. При этом следует отметить склонность значительной части исследователей рассматривать преступление как сложную систему, что предполагает изучение его модели.

Модель преступления традиционно представляется исследователями в виде структуры, которая состоит условно из неделимых элементов, обладающих устойчивыми закономерными связями. При этом важно заметить, что науки уголовно-правового цикла, изучая преступление в преломлении к «собственному» предмету, целям и задачам, включают в состав разрабатываемых моделей (например, криминалистической характеристики, оперативно-розыскной характеристики и др.) структурные элементы, которые по своей сути являются универсальными.

Одним из указанных элементов, имеющих, по нашему мнению, существенное значение при построении информационной модели хищений, совершаемых с использованием реквизитов банковских платежных карточек (БПК), являются следы (следовая картина). Это обусловлено тем, что в процессе обнаружения и первоначального исследования следов сотрудниками подразделений по раскрытию преступлений в сфере высоких технологий устанавливается сущность произошедшего криминального события, а также осуществляется планирование оперативно-розыскной работы с целью получения ответов на вопросы о том, кто, каким способом, при каких условиях совершил преступление рассматриваемого вида.

Традиционно в науке принято выделять идеальные и материальные следы. Применительно к хищениям, совершаемым с использованием реквизитов БПК, под идеальными следами следует понимать образы, сохранившиеся в сознании очевидцев и непосредственных участников преступного события. В свою очередь, к материальным относятся следы, представленные в виде объектов материального мира, таких как комплексы программно-технических средств, иные предметы (например, «белый пластик») и документы, а также следы, свидетельствующие о физическом воздействии лица на указанные объекты (например, следы пальцев рук).

В современной отечественной и зарубежной литературе, в том числе научной, достаточно часто используется термин «виртуальное пространство», предназначенный для описания созданного техническими средствами «мира», включающего объекты и субъекты, воспринимаемые человеком посредством органов чувств. Более того, изучение оперативно-розыскной практики подразделений по раскрытию преступлений в сфере высоких технологий показало, что лица, совершающие хищения с использованием реквизитов БПК, склонны к созданию виртуальных (сетевых) образов, имеющих конкретные имена, с которыми они себя связывают. Поэтому в отношении преступлений рассматриваемого вида мы считаем уместным выделение дополнительной группы следов – виртуальные следы. При этом следует отметить, что относительно данной категории в научном сообществе существует несколько дискуссионных моментов. Так, до настоящего времени нет единого мнения по поводу самого названия. Предлагаются такие варианты, как «компьютерные следы», «виртуальные следы», «электронно-цифровые следы», «информационные следы», «компьютерно-технические следы». Также ученые спорят о природе указанных следов и их месте в общей классификации следов.

Нам наиболее близок подход российского ученого В.А. Мещерякова, который в своем диссертационном исследовании на соискание ученой степени доктора юридических наук достаточно убедительно обосновал необходимость введения понятия виртуальных следов (промежуточного между материальными и идеальными), определяемых как любое изменение состояния автоматизированной информационной системы (образованного ею кибернетического пространства), связанное с событием преступления и зафиксированное в виде компьютерной информации (т. е. информации в виде, пригодном для машинной обработки) на материальном носителе, в том числе на электромагнитном поле. Также уместно обратить внимание на то, что данной позиции придерживаются и многие другие ученые.

В результате изучения специальной литературы и практики работы подразделений по раскрытию преступлений в сфере высоких технологий можно выделить ряд особенностей и свойств виртуальных следов, которые, по нашему мнению, являются значимыми с позиций теории оперативно-розыскной деятельности. Во-первых, следует отметить, что источником виртуального следа является компьютерная информация, которая, в свою очередь, хранится на определенном носителе. Данное утверждение обусловливает то, что в ходе исследования самого носителя возможно получение доступа к материальным следам, при этом фиксация виртуальных следов может быть осуществлена при изучении компьютерной информации. В этом контексте значимой является возможность зафиксировать виртуальный след удаленно, т. е. не имея физического доступа к носителю компьютерной информации.

Во-вторых, важнейшим свойством виртуальных следов является отсутствие единой физически целостной структуры. Речь идет о том, что виртуальный след может состоять из множества отдельных информационных элементов, распределенных в различных областях виртуального пространства. Также следует понимать, что сложность структуры виртуального