

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 обуславливает 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

следа обусловлена включением как значимой уголовно-релевантной информации, так и сопутствующих вспомогательных данных, обеспечивающих его целостность и доступность.

В-третьих, особенностью является и то, что виртуальный след, хранящийся на материальном носителе, недоступен для восприятия человека без применения комплекса программно-технических средств. При этом, с учетом возможности использования средств защиты компьютерной информации, для фиксации виртуальных следов могут быть необходимы специализированные средства. В данном контексте следует учитывать возможность уничтожения следов при попытке фиксации с использованием программно-технических средств, а также возможность неправильного или неточного считывания.

Таким образом, следы являются важнейшим элементом информационной модели хищений, совершаемых с использованием реквизитов БПК. Особенность преступлений рассматриваемого вида заключается в необходимости наряду с идеальными и материальными следами выделять такую группу, как виртуальные следы. Следует также обозначить, что данный элемент указанной информационной модели находится в тесной взаимосвязи с другими ее элементами, и в первую очередь со способом совершения рассматриваемого преступления, так как от последнего зависит то, какие следы, где и каким образом могут быть зафиксированы.

УДК 343

*В.Е. Козлов*

### **О ФУНКЦИЯХ ОПЕРАТИВНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ КОМПЬЮТЕРНОЙ ТЕХНИКИ**

Для постановки и разрешения проблемных вопросов оперативно-технического обеспечения (ОТО) противодействия преступлениям, совершаемым с использованием средств компьютерной техники (ПСИСКТ), нами были выявлены основные тенденции совершения преступлений, обусловленные уровнем развития информационных технологий, социально-экономических отношений в обществе и иными объективно существующими факторами. Такими тенденциями являются:

непрерывный рост уровня так называемой высокотехнологичной преступности, проникновение преступности в информационную сферу жизни общества, усиливающийся криминальный контроль над информационными ресурсами;

расширяющееся применение информационных (компьютерных) технологий в криминальной деятельности, сращивание компьютерной и общеуголовной преступности. Применяемые преступниками современные технологии разнообразны по структуре, содержанию и часто эффективнее технологий правоохранительной деятельности, в том числе технологий оперативно-розыскного назначения. Отмечено использование технологий информационного противодействия;

повышение «криминальной квалификации» субъектов совершения преступлений, совершенствование средств компьютерной техники (СКТ), используемых в качестве орудия их совершения, исследование организации работы с конфидентами оперативных подразделений правоохранительных органов и, как следствие, совершенствование конспиративности действий правонарушителей, направленных на подготовку и совершение преступлений, активное противодействие проведению ОРМ;

совершенствование способов криминогенных воздействий средств массовой информации, в том числе использование глобальных телекоммуникаций при приготовлении и совершении преступлений. Активное дискуссионное обсуждение характерных ошибок преступников, моделирование определенных информационных объектов и отношений, благоприятствующих решению противоправных задач;

неконтролируемое использование специальной техники и СКТ для достижения результатов преступной деятельности.

Порождаемые указанными обстоятельствами проблемные вопросы требуют от национальных правоохранительных органов эффективных и адекватных мер, направленных на их разрешение. Разработка и совершенствование этих мер обуславливаются следующим:

применением специально уполномоченными государством субъектами сил, средств, методов, технологий, недоступных (выходящих за пределы компетенции) для ряда субъектов правоохранительной деятельности;

появлением и развитием новых видов деятельности правоохранительных органов, вызванным резким возрастанием объема компьютерной информации (КИ), представляющей оперативный интерес, хранящейся, передаваемой и обрабатываемой в информационных сетях при помощи СКТ. Следует признать, что во многих случаях выявления и расследования преступлений единственным источником поступления информации о преступной деятельности являются материалы, полученные в ходе ОТО.

Выявленные тенденции развития преступности корректируют содержание деятельности по противодействию ей, детерминируемое необходимостью получения и документирования в ходе осуществления ОРД КИ из СКТ с использованием специальных технологий и средств; обеспечения компьютерной безопасности (КБ) субъектов ОРД; использования для этого специфических знаний и методов, а также непрерывным процессом повышения квалификации субъектов, осуществляющих рассматриваемые аспекты противодействия.

Новеллой, по нашему мнению, является выделение оперативно-технической составляющей ОРД как деятельности, направленной на противодействие преступности, и одновременно элемента национальной системы противодействия ей в самостоятельное направление научных исследований. Субъекты, цель, задачи, функции ОТО определены его местом и ролью в национальной системе противодействия преступности, а используемые силы, средства и методы – местом и ролью в структуре ОРД правоохранительных органов. Причем с методами ОРД в процессе противодействия преступности сочетаются методы иных отраслей науки (КБ, криминалистики, криминологии, уголовного процесса, информационного, уголовного и