ОСОБЕННОСТИ МЕТОДИКИ РАССЛЕДОВАНИЯ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ПОМОЩЬЮ СЕТИ ИНТЕРНЕТ

FEATURES OF THE INVESTIGATION OF THE THEFT COMMITTED IN THE INTERNET

N. Korovin

Annotation

The article examines the elements of the forensic characteristics, points out the need for interaction of the investigator with specialists and operational personnel, proposed an investigation program at the initial and subsequent stage of investigation of the theft committed with the help of the Internet.

Keywords: criminalistic characteristics, investigative actions, operative–search measures, the program of investigation of crimes.

Коровин Николай Кондратьевич
Ст. преподаватель,
Новосибирский государственный технический университет

Аннотация

В статье рассмотрены элементы криминалистической характеристики, указано на необходимость взаимодействия следователя со специалистами и оперативными работниками, предложена программа расследования на первоначальном и последующем этапе расследования хищений, совершённых с помощью сети Интернет.

Ключевые слова:

Криминалистическая характеристика, следственные действия, оперативно–розыскные мероприятия, программа расследования преступлений.

Использование потенциалов глобальной сети Интернет имеет тенденцию к устойчивому росту преступной деятельности в сфере компьютерных преступлений, раскрытие которых осложняется новым типом преступников, использовавших новые способы совершения с применением технически сложных аппаратных и программных средств.

Согласно п. 1 примечания к ст. 158 УК РФ: "под хищением понимаются совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества" [9].

В основе методики расследования преступлений лежит использование элементов криминалистической характеристики, основывающихся на типичных ситуациях ранее раскрытых дел, знание которых позволяет значительно сузить круг лиц, среди которых следует искать преступника, путем проведения следственных действий и оперативно–розыскных мероприятий, как на первоначальном, так и последующем этапах расследования хищений, совершённых с помощью сети Интернет.

По мнению Р.С. Белкина: криминалистическая характеристика состоит из таких элементов: "характеристика типичной исходной информации; система данных о типичных способах совершения и сокрытия данного вида преступлений и типичных последствиях их применения; личность вероятного преступника и вероятные мотивы и цели преступления; личность вероятной жертвы преступления и данные о типичном предмете посягательства; данные о некоторых типичных обстоятельствах совершения преступления (место, время, обстановка); данные о типичных обстоятельствах, способствовавших совершению конкретного вида, рода преступлений" [1].

Наиболее распространённым способом хищения денежных средств с помощью сети Интернет, является взлом страниц в социальных сетях (аккаунтов). Социальная сеть понимается, как часть информационного пространства сети Интернет (совокупность веб–сайтов, платформ, онлайн–сервисов), в которой возможна организация социального взаимодействия. Такое понимание способствует тому, что объектами преступления становятся не только "традиционные" социальные сети ("ВКонтакте", "Одноклассники"), но и такие сервисы, как ICQ, Skype, mail.ru и др. [3]

Основными способами являются взлом аккаунтов, кардинг, фишинг, получение кредита, писем, интернет магазины, "инвестиционные схемы" и "заработок", а так же мошенничество в онлайн–играх и прочее, как особенность представлены электронные следы, в виде переписок, в электронной почте, в различных служебных журналах, в виде показаний регистрирующей аппаратуры, пеленгующих и радиосканирующих устройств, компьютери–

зированных анализаторов для проводных сетей электросвязи; аппаратуры по контролю и регистрированию соединений абонентов в сетях электросвязи и т.д. Преступления совершают, как правило, мужчины в возрасте 18–35 лет, обладающие высоким интеллектом и имеющие высокий уровень познаний в области информационно-телекоммуникационных технологий в отношении лиц имеющих доверчивый характер, имеющих желание купить подешевле, получить какую-либо при этом выгоду и слабо знакомых с техникой безопасности при работе в сети Интернет.

Знание совокупности взаимосвязанных, криминалистически значимых данных о хищениях, совершаемых с помощью сети Интернет, содержащихся в криминалистической характеристике, позволяет методически правильно определить типовые следственные ситуации, и в целом организовать расследование.

При организации расследования хищений, совершённых с помощью сети Интернет, при выдвижении и проверке версий необходимо учитывать в первую очередь сообщение об обстоятельствах и способах совершения преступления, а именно о нарушении целостности информации, информационных систем, об Интернет соединениях, балансе счетов и только далее о наличии причинной связи между криминальным пользованием и наступившими последствиями. Направление расследования во многом определяется общими следственными версиями и версиями об основных обстоятельствах события преступления. В сложных следственных ситуациях проверка каждой указанной версии образует отдельное направление расследования [6]. Разработка версий и их проверка является основой построения плана [5].

В целях организации эффективного расследования хищений, совершённых с помощью сети Интернет, необходимо: при составлении плана отталкиваться от конкретной сложившейся следственной ситуации; выдвинуть в соответствии с данной сложившейся ситуацией все возможные версии; определить в соответствии с выдвинутыми версиями задачи; в соответствии с определёнными задачами выработать программу комплекса следственных действий и оперативно розыскных мероприятий для их решения. Для разрешения проверочных ситуаций могут осуществляться оперативно-розыскные мероприятия [7], а в соответствии со ст. 186.1 УПК РФ информация о соединениях между абонентами и (или) абонентскими устройствами может быть получена следователем на основании судебного решения, если имеются достаточные основания полагать, что такая информация имеет значение для уголовного дела [8].

Основными следственными действиями и оперативно – розыскными мероприятиями, востребованными при расследовании хищений, совершённых с помощью сети Интернет на первоначальном этапе расследования и имеющими существенные особенности, в первую очередь является и производится осмотр места происшествия, а также осмотр предметов, документов и иных носителей информации, в том числе виртуальных.

Первейшей задачей является определение местонахождения всех компьютеров (планшетов, телефонов и т.д.), связанных с совершением хищения. Следует иметь ввиду, что подключенные к компьютеру периферийные устройства, а также несколько компьютеров, объединенных в сеть, могут располагаться в разных помещениях – при этом проводится обыск (осмотр) одновременно во всех помещениях, где установлены компьютерные средства. Не нужно ограничиваться поиском информации только в компьютере, также нужно внимательно осмотреть имеющиеся документы, вплоть до записей на клочках бумаги (например, записи о паролях, пользователях, какой-либо план и т.д.) [4].

Важно уделить особое внимание тому, что, как и любое следственное действие, следственный осмотр разделяют на следующие стадии: подготовительную, рабочую, фиксации и оценки результатов. На подготовительной стадии определяются цели и объекты осмотра, состав следственно-оперативной группы, в которую входят: следователь, являющийся руководителем группы, оперативный работник, специалист и др. На рабочей стадии осмотра при расследовании хищения, совершённого с помощью сети Интернет следует в первую очередь определить состояние компьютера, его подключение к сети Интернет, локальной или иной сети. По результатам осмотра и по мере обнаружения вещественных доказательств происходит фиксация следов и их упаковка. При этом, как правило, следует персональные компьютеры, а именно системные блоки, после внешнего осмотра, выключить, по возможности все разъёмы опечатать. Упаковку и перевозку осуществлять в обстановке, исключающую повреждение информации в устройствах. Стадия оценки результатов является заключительной формой проведения следственного действия, на которой следователь и иные участники осмотра оценивают полученные результаты с возможностью их использования в дальнейшем расследовании преступления. Важно своевременно проводить анализ, привлекая к этому квалифицированных специалистов. Для участия в осмотре места преступления, связанного с хищениями, совершёнными с помощью сети Интернет, должны быть приглашены специалисты, которые знают специфику работы данного объекта, но не заинтересованы в деле [2].

Особенностью является то, что при хищениях, совершённых с помощью сети Интернет осмотр места происшествия может состоять из нескольких осмотров: осмотр компьютера у потерпевшего, выемка электронной информации, с электронной почты, переписки в социальных

сетях, электронные платежи и т.д.; осмотр или снятие информации с сервера провайдера; осмотр компьютера у подозреваемого, выемка электронной информации, с электронной почты, переписки в социальных сетях, электронные платежи и т.д. В связи с большим многообразием технических устройств, имеющих функции обработки компьютерной информации, объектом осмотра могут быть также планшеты, смартфоны, сотовые устройства и иные устройства. При этом необходимо проводить фиксацию событий с помощью видео– и аудиозаписи, фотосъёмки, информационных систем и других технических средств. Обязательным считается приложение к протоколу осмотра плана или схемы места преступления. Необходима принципиальная схема, отображающая соединения компьютерных и технических средств снабжения информацией между собой и подсоединение к каналам электросвязи. Ещё одной особенностью является то, что кроме информации, размещённой на видимых местах сайтов, она может быть расположена в различных специальных журналах, в виде истории переписки или служебных файлах, в чём нам может помочь проведение компьтерно–технических экспертиз.

При расследовании хищений, совершённых с помощью сети Интернет на последующем этапе основной задачей является процесс доказывания, осуществляемый путём развёртывания уже имеющихся исходных данных и получение новых фактов и обстоятельств в целях собирания, исследования, оценки и использования доказательств и установления всех элементов предмета доказывания.

Предлагается следующая программа, которая выражается в определённой последовательности следственных действий:

- обыск, предметом которого могут быть не только разнообразные средства вычислительной техники (компьютер, планшет, телефон и т.д.), машинные носители и содержащаяся на них компьютерная информация, но и документы, средства электросвязи, разработанные и приспособленные специальные технические средства и устройства, бытовые электротехнические устройства и оборудование, материалы и инструменты;
- выемка проводится в целях изъятия машинных носителей и технических средств, содержащих искомые файлы или программы, используемых для подготовки и совершения преступлений рассматриваемой категории. Такие носители информации чаще всего находятся в компьютерах лиц, подозреваемых в совершении преступления;
- допрос при расследовании хищений, совершённых с помощью сети "Интернет", предполагает участие специалиста или в качестве консультанта (перед началом следственного действия);
- наложение ареста на имущество – чаще всего используется с электронными денежными средствами, числящимися на счетах, открытых преступниками на себя или иных лиц в электронных платёжных системах;
- по необходимости, в зависимости от конкретной ситуации: очные ставки; назначение и производство экспертиз, предъявление для опознания, следственный эксперимент, проверка показаний на месте и т.д.

ЛИТЕРАТУРА

1. Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. От теории – к практике. – М.: Юрид. лит. 1988. – 304 с.
2. Вехов В.Б., Попова В.В., Илюшин Д.А. Тактические особенности расследования преступлений в сфере компьютерной информации: Научно–практическое пособие. – Самара: ООО "Офорт", 2003. – 188 с.
3. Ефимов Е.Г. Социальные интернет–сети (методология и практика исследования) : монография / Е.Г. Ефимов. – Волгоград : Волгоград. науч. изд–во, 2015. – 169 с.
4. Комиссаров В., Гаврилов М., Иванов А. Обыск с извлечением компьютерной информации / Законность, 1999. – № 3. – С. 12–15.
5. Лузгин И.М. Методологические проблемы расследования.– М.: Спарк–1973.– 216 с.
6. Морозова Е.А. Теория и практика первоначального этапа расследования фальшивомонетничества : автореферат дис. ... канд. юрид. наук/ МГЮА имени О.Е. Кутафина.– Москва, 2013.– 25 с.
7. Об оперативно–розыскной деятельности: Федеральный закон: принят 12 августа 1995 г. (№ 144–ФЗ) // Официальный интернет–портал правовой информации http://www.pravo.gov.ru (дата обращения: 17.09.2017).
8. Уголовно–процессуальный кодекс Российской Федерации: принят 18 декабря 2001 г. (№ 174–ФЗ) // Официальный интернет–портал правовой информации http://www.pravo.gov.ru (дата обращения: 17.09.2017).
9. Уголовный кодекс Российской Федерации: принят 13 июня 1996 г. (№ 63–ФЗ) // Официальный интернет–портал правовой информации http://www.pravo.gov.ru (дата обращения: 17.09.2017).