ТИПИЧНЫЕ СЛЕДСТВЕННЫЕ СИТУАЦИИ ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ ХИЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ

БЕЛОМЫТЦЕВ Н.Н.,
адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь

На основе анализа судебно-следственной практики выделены наиболее типичные следственные ситуации, складывающиеся на первоначальном этапе расследования хищений, совершенных путем использования компьютерной техники. Разработаны и предложены алгоритмы (программы) деятельности следователя применительно к каждой из них.

Based on the analysis of forensic practice, the author identifies the most typical investigative situations that develop at the initial stage of the investigation of thefts committed with the use of computer technology and suggests algorithms (programs) of the investigator's activity in relation to each of them.

В ходе расследования уголовных дел деятельность следователя направлена на решение задач, изложенных в ст. 7 УПК Республики Беларусь. В этой связи УПК предлагает достаточно широкий арсенал уголовно-процессуальных средств, эффективность применения которых значительно возрастает при условии использования криминалистических средств и методов. В силу ряда объективных и субъективных причин в то же время они в практической деятельности в полной мере используются не всегда. Представляется, что наиболее эффективное криминалистическое средство – ситуационный подход в процессе расследования рассматриваемых преступлений. На наш взгляд, это дает возможность алгоритмизировать процесс расследования уголовных дел; разрабатывать и вводить в следственную практику на основании практического опыта современные методы и средства, показывающие свою эффективность и позволяющие уменьшить количество процессуальных и тактических ошибок, допускаемых сотрудниками органа дознания и следователями; производить исследования обстоятельств дела в полном объеме, всесторонне и объективно; оптимизировать образовательный процесс в учебных заведениях и т.д.

В криминалистике широко используется *ситуационный подход* (Л.Я.Драпкин, Р.С.Белкин, Т.С.Волчецкая, В.К.Гавло, А.Н.Колесниченко, Г.А.Зорин и др.). Анализ научных работ позволяет предложить свое определение типичных следственных ситуаций по делам о хищениях с использованием компьютерной техники на первоначальном этапе расследования. Здесь понимается неоднократно повторяющиеся условия (обстановка), в которых осуществляется процесс расследования преступлений, обусловленный преимущественно информационным компонентом (наличием либо отсутствием подозреваемого), а также факторами объективного, субъективного и случайного характера в определенный момент расследования.

Самым сложным и трудоемким, требующим от следователя значительных усилий для успешного проведения следственных и иных процессуальных действий, как правило, является первоначальный этап расследования уголовного дела. Так, исследование показало, что для 56,1 % следователей исправление допущенных ошибок на первоначальном этапе расследования в дальнейшем было невозможным, либо очень затруднительным, 65,9 % сотрудников отметили, что именно первоначальный этап вызывает наибольшие затруднения.

Содержание ситуационного подхода при расследовании хищения путем использования компьютерной техники на всех стадиях предварительного расследования заключается в его рассмотрении и анализе с точки зрения составляющих его ситуаций.

Иначе говоря, любая незнакомая ситуация сводится к ранее известной. В связи с чем необходимо выделить основания для типизации ситуаций и определение наиболее подходящих алгоритмов для их разрешения [1, с. 4].

Изучение следственных ситуаций, складывающихся при хищении путем использования компьютерной техники, осуществлялось В.В.Крыловым [2], А.В.Остроушко [3], Ю.В.Гаврилиным и соавторами [4], В.В.Коломиновым [5], А.Н.Яковлевым и Н.В.Олиндер [6]. Исследования названных авторов проводились с учетом российского законодательства и не в полной мере могут быть адаптированы к белорусским условиям. В этой связи был проведен анализ и обобщение судебно-следственной практики с целью выделения наиболее типичных следственных ситуаций, имеющих место на первоначальном этапе расследования (изучено 231 уголовное дело, в их числе приостановленные производством в порядке п. 1 ч. 1 ст. 246 УПК (в связи с неустановлением лица, подлежащего привлечению в качестве обвиняемого), а также дела, по которым приговор вступил в законную силу). За основу деления ситуации, складывающейся на первоначальном этапе расследования, нами использовался информационный компонент следственной ситуации – наличие либо отсутствие подозреваемого лица (по уголовному делу оказывает огромное влияние на установление всех обстоятельств совершенного преступления, полноту, объективность и всесторонность расследования).

С учетом этого при изучении уголовных дел, приостановленных (прекращенных) производством, а также тех, по которым приговоры вступили в законную силу, ниже автором были выделены *типичные следственные ситуации*, присущие первоначальному этапу расследования хищений с использованием компьютерной техники, и их разновидности:

1. Лицо, причастное к хищению, не установлено (61,9 % изученных уголовных дел). Разновидности: 1.1. Какая-либо информация о лице (лицах), причастном к его совершению, отсутствует (46,7 % изученных уголовных дел). 1.2. Информация о лице (лицах), причастном к его совершению, неполная либо неточная (15,2 % изученных уголовных дел).

2. Лицо, причастное к хищению, установлено (38,1 % изученных уголовных дел). Разновидности: 2.1. Достоверно установлена причастность к его совершению некоторых лиц (29,1 % изученных уголовных дел); 2.2. Установлены все или основной состав преступной группы (9,0 % изученных уголовных дел).

Алгоритм действия следователя *при наличии ситуации* 1.1. В первую очередь следственные и иные процессуальные действия должны быть направлены на установление личности субъекта преступления; определение способа совершения несанкционированного доступа к электронно-цифровой системе или сети, повлекшие достижение преступного результата (хищение денежных средств); установление места, времени и других обстоятельств, относящихся к обстановке места происшествия и образующих предмет доказывания. При этом осуществляется выявление обстоятельств, способствовавших неправомерному доступу к электронно-цифровой информации, после чего «прибегают» к мысленному моделированию события, выдвигая следственные версии об обстоятельствах происшедшего и т.д.

В этой связи анализ судебно-следственной практики свидетельствует о необходимости проведения определенных действий. К ним относятся следующие. А. Проведение выемки (либо изъятия в ходе осмотра места происшествия) носителей электронно-цифровых данных (флеш-накопители, винчестеры и т. д.), других документов и сведений у потерпевшего. По возможности следует создать побитовую копию с хеш-суммой данных, хранящихся на указанных носителях, и провести последующий ее осмотр в удобное для следователя время и месте; при необходимости привлечь специалиста. Б. Осуществление выемки электронной формы журнала сведений об интернет-сессиях в компании интернет-провайдера или оператора связи программно-технических устройств потерпевшей стороны за период предположительного осуществления хищения.

В. Проведение выемки в финансовых организациях отправителя и получателя похищенных денежных средств, материалов внутренней проверки по факту хищения, а также журналов работы учетной записи потерпевшего в системе интернет-банкинг и иных дистанционных продуктов обслуживания за необходимый период, сведений о платежном распоряжении, использованных для похищения денежных средств, сведений о получателях платежей, их назначении и других документов и сведений в связи с происшедшим; носителей электронно-цифровой информации, содержащих записи с видеокамер банкомата и других видеокамер, имеющих отношение к хищению денежных средств (либо копии файлов данных записей) и т.д. Г. Проведение осмотра изъятых (либо в ходе осмотра места происшествия) носителей электронно-цифровых данных с имеющейся на них информацией, а также иных документов с участием специалиста в области информационных технологий. Д. Принятие решения о признании потерпевшим, а также признании организации гражданским истцом и его представителем. Е. Осуществление допросов: потерпевшего (его представителя), работников финансовых организаций отправителя и получателя похищенных денежных средств (уполномоченных на оформление и проверку платежных распоряжений, администраторов систем ДБО и АБС кредитной организации, администраторов безопасности кредитной организации) и иных свидетелей. Ж. Назначение компьютерно-технической экспертизы носителей электронно-цифровых данных, программно-технических средств, а также экспертизы радиоэлектронных устройств. З. Проведение комплексных оперативно-розыскных мероприятий (далее – ОРМ) по установлению пользователей данных устройств и их проверки на причастность к совершению преступления (поручить сотрудникам оперативного подразделения) при установлении местонахождения программно-технических устройств, с которых производилось распространение вредоносных программ и их принадлежность. И. Установление в процессе проведения перечисленных мероприятий и следственных действий возможности идентификации лиц, осуществивших покупку, либо получение имущества, купленного за похищенные средства, осуществивших обналичивание похищенного имущества через банкомат или кассу финансовой организации; установление таких лиц (поручить сотрудникам оперативных подразделений) («мулов») путем проведения необходимых ОРМ. К. Разработка дополнительного плана следственных, оперативно-розыскных и иных мероприятий (в частности о некоторых из них пойдет речь далее) в случае установления лиц (-а), причастных (-ого) к совершению хищения, следует с участием сотрудников оперативных подразделений и специалиста в сфере информационных технологий.

Алгоритм действий следователя *при возникновении ситуации 1.2*, когда информация о лице (-ах), причастном (-ых) к его совершению, неполная либо неточная. 1. Осуществление комплекса следственных и иных действий, предусмотренных п. 1–9 указанной ранее следственной ситуации. 2. Поручение сотрудникам оперативного подразделения установить личности и местонахождение лиц, осуществивших написание вредоносного программного обеспечения, лиц, осуществлявших снятие денежных средств или обналичивание, их непосредственных руководителей и иных фигурантов преступления, путем осуществления ОРМ и иных мероприятий. 3. Проведение совместно с сотрудниками оперативных подразделений и специалиста в информационной сфере аналитической работы по установлению связей с другими участниками преступной группы и причастности к другим фактам хищений, а также всех остальных обстоятельств расследуемого хищения. В случае если виновное лицо продолжает снятие денежных средств, необходимы следующие действия. А. Направить поручение сотрудникам оперативного подразделения о проведении комплекса ОРМ в отношении установленных лиц с целью проверки их на причастность к совершенному преступлению; осуществить прослушивание и запись переговоров (ст. 214 УПК); наложение ареста на почтово-телеграфные и иные отправления, их осмотр и выемка (ст. 213 УПК); прослушать и осмотреть аудиозаписи, полученные в ходе осуществления контроля и записи переговоров.

Произвести осмотр документов, содержащих информацию о соединениях между абонентами, осмотр информации, полученной в ходе ОРМ – контроль в сетях электросвязи; провести проверку имеющихся (полученных) данных по оперативно-справочным, криминалистическим и иным учетам, и базам данных на предмет причастности к хищению. Б. Осуществить выемки всех сведений и документов по счетам, имеющихся у лиц, причастных к расследуемому хищению. В. Провести осмотр, а также последующий анализ имеющихся сведений и документов с целью определения периодов, конкретного времени, сумм, путей и цепочки перевода имущества (иные счета, электронные кошельки, обналичивание и т.д.), полученного в результате совершения преступления.

Данная программа может корректироваться с учетом поступающей информации (о связях участников преступной группы.). При этом необходимо также провести ряд ОРМ и следственных действий, направленных на фиксацию связей (контактов) между установленными участниками преступной группы и их руководителем, а также с организатором программных атак на компьютерную систему, сеть, и по возможности с другими членами преступной группы (заливщиками, операторами, «мулами», прозвонщиками и т.д.).

При поступлении информации об организаторах атак и обналичивании, а также других членах преступной группы программу действий рекомендуется корректировать с целью установления их связей и установления их преступных функций и деятельности остальных неустановленных соучастников (программисты, траферы, владельцы или авторы связки эксплойтов, иного вредоносного программного обеспечения, криптора, поставщика доменов и серверов и иных). Далее по мере поступления информации логично запланировать следственные действия и ОРМ, направленные на задержание всех установленных членов преступной группы. В зависимости от складывающейся следственной ситуации задержание необходимо производить одновременно, чтобы исключить возможность скрыться кому-либо из участников преступной группы, уничтожить какие-либо следы преступления и оказать противодействие расследованию в иных формах. Вместе с тем в некоторых случаях следует планировать задержание отдельных участников хищения (например, «мулов», руководителя обнальщиков и дроперов и др.). Обстоятельствами, которые могут повлиять на принятие такого решения, являются отсутствие прямой связи между отдельными членами преступной группы, общение между некоторыми из них с использованием программно-технических средств, с элементами анонимности, а также возможность и сведения о намерении участника скрыться (выехать за рубеж и т.д.) и др. Г. Проведение мероприятий, направленных на задержание и допрос в качестве подозреваемых членов преступной группы. Желательно сам факт задержания «мула» и руководителя обнальщиков осуществить в момент очередного снятия и обналичивания денежных средств. При этом во время задержания необходимо изымать кроме средств обналичивания также все электронно-цифровые средства связи и иные устройства, которые следует осмотреть на предмет установления контактов (связей), мест нахождения в конкретный период времени и т.д. Д. Проведение обысков с участием соответствующих специалистов по месту жительства, регистрации задержанных, иных членов преступной группы и иных местах, где предположительно могут находиться средства хищения, программно-технические устройства, электронно-цифровые средства связи, а также устройства обналичивания и т.д. Е. Проведение опознания свидетелями участников преступной группы как лиц, причастных к хищению денежных средств. Ж. Оценка собранных по уголовному делу доказательств для принятия решения о предъявлении обвинений участникам преступной группы, избрание меры пресечения. З. Рассмотрение и разрешение возможно поданных заявлений, ходатайств и жалоб.

При наличии ситуации 2.1, когда достоверно установлена причастность к ее совершению некоторых лиц, рекомендуется использовать алгоритм действий, сходный со

следственной ситуацией 1.2. с учетом того, что некоторые участники преступной группы идентифицированы и установлены на момент возбуждения уголовного дела.

Алгоритм действий следователя *при наличии ситуации 2.2* применяется в том случае, когда установлены все или основной состав преступной группы для дальнейшего успешного расследования уголовного дела и важнейшее значение имеют вопросы взаимодействия следователя с сотрудниками иных правоохранительных органов. На наш взгляд, следует создать следственную оперативную группу, в которую должны входить следователи, оперативные сотрудники УРПСВТ, специалисты в том числе в сфере ИТ. Рекомендуется также определиться с порядком и последовательностью проведения первоначальных (неотложных) следственных действий, задержания участников преступной группы и т.д.

При хищении с использованием компьютерной техники, совершаемом в другом государстве, либо с участием (в отношении) иностранных граждан, к перечисленному следует добавить организационные мероприятия получения доказательств в соответствующих странах. В первую очередь направление следователем поручений либо просьб о производстве процессуальных действий компетентным органом или должностным лицом иностранного государства в соответствии с международными договорами Республики Беларусь, международными соглашениями или на основе принципа взаимности. Кроме этого, следователю необходимо направить соответствующее поручение в оперативные подразделения (как правило, в соответствующее управление или отдел РПСВТ МВД), которые, в свою очередь, могут в порядке взаимодействия и сопровождения следствия: 1) по каналам связи Интерпол передавать копии указанных запросов, в том числе копии запросов о выдаче для уголовного преследования лиц, объявленных ими в международный розыск; 2) самостоятельно инициировать запросы о получении информации: о сетевых адресах, именах доменов и серверов пользователей и организаций; о содержании протоколов, трейсингов («отслеживания происхождений данных»), логических файлов; об электронно-цифровых данных, заблокированных в связи с пресечением международных преступлений; о дистрибьюторах и провайдерах телекоммуникационных и сетевых услуг; о юридических и физических лицах, имеющих какое-либо отношение к хищению имущества с использованием компьютерной техники.

Обобщая изложенное представляется возможным сформулировать соответствующие выводы.

1. Под *типичной следственной ситуацией* по делам о хищениях путем использования компьютерной техники следует понимать неоднократно повторяющиеся условия (обстановку), в которых осуществляется процесс расследования преступления, обусловленного преимущественно информационным компонентом (наличием либо отсутствием подозреваемого), а также факторами объективного, субъективного и случайного характера в определенный момент расследования. Значение типизации следственных ситуаций в зависимости от объема и содержания информации на первоначальном этапе расследования заключается в том, что они предопределяют последовательность и содержание отдельных следственных, розыскных действий, оперативно-розыскных, организационных и иных мероприятий.

2. Анализ судебно-следственной практики позволил выделить следующие наиболее типичные следственные ситуации по рассматриваемым хищениям: 1) лицо, причастное к хищению, не установлено. Разновидностями этой следственной ситуации являются: 1.1) какая-либо информация о лице (-ах), причастном (-ых) к его совершению, отсутствует; 1.2) информация о лице (-ах), причастном (-ых) к его совершению, неполная либо неточная; 2) лицо, причастное к хищению, установлено. Ее разновидностями являются: 2.1) достоверно установлена причастность к его совершению некоторых лиц; 2.2) установлены все или основной состав преступной группы. Наличие той или иной типичной следственной ситуации предполагает определенный алгоритм действий следователя.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Волчецкая, Т. С. Ситуационный подход в практической и исследовательской криминалистической деятельности : учеб. пособие / Т. С. Волчецкая. – Калининград : Калинингр. ун-т, 1999. – 74 с.

2. Крылов, В. В. Информационные компьютерные преступления : учеб. и практ. пособие / В. В. Крылов. – М. : Инфра-М – Норма, 1997. – 285 с.

3. Остроушко, А. В. Организационные аспекты методики расследования преступлений в сфере компьютерной информации : дис. ... канд. юрид. наук : 12.00.09 / А. В. Остроушко. – Волгоград, 2000. – 226 л.

4. Преступления в сфере компьютерной информации: квалификация и доказывание : учеб. пособие / Ю. В. Гаврилин [и др.] ; под ред. Ю. В. Гаврилина. – М. : Книжный мир, 2003. – 245 с.

5. Коломинов, В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа : дис. ... канд. юрид. наук : 12.00.12 / В. В. Коломинов. – Иркутск, 2017. – 230 л.

6. Яковлев, А. Н. Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем : науч.-метод. пособие / А. Н. Яковлев, Н. В. Олиндер. – М., 2012. – 182 с.

Дата поступления в редакцию: 03.03.2020