УДК 343.985.7

Первоначальный этап расследования хищений, совершаемых посредством использования информационно-телекоммуникационных технологий

Попов Владимир Анатольевич,
кандидат юридических наук, начальник кафедры криминалистики, Рязанский филиал Московского университета МВД России им. В.Я. Кикотя. Россия, г. Рязань.
E-mail: volpopov@mail.ru
Владимиров Денис Михайлович,
преподаватель кафедры криминалистики, Рязанский филиал Московского университета МВД России им. В.Я. Кикотя. Россия, г. Рязань.
E-mail: den.vladimirov94@mail.ru

Аннотация. Новые информационные технологии, широко внедряясь в жизнь каждого человека, одновременно создают почву для использования глобального информационного пространства в качестве инструмента совершения преступлений. В данной статье нами рассмотрены некоторые особенности методики первоначального этапа расследования хищений совершаемых посредством использования информационно-телекоммуникационных технологий.

Ключевые слова: информационно-телекоммуникационные технологии, хищение, сеть «Интернет», криминалистическая методика расследований, тактика расследования.

Криминалистическая методика расследования хищений, совершенных в сфере информационно-телекоммуникационных технологий (далее – ИТТ), является относительно новой областью криминалистики. Она появилась в связи с быстрым развитием информационных технологий, которые проникли во все аспекты жизнедеятельности человека [2, с. 19], и увеличением числа преступлений, связанных с использованием современных технических средств и информационно-телекоммуникационных сетей. Теоретические основы криминалистической методики расследования хищений в сфере ИТТ основаны на знаниях о компьютерных системах, программном обеспечении, сетевых технологиях и методах защиты информации. Важными элементами являются знания о методах сбора и анализа цифровых доказательств, а также о правовых аспектах расследования исследуемой категории преступлений.

Основными задачами криминалистической методики расследования хищений в сфере ИТТ являются: выявление факта преступления, установление личности преступника, сбор и анализ цифровых доказательств, а также предотвращение дальнейшего распространения информации, полученной преступником.

Основные характеристики хищений в сфере информационно-телекоммуникационных технологий:

1. Виртуальность. Хищения могут быть совершены удаленно, без физического доступа к объекту;

2. Скрытность, т. е. без видимых материальных следов преступлений, с высокой степенью анонимности;

3. Масштабность и транснациональность, за счет глобальной зоны покрытия и обширной аудитории;

4. Сложность. Хищения в сфере информационно-телекоммуникационных технологий могут быть совершены с использованием сложных технологий и методов,

что подразумевает высокую квалификацию и достаточный опыт у преступников, а соответственно и у сотрудников правоохранительных органов, занимающихся расследованием;

5. Многовариантность, обусловленная разнообразием способов и методов реализации своих противоправных целей, которые постоянно трансформируются с учетом развития современных технологий.

Основные способы исследуемых хищений можно разделить на три группы. Первая группа – это мошенничества, при которых потерпевшее лицо добровольно передает принадлежащие ему денежные средства лицу, совершающему преступление, в счет приобретения какого-либо товара, оказания услуг или выполнения работ. Вторая группа – это хищения электронных денежных средств, находящихся на принадлежащих потерпевшему электронных кошельках, совершенные путем их взлома, осуществляемого посредством использования вирусного программного обеспечения, взломщиков электронных кошельков, фишинговых сайтов, сайтов-клонов и др. Третья категория краж основана на изменении компьютерной информации или нарушении функционирования информационных систем, чтобы преступник мог получить доступ к финансовым средствам, находящимся на счете жертвы. Преступник выдает себя за владельца этих денежных средств и использует их в своих интересах, не имея прямого контакта с потерпевшими.

Для расследования хищений в сфере информационно-телекоммуникационных технологий необходимо использовать специализированные методы и техники, включая киберкриминалистику, анализ данных, экспертизу компьютерных систем и т. д. Ввиду большого разнообразия преступлений в сфере информационно-цифрового пространства, план расследования и алгоритмы работы могут рачительно отличаться друг от друга [3, с. 167]. Правильно спланированная тактика проведения и эффективность допроса потерпевшего на начальном этапе расследования хищений рассматриваемой категории позволит выявить и зафиксировать достаточный объем информации, раскрывающей важные для дальнейшего расследования обстоятельства преступления.

Также на первоначальном этапе расследования необходимо установить круг очевидцев, которые могли знать о совершаемых в отношении пострадавшего лица действиях. При установлении очевидцев преступления, необходимо провести их опрос в целях установления информации, имеющей значение для раскрытия преступления. Допрос свидетелей в настоящих ситуациях будет различаться в зависимости от обстоятельств дела. В качестве свидетелей могут быть допрошены:

–сотрудники отделения оператора сотовой связи, сотрудники финансовых организаций, а также сотрудники этих же организаций, но осуществлявшие ранее в отношении потерпевшего юридически значимые действия, к примеру, оформление SIM-карты, банковской карты;

–фактические оформители SIM-карт, банковских карт, в случае если они передали свои реквизиты в использование потерпевшему;

–близкие лица, родственники потерпевшего, имевшие законный доступ к банковскому его счету;

–лица, которые в момент хищения находились в непосредственной близости с пострадавшим;

–лица, осведомленные об отдельных действиях подозреваемого в связи с совершением преступления и т. д.

Согласно общим правилам проведения допроса свидетелей, ими принято считать лиц, не имеющих общих интересов с результатами расследования, в силу этого их показания считаются наиболее объективными для дела. Однако они могут давать неполное описание ситуации в силу субъективных причин (например, испытывая чувство стыда, опасаясь за деловую репутацию). Поэтому при осуществлении допроса

считаем необходимым избрать такую тактику, которая позволит установить с опрашиваемым психологический контакт.

Учитывая, что способ совершения хищений в сфере информационно-телекоммуникационных технологий позволяет преступнику совершать преступные действия инкогнито, по уголовным делам данной категории установление виновного лица является весьма сложной проблемой. Поэтому нередки бывают следственные ситуации, когда совершившее хищение лицо не установлено.

Если, несмотря на все предпринятые в ходе расследования уголовного дела оперативно-розыскные мероприятия, комплекс следственных и процессуальных действий, установить лицо, причастное к его совершению, не представилось возможным, то по истечении срока расследования (как правило, двух месяцев с момента возбуждения уголовного дела) следователь приостанавливает предварительное следствие на основании п. 1 ч. 1 ст. 208 УПК РФ, то есть в связи с неустановлением лица, подлежащего привлечению в качестве обвиняемого.

Обязательным условием приостановления предварительного следствия по данному основанию является необходимость выполнения следователем всех следственных действий, производство которых возможно в отсутствие подозреваемого или обвиняемого, и принятие им мер по установлению лица, совершившего преступление (ч. 5 ст. 208 УПК РФ).

В ходе расследования может сложиться и иная ситуация, когда лицо, совершившее хищение, известно, но скрывается от правосудия. В этом случае процессуальная деятельность имеет свои особенности и является согласно п. 2 ч. 1 ст. 208 УПК РФ самостоятельным основанием для приостановления предварительного следствия. Однако следователю до приостановления производства по уголовному делу надлежит выполнить максимальный объем следственных действий, которые возможно осуществить в отсутствие подозреваемого, а также принять меры по его розыску. Процессуальный порядок осуществления розыска подозреваемого закреплен в ст. 210 УПК РФ. В соответствии с данной статьей следователь поручает его розыск органам дознания, о чем указывает в постановлении о приостановлении предварительного следствия или выносит отдельное постановление. До объявления подозреваемого в розыск следователь должен осуществить меры по установлению его местонахождения, то есть посредством производства соответствующих процессуальных действий: допросить знакомых и родственников подозреваемого, произвести обыски в известных следствию местах его возможного пребывания (проживания), собрать данные, характеризующие личность подозреваемого, направить необходимые запросы в различные органы и учреждения (отдел адресно-справочной работы УВМ УМВД России по субъекту Федерации, ИЦ и ГИАЦ МВД России, вокзалы, аэропорты, морги и т. д.), направить поручение в орган дознания о производстве оперативно-розыскных мероприятий, направленных на установление местонахождения подозреваемого.

В случаях, когда местонахождение подозреваемого все же так и не было установлено, и есть основания полагать, что он скрылся от следствия, то у следователя есть все основания для приостановления предварительного следствия. Кроме того, до объявления подозреваемого в розыск и приостановления предварительного следствия, следователь при наличии достаточных данных, руководствуясь ст. 171 УПК РФ, может вынести постановление о привлечении данного лица в качестве обвиняемого. При этом в соответствии с ч. 6. 172 УПК РФ обвинение предъявляется в день фактической явки обвиняемого. В случае, если скрывшийся подозреваемый будет обнаружен, то он в соответствии с ч. 3, 4 ст. 210 УПК РФ может быть задержан в порядке, предусмотренном главой 12 УПК РФ, также в отношении него может быть избрана мера пресечения, в том числе заключение под стражу.

Ситуация, когда подозреваемый в совершении хищения, совершенного с использованием информационно-телекоммуникационных технологий, известен и от правосудия не скрывается, по данной категории уголовных дел бывает крайне редко, поскольку психологические качества лиц, совершающих мошенничество, практически исключают раскаяние и осознание вины, разве только в случаях, когда под давлением доказательств они выбирают линию поведения, предполагающую меньшее наказание. И все же, учитывая то, что такие следственные ситуации возможны, у следователя имеется возможность получить признательные показания подозреваемого и уже на них «накладывать» доказательства.

От следователя (дознавателя) требуется тщательная подготовка к проведению допроса подозреваемого. Важно не только внимательно изучить все материалы дела, но и разобраться, какими личностными чертами обладает подозреваемый. Во-первых, допрос подозреваемого зачастую является конфликтным следственным действием. Подозреваемый чаще всего либо отказывается от дачи показаний, либо отрицает свою вину. Лица, совершающие преступлений, склонны к лживости, изворотливости и цинизму, очень часто ведут себя на допросе нагло, беззастенчиво лгут, искажают факты, отрицают даже очевидные доказательства. Поэтому следователю (дознавателю) важно психологически подготовиться к возможному конфликту, тщательно промыслить тактику допроса, настроиться на то, чтобы сохранять спокойствие и профессиональную выдержку при любых обстоятельствах.

Во-вторых, следователь (дознаватель) должен учитывать, киберпреступник вполне может использовать свою осведомленность в компьютерных технологиях, употреблять сложную специфическую терминологию, бравировать техническими жаргонизмами. Такое поведение можно назвать «интеллектуальным противодействием» при допросе.

В-третьих, при подготовке к допросу следователю (дознавателю) предстоит изучить существенный объем данных, содержащихся, в основном, в электронном виде, поскольку именно эти данные и будут составлять предмет допроса подозреваемого и уточняться в ходе следственного действия.

В-четвертых, нужно учитывать дефицит времени и динамичность обстановки в сетевом окружении, которые определяются краткосрочностью существования и высокой изменчивостью отдельных видов доказательств, находящихся в электронной форме [1, с. 270].

В связи с этим, для проведения допроса подозреваемого представляется необходимым привлекать специалиста в сфере информационно-телекоммуникационных технологий, который поможет следователю (дознавателю) грамотно построить ту часть допроса, которая касается способа совершения хищения и, следовательно, предполагает наличие глубоких технических знаний в этой сфере. Профессиональные знания специалиста помогут выстроить допрос более точно, конкретно и продуктивно.

Список литературы

1. Билан, А. Н. Тактика допроса при расследовании кибермошенничества / А. Н. Билан // Молодой ученый. – 2022. – № 2 (397). – С. 270–271.

2. Владимиров, Д. М. Публичные призывы к осуществлению экстремистской деятельности, совершаемые посредством использования сети Интернет // В книге: Борьба с преступностью: теория и практика. Тезисы докладов XI Международной научно-практической конференции. Могилев, 2023. – С. 19–20.

3. Попов, В. А., Рудавин, А. А. Особенности планирования расследования по делам о преступлениях в сфере компьютерной информации // В сборнике: Уголовный процесс и криминалистика: теория, практика, дидактика. Сборник материалов VIII Всероссийской научно-практической конференции. Рязань, 2023. – С. 167–174.