КРИМИНАЛИСТИКА

УДК 343.985.3

А. И. Гайдин
начальник кафедры уголовного процесса
Воронежского института МВД России,
кандидат юридических наук, доцент

ОСОБЕННОСТИ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ ТАКТИЧЕСКИХ ОПЕРАЦИЙ ПО УСТАНОВЛЕНИЮ ЛИЦ, ПРИЧАСТНЫХ К СОВЕРШЕНИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Обобщение практики расследования преступлений, совершаемых в сфере информационно-телекоммуникационных технологий, свидетельствует, что наиболее сложными для установления являются обстоятельства причастности конкретных лиц к совершению преступных деяний. В условиях, когда полностью отсутствует криминалистически значимая информация о виновных лицах или имеет место ее значительный дефицит, планирование следственных действий и оперативно-розыскных мероприятий, которые направлены именно на решение указанной задачи, должно основываться на реализации разработанных в науке алгоритмов, учитывающих особенности современных способов совершения и сокрытия преступлений в информационно-телекоммуникационной среде [1]. При этом необходимо выдвигать и разрабатывать версии относительно личности преступника, учитывая степень его квалификации в области информационных технологий.

Отличительной особенностью поисковой деятельности в сетевом пространстве является последовательное движение по следам, которое позволяет сначала обнаружить оборудование, посредством которого были осуществлены преступные действия, а затем доказать причастность конкретных лиц, использовавших данную технику. Это обусловлено тем, что идентификация личности пользователя сети Интернет, в том числе и использующего Интернет в преступных целях, осуществляется посредством идентификации аппаратных средств, используемых им для соединения. При этом необходимо решить задачу, связанную с применением злоумышленниками средств анонимизации, которые скрывают следы, связывающие факты использования каких-либо устройств с его личностью и (или) маскируют идентификационные свойства используемых им компьютерных и сетевых средств.

Ключевое значение в установлении лиц, причастных к совершению компьютерных преступлений, имеет умелая реализация следователем возможностей операторов сотовой связи и интернет-провайдеров по определению местонахождения оконечного оборудования, хранению информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, видео или иного трафика.

Для установления личности лица, причастного к совершению преступления в сфере информационно-телекоммуникационных технологий, планируются и осуществляются как следственные действия, так и организационные, оперативно-розыскные и технические мероприятия.

Комплексный характер проводимых действий позволяет вести речь о тактической операции. Ее осуществление в процессе раскрытия преступлений, совершенных с использованием современных коммуникационных технологий, наиболее эффективно в условиях, когда преступники использовали средства анонимизации для сокрытия следов в сетевом пространстве, поскольку способствует задержанию виновных лиц и со всей очевидностью носит определяющий характер для последующего этапа предварительного расследования.

Содержание рассматриваемой тактической операции включает в себя осуществление взаимосвязанных и взаимообусловленных действий: по получению показаний от всех лиц, имеющих отношение к проверяемому факту (заявителя, потерпевшего, очевидцев, сотрудников кредитных организаций и банков, представителей интернет-провайдера, операторов сотовой связи, организаций, предоставляющих интернет-услуги); истребованию и (или) изъятию документов и предметов (выписок о движении денежных средств, документов, подтверждающих операции по списанию и перечислению денежных средств, сведений от провайдера о владельце IP-адреса и т. п.); производству необходимых исследований и (или) судебных экспертиз (прежде всего судебно-компьютерных); проведению оперативно-розыскных мероприятий; проведению осмотра места происшествия (осмотр компьютерной техники с установленной системой дистанционного банковского обслуживания, осмотр банкоматов, квартир, помещений организаций и предприятий); проверке по оперативно-справочным и криминалистическим учетам (прежде всего работа с подсистемой ИБД-Ф «Дистанционное мошенничество»); установлению отношения абонентского номера к номерной емкости оператора связи, банковской карты конкретной банковской организации, IP-адреса, с использованием которого осуществлялись преступные действия, организации, зарегистрировавшей доменное имя и оказывавшей услуги хостинга сайту; получению образцов для сравнительного исследования [2].

Тактической операции по установлению лиц, причастных к совершению преступлений в сфере информационно-телекоммуникационных технологий, свойственны общие признаки тактических систем [3]:

1. Целостность (алгоритмичность). Все структурные элементы содержания операции взаимообусловлены результатами и взаимосвязаны особенностями познавательной эффективности.

2. Структура. Предполагает набор конкретных организационных, технических процессуальных и оперативно-розыскных мероприятий, сочетание и последовательность осуществления которых зависят от следственной ситуации.

3. Иерархичность системы. Рассматриваемая тактическая операция является компонентом более широкой системы — криминалистической тактики. При этом содержание каждого элемента системы наполнено тактическими приемами соответствующих этапов, выбор которых обусловлен тактической задачей производства мероприятия и ситуацией.

4. Динамичность и гибкость. Реализация тактической операции предусматривает возможность ее применения при расследовании значительного числа видов преступлений, совершаемых в сфере информационно-телекоммуникационных технологий, а также варианты изменения плана деятельности с учетом способов сокрытия преступления, действий по противодействию расследованию и особенностей способов достижения преступного замысла.

Особенности рассматриваемой операции проявляются в ее специфических признаках, которые позволяют отнести ее к различным группам при классификации тактических операций по различным основаниям: по уровню общности — типичная; по характеру следственных ситуаций, в которой она проводится, — проводимая в условиях ситуации, характеризующейся дефицитом информации о лицах, причастных к совершению преступления; по характеру и содержанию действий — состоящая из различных действий (организационных, следственных, оперативно-разыскных и технических); по содержанию решаемых задач — направленная на установление людей и материальных ценностей; по отношению к предмету доказывания — направленная на установление обстоятельств, входящих в предмет доказывания; по отношению к этапам расследования — проводимая на этапе возбуждения уголовного дела и первоначальном этапе расследования; по организационной структуре — проводимая участниками следственно-оперативной группы, созданной для расследования конкретного преступления [4].

Таким образом, решение задачи по установлению лиц, причастных к совершению преступлений в сфере информационно-телекоммуникационных

технологий, при производстве по уголовным делам осуществляется путем организации и проведения типовых тактических операций, содержание которых составляют организационные, следственные, оперативно-розыскные и технические мероприятия, в условиях активного противодействия обеспечивающие возможность обнаружения средств компьютерной техники, применяемой при совершении деяния, и идентификации правонарушителей.

Список основных источников

1. Трубчанинов А. В. Особенности возбуждения уголовного дела и планирования на первоначальном этапе расследования преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ [Электронный ресурс] // Вестн. Волгогр. акад. МВД России. 2019. № 1 (48). С. 153–158. URL: https://cyberleninka.ru/article/n/osobennosti-vozbuzhdeniya-ugolovnogo-dela-i-planirovaniya-na-pervonachalnom-etape-rassledovaniya-prestupleniy-svyazannyh-s (дата обращения: 10.04.2024). Перейти к источнику Вернуться к статье

2. Гайдин А. И., Звягин И. С., Садырин И. С. Механизм хищений денежных средств, совершаемых с использованием технологий IP-телефонии и программ подмены номеров [Электронный ресурс] // Вестн. Воронеж. ин-та МВД России. 2022. № 3. С. 202–207. URL: https://cyberleninka.ru/article/n/mehanizm-hischeniy-denezhnyh-sredstv-sovershaemyh-s-ispolzovaniem-tehnologiy-ip-telefonii-i-programm-podmeny-nomerov (дата обращения: 10.03.2024). Перейти к источнику Вернуться к статье

3. Шишкина Е. В. Тактические комплексы в системе криминалистических средств расследования преступлений [Электронный ресурс] // Российское право: образование, практика, наука. 2023. № 1. С. 40–50. URL: https://cyberleninka.ru/article/n/takticheskie-kompleksy-v-sisteme-kriminalisticheskih-sredstv-rassledovaniya-prestupleniy (дата обращения: 07.03.2024). Перейти к источнику Вернуться к статье

4. Завьялов В. А. Классификация тактических операций [Электронный ресурс] // Юрид. наука. 2020. № 1. С. 96–102. URL: https://cyberleninka.ru/article/n/klassifikatsiya-takticheskih-operatsiy (дата обращения: 08.03.2024). Перейти к источнику Вернуться к статье