УДК 343.98

А. В. Даниленко
курсант 3 курса факультета милиции
Могилевского института МВД Республики Беларусь

Научный руководитель:

Д. И. Шнейдерова
преподаватель кафедры
уголовного процесса и криминалистики
Могилевского института МВД Республики Беларусь

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ОБНАРУЖЕНИЯ ЦИФРОВЫХ СЛЕДОВ ПО МАТЕРИАЛАМ ПРОВЕРКИ И УГОЛОВНЫМ ДЕЛАМ

Информационные технологии и порождаемые их инструментами цифровые следы занимают особое место среди объектов, на которые обращен исследовательский вектор криминалистической науки XXI века, что продиктовано повсеместным использованием компьютерных и сетевых технологий в преступных целях. Понятие цифрового следа сегодня вызывает полемику среди авторов (А. Н. Колычева, Е. Р. Россинская, А. Г. Себякин, В. А. Мещеряков, В. А. Милашев, Г. М. Шаповалов), которые не могут прийти к общему мнению относительно терминологии и содержания определения. Не останавливаясь на анализе авторских точек зрения, следует отметить, что общим является факт признания цифровых следов разновидностью компьютерной информации, имеющей криминалистическое значение ввиду связи с событием преступления, которая структурно представлена различными конфигурациями двоичного машинного кода, преобразуемого в доступный для анализа человеком вид, образуется, хранится, модифицируется, копируется, передается и удаляется с помощью компьютерной техники и программного обеспечения, существует при неразрывной связи с материальным носителем.

Следует согласиться с мнением Я. Г. Варакина о том, что «классический взгляд на образование следов преступления в криминалистике в виде взаимодействия двух материальных объектов с последующим наложением следа от одного объекта на другой претерпел вынужденную трансформацию», поскольку цифровой след образуется операционной системой под воздействием как команд, поступающих от пользователя, так и программных алгоритмов в автоматическом режиме [1, с. 82]. Также до сих пор не решен вопрос о том, к какой группе относятся цифровые следы: представляют ли собственное ответвление или являются разновидностью материальных следов, поскольку с точки зрения физики цифровая информация является материальными электромагнитными

сигналами, но при этом существовать отдельно от физического носителя не может, что исключает ее самостоятельность.

Наличие приведенных выше теоретических проблемных вопросов, а также трудности, с которыми сталкиваются правоохранительные органы при практической работе с цифровыми следами, подтверждают актуальность разработки научно обоснованных рекомендаций по обнаружению, фиксации, изъятию и исследованию цифровых следов, которые имели бы общий характер и были применимы независимо от вида преступления и сложившейся следственной ситуации. Обнаружение — первичный этап работы с цифровыми следами, который требует от сотрудников органов дознания и следствия не только должного уровня подготовки и теоретической подкованности по последним тенденциям в сфере IT, но и применения специальных технических и программных средств, предназначенных для поиска информации и получения к ней доступа. В этой связи можно обозначить несколько вопросов, в том числе имеющих проблемный характер, которые формируют тактику обнаружения цифровых следов: в первую очередь, что может являться источником цифровых следов; какие необходимы вспомогательные средства для обеспечения их поиска и имеются ли они в распоряжении правоохранительных органов; в ходе каких действий и мероприятий может проводиться обнаружение; какие для этого нужно задействовать методики.

Обнаружение цифровых следов как процесс направлено на поиск компьютерной информации, имеющей значение для установления всех обстоятельств совершенного преступления и формирования доказательственной базы по делу, который проводится в рамках проверочных и оперативно-розыскных мероприятий, следственных и процессуальных действий. Исходя из сложившейся практики и уровня развития современных технологий, можно выделить следующие группы источников: компьютеры и мобильные устройства; съемные накопители данных; ресурсы сети Интернет. Если источником выступают компьютеры и смартфоны, то тактика работы с ними зависит от нескольких факторов: в рамках какого следственного действия обнаружены, может ли содержимое их памяти быть осмотрено на месте, нужны ли для этого аппаратно-программные комплексы, либо, исходя из соображений безопасности, устройство необходимо изъять и поручить проведение осмотра специалистам, либо назначить компьютерно-техническую экспертизу для установления и выгрузки информации. При работе со съемными накопителями сотрудники не рискуют подключать их к своим рабочим компьютерам, опасаясь порчи как своего содержимого, так и данных на носителе. Поэтому сложилась устоявшаяся практика изъятые носители направлять эксперту в рамках экспертизы для копирования данных, а при наличии в подразделениях следственных органов или органов дознания специальных отделов и соответствующих аппаратно-программных комплексов — поручать

проведение осмотра их сотрудникам. Выбор места и средств поиска цифровых следов при исследовании ресурсов сети Интернет зависит от технического обеспечения каждого правоохранительного органа. Так, если в подразделении имеется специально оборудованный компьютер, имеющий подключение к Интернету, то, конечно же, целесообразно использовать его. Но, как показывает практика, такое оснащение имеется лишь в областных и крупных районных городах и его количества не хватает на всех сотрудников. Поэтому поиск осуществляется либо с устройства потерпевшего, либо с личного устройства сотрудника, что может угрожать безопасности его личных данных и видится недопустимым.

Исходя из вида методики поиска, он может быть ручной или программный. При ручной методике сотрудник простым перебором содержимого хранилища данных осуществляет поиск информации, имеющей значение для доказывания. На это затрачивается много времени, и есть опасность пропустить нужную информацию. Поэтому использовать данную методику стоит только в том случае, если объемы поиска малы и сотрудник знает, какие именно данные нужно установить. Если объем информации большой, нужно отыскать скрытые, зашифрованные или удаленные файлы и открыть их, следует использовать программную методику, которая предполагает использование специальных программ или аппаратных комплексов, предназначенных для поиска и копирования данных («Мобильный криминалист», Belkasoft, UFED и т. д.).

Субъектный состав лиц, осуществляющих обнаружение цифровых следов, представлен лицами, производящими дознание, следователями, экспертами и специалистами. Из них следователи и лица, производящие дознание, не обладающие специальными навыками работы с информационными технологиями, образуют группу субъектов, которые самостоятельно могут осуществлять лишь целенаправленный поиск цифровой информации, для производства которого достаточно базовых знаний компьютерных устройств и сетей (например, могут осмотреть страницу в социальной сети, установить ее ID, данные владельца). В остальных случаях поиск должен осуществляться либо привлеченными специалистами (сотрудники криминалистических отделов следственных подразделений и лица, осуществляющие дознание, из подразделений Министерства внутренних дел Республики Беларусь по борьбе с киберпреступлениями), которые могут непосредственно участвовать в следственных действиях или осуществлять их по поручению, либо экспертами государственных и частных экспертных учреждений в рамках экспертиз.

Центральное место среди следственных и процессуальных действий, в рамках которых реализуется поиск цифровых следов, занимает осмотр, который может быть целенаправленным или поисковым в зависимости от того, владеет ли сотрудник информацией о тех следах, которые предстоит осмотреть.

Такая информация получается либо из показаний участников процесса, либо по результатам иных следственных действий. Также обнаружение цифровых следов может быть произведено при проверке показаний или следственном эксперименте с участием подозреваемого, в ходе обыска или выемки, если обнаруженное устройство находится во включенном состоянии и выполняет процессы, остановка которых угрожает потерей данных (в иных ситуациях устройства изымаются и отдельно осматриваются), при осмотре носителей, полученных по результатам экспертиз или запросов к организациям.

Таким образом, при определении тактики поиска цифровых следов следует учитывать разновидность источника, который предстоит исследовать, перечень технических и программных средств, которые могут понадобиться в этих целях, а также необходимость привлечения специалистов, если поисковые действия требуют узкопрофилированного спектра знаний, выходящего за рамки общих навыков работы с компьютерами и сетевыми ресурсами.

---

1. Варакин Я. Г. Криминалистические технологии обнаружения, фиксации, изъятия цифровых следов преступления и иной доказательной информации // Вестн. Сургут. гос. ун-та. 2021. № 4. С. 81–87. Вернуться к статье