Кемпирова Ж. С., старший преподаватель кафедры криминалистики, капитан полиции
(Карагандинская академия МВД РК им. Б. Бейсенова)

ТАКТИКА ОБНАРУЖЕНИИ, ФИКСАЦИИ И ИЗЪЯТИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПРИ ПРОИЗВОДСТВЕ СЛЕДСТВЕННЫХ ДЕЙСТВИИ И ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИИ

Как показывает практика расследования, особые проблемы процессуального и психологического плана следователи встречают при производстве отдельных следственных действий, в ходе которых необходимо произвести обнаружение, фиксацию и изъятие компьютерной информации.

Отношения к компьютерной технике среди практических работников органов внутренних дел неоднозначно. Сопротивление новых пользователей вычислительных систем достаточно велико, следователь становится пользователем компьютера в прямом смысле, собирая в нем информацию о преступлении. Сопротивление внедрению информатики является результатом страха перед новым и неизвестным. Такое сопротивление является одной из причин подавляющего числа ошибок, имеющих место в следственной практике. Часто страх, возникающий у практического работника, вызван его собственной убежденностью в том, что он не

способен освоить что-то новое, что это «наверняка очень сложно для него, особенно в его возрасте, при его загруженности на работе» и т. д.

Особенности тактики проведения отдельных процессуальных действий давно и глубоко разрабатываются учеными-криминалистами, однако криминалистической наукой не выработаны рекомендации, касающиеся особенностей тактических приемов и методов, используемых при собирании компьютерной информации[1]. Объясняется это, прежде всего новизной возникшей проблемы, стремительным приростанием массы компьютерной техники и компьютерного обеспечения.

Моделирование возможных следственных ситуаций на основе изучения специальной юридической и технической литературы, изучение практики расследования уголовных дел показывает, что компьютерная информация может быть добыта в ходе проведения осмотра места происшествия (местности, помещений, предметов, документов), личного обыска, обыска на местности и в помещении, выемки предметов, документов, почтово-телеграфной корреспонденции, документов, содержащих государственную тайну, прослушивания телефонных или иных переговоров.

Мы не будем проводить резкой грани между особенностями собирания компьютерной информации при производстве различных следственных действий. Объясняется это едиными объектами — компьютером и информационным массивом, находящемся в нем. Тем более, как мы уже это отметили, тактика проведения самих названных следственных действий достаточно давно и широко разработана в криминалистике.

На подготовительном этапе следователю необходимо оценить всю имеющуюся у него информацию о расследуемом преступлении. На необходимость изъятия криминалистически значимой компьютерной информации могут указывать: совершение компьютерного преступления; наличие у подозреваемого (обвиняемого) в личном пользовании компьютерной техники, специального образования в области вычислительной техники и программирования; наличие у потерпевшего (в некоторых случаях свидетелей) специального образования в области вычислительной техники и программирования; присутствие в материалах дела документов, изготовленных машинным способом (ответы на запросы, справки, полученные от обвиняемого или потерпевшей стороны); хищение носителей компьютерной информации; получение в ходе изучения личности обвиняемого сведений об его увлечении вычислительной техникой и программированием; частое общение с людьми обвиняемого или потерпевшего «компьютерного» круга и др.

Тактика поиска информации в компьютере заключается в правильном применении криминалистических приемов ее обнаружения. Знание этих приемов позволит следователю: избежать уничтожения или повреждения искомой информации; правильно разобраться в сложном информационном массиве и найти требуемое; правильно зафиксировать изъятую информацию в криминалистическом и процессуальном плане.

В отличие от традиционных следов преступления природа компьютерной информации заставляет искать новые методы ее собирания. Современное развитие электроники позволяет хранить огромные массивы информации в незначительных по объему устройствах. Электронная сущность самой информации предъявляет особые требования к следователю по подготовке и проведению следственных действий[2].

Владение достоверными данными об элементах объекта позволит следователю решить основные задачи собирания доказательственной компьютерной информации в ходе расследования: 1) получить все возможные доказательства, хранящиеся в компьютере; 2) максимально повысить доказательственную значимость добытой информации. В первом случае информированность следователя о характеристике осматриваемой информационной системы ведет к эффективному и рациональному поиску доказательств, позволяет избежать возможной порчи или утраты следов преступления в информационном массиве ЭВМ. Во втором случае правильный анализ, например, возможности несанкционированного доступа к компьютерной базе данных подозреваемого (обвиняемого) позволит правильно организовать деятельность по сбору доказательств в компьютере, чтобы затем иметь возможность на основании их изобличить преступника.

В ходе подготовки к следственному действию необходимо заранее позаботиться о приглашении понятых. Участие понятых обязательно при проведении любых следственных действий, в ходе которых происходит сбор и фиксация компьютерной информации.

Не следует ограничиваться поиском информации только в компьютере. Необходимо внимательно осмотреть имеющуюся в помещении документацию, записи даже на клочках бумаги могут иметь значение для успешного достижения цели. Сделать это необходимо в виду того, что программисты часто не надеются на свою память и оставляют записи о паролях,

изменениях конфигурации системы, особенностях построения информационной базы компьютера. Многие пользователи хранят копии своих файлов на дискетах для избежания утраты их при выходе компьютера из строя. Поэтому обнаружение любых носителей информации должно побуждать следователя к их изъятию, изучению и использованию[3].

Только после перечисленных подготовительных мер следует приступать к рабочему этапу следственного действия. Несоблюдение элементарных правил, как свидетельствует следственная практика, ведет к тому, что деятельность следователя по сбору компьютерной информации своей цели не достигает. По нашему мнению, тактика поиска компьютерной информации должна избираться исходя из, во-первых, степени защищенности данных, во-вторых, — функционального состояния компьютера и периферийных устройств на момент проведения следственного действия.

Основываясь на градации степени защищенности от низшего уровня к высшему, мы считаем, что при производстве следственного действия разделить уровни защиты можно на защиту высокого, низкого уровня надежности и незащищенные данные. Следователь анализирует данный критерий в соответствии с целью следственного действия для выбора наиболее оптимальной деятельности по поиску необходимой информации, максимально эффективного добывания искомых доказательств. Получение достоверных данных об уровне защищенности компьютера — объекта осмотра — дает возможность произвести поиск доказательственной информации в компьютере в максимально короткое время, безопасно для искомой информации, полно и последовательно.

По нашему мнению, деятельность следователя по преодолению защиты компьютера от несанкционированного доступа — одна из самых ответственных. Именно при некорректном обращении к защищенным данным последние могут быть самоуничтожены, искажены, спрятаны и т. д. с помощью специальных программ[4]. В период подготовки к проведению следственного действия важно как можно более точно и полно определить степень защищенности компьютера, средства защиты, пароли, ключевые слова и т. д.

Анализ некоторых программно-технических средств защиты компьютерной информации свидетельствует, что использование оперативной информации зачастую может оказаться решающей при осуществлении поиска доказательственной информации в компьютере. Только полное уяснение основной и дополнительных целей предстоящего следственного действия, получение сведений об объекте, сбор информации о лицах позволят тактически правильно произвести поиск необходимых доказательств.

Успех расследования во многом зависит от правильной фиксации и изъятия найденных следов преступной деятельности в процессуальном и криминалистическом плане[5]. Поскольку процессуальный закон основным средством фиксации определяет протокол следственного действия, следователь должен описать основные физические характеристики изымаемых устройств, магнитных и других постоянных носителей информации, серийные номера аппаратуры, их видимые индивидуальные признаки.

По общим правилам криминалистической фиксации следов, каждый объект должен быть опечатан так, чтобы у суда не было сомнений в подлинности доказательств. Накопители на гибких магнитных дисках удобнее всего упаковывать в бумажные конверты либо в картонные коробки. Нельзя что-либо приклеивать к дискетам, надписывать их, прошивать и т. д.

Изымать необходимо сразу все зафиксированные объекты. Нельзя оставлять их на ответственное хранение на самом объекте или в другом месте, где к ним могут иметь доступ посторонние лица. Содержащаяся на магнитных носителях информация может быть легко уничтожена преступником, например, с помощью источника электромагнитного излучения. При этом визуально по внешним признакам определить это невозможно.

Таким образом, при расследовании уголовных дел, в которых в качестве доказательств фигурирует компьютерная информация, следователю нет необходимости постигать азы программирования, кибернетики и т. д. Расследование данной категории дел подчиняется общим правилам. Задача следователя — умело организовать работу, правильно использовать знания профессионалов в области ВТ для эффективного поиска информации в компьютере и правильной ее фиксации в криминалистическом плане, исследовании, оценке и использовании. Ведь, как показывает практика, основными проблемами для следователей в ходе производства следственных действий являются отсутствие минимальных познаний в области ВТ и, как следствие этого, сложности в вопросах терминологии, определения понятия составных частей компьютерной системы и сетей, правильного понимания общего режима их функционирования в различных технологических процессах.

1 Баев О. Я. Тактика следственных действий: Учеб.пос. — Воронеж, 1995 — С. 65.

2 Галатенко В. Информационная безопасность // Открытые системы. — 1996. — № 4. — С. 40-47.
3 Ярочкин В. И. Безопасность информационных систем. — М., 1996. — С. 99-100.
4 Защита информации в базах данных. Иностранная печать о техническом оснащении полиции капиталистических государств// ВИНИТИ. — 1992. № 2. — С. 22-23.
5 Белкин Р. С. Собирание, исследование и оценка доказательств. — М., 1966.