УДК 343.98

Д. С. Захаров,
курсант 3-го курса факультета милиции
Могилевского института МВД
Научный руководитель: Д. И. Шнейдерова,
преподаватель кафедры
правовых дисциплин
Могилевского института МВД

ОСОБЕННОСТИ ТАКТИКИ ПРОВЕДЕНИЯ ОБЫСКА ПО ДЕЛАМ О ХИЩЕНИЯХ ПОСРЕДСТВОМ СЕТИ ИНТЕРНЕТ

Одним из ключевых следственных действий, проводимых как на стадии проверки заявлений о совершенных преступлениях, так и на стадии расследования возбужденного уголовного дела, является обыск. По делам о хищениях путем использования сети Интернет обыск направлен в первую очередь на выявление средств их совершения, к которым следует относить компьютерную технику (стационарные и переносные персональные компьютеры, планшеты, моноблоки, смартфоны), оборудование для подключения к Глобальной сети (маршрутизаторы, мобильные 3G-модемы), переносные накопительные устройства для хранения данных (флеш-карты, диски, внешние винчестеры, холодные кошельки для криптовалют), комплектующее оборудования для компьютерной техники, также оперативный интерес могут представлять блокноты с записями, литература в сфере IT и программирования и другие.

В связи с особенностью хищений, совершаемых посредством сети Интернет, на практике правоохранительные органы все чаще встречаются с таким видом следов, как цифровые, под которыми понимают совокупность данных, хранящихся в памяти устройств и цифровых носителей, содержащие информацию о действиях пользователя как на самом устройстве, так и в компьютерных сетях. Выделяют активные и пассивные цифровые следы. Активные — данные, создаваемые самим пользователем (электронные письма, переводы в криптокошельках и т. д.), пассивные содержат информацию, фиксируемую устройством о действиях пользователя (время, IP-адрес, история браузера, журнал загрузок и другие) [1, с. 258]. Поиск источников таких следов и составляет ключевую цель обыска по делам рассматриваемой категории.

Эффективность и достижение поставленной цели обыска зависят от тщательной подготовки к нему, которая должна включать в себя анализ материалов уголовного дела (материалов проверки), определение мест возможного нахождения искомых предметов и характеристик их обустройства, снабжения этих мест

точками доступа в сеть Интернет (т. е. установление провайдера, обеспечивающего доступ в сеть, с целью последующего анализа трафика, использованного конкретным пользователем), установление механизма совершения хищения и выдвижение предположений о средствах, которые могли использоваться киберпреступником для его реализации, а также местах, где такие средства могут быть скрыты на месте обыска.

На подготовительном этапе необходимо рассмотреть возможность участия специалистов как при подготовке к обыску (к примеру, допустимо проведение специалистом инструктажа с участниками обыска, которые будут производить поисковые действия), так и на рабочем этапе в качестве консультанта при производстве поиска цифровых следов. Кроме того, практические навыки специалистов в сфере IT необходимы и на заключительном этапе обыска, когда производится оценка достигнутых результатов и принимается решение о назначении соответствующих экспертиз, постановку вопросов на которые необходимо осуществлять при помощи специалиста.

В случае обнаружения источника или носителя цифровой информации целесообразно зафиксировать место обнаружения, а, в последующем его изъять для дальнейшего исследования в рамках производства осмотра, по итогам которого такой предмет может быть признан вещественным доказательством и приобщен к материалам уголовного дела. В случае если лицо, осуществляющее расследование уголовного дела, не обладает достаточными навыками для качественного осмотра содержимого источника цифровой информации, то оно может привлечь к участию в осмотре специалиста или назначить компьютерно-техническую экспертизу.

Нецелесообразно производить исследование обнаруженных объектов на месте проведения обыска, так как это способствует затягиванию процесса производства следственного действия, обстановка и количество посторонних лиц являются отрицательными факторами для осуществления специалистом своей работы качественно и эффективно, а также для получения необходимой информации может отсутствовать требующееся специалисту оборудование для осмотра скрытых и засекреченный файлов.

Таким образом, резюмируя вышеизложенное, необходимо отметить, что развитие и распространение информационных технологий способствовало появлению новых способов и средств совершения хищений, а именно посредством компьютерной техники и сети Интернет. В связи с чем сложившаяся методика расследования указанной группы преступлений, включая тактику проведения отдельных следственных действий, нуждается в модернизации и приведении в соответствие с потребностями современного уголовного процесса и криминалистики. И так как обыск является одним из ключевых следственных действий,

поскольку позволяет выявить, изъять и исследовать источники цифровых доказательств, представляется целесообразной разработка новой тактики его проведения на базе практических примеров и рекомендаций специалистов в сфере информационных технологий и программирования, которая в последующем подлежит апробации на практике.

1. Шнейдерова Д. И. Криминалистический аспект установления по цифровым следам лица, совершившего хищение в сфере оборота криптовалют // Актуальные проблемы обеспечения общественной безопасности в Республике Беларусь: теория и практика : тез. докл. XXII Респ. науч.-практ. конф., Минск, 21 мая 2020 г. : в 2 ч. / Факультет внутренних войск УО «Военная академия Республики Беларусь» ; редкол.: В. А. Талалаев [и др.]. Минск, 2020. Ч. 2. С. 258–261. Вернуться к статье