УДК 343.985.7

Т. Л. Щерба
доцент кафедры расследования преступлений
следственно-экспертного факультета
Академии МВД Республики Беларусь,
кандидат юридических наук, доцент

Ю. В. Полковниченко
курсант Академии МВД Республики Беларусь

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Киберпреступления — чрезвычайно многогранное и сложное явление. Объектами таких преступных посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты или программное обеспечение и базы данных, для которых технические средства являются окружением; компьютер может выступать как предмет посягательств или как инструмент. При этом киберпреступления следует отличать от иных преступлений, совершаемых с использованием высоких технологий.

При расследовании уголовных дел вышеуказанной категории не всегда следователь обладает необходимым объемом знаний, достаточным для качественного сбора необходимых доказательств. В связи с этим необходимым является использование специальных знаний в области высоких технологий.

Как справедливо отмечают Е. Р. Россинская и А. И. Усов, участие специалиста обязательно в осуществлении любого следственного действия, связанного с манипуляциями ЭВМ, т. к. малейшие неквалифицированные действия с компьютерной системой могут закончиться в ряде случаев безвозвратной утратой ценной доказательственной информации [1, с. 93–94].

Анализ практики показывает, что применение специальных знаний при расследовании киберпреступлений чаще всего осуществляется при проведении следственных и иных процессуальных действий, а также судебной компьютерно-технической экспертизы (далее — КТЭ).

При проведении следственных действий специальные знания могут использоваться как в процессуальной, так и в непроцессуальной формах. Наиболее целесообразным и необходимым при расследовании киберпреступлений является участие специалиста при проведении следующих следственных действий: осмотр (в том

числе осмотр места происшествия), обыск, выемка, следственный эксперимент, допрос (чаще в непроцессуальной форме при непосредственной подготовке к допросу). Вместе с тем, как показывает практика, зачастую следователи не могут привлечь специалиста в области высоких технологий в связи с их дефицитом. Поэтому представляется обоснованным развитие практики самостоятельного изучения следователем тонкостей сферы высоких технологий, в том числе и в рамках повышения квалификации, что позволит ему объективно, всесторонне и полно изучить все обстоятельства уголовного дела.

При этом данный аспект является актуальным не только в отношении следователей, специализирующихся на расследовании киберпреступлений. В настоящее время преступники все чаще для совершения преступлений используют компьютерные технологии. Наиболее ярко данная тенденция проявляется при совершении преступлений в сфере незаконного оборота наркотиков, мошенничеств и др. Вышеуказанное обуславливает необходимость изучения модификации высоких технологий для большого круга следователей.

Следующим способом использования специальных знаний по данной категории дел является проведение КТЭ. В зависимости от обстоятельств уголовного дела (материалов проверки) можно выделить следующие виды КТЭ: а) аппаратно-компьютерная экспертиза; б) программно-компьютерная экспертиза; в) информационно-компьютерная экспертиза; г) компьютерно-сетевая экспертиза. Такое деление наиболее полно охватывает технологические особенности и эксплуатационные свойства объектов экспертизы, предъявляемых для исследования.

В соответствии с ч. 1 ст. 226 УПК экспертиза назначается, если есть необходимость решения каких-либо вопросов с помощью специальных знаний в науке, технике, искусстве или ремесле. В нашем случае этими специальными познаниями являются познания в следующих научных областях: электроника, электротехника, информационные системы и процессы, радиотехника и связь, вычислительная техника (в т. ч. программирование) и автоматизация.

Необходимость назначения КТЭ определяется следователем или судом. Она не относится к числу обязательных экспертиз, предусмотренных ст. 228 УПК. При проведении исследования в соответствии с п. 3 ч. 2 ст. 61 УПК эксперт вправе потребовать, кроме представленных следователем объектов, материалы уголовного дела, относящиеся к предмету экспертизы; заявлять хо-

датайства о предоставлении ему необходимых дополнительных материалов; присутствовать при производстве следственных действий. Последнее имеет важное значение особенно по делам о киберпреступлениях, когда ввиду особенностей работы с ЭВМ, а в некоторых случаях массивности техники (например, проведение компьютерно-сетевой экспертизы сервера (с учетом того, что в некоторых организациях для размещения сервера выделены отдельные технические помещения), исследование проводится на месте (в офисах организаций, учреждениях, помещениях, квартирах и иных местах, где находится компьютерная техника и информация). В таком случае после обзорной стадии следственного действия и ознакомления эксперта с обстановкой выносится постановление о назначении экспертизы и эксперт приступает к исследованию.

Таким образом, участие специалиста в следственных действиях не только обеспечивает более квалифицированные действия следователя при их проведении, но и позволяет самому специалисту «на месте» вникнуть в суть дела, помочь следователю при назначении вопросов КТЭ, а также в случае необходимости провести ее на месте происшествия. Вместе с тем дефицит специалистов в области высоких технологий, а также распространенность не только киберпреступлений, но и других преступлений, совершаемых с использованием компьютерных технологий, обуславливают необходимость самообучения либо повышения квалификации следователей в рассматриваемой сфере.

1. Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М. : Право и закон, 2001. 414 с.