УДК 343.98

А. В. Даниленко,
курсант 2-го курса факультета милиции
Могилевского института МВД
Научный руководитель: Д. И. Шнейдерова,
преподаватель кафедры
уголовного процесса и криминалистики
Могилевского института МВД

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАБОТЕ С ЭЛЕКТРОННО-ЦИФРОВЫМИ СЛЕДАМИ: КРИМИНАЛИСТИЧЕСКОЕ ЗНАЧЕНИЕ

Планомерное масштабирование процессов компьютеризации на все сферы жизнедеятельности современного человека ежегодно приводит к увеличению количества пользователей компьютерными технологиями различных возрастных категорий, о чем свидетельствуют и данные статистики. Так, на начало 2022 года на территории Республики Беларусь 73 % населения в возрасте от 6 до 72 лет пользуются функционалом персональных компьютеров [1], 85,1 % активно взаимодействуют с сетью Интернет через компьютерные (57 %) и мобильные устройства (43 %) [2]. Однако общедоступность информационных технологий не во всех случаях производит положительный эффект, что проявляется в становлении преступного сектора, включающего возможности использования компьютерных технологий и сетей в целях реализации преступных намерений.

При этом само устройство, в зависимости от вида и способа совершения преступления, может восприниматься как средство достижения преступной цели (например, при корыстных и иных киберпреступлениях, доведении до самоубийства, распространении наркотических средств, даче взятки и др.), так и как средство подготовки (приискание подставных банковских карт, сим-карт на несуществующих лиц, поиск данных о предполагаемой жертве), сокрытия совершенного деяния или его результата (перевод похищенных средств в криптовалюты, реализация имущества через торговые площадки, анонимизации личности и т. д.). Но стоит заметить, что в каком бы целевом назначении ни использовалось устройство, оно в любом случае сохранит в своей памяти электронно-цифровые следы преступного события, даже если преступник пытался их уничтожить.

Обнаружение, фиксация, изъятие и последующее исследование электронно-цифровых следов — ключевые задачи при расследовании в большей степени киберпреступлений, которая требует от следователей и лиц, производящих дознание, не только профессионализма и применения накопленного опыта,

но и демонстрирования специальных познаний в области IT, с чем, как показывает практика, возникают определенные трудности. Поскольку специфика IT многогранна и узко профилирована, сотрудники правоохранительных органов, обладая, как правило, юридическим образованием, зачастую не в состоянии самостоятельно справиться с оперативными задачами расследования, в связи с чем появляется необходимость в привлечении специалистов, обладающих необходимым комплексом знаний в области компьютерной техники, радиоэлектроники, программирования, криптографии, веб-администрирования и т. д.

Задача таких специалистов — оказать консультативную и практическую помощь органам предварительного расследования при установлении источников электронно-цифровых следов, обнаружении и изъятии из их памяти информации, в том числе скрытой и блокированной, получении доступа к устройствам, программам, приложениям или интернет-ресурсам, защищенным паролем, восстановлении умышленно поврежденных носителей компьютерной информации, отыскании вирусных программ-шпионов и блокираторов файлов и в иных случаях. Как правило, следственная ситуация базируется на исследовании единичного компьютерного или мобильного устройства, с отысканием и изъятием которых при обыкновенных условиях способен справиться и сотрудник правоохранительных органов. Однако если следствию приходится иметь дело с компьютерными сетями, работа которых в отдельных случаях не может быть приостановлена ввиду непрерывности обеспечения рабочего процесса, то придется прибегнуть к анализу содержимого по месту нахождения устройств, что уже выходит за рамки специализации рядового сотрудника правоохранительных органов и требует участия специалиста.

Кроме того, работа с электронно-цифровыми носителями данных требует не только стандартных познаний в использовании компьютера или мобильного телефона, доступных каждому рядовому пользователю, но и умений применять специализированные программно-аппаратные комплексы, позволяющие вычленять криминалистически значимую информацию с исследуемого устройства, эффективную работу с которыми может осуществлять специально обученный сотрудник. Так в Республике Беларусь криминалистическими отделами управлений и центрального аппарата Следственного комитета, главным управлением по противодействию киберпреступности и управлениями по противодействию киберпреступности УВД, подразделениями Государственного комитета судебных экспертиз в практической деятельности используются такие программно-аппаратные комплексы, как Belkasoft Evidence Centre, «Мобильный криминалист», «Элкомсофт», PC-3000, Cellebrite UFED 4 PC и иные, позволяющие извлекать из памяти устройств массивы необходимых для расследования данных.

Таким образом, исходя из возникающей практической необходимости, привлечение лиц, специализирующихся на работе с компьютерными технологиями и программным обеспечением, видится криминалистически оправданным и целесообразным для достижения целей предварительного расследования.

1. Информационное общество в Республике Беларусь [Электронный ресурс] // Национальный статистический комитет Республики Беларусь. URL: https://www.belstat.gov.by/upload/iblock/50e/50e0f7e0b7e5875db07fb6c8350e8ec8.pdf (дата обращения: 01.06.2022). Перейти к источнику Вернуться к статье

2. Чем живет виртуальная Беларусь [Электронный ресурс] // Экономическая газета «Neg.by». URL: https://neg.by/novosti/otkrytj/digital-2022-ispolzovanie-interneta-i-socsetej-v-belarusi/ (дата обращения: 01.06.2022). Перейти к источнику Вернуться к статье