УДК 343.98

К. В. Сечина
преподаватель кафедры криминалистики
Рязанского филиала
Московского университета МВД России имени В. Я. Кикотя

ОБНАРУЖЕНИЕ ЦИФРОВЫХ СЛЕДОВ ПРЕСТУПЛЕНИЙ ПРИ ПУБЛИЧНОМ РАСПРОСТРАНЕНИИ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ О ДЕЙСТВИЯХ ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФЕДЕРАЛЬНОЙ СЛУЖБЫ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ, ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ, ОРГАНИЗАЦИЙ И ИНЫХ ДОБРОВОЛЬЧЕСКИХ ФОРМИРОВАНИЙ

Современный период развития общества характеризуется стремительным возникновением новых угроз, посягающих как на безопасность граждан, так и на суверенитет нашей страны. Проведение специальной военной операции явилось своеобразным толчком к распространению фейковой информации о деятельности Вооруженных Сил Российской Федерации в информационно-телекоммуникационной сети Интернет. Целью распространения заведомо ложной информации является искажение объективного восприятия гражданами Российской Федерации происходящих событий в Украине. В связи с этим была разработана и введена в действие ст. 207.3 Уголовного кодекса Российской Федерации, предусматривающая уголовную ответственность за совершение указанных деяний в контексте специальной военной операции [1, с. 186].

Совершая распространение заведомо ложной информации о деятельности Вооруженных Сил Российской Федерации, Федеральной службы войск национальной гвардии Российской Федерации, органов государственной власти и иных добровольческих формирований, преступники оставляют в информационно-телекоммуникационной сети Интернет цифровые следы (цифровые цепочки) преступления, порядок работы с которыми в настоящее время в уголовно-процессуальном законодательстве отсутствует.

Обнаружение цифровых следов при производстве следственных действий следователь должен осуществлять с участием специалиста, имеющего знания в области компьютерной информации. Участие специалиста при работе с цифровыми следами регламентируется ст. 164.1 Уголовно-процессуального кодекса Российской Федерации, из контекста данной статьи можно сделать логический вывод, что и при осмотре цифровых следов участие специалиста будет обязательным [2].

При анализе материалов уголовных дел, возбужденных по ст. 207.3 Уголовного кодекса Российской Федерации, нами установлено, что цифровые следы преступления обнаруживаются в ходе проведения следственных действий на устройствах, а именно:

− технические устройства (мобильные телефоны, персональные компьютеры и иные технические средства);

− в сети Интернет (бесплатные мессенджеры для обмена информацией, социальные сети, облачные хранилища).

Таким образом, при работе с цифровыми следами следователь должен обладать знаниями и навыками по работе с ними, иметь познания в работе специализированных программных комплексов («Мобильный криминалист», UFED), которые применяет специалист при производстве следственных действий. Вызов специалиста экспертно-криминалистического подразделения Министерства внутренних дел необходимо запланировать заранее, так как, согласно Наставлению по организации экспертно-криминалистической деятельности в системе МВД России (приказ Министерства внутренних дел России от 11 января 2009 г. № 7) [3], вызов сотрудника экспертно-криминалистического подразделения для участия в проведении процессуального действия, за исключением осмотра места происшествия, в качестве специалиста осуществляется только по письменному запросу (поручению) дознавателя, следователя, в связи с чем процедура обеспечения участия специалиста в следственном действии может занять некоторое время.

Аппаратно-программный комплекс UFED применяется для упрощенного и быстрого исследования мобильных телефонов, планшетов, смартфонов, сим-карт мобильных устройств и карт памяти. Также важной и часто применяемой функцией комплекса UFED является поиск и извлечение удаленной информации (переписка в мессенджерах, СМС-сообщения, фотографии, видеофайлы и т. п.). В целях восстановления координат GPS при использовании современных мобильных устройств, имеющих выход в глобальную сеть Интернет, UFED применяется с аппаратно-программным средством — Physical Analyzer. Благодаря применению этого комплекса возможно сгенерировать маршрут перемещения исследуемого объекта [4, с. 409].

Но наряду с положительными сторонами применения аппаратно-программного комплекса UFED имеется фактор, создающий препятствие для более широкого применения — трудозатратность. В связи с тем, что модели исследуемых мобильных устройств уникальны относительно извлекаемой информации, время криминалистического осмотра предмета может составлять от 2 до 5 часов.

Особенностью программы «Мобильный криминалист» является возможность извлечения криминалистически значимой информации, хранящейся в облачном хранилище (iCloud, Microsoft OneDrive, Amazon Drive и др.) мобильного устройства, компьютера, даже в заблокированном режиме. Применяется программа для извлечения данных из резервных копий мобильных устройств за счет декодирования аппаратных ключей шифрования различных операционных систем, включая Android и iOS.

Таким образом, использование специальных программ по обнаружению и изъятию цифровых следов с компьютерных устройств, мобильных телефонов, облачных хранилищ и т. п. значительно упрощает процесс раскрытия и расследования распространения заведомо ложной информации о деятельности Вооруженных Сил Российской Федерации, Федеральной службы войск национальной гвардии Российской Федерации, органов государственной власти и иных добровольческих формирований.

Список основных источников

1. Сечина К. В. Тактика производства отдельных следственных действий по делам о распространении заведомо ложной информации в сфере общественной безопасности с использованием сети «Интернет» // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск : Вост.-Сиб. ин-т МВД России. 2024. Т. 32. № 4. С. 186–193. Вернуться к статье

2. Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс] : 18 дек. 2001 г. № 174-ФЗ : принят Гос. Думой 22 нояб. 2001 г. : одобр. Советом Федерации 5 дек. 2001 г. : в ред. от 28 дек. 2024 г. № 510-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс». Вернуться к статье

3. Об утверждении Наставления по организации экспертно-криминалистической деятельности в системе МВД России [Электронный ресурс] : приказ М-ва внутр. дел России от 11 янв. 2009 г. № 7 : с изм. от 9 марта 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс». Вернуться к статье

4. Чуб В. С. Программные и аппаратные средства для экспертного исследования мобильных телефонов // Вестн. соврем. исслед. № 12.10 (27). 2018. С. 409–410. Вернуться к статье