УДК 343.98.067

В. А. Попов
начальник кафедры криминалистики
Рязанского филиала Московского университета МВД России
имени В. Я. Кикотя,
кандидат юридических наук
Д. М. Владимиров
преподаватель кафедры криминалистики
Рязанского филиала Московского университета МВД России
имени В. Я. Кикотя

КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ, СОВЕРШАЕМЫХ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Несмотря на то, что Всемирная паутина имеет массу положительных свойств, которые полезны для человека как в его профессиональной деятельности, так и в быту, учебе, саморазвитии, проведении досуга, хобби и т. д., стоит признать, что имеется и обратная сторона медали [1, с. 30]. Адептам экстремистской идеологии открылись новые возможности, значительно облегчающие им реализацию противоправных целей за счет скорости передачи информации, транснациональной зоны покрытия, уровня анонимности и прочее. Однако правоохранительные органы адаптируются к современным реалиям, совершенствуя способы и средства обнаружения и изъятия так называемых электронных (цифровых) следов преступлений для обеспечения процесса расследования преступлений исследуемой категории.

В частности, помимо привычных способов обнаружения признаков составов преступлений экстремистской направленности в сети Интернет (например, мониторинга («серфинга») сайтов, социальных сетей или мессенджеров, осмотра электронных устройств подозреваемых, получения данных с электронно-вычислительных мощностей и т. п. [2, с. 108]), правоохранительные органы Российской Федерации используют отечественные информационно-поисковые системы «СЕУС», «Окулус» и другие, способные автоматически анализировать общедоступные интернет-ресурсы на предмет обнаружения запрещенных данных, в том числе экстремистского толка. Подобные системы находятся в постоянном совершенствовании, что позволило добиться поражающей скорости обработки информации. В частности, система «Окулус» способна изучать свыше

200 тысяч изображений в сутки, таким образом, ей необходимо всего около 2 секунд на анализ одного изображения [3].

Что касается непосредственно изъятия цифровых следов преступлений с компьютеров, винчестеров, сотовых телефонов, флеш-накопителей и т. д., то с этим отлично справляются современные аппаратно-программные комплексы, находящиеся в распоряжении сотрудников экспертно-криминалистических подразделений Российской Федерации. К сожалению, некоторые зарубежные производители вследствие санкционной политики в отношении России прекратили предоставлять обновления аппаратных комплексов. В связи с этим они стали практически бесполезны для работы с более современными техническими средствами и операционными системами. Например, одна из самых ранее востребованных программ у экспертов — UFED Touch (израильского производства компании Cellibrite Di Ltd.) — уже несколько лет не обновляется на территории России. Несмотря на сложную геополитическую обстановку, российские производители аппаратно-программных комплексов смогли усовершенствовать свои продукты, и сейчас экспертно-криминалистическим подразделениям доступны такие наиболее распространенные и эффективные аппаратно-программные комплексы, как «Мобильный криминалист», PC-3000 и Elcomsoft.

Каждый из перечисленных аппаратно-программных комплексов российских производителей имеет различные модули и вариации продуктов в зависимости от выполняемых задач. Так, например, возьмем компанию Elcomsoft, ей разработаны и постоянно совершенствуются следующие продукты:

− Elcomsoft Desktop — пакет программ для снятия парольной защиты, а также восстановления паролей;

− Elcomsoft Mobile — инструментарий мобильного криминалиста включает все необходимое для извлечения данных из мобильных устройств методами физического, логического и облачного анализа [4].

В связи с этим для наиболее эффективного криминалистического обеспечения расследования преступлений в распоряжении экспертов находится несколько аппаратно-программных комплексов разных производителей, и там, где один не может изъять достаточное количество информации, имеющей значение для уголовного дела, сможет помочь другой. Каждый из них дополняет друг друга в зависимости от поставленных для разрешения вопросов в рамках назначенной судебной экспертизы, а также их функционала в данный момент времени. Стоит отметить, что для работы с ними глубоких познаний в программировании не требуется.

Существуют и другие способы изъятия информации, такие как Root-доступ (получение прав суперпользователя), метод Chip-off, JTAG и прочее. Однако все вышеперечисленное не дает абсолютной гарантии постоянного успешного извлечения данных с того или иного устройства, на что влияет множество факторов (своевременное обновление программ, степень защиты операционной системы сотового телефона, установка дополнительных программ шифрования типа Vera crypt, неисправность изъятого устройства и т. д.). В связи с этим производителям аппаратно-программных комплексов следует и дальше совершенствовать свою продукцию, которая полностью обеспечит расследование преступлений экстремистской направленности, совершаемых с использованием сети Интернет, что положительно скажется на работе сотрудников правоохранительных органов.

Список основных источников

1. Владимиров Д. М. Экстремизм в глобальной сети Интернет [Электронный ресурс] // Борьба с преступностью: теория и практика : тез. докл. VIII Междунар. науч.-практ. конф., Могилев, 23 апр 2020 г. / М-во внутр. дел Респ. Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь» ; редкол.: Ю. П. Шкаплеров (отв. ред.) [и др.]. Могилев : Могилев. ин-т МВД, 2020. 1 электрон. опт. диск (CD-R). С. 30–32. Вернуться к статье

2. Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 106–123. Вернуться к статье

3. В России запустили систему поиска запрещенной информации в Интернете // Лента.ру. URL: https://lenta.ru/news/2023/02/13/oculus/ (дата обращения: 10.02.2024). Перейти к источнику Вернуться к статье

4. ELCOMSOFT. Desktop, Mobile & Cloud Forensics // Elcomsoft. URL: https://www.elcomsoft.ru/police_and_law_enforcement_solutions.html (дата обращения: 11.02.2024). Перейти к источнику Вернуться к статье