УДК 343.98

ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ ПРЕСТУПНИКА ПО ЦИФРОВЫМ СЛЕДАМ

А. В. Даниленко
курсант 4 курса факультета милиции
Могилевского института МВД Республики Беларусь
Научный руководитель: ***Д. И. Шнейдерова****,*
старший преподаватель кафедры уголовного права,
уголовного процесса и криминалистики
Могилевского института МВД Республики Беларусь

С увеличением количества преступлений, совершаемых с использованием компьютерных технологий и информационных сетей, приобретают особую актуальность и практическую значимость вопросы криминалистической идентификации личности преступников по цифровым следам. Совершая любые манипуляции с программами, приложениями и ресурсами сети Интернет, преступник, как осознанно своими умышленными действиями, так и бессознательно ввиду алгоритмов программ, оставляет в памяти технических устройств и на серверах веб-ресурсов информацию, имеющую криминалистическое значение, поскольку в зависимости от ее характера и содержания последняя может иметь ориентирующий характер и способствовать установлению личности преступника, а также использованного им устройства, платежных финансовых инструментов, мобильной связи и т. д.

Криминалистический анализ способов совершения киберпреступлений и используемых при этом средств позволил выделить ряд цифровых следов идентификационного характера, к которым следует относить IP и MAC-адреса технических устройств (сетевой и аппаратный идентификаторы), ID и никнеймы аккаунтов в социальных сетях, мессенджерах, форумах, торговых площадках и иных веб-ресурсах, адреса электронных и криптовалютных кошельков, реквизиты банковских платежных карт, адреса электронной почты, номер мобильного телефона, доменные имена сайтов, цифровые фотоснимки (в том числе аватары) и видеозаписи с изображением признаков внешности преступника.

Обнаружение указанных цифровых следов должно сопровождаться последующим анализом, протекающим в рамках обработки полученной информации через общедоступные поисковые ресурсы OSINT. Такие сервисы реализуют сбор и анализ публично размещенной информации, содержащейся в ресурсах глобальной сети Интернет, преимущественно в чатах, социальных сетях, базах данных, на форумах [1]. Они позволяют аккумулировать сведения, связанные с анализируемыми цифровыми следами, и выявлять потенциальные

источники доказательственной информации (например, мобильных операторов, банки, платежные сервисы, провайдеры и иные организации, обладающие сведениями об искомом лице), ведущей к раскрытию личности преступника.

---

1. OSINT: в чем опасность и как защититься [Электронный ресурс] // АО «Лаборатория Касперского». URL: https://www.kaspersky.ru/blog/osint-open-source-intelligence/35955/ (дата обращения: 11.01.2024). Перейти к источнику Вернуться к статье