УДК 343.98

И. В. Пашута
доцент кафедры криминалистики
Академии МВД Республики Беларусь,
кандидат юридических наук, доцент

ВИДЫ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В СОТОВОМ (МОБИЛЬНОМ) ТЕЛЕФОНЕ

В век цифровых технологий трудно себе представить жизнь человека без ежедневного использования сотового (мобильного) телефона (далее — мобильное устройство), который стал не только устройством связи, но и многофункциональным средством общения, управления финансами, досуга и даже средством заработка. В то же время мобильный телефон часто является средством общения между преступниками, вовлечения в преступную деятельность других лиц, а также выступает в качестве орудия преступления или предмета преступного посягательства.

Являясь средством или объектом преступной деятельности, мобильное устройство выступает важным источником криминалистически значимой информации, которая может быть использована для установления обстоятельств, имеющих значение для выявления (раскрытия), расследования и предупреждения преступлений.

Криминалистически значимую информацию, связанную с мобильным устройством, целесообразно разделить на два вида: внешнюю и внутреннюю. Внешняя информация включает в себя данные о марке, модели устройства, его физическом состоянии; мобильное устройство является источником многих традиционных криминалистических следов (рук, пота, слюны и др.).

Внутренние криминалистически значимые данные представлены в виде компьютерной информации (включающей в себя и электронно-цифровые следы), которая содержится во внутренней памяти устройства, на сим-карте и во внешней памяти (если она имеется).

Внутренняя память мобильного устройства и сим-карта выступают источниками криминалистически значимой информации о контактах, входящих/исходящих звонках, их аудио-, видеозаписях, содержании текстовых и мультимедийных сообщений (СМС/ММС), заметках и напоминаниях, установленных приложениях, хранящихся личных и служебных документах, фото-, аудио-, видео- и иных файлах.

Так, например, при изучении контактов можно выявить имеющую значение для раскрытия и расследования преступлений дополнительную

информацию о дате рождения, адресе проживания, месте учебы, работы, имейле, наличии профиля в социальных сетях, фотографиях контактов, сохраненных пользователем. Посредством исследования СМС-сообщений можно получить информацию о переписке между контактами лица (членами семьи, родственниками, друзьями, коллегами по работе и др.), движении по банковским счетам (зачисление, перевод, списание денежных средств), включая различные оплаты услуг банковской картой (время, место, сумма списания денежных средств), государственном номере автомобиля, дате, времени, нахождении на платной городской парковке (в случаях, если оплата парковки осуществлялась посредством СМС); установить время, когда лицо находилось вне зоны действия сети (в лифте, на подземной парковке, вне зоны покрытия и т. п.) или когда телефон был выключен (в случаях, если в это время поступал звонок) и др.

Не стоит забывать, что мобильное устройство является и средством доступа в Интернет. В этой связи криминалистически значимыми являются данные приложений, связанных с веб-пространством (сведения о дате установки, контактах лица в мессенджерах, социальных группах, подписанных телеграм-каналах, наличие фотографий и медиафайлов, информация о местоположении, маршруте движения, посещенных пользователем местах, движении денежных средств и т. д.); истории просмотров веб-страниц и закладок в браузерах (социальных сетей, форумов и т. д.), наличие браузера Tor; данные средств синхронизации (представляющие интерес сведения при установлении соответствующих настроек могут сохраниться в Интернете в облачных хранилищах, реализующих синхронизацию файлов, например, Google Disk, OneDrive Dropbox, iCIoud, «Яндекс.Диск», Samsung Cloud, Xiaomi Cloud и др., даже если они удалены в самом устройстве); данные геолокации устройства (сведения о перемещениях: пешком, на автомобиле, городском транспорте, авиаперелетах и др.).

Широкий спектр важной информации можно получить при осмотре установленных на телефоне приложений для мгновенного обмена сообщениями (мессенджеров). Помимо содержащихся в них различных текстовых сообщений, изображений, аудиофайлов и документов, интерес представляют сведения о входящих/исходящих голосовых и видеосоединениях, в том числе и с абонентами, которых нет в записной книге самого телефона (дата, время, количество, продолжительность соединений и т. п.). Следует помнить, что используемая мессенджерами технология автоматического сквозного шифрования общения и обмена различной информацией через Интернет (E2EE или end-to-end encryption) исключает возможность ее дешифрования со стороны третьих лиц.

Внешняя память представляет собой съемный носитель данных, используемый для расширения памяти в Android-телефонах. Посредством исследования такого носителя можно получить криминалистически значимую информацию.

Производя поиск криминалистически значимой информации, содержащейся в мобильном телефоне, можно получить сведения и о самом устройстве. К таким сведениям относятся, например: IMEI (международный идентификатор мобильного оборудования), марка и модель телефона, серийный номер, версия прошивки операционной системы, телефонный номер сим-карты, IP-адрес, MAC-адрес, наименование сетей Wi-Fi, к которым ранее подключался телефон, и др.).

Анализ вышеуказанных данных позволяет лучше понять (изучить) личность, поведенческие паттерны лица, в некоторых случаях — установить его возможное местонахождение, знакомство с конкретным лицом (никнеймом), может свидетельствовать и о наличии у лица алиби.

Таким образом, при исследовании мобильного устройства можно получить большой объем криминалистически значимой информации, которую целесообразно разделить на два вида: внешнюю и внутреннюю. Изучение такой информации, как видится, позволит лучше подготовиться к проведению конкретных следственных действий с лицом — владельцем телефона, установить различные обстоятельства, имеющие значение для выявления (раскрытия), расследования и предупреждения преступлений.