стина и др.) понимают цифровую криминалистическую логистику как систему управления информационными потоками в процессе расследования по уголовным делам, когда вся электронная документация и иная цифровая информация, имеющая криминалистическое значение, используется следователем в качестве логических (оптимальных) цепочек (алгоритмов), позволяющих эффективно решать задачи по раскрытию и расследованию преступлений, используя единую цифровую среду.

Цифровая криминалистическая логистика призвана в процессе расследования преступления разрешать важные для расследуемого уголовного дела оперативные и тактические задачи, используя цифровую информацию.

Рассматриваемые направления криминалистики (алгоритмизация и программирование расследования, криминалистическая логистика) непосредственно влияют на процесс организации следователем предварительного следствия, содействуют построению точных и наиболее приближенных к реальным событиям криминалистических версий, планированию следователем необходимых следственных действий, оперативно-розыскных и других важных для расследования уголовного дела мероприятий, а в целом повысят, по нашему мнению, результативность расследования преступлений.

УДК 343.98

И.В. Пашута

КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМАЯ ИНФОРМАЦИЯ, СОДЕРЖАЩАЯСЯ В МОБИЛЬНОМ УСТРОЙСТВЕ

Мобильный телефон либо смартфон (далее – мобильное устройство) представляет собой многофункциональное устройство, содержащее большой объем криминалистически значимой информации, способствующей установлению многих обстоятельств, имеющих значение для раскрытия и расследования различных видов и групп преступлений. Под криминалистически значимой информацией при этом понимается любая информация (сведения, данные), любой природы, имеющая отношение к расследуемому противоправному событию. Наиболее часто получение криминалистически значимой информации о мобильном устройстве и его содержимом связано с проведением осмотра. При этом, как правило, проводится осмотр самого мобильного устройства (как разновидности компьютерной техники) и находящейся в нем компьютерной информации.

Внешним осмотром мобильного устройства как предмета устанавливаются данные о его марке, модели, что дополнительно позволяет судить о его стоимости и, соответственно, в некоторой степени – о финансовом положении его владельца. Состояние корпуса мобильного устройства (наличие царапин, сколов) может свидетельствовать о происходившей борьбе между его владельцем и пострадавшим. Кроме того, на корпусе устройства могут быть обнаружены различные следы (биологические следы, следы рук и др.), имеющие отношение к раскрытию и расследованию преступления. В отдельных случаях осмотр корпуса мобильного устройства позволяет выдвинуть версию о том, что его владелец имеет отношение к преступной деятельности. Так, повреждение камеры мобильного устройства (позволяющей осуществить разблокировку телефона с помощью функции Face ID) и кнопки ввода отпечатка пальца (Touch ID, также использующейся для разблокировки), влекущие за собой доступ к мобильному устройству только путем введения пароля, может свидетельствовать о том, что с помощью мобильного устройства осуществляются действия, связанные с незаконным оборотом наркотических средств, психотропных веществ, огнестрельного оружия, боеприпасов, взрывчатых веществ, с торговлей людьми, распространением порнографических материалов и др. Визуальный осмотр экрана мобильного устройства при косопадающем освещении в некоторых случаях, когда устройство заблокировано, может помочь в установлении конфигурации графического ключа, остающейся на поверхности в виде слабовидимой потожировой полосы от касания пальцами рук.

Важную криминалистически значимую информацию возможно получить путем осмотра компьютерной информации, содержащейся в мобильном устройстве. При этом решаются следующие задачи:

поиск и фиксация следовой уголовно-релевантной информации (электронно-цифровых следов), в том числе указывающей на совершение преступления конкретным известным или неизвестным лицом;

выявление и фиксация обстоятельств, имеющих значение для уголовного дела (время и дата создания, изменения, удаления файла, время и дата скачивания вредоносной программы, содержание и характер переписки между потерпевшим и подозреваемым и др.);

установление административно-территориальных и географических координат места происшествия;

выявление причин и условий, способствовавших совершению преступления.

Решая вышеуказанные задачи, мобильное устройство следует рассматривать как источник представляющей большую ценность криминалистически значимой информации, расположенной во встроенной памяти мобильного устройства, на карте памяти и SIM-карте.

Такая информация содержится в контактах абонента, входящих и исходящих звонках, аудио-, видеозаписях таких соединений, текстовых и мультимедийных сообщениях (SMS, MMS), заметках, напоминаниях, личных и служебных фото-, аудио-, видео- и иных файлах. Так, при изучении контактов можно выявить имеющую значение для раскрытия и расследования преступления дополнительную информацию о дате рождения, адресе проживания, месте учебы, работы, адресе электронной почты, наличии профиля в социальных сетях, фотографиях контактов, сохраненных пользователем. Исследованием SMS можно получить информацию о переписке между контактами лица (члены семьи, родственники, друзья, коллеги по работе и др.); движении по банковским счетам (зачисление, перевод, списание денежных средств), включая оплаты различных услуг банковской картой (время, место, сумма списания денежных средств); государственном номере автомобиля, дате, времени его нахождения на платной городской парковке (в случаях, если оплата парковки осуществлялась посредством SMS); установить время, когда лицо находилось вне зоны действия сети (лифт, подземная парковка, вне зоны покрытия и т. п.) или мобильное устройство было выключено (в случаях, если в это время поступал звонок), и др.

Помимо самого списка контактов и SMS, MMS изучению подлежат журнал звонков (содержит сведения о количестве соединений, их длительности, дате их осуществления, нахождении в группе абонентов, псевдонимах, регистрации контактов в мессенджерах, социальных сетях и др.); данные приложений (сведения о дате установки, контактах лица в мессенджерах, социальных группах, подписанных телеграм-каналах, наличие фотографий и медиафайлов, информация о местоположении, маршруте движения пользователя, посещенных им местах, движении денежных средств и т. д.); истории просмотров веб-страниц и закладок в браузерах (социальных сетей, форумов и т. д.); данные средств синхронизации (представляющие интерес сведения при установлении соответствующих настроек могут сохраниться в сети Интернет в облачных хранилищах, реализующих синхронизацию файлов, например, Google Disk, OneDrive Dropbox, iCloud, «Яндекс.Диск», Samsung Cloud, Xiaomi Cloud и др., даже если они удалены в самом устройстве); данные геолокации устройства.

Указанная информация, как правило, расположена на SIM-карте и во внутренней памяти мобильного устройства, которое в то же время является и средством доступа к сведениям, хранящимся удаленно. С помощью мобильного устройства могут создаваться и вестись различные учетные записи (Google, Apple, Яндекс ID-аккаунты), профили в социальных сетях (Facebook, YouTube, Instagram, TikTok, X, «ВКонтакте», «Одноклассники» и др.), мессенджерах (Viber, Telegram, WhatsApp и др.) и других приложениях. Аккаунты могут содержать огромный объем криминалистически значимой информации о связях лица, его интересах, местах и времени нахождения, социальных, экономических, политических предпочтениях и о многом другом. Например, исследование групп, в которых состоит аккаунт лица, владеющего мобильным устройством, дает доступ к контактам, которых нет в записной книжке устройства, расширяя тем сам круг источников информации, имеющей значение для раскрытия и расследования преступления. Изучение Google, Apple, Яндекс ID-аккаунтов помимо отмеченного позволяет получить доступ к электронной почте лица, облачным хранилищам, узнать список устройств, с которых осуществлялся доступ к учетной записи, данные геолокации, банковских карт и др.

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

Таким образом, следует сделать вывод о том, что мобильное устройство является важным источником криминалистически значимой информации. Ее получение возможно путем внешнего и внутреннего исследования указанного объекта. Предложенные рекомендации по направлениям поиска криминалистически значимой информации при осмотре мобильного устройства позволят, по нашему мнению, в значительной степени оптимизировать деятельность органов уголовного преследования по установлению обстоятельств, имеющих значение для раскрытия и расследования преступлений.

УДК 343.98

Н.Н. Пашута

ЗНАЧЕНИЕ ОБЪЯСНЕНИЯ ПРИ ПРОВЕДЕНИИ ПРОВЕРКИ ПО ЗАЯВЛЕНИЯМ ИЛИ СООБЩЕНИЯМ О ПРЕСТУПЛЕНИЯХ

Уголовно-процессуальная деятельность на стадии возбуждения уголовного дела состоит из системы следственных и иных процессуальных действий, направленных на проверку поступивших заявлений или сообщений о любых готовящихся, совершаемых или совершенных преступлениях, что создает основу для принятия законного и обоснованного уголовно-процессуального решения. В указанной системе процессуальных действий особое место занимает объяснение, роль и значимость которого на практике неуклонно растет, о чем свидетельствуют проведенные в различные годы исследования. Результаты изученных нами 145 материалов проверок по заявлениям или сообщениям о преступлениях в территориальных ОВД Республики Беларусь с 2020 по 2023 г. свидетельствуют, что получение объяснений является самым распространенным процессуальным действием. Так, нами не установлено ни одного материала, в котором бы не содержалось хотя бы одно объяснение.

Целью получения объяснения является установление данных, указывающих на признаки преступления. Данная цель достигается путем решения следующих задач:

получения криминалистически значимой информации о признаках совершенного деяния (сведения об обстоятельствах обнаружения деяния, в отношении кого совершено, когда, где, каким способом, в какой обстановке и при каких обстоятельствах, какова степень вреда, причиненного пострадавшему, причинно-следственная связь между совершенным деянием и наступившими последствиями, сведения о лице, предположительно совершившем деяние, его приметы, образ жизни, наличие специальных знаний и др.);

проверки либо устранения противоречий, возникших как при получении объяснений, так и при производстве иных процессуальных действий в ходе проведения проверки;

установления новых источников информации, имеющих значение для проверки (например, фотографии похищенного имущества; данные лица, с которым приобреталось похищенное имущество; фото- и видеоизображения лица, с которым произошел конфликт, и др.);

установления обстоятельств, исключающих производство по уголовному делу;

установления причин и условий, способствующих совершению деяния;

получения иной криминалистически значимой информации в зависимости от особенностей совершенного деяния.

Изучение специальной литературы, анализ материалов проверок, а также электронного банка судебных решений (программный комплекс судебных решений судов общей юрисдикции, созданный Национальным центром правовой информации