DOI: 10.34076/2219-6838-2020-2-48-52

КРИМИНАЛИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ МОБИЛЬНЫХ УСТРОЙСТВ

Смушкин Александр Борисович
Доцент кафедры криминалистики Саратовской государственной юридической академии (Саратов), кандидат юридических наук, доцент,
e-mail: Skif32@yandex.ru

Рассматриваются возможности использования при расследовании преступлений информации, извлекаемой из мобильных устройств. Предлагаются тактические рекомендации по осмотру мобильного устройства на стадиях статического и динамического осмотра.

Ключевые слова: цифровая криминалистика, мобильная криминалистика, исследование мобильных устройств, электронная информация

A CRIMINAL STUDY OF MOBILE DEVICES

Smushkin Aleksander
Associate professor, Saratov State Law Academy (Saratov), candidate of legal sciences,
e-mail: Skif32@yandex.ru

The article is devoted to the possibilities of using information extracted from various mobile devices for the sake of crime investigation. The author proposes some tactical recommendations for inspecting a mobile device at the stages of static and dynamic inspection.

Key words: digital forensics, mobile device forensics, research on mobile devices, digital information

Достаточно часто на месте задержания подозреваемых или при них обнаруживаются мобильные телефоны, иные мобильные устройства или их части. Мобильные устройства могут как использоваться по прямому назначению, так и являться элементами других устройств, которые применяются для совершения преступления (например, взрывных устройств).

Современные гаджеты (смартфоны, смартчасы, навигаторы, радар-детекторы, электронные книги) нередко сопоставимы с мощными компьютерами. Компьютеризированные блоки используются в различных устройствах и механизмах (компьютеризированные системы автомобилей, автопилоты и «черные ящики» летательных аппаратов и т. д.), и специалисты могут восстановить по цифровым следам маршруты передвижения и некоторые действия подозреваемых на протяжении большого отрезка времени. Информация, извлекаемая из или с помощью данных устройств, а также фиксируемая устройствами, крайне разнообразна (от виртуальных следов до цифровых аудио- и видеозаписей, цифровых фотографий и т. д.).

Чтобы отвечать современным требованиям, криминалистика должна активно разрабатывать вопросы осмотра, исследования мобильных устройств, изучения и анализа содержащейся в них информации. Фактически уже можно говорить о развитии подотрасли цифровой криминалистики, которую условно можно назвать «мобильной криминалистикой» *(mobile device forensics)*. Многие авторы ведут речь о формировании частной теории, направленной на изучение мобильных устройств[1].

[1] См., например: *Максимович А. Б.* Средства сотовой связи как объект криминалистического исследования: автореф. дис. ... канд. юрид. наук. М., 2018; *Его же.* Содержание и структура криминалистического учения о средствах сотовой связи // Актуальные проблемы российского права. 2016. № 11. С. 179–185; *Грибунов О. П.* Средства сотовой связи как источник криминалистически значимой информации // Вестник Восточно-Сибирского института МВД России. 2017. № 4. С. 137–142; *Архипова Н. А.* Организационно-

В. Жуланов и Е. Ищенко подчеркивают, что «особенности функционирования мобильной сотовой связи предоставляют следственным органам дополнительные возможности по раскрытию и расследованию преступлений, при организации и совершении которых она использовалась... Наиболее криминалистически значимой представляется персональная биллинговая и коммуникационная информация»[1].

Рассматривая практические аспекты мобильной криминалистики, В. А. Мещеряков и А. Н. Яковлев отмечают, что, определив «пространственную конфигурацию сегмента инфраструктуры оператора мобильной связи, обеспечивавшего функционирование обнаруженного на месте происшествия мобильного телефона», «зафиксировав время преступного события (или временной интервал), возможные траектории движения его участников, определив перечень базовых станций, обслуживающих участки каждой из траекторий, мы сможем достаточно четко сформулировать задачу поиска в информационной базе оператора сотовой связи тех номеров IMEI мобильных телефонов, которые в требуемое время обслуживались на проверяемых участках местности»[2].

Обратимся к вопросам проведения осмотра мобильных устройств, обнаруженных на месте происшествия.

В ходе статической стадии осмотра мобильного устройства подлежат изучению его размер, модель, цвет, устанавливается наличие на нем чехла или иных аксессуаров, предохраняющих аппарат от повреждения, рисунков на них, следов и повреждений.

На динамической стадии в первую очередь определяется возможность включения телефона (реакция на кнопку питания, иные кнопки, датчик отпечатка пальца и др.). Следующий шаг – выявление факта установки защиты и ограничения доступа к смартфону посторонних лиц (пароль, цифровой код, графический ключ, доступ по отпечатку пальца, доступ после сканирования лица пользователя или сетчатки его глаза). При отсутствии пароля или иных мер защиты производится подробный осмотр хранящейся на телефоне информации.

В. А. Мещеряков и А. Н. Яковлев указывают, что «если обнаруженный на месте происшествия мобильный телефон выключен и уровень зарядки батареи позволяет выполнить простейшие действия, то необходимо установить только его IMEI-код»[3]. IMEI-код, состоящий из 15 цифр, уточняется путем введения короткой команды *#06# либо изучения пункта «Об устройстве» в настройках телефона. Этот код присваивается на заводе-изготовителе и указывается в документах при продаже устройства; его крайне сложно изменить вне заводских условий. После определения и фиксации в протоколе IMEI-кода приводятся сведения о самом телефоне: версия прошивки, информация о сети.

Трудно согласиться с мнением В. А. Мещерякова и А. Н. Яковлева о том, что «все остальные операции следует проводить уже после завершения осмотра места происшествия в рамках иных следственных действий»[4]. Разумнее предположить необходимость изучения информации, хранящейся на самом телефоне, без подключения к беспроводным сетям. Изучение же информации, расположенной на серверах, доступ к которым осуществлялся с данного телефона, является как раз предметом иных следственных действий и оперативных мероприятий.

Подлежит изучению также список последних звонков и SMS, перечень адресатов. Криминалистическое значение могут иметь наличие определенных контактов, частота общения, продолжительность звонков на конкретные номера, время звонков. Сле-

---

тактические аспекты раскрытия и расследования преступлений в ситуациях использования средств мобильной связи: автореф. дис. ... канд. юрид. наук. СПб., 2011; *Старичков М. В.* Устройства мобильной связи как источники криминалистической информации // Криминалистические чтения на Байкале – 2015: материалы междунар. науч.-практ. конф. / отв. ред. Д. А. Степаненко. Иркутск, 2015. С. 234–236; *Третьякова Е. И.* Мобильный телефон как источник криминалистически значимой информации // Вестник Уральского финансово-юридического института. 2018. № 3. С. 49–51.

[1] *Жуланов В., Ищенко Е.* Анализ информации из электронных баз данных в следственной группе // Законность. 2007. № 4. С. 26.

[2] *Мещеряков В. А., Яковлев А. Н.* «Электронная» составляющая осмотра места происшествия // Библиотека криминалиста. 2015. № 5. С. 281.

[3] *Мещеряков В. А., Яковлев А. Н.* Указ. соч. С. 280.

[4] Там же.

дует обращать внимание на место сохранения контактов: память сим-карты, память телефона, облачные сервисы.

Большое значение для расследования имеет информация сим-карты. На ней хранятся сведения о международном мобильном идентификаторе абонента; список номеров, на которые он звонил; данные о номерах, выделенных в особые группы (быстрого набора, избранные или иные), а также последних набранных номерах; информация о последнем местоположении устройства (имеется в виду местоположение относительно обслуживающих станций); информация о провайдере; информация о предпочитаемых языках; информация о системе и др.[1]

Имеющееся у криминалистов программное оснащение позволяет провести анализ звонков, поступавших на осматриваемый смартфон и с него, с учетом информации, хранящейся на всех установленных сим-картах. Специалисты могут построить графическую схему системы контактов. Таким образом могут быть установлены структура преступной группы, источники получения информации и руководящих указаний. При дальнейшем обнаружении других телефонов возможна агрегация полученных данных и построение расширенных схем.

Далее изучается содержание полученных SMS, сохранившейся переписки в мессенджерах или открытых электронных писем, а также аудиозаписей телефонных разговоров, хранящихся в памяти устройства. Представляется, что просмотр (прослушивание) этих записей относится к элементам осмотра и не требует судебного санкционирования.

В большинстве современных смартфонов имеется приложение «Галерея», где собраны фотоснимки и видеозаписи; причем однажды открытые фотоснимки и видеозаписи, отправленные через мессенджер, также сохраняются в этом приложении. Содержание «Галереи» может иметь существенное значение для целей расследования преступлений. Часто представители незаконных вооруженных формирований активно используют фото- и видеофиксацию своих действий, издевательств над жертвами и т. д. Кроме непосредственного содержания фотоснимков (наличия на них определенных лиц, местности, зданий и сооружений, иных элементов обстановки), криминалистическое значение может иметь дополнительная информация, отмеченная на кадре: дата и время съемки, геотеги[2]. В свойствах файла фотографии также имеется информация о времени и дате съемки, а во многих случаях – о дополнительных параметрах съемки: диафрагма, выдержка, уровень светочувствительности (ISO), применение вспышки, фильтров и т. д.

Еще одна составляющая информационного содержимого современных смартфонов – датчики геопозиционирования. Работа данных датчиков используется во многих программах. Кроме указанных выше геотегов на фотографиях, в большинстве современных смартфонов имеются карты и навигаторы. В ходе изучения данных программ могут быть определены последние поисковые запросы адресов, проложенные маршруты, промежуточные точки маршрутов; кроме того, пользователем могут быть установлены ключевые точки (дом, работа и иные). Отчасти подобные данные помогут установить маршрут выдвижения подозреваемых, подхода к объекту и т. д.

Большой объем информации может быть получен при изучении приложений «Планировщик» и «Заметки». В «Планировщике», как правило, отмечены значимые для пользователя события (дни рождения знакомых и родственников, определенные даты), а также планы на день. «Заметки», как и обычные бумажные записные книжки, могут содержать любые записи – от телефонных номеров до распределения ролей в группе, ключей к коду, используемому соучастниками, списка необходимых закупок и т. д.

Тщательному изучению подлежат и все установленные на смартфон браузеры. В них, даже если телефон отключен от сетей, сохраняется информация о последних открытых страницах, поисковых запросах, закладках.

---

[1] *Casadei F., Savoldi A., Gubian P.* Forensics and SIM cards: an overview // International Journal of Digital Evidence. 2006. Vol. 5. Iss. 1.

[2] Геотеггинг – функция, позволяющая помечать фотографии географическими координатами. Подробнее см: *Гришанков В.* Geo Tagging (геотеггинг) в смартфоне – что это такое? // AndroidLime. 2018. 18 дек. URL: https://androidlime.ru/geo-tagging-smartphone-function (дата обращения: 22.04.2020).

Согласимся с А. Н. Яковлевым в том, что «вне границ технической ответственности оператора связи, а именно на серверах правообладателей коммуникационных сервисов типа ООО „Мэйл.Ру“ и на компьютерном средстве пользователя – отправителя информации, она представляет собой данные, пересылаемые деперсонализированными пользователями сети Интернет в рамках взаимной договоренности об использовании коммуникационных сервисов. Стороны, использующие коммуникационный сервис, договариваются с его правообладателем об отсутствии какой-либо ответственности за пересылку последним данных. Правообладатель коммуникационного сервиса преднамеренно создает технические и правовые условия, исключающие ситуацию, когда пересылаемые данные на его стороне или стороне пользователя подпадают под тайну связи...»[1]. Соответственно, когда письма электронной почты и иных обезличенных сервисов находятся «на компьютерных средствах пользователей, они могут быть получены лицом, проводящим расследование, в порядке ст. 86 УПК РФ в ходе следственных действий, а также истребованием от правообладателя коммуникационного сервиса»[2].

В памяти смартфона могут содержаться текстовые, видео-, аудио- или другие файлы, «скачанные» пользователем, или аудиофайлы, записанные пользователем на диктофон. Содержимое папок, в которых хранится информация, должно быть изучено через приложение «Проводник» смартфона или с помощью специальных программных комплексов. В первую очередь изучению подлежат директории «Download», «Music», «Documents» или аналогичные.

В ходе осмотра телефона подозреваемого могут быть обнаружены установленные на нем специализированные программы, например для расчета баллистических траекторий снаряда или объема и точки закладывания в здании взрывных устройств, для перехвата и управления системами контроля и управления доступом или наблюдения и т. д.

Более сложные исследования проводятся экспертами с использованием логического, физического, файлового анализа, в том числе с помощью специализированного программного обеспечения «Мобильный криминалист»[3], позволяющего даже разблокировать смартфоны, защищенные паролем.

Указанные обстоятельства предопределяют важность дальнейших теоретических разработок и составления практических рекомендаций по обращению с мобильными устройствами для наиболее полного и эффективного расследования преступлений.

Список литературы

Архипова Н. А. Организационно-тактические аспекты раскрытия и расследования преступлений в ситуациях использования средств мобильной связи: автореф. дис. ... канд. юрид. наук. СПб., 2011.

Грибунов О. П. Средства сотовой связи как источник криминалистически значимой информации // Вестник Восточно-Сибирского института МВД России. 2017. № 4.

Гришанков В. Geo Tagging (геотеггинг) в смартфоне – что это такое? // AndroidLime. 2018. 18 дек. URL: https://androidlime.ru/geo-tagging-smartphone-function (дата обращения: 22.04.2020).

Жуланов В., *Ищенко Е.* Анализ информации из электронных баз данных в следственной группе // Законность. 2007. № 4.

Максимович А. Б. Содержание и структура криминалистического учения о средствах сотовой связи // Актуальные проблемы российского права. 2016. № 11.

Максимович А. Б. Средства сотовой связи как объект криминалистического исследования: автореф. дис. ... канд. юрид. наук. М., 2018.

Мещеряков В. А., *Яковлев А. Н.* «Электронная» составляющая осмотра места происшествия // Библиотека криминалиста. 2015. № 5.

Старичков М. В. Устройства мобильной связи как источники криминалистической информации // Криминалистические чтения на Байкале – 2015: материалы междунар. науч.-практ. конф. / отв. ред. Д. А. Степаненко. Иркутск, 2015.

[1] *Яковлев А. Н.* Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств: «электронная почта» // Вестник Воронежского института МВД России. 2014. № 4. С. 45.

[2] Там же. С. 47.

[3] Программно-аппаратный комплекс «Мобильный Криминалист». URL: https://www.oxygensoftware.ru/ru/company/target/police (дата обращения: 22.01.2020).

Третьякова Е. И. Мобильный телефон как источник криминалистически значимой информации // Вестник Уральского финансово-юридического института. 2018. № 3.

Яковлев А. Н. Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств: «электронная почта» // Вестник Воронежского института МВД России. 2014. № 4.

Casadei F., Savoldi A., Gubian P. Forensics and SIM cards: an overview // International Journal of Digital Evidence. 2006. Vol. 5. Iss. 1.

References

Arkhipova N. A. Organizatsionno-takticheskie aspekty raskrytiya i rassledovaniya prestuplenii v situatsiyakh ispol'zovaniya sredstv mobil'noi svyazi: avtoref. dis. ... kand. yurid. nauk. SPb., 2011.

Casadei F., Savoldi A., Gubian P. Forensics and SIM cards: an overview // International Journal of Digital Evidence. 2006. Vol. 5. Iss. 1.

Gribunov O. P. Sredstva sotovoi svyazi kak istochnik kriminalisticheski znachimoi informatsii // Vestnik Vostochno-Sibirskogo instituta MVD Rossii. 2017. № 4.

Grishankov V. Geo Tagging (geotegging) v smartfone – chto eto takoe? // AndroidLime. 2018. 18 dek. URL: https://androidlime.ru/geo-tagging-smartphone-function (data obrashcheniya: 22.04.2020).

Maksimovich A. B. Soderzhanie i struktura kriminalisticheskogo ucheniya o sredstvakh sotovoi svyazi // Aktual'nye problemy rossiiskogo prava. 2016. № 11.

Maksimovich A. B. Sredstva sotovoi svyazi kak ob"ekt kriminalisticheskogo issledovaniya: avtoref. dis. ... kand. yurid. nauk. M., 2018.

Meshcheryakov V. A., Yakovlev A. N. «Elektronnaya» sostavlyayushchaya osmotra mesta proisshestviya // Biblioteka kriminalista. 2015. № 5.

Starichkov M. V. Ustroistva mobil'noi svyazi kak istochniki kriminalisticheskoi informatsii // Kriminalisticheskie chteniya na Baikale – 2015: materialy mezhdunar. nauch.-prakt. konf. / otv. red. D. A. Stepanenko. Irkutsk, 2015.

Tret'yakova E. I. Mobil'nyi telefon kak istochnik kriminalisticheski znachimoi informatsii // Vestnik Ural'skogo finansovo-yuridicheskogo instituta. 2018. № 3.

Yakovlev A. N. Pravovoi status tsifrovoi informatsii, izvlekaemoi iz komp'yuternykh i mobil'nykh ustroistv: «elektronnaya pochta» // Vestnik Voronezhskogo instituta MVD Rossii. 2014. № 4.

Zhulanov V., Ishchenko E. Analiz informatsii iz elektronnykh baz dannykh v sledstvennoi gruppe // Zakonnost'. 2007. № 4.