К объективным факторам относятся: погодные условия, в которых происходило восприятие описываемых событий; условия видимости, в которых свидетель воспринимал происходящее; расстояние от места нахождения свидетеля до места, где происходили описываемые им события; наличие посторонних раздражителей при восприятии интересующих правоохранительные органы событий (звуковой или световой фон) и др.

К субъективным факторам можно отнести: состояние органов зрения, слуха; особенности памяти свидетеля; физическое и психологическое состояние; заинтересованность лица в происходящем событии; профессиональная подготовленность и др. [2, с. 41].

Установление факторов, которые могли оказать влияние на формирование показаний свидетелей массовых беспорядков, позволяет избирать оптимальные тактические приемы допроса, способные минимизировать их воздействия.

На практике часто встречаются ситуации, когда свидетелями преступления или потерпевшими выступают большое количество сотрудников органов внутренних дел. Их целесообразно допрашивать незамедлительно, без предварительной подготовки по ограниченному кругу вопросов. Для сокращения трудоемкости данного процесса в условиях дефицита времени желательно, чтобы свидетели записывали свои показания собственноручно. Следователь может предложить им вопросники, которые охватывают весь предмет допроса и дифференцируются в зависимости от категории допрашиваемых лиц [3].

Вопросы, подлежащие выяснению в ходе допроса свидетелей, могут касаться обстоятельств, предшествовавших массовым беспорядкам и приведших допрашиваемого на место происшествия, действий конкретных участников беспорядков (выкрики, лозунги, призывы к расправам, сопротивление работникам милиции и военнослужащим и т. д.), их вооруженность, действия сотрудников правоохранительных органов, передвижение транспортных средств и т. д.

У военнослужащих, как правило, должны уточняться содержание поступивших команд, экипировка, вооружение, маршрут передвижения, характер поведения толпы, порядок их действий при ее рассеивании и т. д.

Полезно, чтобы у следователя имелась карта местности, схема зданий, где произошли массовые беспорядки. Карта должна быть без каких-либо пометок, чтобы допрашиваемый мог указывать на ней необходимые сведения.

По мере накопления значительного объема показаний потерпевших и свидетелей руководителю следственной группы целесообразно организовать их обобщение и систематизацию, используя с этой целью различного вида накопительные ведомости, таблицы, схемы и т. д.

Учитывая изложенное, представляется необходимым перед проведением допроса свидетелей и потерпевших по факту массовых беспорядков проводить сбор сведений, которые могут оказать помощь в установлении психологического контакта с допрашиваемыми, а также в выборе наиболее эффективных методов и тактических приемов его проведения. В процессе допроса следователю необходимо максимально учитывать факторы, которые могли оказать влияние на формирование показаний.

1. Порубов Н.И. Тактика допроса на предварительном следствии : учеб. пособие. Минск, 1998.

2. Грицаев С.И., Влезько Д.А., Шевель Д.В. Использование психологических знаний в расследовании преступлений : учеб. пособие. Краснодар, 2013.

3. Григорьев В.Н. Организация следственной работы в условиях чрезвычайного положения : учеб. пособие. Ташкент, 1991.

УДК 343.98.06

А.В. Полякова

ИСПОЛЬЗОВАНИЕ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ БИОМЕТРИЧЕСКИХ СИСТЕМ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В МОБИЛЬНЫХ УСТРОЙСТВАХ СВЯЗИ

В настоящее время широко распространены средства мобильной связи, портативные персональные компьютеры: информационно-телекоммуникационные технологии развиваются высокими темпами. В связи с этим, как подтверждает Н.А. Архипова, правоохранительные органы все чаще сталкиваются с необходимостью вовлечения в процесс раскрытия и расследования преступлений материалов, связанных с использованием средств мобильной связи [1, с. 6], что вызывает необходимость разработки более эффективных приемов и методов обнаружения, фиксации использования мобильных телефонов для сбора информации.

Под аутентификацией понимается процесс опознавания субъекта или объекта путем сравнения введенных идентификационных данных с его эталоном (образом), хранящимся в памяти системы [2].

Биометрическая аутентификация, основанная на использовании индивидуальных физических признаков человека, предусматривает наличие в мобильном устройстве связи специальных программно-аппаратных средств, таких как биометрический сканер, считывающий информацию.

Разработаны биометрические сканеры, которые учитывают статические признаки (распознавание по отпечаткам пальцев, геометрии руки, радужной оболочке глаза), а также динамические характеристики человека (распознавание по клавиатурному почерку, голосу, походке).

Мобильные устройства с возможностью идентификации личности по отпечаткам пальца имеют огромную популярность. В них предусмотрена система датчиков разблокировки смартфона с помощью данных отпечатка пальца. Такая система начиная с момента ее внедрения компанией Apple (сканер TouchID) показала свою эффективность при подтверждении личности владельца устройства и защите персональной информации от доступа посторонних лиц, преступников в первую очередь. По данным International Biometric Group, доля систем распознавания по отпечаткам пальцев составляет примерно 52 % всех используемых в мире биометрических систем [3].

Разработаны следующие типы сканеров отпечатков пальцев. Оптический формирует изображение всей панели пальцев, используя CCD-матрицу: в местах, куда свет не приходит (гребни), матрица записывает черные пиксели, создавая точно отображаемое изображение пальца. В емкостном сканере вместо матрицы предусмотрены специальные миниатюрные схемы конденсаторов (емкостных датчиков), которые после приложения пальца к считывателю изменяют свою емкость. Тепловой сканер использует микроскопические тепловые датчики, которые определяют разницу температур между гребнями и долями пальцевой подушки. Ультразвуковой сканер основан на явлении дифракции: в момент приложения пальца к датчику тот начинает генерировать не слышимые для нас звуки, так как поведение звуковых волн при контакте папиллярных линий пальца со сканером отличается от промежутков между ними.

Принцип работы всех сканеров практически един: с поверхности приложенного пальца по гребням и впадинам папиллярного узора сенсором считывается информация, которая регистрируется, а затем строится полная цифровая картина отпечатка. Система определяет тип узора (дуговой, петлевой, завитковый), сканер идентифицирует минуции (детали Гальтона) – окончания линий папиллярного узора, разветвления и пересечения этих линий, которые, являясь локальными и уникальными признаками отпечатка пальца, позволяют идентифицировать человека. Сканер определяет положение минуций относительно друг друга на каждом снимке: он разбивает отпечаток на небольшие блоки 9 × 9 пикселей, каждый из которых содержит определенное число минуций. Координаты обнаруженных минуций и их углы ориентации записываются в вектор. Затем идентичные блоки со сканера и снимков из базы данных

сопоставляются, и если узоры в них идентичны, то отпечатки пальцев принадлежат одному и тому же владельцу.

Существенным достоинством данного типа аутентификации пользователей, детерминирующим его распространенность и надежность, является отсутствие необходимости в запоминании различных паролей, графических ключей, формировании запросов на их восстановление при потере, взломе. Информация, сохраняемая на устройстве, получается только владельцем, что подтверждается свойством объектов криминалистической идентификации – индивидуальности папиллярных узоров каждого человека.

Однако данная система имеет ряд существенных недостатков. При попадании к преступникам мобильного устройства есть вероятность снятия отпечатка пользователя для полноценного его использования: информация об отпечатках пальцев владельца мобильного телефона в большинстве моделей содержится в виде незашифрованных файлов (изображения) в локальной памяти, а следовательно, возможен взлом и хищение данной информации злоумышленниками. Некоторые производители смартфонов ввели специальный элемент защиты чип – область в чипсете для хранения данных об отпечатках пальцев, внедрили сенсоры, создающие высококачественные изображения отпечатков, информация о которых в защищенных зонах хранится в виде математических образов (TrustZone (ARM), SecureEnclave (Apple) и Snapdragon Mobile Security (Qualcomm)). Кроме того, для защиты от взлома возможны ситуации выхода из строя датчика распознавания отпечатков пальцев.

Для преодоления защиты биометрических систем преступники используют различные способы фальсификации отпечатков пальцев рук пользователей. Профессор С.С. Самищенко определил поддельные следы рук как такие следы рук, которые были изготовлены с использованием способов, не имеющих места в обычном процессе следообразования (с помощью клише, путем опыления отпечатков пальцев и др.). Подложные следы, по его мнению, появляются в случаях умышленного введения в процесс расследования уголовного дела следов рук обычного происхождения, но не имеющих отношения к событиям преступления [4, с. 10, 27–28.].

А.Г. Сухарев, А.В. Стальмахов, Р.Ю. Трубицын предлагают существующие способы фальсификации папиллярных узоров, имеющие криминалистические цели, условно разделить на две группы: изменение рисунка папиллярного узора непосредственно на кожном покрове руки и изготовление искусственных папиллярных узоров в виде объемных муляжей или плоскостных копий, а также при помощи современных технологических средств [5, с. 65]. Способом, связанным с

технологическим процессом, может быть изготовлен как оттиск следа в полном объеме, так и какая-то его часть. Для изготовления искусственных папиллярных узоров пальцев рук применяются следующие технологии (способы): использование пластичных масс, метод фотолитографии, фотополимерный способ, лазерное гравирование на резине, флеш-технологии, вулканизация резины с матриц, полученных на основе использования твердых фотополимерных композиций и др.

Производители мобильных телефонов и правоохранительные органы объединяют усилия в борьбе с изготовлением искусственного папиллярного узора. Так, ведомство по патентам и товарным знакам США опубликовало на своем сайте патентную заявку компании Apple о биометрическом захвате неавторизованных пользователей, направленном на помощь полиции в розыске преступников. Предполагается использование сканера отпечатков пальцев Touch ID для активации режима сбора чужих отпечатков и изображений. Если датчик фиксирует прикосновение неавторизованного пользователя, встроенные камеры смартфона начинают снимать потенциального похитителя на фото и записывать видео. Затем эти данные сохраняются на устройстве или пересылаются на сервер, где отпечатки сравниваются с базой пользователей [6].

Наряду со сканером пальца в смартфонах используется и другой вид идентификации владельца устройства – распознавание лица (Face ID), предложенное компанией Apple (модель X). Комплекс сенсоров составляет 3D-модель лица из 30 тыс. точек для возможности распознания с разных ракурсов. Если лицо изменит внешность с помощью прически, бороды, макияжа и т. п., программа все равно распознает его. А встроенная ИК-камера позволяет программе функционировать даже при недостаточных условиях освещения.

Работа системы распознавания лиц в различных телефонах осуществляется в четыре этапа. Лицо сканируется: ИК-датчик определяет, есть ли лицо перед смартфоном, проектор передает на лицо 30 тыс. точек в ИК-диапазоне, ИК-камера считывает 3D-карту спроецированных точек, происходит извлечение уникальных данных лица (контуры глазниц, форма скул, ширина носа, иногда и шрамы). Полученные данные передаются в специальный сопроцессор SecureEnclave, встроенный в процессор A11 Bionic, в котором хранится паттерн лица владельца смартфона в зашифрованном виде. Далее происходит поиск сопоставлений. Если данные совпадут с паттерном, смартфон разблокируется.

В телефонах серии Galaxy S9 реализована технология Intelligent Scan, которая дополнительно сканирует сетчатку глаза, хотя распознавание лица возможно и при закрытых глазах.

Распознавание лиц реализовано в смартфонах Huawei, Xiaomi, Meizu, OnePlus, Nokia, Vivo, OPPO. Только в OPPO Find X система похожа на

Face ID, в остальных телефонах используется обычная фронтальная камера и 2D-карта.

Система аутентификации пользователя путем распознавания лиц также не лишена недостатков, к которым относятся: возникновение ошибок при идентификации близнецов или людей с очень схожими чертами лица, обман системы с помощью масок, распечатанных на 3D-принтерах; возможность сбоя системы; несовершенство системы из-за использования данных фронтальной камеры, которые существенно зависят от условий съемки. Датчики виртуально выводят на лицо большее количество точек, что позволяет ей срабатывать при появлении бороды, очков и других помех.

Для решения задач по раскрытию и расследованию преступлений становится интересным новое российское приложение FindFace, с помощью которого по фотографии возможно найти аккаунт человека в социальной сети «ВКонтакте». Достаточно сделать снимок человека на смартфон, загрузить в программу и получить его аккаунт в социальных сетях. Программа является инструментом поиска российскими правоохранительными органами подозреваемых, обвиняемых, свидетелей, но приложение пока не получило повсеместного внедрения. Например, в октябре 2017 г. система распознавания лиц FindFace уже использовалась во время протестных акций в Москве и ряде других регионов [7].

Отдельно отметим, что система распознавания лиц используется не только в мобильных устройствах. Она активно внедряется в камеры видеонаблюдения Московского метрополитена для предотвращения преступлений, розыска преступников. Система также включает особую программу сбора и анализа информации, позволяющую идентифицировать любого подозрительного пассажира по некоторым особенностям его внешности. Данный комплекс специальных средств определяет лицо каждого пассажира и сравнивает его с базой данных о людях, находящихся в розыске, анализируя и находя совпадения. Вначале камеры фиксируют человека при входе или выходе из станции, определяют подозрительные задержки в неустановленных местах и отмечают проявление странного поведения. Помимо того, возможности системы позволят быстро отслеживать любые предметы, что долгое время находятся без движения.

В начале 2017 г. в полицию китайского города Шэньчжэнь обратился молодой мужчина с заявлением о пропаже его трехлетней дочери. Случаи похищения детей в Китае не редкость. Раскрываемость таких преступлений раньше была крайне низка, так как зацепок у полицейских практически не было. Полицейские взяли у отца фотографию девочки, и поиск начался. Фотография была загружена в базу данных, нейросети стали ее сравнивать с данными районных видеокамер. В течение нескольких ми-

нут была обнаружена запись с уличной камеры, на которой видно, как неизвестная женщина идет по улице с пропавшим ребенком на руках.

В июле 2017 г. в Орегоне мужчина в магазине положил в корзину множество дорогих товаров и вышел, не воспользовавшись кассой самообслуживания. Камеры магазина зафиксировала признаки внешности вора. Полицейские, расследующие это дело, подключившись к системе распознавания лиц Amazon Rekognition, прогнали через базу данных с 300 тыс. фотографий преступников из их округа лицо магазинного вора. Сервис показал четырех людей с похожими лицами, аккаунты которых в социальной сети Facebook полицейские проверили и нашли преступника.

Таким образом, внедрение в деятельность по раскрытию и расследованию преступлений новых методов, разработанных на базе научно-технического прогресса, расширяет ее возможности, позволяет решать задачи на более высоком уровне, совершенствовать теоретические и методологические подходы к решению этих задач. Наука не стоит на месте, разрабатываются все более и более усовершенствованные технические приборы, устройства, программное обеспечение, которые должны внедряться в криминалистическую деятельность для борьбы с преступностью на новом, совершенном уровне. Также необходимо дальнейшее объединение усилий производителей мобильных устройств связи, сотрудников правоохранительных органов для раскрытия преступлений.

Тема работы не теряет своей актуальности и может быть предметом дальнейших исследований в сфере производства компьютерно-технической экспертизы для постановки новых задач, расширения возможностей получения содержащейся в мобильном телефоне информации.

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

2. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний [Электронный ресурс] : ГОСТ Р 51241-2008 : утв. приказом Федер. агентства по техн. регулированию и метрологии, 17 дек. 2008 г., № 430-ст. Доступ из справ.-правовой системы «КонсультантПлюс. Россия».

3. Подделка отпечатков пальцев [Электронный ресурс] // TECHPORTAL.RU: отраслевой медиаканал. URL: http://www.techportal.ru/glossary/poddelka-ot-pechatkov-palcev.html (дата обращения: 16.09.2018).

4. Самищенко С.С. Современная дактилоскопия: теория, практика и тенденции развития : автореф. дис. … д-ра юрид. наук. М., 2003.

5. Сухарев А.Г., Стальмахов А.В., Трубицын Р.Ю. Искусственные папиллярные узоры как негативные аспекты дактилоскопической идентификации и верификации // Судеб. экспертиза. 2011. № 1.

6. Apple запатентовала метод ловли преступников при помощи датчика Touch ID [Электронный ресурс] // Newsru.com. URL: https://hitech.newsru.com/article/26aug2016/apple (дата обращения: 18.09.2018).

7. Решения FindFace.PR. Идентификация личности. Поиск по огромным базам фотографий. Идентификация личности по фотографии за долю секунды [Электронный ресурс]. URL: https://findface.pro/ru/ (дата обращения: 03.10.2018).

УДК 343.13

А.В. Руденко

ДИАЛЕКТИЧЕСКИЕ ОСНОВЫ ЗАКОНОМЕРНОСТЕЙ СОБИРАНИЯ, ПРОВЕРКИ И ОЦЕНКИ ДОКАЗАТЕЛЬСТВ

Доказывание как деятельность, включающая в себя работу с людьми – носителями информации, версиями, доказательствами, доказательственными, промежуточными и искомыми фактами, представляет собой сложный процесс формирования достоверного вывода по делу. Основу этого процесса составляют конкретные факты объективной действительности, которые многократно отражаются в следах материального и идеального характера, сознании субъектов доказывания, в выдвигаемых ими версиях, выводимых из них логических следствиях, в результатах сопоставления доказательств, логических следствий и новых доказательств, в протоколах, в процессуальных решениях.

Сами факты не меняются, меняется оценка их отображения в различных обстоятельствах: при собирании, проверке, оценке и использовании доказательств. Для отображения фактов объективной действительности применяется воздействие, связанное не только с практической, но и с логической деятельностью, как формальной, так и содержательной. Появляется новое качество отображений, которое формирует субъективное представление об их основе. Это представление-образ является неполным, обрывочным, часто ошибочным, так как составлено из отображений различных фактических обстоятельств событий прошлого. Постепенно, в результате деятельности, направленной на достижение достоверного знания об обстоятельствах преступления, этот образ приобретает четкие очертания, границы, общие с образами иных событий, наполняется красками. Реализация конкретными субъектами процессуальной деятельности задач доказывания приводит к достижению характеристики знания об обстоятельствах преступного деяния и лице его совершившем как достоверного. При этом знание становится достоверным только при соблюдении предусмотренных законом требований к процессу доказывания.