конодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

3. Инструкции по делопроизводству в государственных органах, иных организациях, утв. постановлением М-ва юстиции Респ. Беларусь от 19 янв. 2009 г. № 4 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь.– Минск, 2023.

4. Ожегов, С. И. Толковый словарь русского языка / С. И. Ожегов, Н. Ю. Шведова. – 4-е изд., доп. – М.: Азбуковник, 1999. – 944 с.

АКТУАЛЬНЫЕ ВОПРОСЫ ПОИСКА И АНАЛИЗА ЦИФРОВЫХ СЛЕДОВ В МОБИЛЬНЫХ УСТРОЙСТВАХ (ПРОБЛЕМА ИСКУССТВЕННЫХ ПАПИЛЛЯРНЫХ УЗОРОВ)

Короневич М. А.

Центральный аппарат Государственного комитета судебных экспертиз Республики Беларусь, ул. Кальварийская, 43, 220073, г. Минск, Беларусь, m4xemka@gmail.com

Исследуется использование современных мобильных устройств как средств фиксации информации и помощи в ведении дел, связи и коммуникации, так и в качестве средств совершения преступления, содержащие, а также оставляющие важные и специфические следы. С учетом ценности содержательных цифровых следов и информации, хранящейся в мобильных устройствах, как наиболее достоверных ее источниках и носителях, отражены значимость и возможности современных программно-аппаратных средств и комплексов в обнаружении, фиксации, извлечении информации для последующего ее изучения, в том числе в целях успешного раскрытия, а также всестороннего, полного и оперативного расследования преступления, изобличения лица его совершившего. Рассматривается один из актуальных и проблемных вопросов, связанных с возможной фальсификацией точных и надежных методов идентификации личности, в том числе широко используемых в ходе раскрытия и расследования преступлений. Изучение данного проблемного вопроса в своих научных исследованиях российскими учеными обуславливает и научную значимость темы исследования.

В работе указывается на необходимость дальнейшей проработки проблемы искусственных папиллярных узоров в контексте противодействия фальсификации вещественных доказательств, а также процессуального закрепления способов получения копий следов пальцев рук подозреваемого, обвиняемого. Изложенные выводы, а также дальнейшее исследование обозначенных вопросов может не только положительно отразиться в ходе предварительного расследования, но и способствовать развитию отдельных теоретических положений, решению задач по защите интересов общества и государства от преступных и иных противоправных посягательств.

Ключевые слова: электронные устройства; мобильные устройства; цифровой след; информация; информационные технологии; отпечатки пальцев рук; идентификация; искусственные папиллярные узоры; фальсификация; следы пальцев рук

Информационные технологии занимают значительную часть повседневной жизни современного, образованного человека и интегрировались во все возможные сферы жизни общества, став одним из важнейших факторов, влияющих на его развитие.

По мере усложнения и развития форм, методов и средств автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, от которых порой зависит благополучие, а иногда и жизнь людей.

Современные электронные устройства, широко используемые для работы с информацией, не только значительно облегчили жизнь, но и расширили границы общения и дистанционного выполнения различных повседневных задач.

В Республике Беларусь по состоянию на январь 2023 года, в соответствии с отчетом аналитиков DataReportal [1], число интернет-пользователей составило 8,27 миллионов человек (что составляет 86,9% от общей численности населения). Выход в глобальную компьютерную сеть Интернет граждане страны в основном осуществляли посредством использования компактных портативных и стационарных персональных компьютеров (что составляет 50,01% в соответствии с аналитическими данными). При этом следует отметить, что доля использования данных устройств ежегодно падает, в то время как все большее предпочтение отдается использованию в указанных целях мобильных телефонов (доля использования которых составляет 49,13%). В сравнении с январем 2022 года – число интернет-пользователей составило 8,03 миллионов человек или 85,1% от общей численности населения. Выход в глобальную компьютерную сеть Интернет посредством использования компактных портативных и стационарных персональных компьютеров осуществило 57,05%, а посредством использования мобильных телефонов 42,04%.

Обзор научной литературы и работ российских ученых и исследователей: Бессонова А.А. [2, с. 46-52], Карпика А.Г. [3, с. 171-179], Карташова И.И. [4, с. 99-103], Мещерякова В.А. [5, с. 212-232, 6, с. 153-169], Петрова А.А. [7, с. 529-542], Родивилиной В.А. и Цуканова Н.Н. [8, с. 107-114], Соколова Ю.Н. [9, с. 22-26], Третьяковой Е.И. [10, с. 49-51] и др., как по теме исследования, так и по таким актуальным и взаимосвязанным вопросам, касательно механизма образования различного рода цифровых следов, их поиска, анализа и дальнейшего использования в качестве доказательств по уголовному делу, безусловно, не должны вызывать никаких сомнений в важности и эффективности использования цифровых следов в предупреждении, раскрытии и расследовании преступлений в веке информационных технологий.

Отсутствие за последнее десятилетие работ, а также научных исследований по вышеуказанным направлениям и темам белорусских авторов в условиях быстро меняющейся социальной среды, а также динамично развивающегося общества, обуславливает острую необходимость не только в их основательном изучении, но и использовании в целях повышения качества расследования преступлений.

Возможность голосового общения, использования различных прикладных программ, приложений для мгновенного обмена электронными сообщениями и

данными, поиска и получения интересующей информации в сети Интернет, создания, хранения, воспроизведения и передачи файлов различного формата – далеко не полный перечень возможностей современного портативного девайса.

Однако глобальная информатизация и связанная с ней телекоммуникационная среда обуславливают не только прогрессивные изменения в общественных отношениях, но и негативные тенденции развития преступного мира, приводят к появлению новых форм и видом преступных посягательств [11, с. 151].

Проведенный анализ практики расследования позволяет констатировать, что важнейшим элементом криминалистической структуры преступлений против информационной безопасности являются объекты – носители следов преступной деятельности. В процессе его исследования устанавливается сущность происшедшего события, а также обстоятельства, при которых совершено преступное деяние. При этом правильная криминалистическая оценка носителей следов противоправной деятельности позволяет на первоначальном этапе расследования, по исходным данным создать основу для быстрого и полного осуществления предварительного расследования.

Важно понимать, что мобильные устройства, с помощью которых совершаются преступления, оставляют не только широкий спектр специфических цифровых следов, представляющих собой любое изменение состояния автоматизированной информационной системы, зафиксированные в памяти мобильных устройств, но также содержат большое количество информационных источников о его пользователе. Поэтому, прежде всего, на месте их обнаружения и последующего изъятия, в обязательном порядке следует предпринимать меры, исключающие утрату возможно хранящихся в них доказательств и возникновение возможных ограничений по доступу к ним у правоохранительных органов.

В настоящее время единого мнения у различных его представителей касательно того, совершение каких действий позволит исключить возможное искажение, утрату либо ограничение доступа к хранящейся на устройстве информации, не выработано. Однако большинство согласилось с тем, что своевременное привлечение соответствующего специалиста в производстве следственного и иного процессуального действия, связанного с изъятием электронного носителя информации, наиболее эффективно, а также в большей степени позволит избежать наступления возможных негативных последствий, повышая при этом вероятность получения доступа к хранящейся информации для последующего ее извлечения.

Как показывает практика, информационные следы могут быть выявлены в ходе исследования компьютерной техники, а также программного обеспечения, которые образуются в результате воздействия на хранящуюся на устройстве информацию, представляя собой любые изменения, связанные с событием преступления.

Ежедневно, каждый пользователь мобильного устройства, оставляет десятки, сотни цифровых следов, к которым, прежде всего, следует отнести те, что позволяют установить лицо, совершившее преступление, с использованием информационно-коммуникационных технологий: IP-адрес в сети, MAC-адрес сетевого оборудования, адрес электронной почты, идентификатор социальной сети,

номер банковской карты, номер телефона, информация о соединениях абонента, информация базовых станций мобильной связи, данные систем геолокации и т.п. [12, с. 4]. Если говорить о специфике отличия цифровых следов от иных видов следов, то, возможно, следует выделить главное – отсутствие идентификационных признаков их связи с конкретным владельцем мобильного устройства. Нельзя исключать возможность использования одним лицом мобильного устройства другого лица в преступных целях, имея к нему свободный доступ. Именно это и составляет одну из основных проблем – определение владельца устройства.

Современные автоматизированные системы биометрической идентификации личности, основанные на распознании и использовании отпечатков пальцев рук, находят все более широкое распространение в современном мире. Почти каждое мобильное устройство оснащено защитой от доступа посредством распознавания пальца руки. При этом для разблокировки и получения доступа к неограниченному количеству хранящейся на устройстве информации достаточно лишь изготовить копию соответствующего слепка пальца руки его законного владельца.

В настоящее время проблеме искусственных папиллярных узоров в контексте противодействия фальсификации вещественных доказательств посвящены работы следующих белорусских ученых и исследователей: Кирвеля В.К. [13, с. 118-121, 14, с. 320-339, 15, с. 43-46, 16, с. 16-34, 17, с. 27-32, 18, с. 129-145, 19, с. 239-258], Ефременко Н.В. и Башиловой А.В. [20, с. 175-182, 21, с. 61-63], что может свидетельствовать о недостаточном объеме научных исследований и публикаций по данной тематике. Отчасти низкий уровень понимания сути и специфики проблемы, которая может возникнуть, а в некоторых развитых странах уже имеет место быть, в стремительно меняющемся, динамично развивающемся технологическом веке, приводят к обоснованному выводу: точные и надежные методы идентификации личности, в том числе широко используемые в ходе раскрытия и расследования преступлений, обуславливают интерес, создают предпосылки для их возможной фальсификации и подлога, что обуславливает научную новизну и практическую значимость данной темы [22, с. 64].

Следует также отметить, что для возможности получения правоохранительными органами доступа к мобильным устройствам с целью последующего извлечения необходимой доказательственной информации, ограниченной и защищенной посредством распознавания пальца рук их владельцем, при проведении уголовного процесса, проблема искусственных папиллярных узоров требует дальнейшей проработки, как и необходимость процессуального закрепления способов получения копий следов пальцев рук подозреваемого или обвиняемого для последующего получения законного доступа к их мобильным устройствам.

Возвращаясь к вопросу цифровых следов, полученных в процессе исследования устройств и данных, крайне важно принять меры по их сохранению в неизменном виде, чтобы иметь возможность проводить повторные исследования при возникновении новых или вновь открывшихся обстоятельств по уголовному делу.

Современные программно-аппаратные средства и комплексы, используемые для вышеуказанных целей, позволяют решать не только целый ряд задач по ис-

следованию компьютерной информации и техники, но и обеспечить доступ ко всей хранящейся информации на мобильном устройстве.

К таковым относятся: прибор «UFED TOUCH» (предназначен для извлечения данных из мобильных устройств); программное обеспечение «Physical Analyzer» (предназначено для анализа извлеченных из мобильных устройств данных); программное обеспечение «Cloud Analyzer»; программное обеспечение «Мобильный Криминалист» (предназначено для извлечения и анализа данных, содержащихся в памяти мобильных устройств); программное обеспечение «BelcaSoft» (предназначено для компьютерно-технического исследования, поиска, анализа и хранения цифровых следов), в том числе могут быть использованы «EnCase Forensic» и «XRY».

Программно-аппаратный комплекс «UFED TOUCH» используется для глубокого декодирования, анализа и подготовки отчетов, который позволяет извлекать на физическом уровне и декодировать полученные данные с обходом блокировки ввода графического ключа; извлекать на физическом уровне и на уровне файловой системы, а также декодирование данных из устройств на базе Android; широкая поддержка извлечения и декодирования из устройств Appleи иных; простой и быстрый доступ к заблокированным устройствам путем обхода, открытия или отключения пользовательского кода блокировки; восстановление разных типов удаленных данных из нераспределенного пространства в флеш-памяти устройства; возможность дешифрования зашифрованной базы данных истории программного обеспечения для обмена мгновенными сообщениями и данными; декодирование данных приложений, пароли, электронная почта, журнал вызовов, контакты, мультимедийные файлы и т.п.

«UFED Physical Analyzer» обеспечивает тщательную проверку данных при проведении криминалистических исследований мобильных устройств: передовые возможности по декодированию больших объемов данных с поддержкой самого широкого диапазона мобильных устройств; возможность дополнить материалы дела как существующими, так и удаленными данными, извлеченными из мобильных устройств; поиск, фильтрация и расширенное изучение данных, имеющих критически важное значение для расследования; визуализация мобильных данных с помощью инструментов аналитики и хронологии; сокращение объема ручных данных операций благодаря использованию автоматизированного процесса декодирования; извлечение информации из мобильных телефонов и внутренней памяти USB-накопителей информации, а также возможность обмена отчетами и обнаруженной информацией.

Большое распространение получил метод хранения данных на удаленных серверах, называемого облачным хранилищем. Для извлечения указанной информации используется программное обеспечение «Cloud Analyzer», позволяющее предоставить доступ к личным данным, расположенным в облачном хранилище, с помощью информации для входа в систему, извлеченной из мобильного устройства; доступ к персональным облачным данным с помощью имени пользователя и пароля, извлеченного из личных файлов, контактов или с помощью других средств обнаружения; извлечение информации из облачных источников данных с протоколированием и отслеживанием всего процесса с целью обеспе-

чения достоверности данных; визуализация данных в едином формате путем приведения данных разных облачных услуг к единому виду, просмотр данных в унифицированном формате и в формате хронологии, предварительного просмотра файлов, контактов или карт; отчеты, совместное использование и экспорт посредством создания и передачи удобочитаемых отчетов для всех данных или отфильтрованной информации.

Программное обеспечение «Мобильный Криминалист» обеспечивает: обход пароля на экран, сброс блокировки экрана; физическое извлечение устройств на платформе Android, iOS, Windows Phone, Windows Mobile, BlackBerry, Symbian ОС, Bada, китайских телефонов и других; физическое чтение карт памяти; загрузка незашифрованных образов; обработка зашифрованных образов; восстановление пароля к резервной копии; извлечение паролей, данных из облачных сервисов, резервных копий, граф связей, лент событий, поиска данных, списка наблюдения, анализа местоположения и т.п.

Следует отметить, что для оперативного извлечения информации, в том числе из мобильных устройств, сотрудники криминалистических отделов соответствующих следственных управлений Следственного комитета Республики Беларусь, наделены правом проведения осмотров данных устройств с использованием вышеуказанных программно-аппаратных средств и комплексов, с целью оперативного извлечения хранящейся на них информации и последующей ее записи на отдельные электронные носители информации, для дальнейшего осмотра, изучения, анализа и приобщения следователем по материалам уголовного дела.

Как показывает практика, следователи, при расследовании уголовных дел, достаточно широко и часто используют имеющуюся возможность получения информации из мобильных устройств в ходе проведения их осмотра. При этом анализ правоприменительной практики указывает на то, что при процессуально правильно составленном протоколе осмотра предметов, возникающие доводы стороны защиты и ходатайства перед судом о признании полученных вещественных доказательств недопустимыми, недостоверными или с нарушениями закона, а также конституционных прав и свобод подозреваемого или обвиняемого по уголовному делу, остаются неубедительными и без удовлетворения.

Изучение возможностей использования электронных цифровых следов и электронных данных, а также современных программно-аппаратных средств и комплексов открывает новые горизонты для дальнейшего развития указанной проблематики и проведения целенаправленных исследований с учетом сегодняшних современных возможностей.

Библиографический список

1. DIGITAL 2023: BELARUS [Electronic resource] : DataReportal [website]. – Mode of access: http://www.datareportal.com/reports/digital-2023-belarus. – Date of access: 20.03.2023.

2. Бессонов, А. А. О некоторых возможностях современной криминалистики в работе с электронными следами / А. А. Бессонов // Вестник Университета имени О. Е. Кутафина. – 2019. – № 3 (55). – С. 46–52.

3. Карпика, А. Г. Актуальные вопросы поиска и анализа цифровых следов в оперативно-розыскной деятельности / А. Г. Карпика // Юристъ – Правоведъ. – 2019. – № 3 (90). – С. 171–179.

4. Карташов, И. И. Проблемы формирования доказательств в уголовном судопроизводстве на основе цифровой информации / И. И. Карташов // Юридическая наука. – 2018. – № 3. – С. 99–103.

5. Мещеряков, В. А. Цифровые (виртуальные) следы в криминалистике и уголовном процессе / В. А. Мещеряков // Воронежские криминалистические чтения : сб. науч. тр. ; под ред. О. Я. Баева. – Воронеж : Изд-во ВГУ. – 2008. – Вып. 9. – С. 221–232.

6. Мещеряков, В. А. Электронные цифровые объекты в уголовном процессе и криминалистике / В. А. Мещеряков // Воронежские криминалистические чтения : сб. науч. тр. ; под ред. О. Я. Баева. – Воронеж: Изд-во ВГУ. – 2014. – Вып. 5. – С. 153–169.

7. Петров, А. А. Цифровой след человека: плюсы и минусы / А. А. Петров // Большая Евразия: развитие, безопасность, сотрудничество. – 2020. – № 3-2. – С. 529–542.

8. Родивилина, В. А. Изъятие и осмотр мобильного телефона как электронного носителя информации / В. А. Родивилина, Н. Н. Цуканов // Вестник Восточно-Сибирского института МВД России. – 2019. – № 4 (91). – С. 107–114.

9. Соколов, Ю. Н. Электронный носитель информации в уголовном процессе / Ю. Н. Соколов // Информационное право. – 2017. – № 3. – С. 22–26.

10. Третьякова, Е. И. Мобильный телефон как источник криминалистически значимой информации / Е. И. Третьякова // Вестник Уральского финансово-юридического института. – 2018. – № 3 (13). – С. 49–51.

11. Старичков, М. В. Тактика получения материалов для проведения компьютерной экспертизы из информационно-телекоммуникационных сетей / М. В. Старичков // Криминалистика: вчера, сегодня, завтра: сб. науч. тр. – 2016. – С. 150–154.

12. Гаврилин, Ю. В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации / Ю. В. Гаврилин, В. В. Шипилов // Российский следователь. – 2013. – № 23. – С. 2–6.

13. Кирвель, В. К. Искусственные папиллярные узоры : миф или реальность / В. К. Кирвель, А. С. Башилова // Вестн. Акад. МВД Респ. Беларусь. – 2010. – № 2 (20). – С. 118–121.

14. Кирвель, В. К. Фальсификация следов пальцев рук (искусственные папиллярные узоры) / В. К. Кирвель // Криминалистика и судебная экспертология : наука, обучение, практика : сб. науч. стат. XIII Междунар. науч.-практ. конф., Паланга, 14-16 сентября 2017 г. / Литовское криминалистическое общество, Литовский центр суд. экспертиз; редкол. Г. Юодкайте-Гранскене [и др.]. – Вильнюс, 2017. – С. 320–339.

15. Кирвель, В. К. Дактилоскопическая экспертиза: проблема искусственных папиллярных узоров / В. К. Кирвель // Судебная экспертиза Беларуси. – 2018. – № 2. – С. 43–46.

16. Кирвель, В. К. Дактилоскопическая экспертиза (АДИС) и биометрические системы идентификации личности по отпечаткам пальцев рук : проблема искусственных папиллярных узоров / В. К. Кирвель // Международные и национальные тенденции и перспективы развития судебной экспертизы : сб. науч. стат. Междунар. науч-практ. конф., Нижний Новгород, 16–17 мая 2019 г. / Национальный исследовательский Нижегородский исследовательский университет им. Н. И. Лобачевского. – Н. Новгород: Нижегород. исслед. ун-т им. Н. И. Лобачевского, 2019. – С. 16–34.

17. Кирвель, В. К. Проблема искусственных папиллярных узоров при идентификации личности по отпечаткам пальцев рук / В. К. Кирвель // Судебная экспертиза Беларуси. – 2019. – № 2 (9). – С. 27–32.

18. Kirvel, V. Fingerprint analysis (AFIS) and biometric system of identification by fingerprints: issue of artificial papillary pictures / V. Kirvel // Society and innovations. – Tashkent, 2020. – Issue 1. – № 3. – P. 129–145.

19. Kirvel, V. Fingerprint analisis (AFIS) and biometric system of identification by fingerprints: the issue of artificial papillary pictures / V. Kirvel / Economic crime and cybercrime : collection of scientific articles under the General editorship of Isabel Augsburg-Buchli (Crimilinalite economigue et cybercrimilinalite Melanges en I honneur de la professeure Isabele Augsburger-Bucheli) / Higher school Arc management at the University of applied Sciences of Western Switzerland; editorial : Jaguier, S., Beaudet-Labrecgue, O., Zbinden R. – Basel (Switzerland) : Helbing Lichtenhahn, 2021. – P. 239–258.

20. Ефременко, Н. В. Установление факта фальсификации следов пальцев рук / Н. В. Ефременко, А. В. Башилова // Вестн. Полоц. ун-та. Сер. D. Экон. и юрид. науки. – 2014. – № 13. – С. 175–182.

21. Ефременко, Н. В. О возможности фальсификации следов рук / Н. В. Ефременко, А. С. Башилова // Актуальные вопросы совершенствования судебно-экспертной деятельности : тез. докл. междунар. науч.-практ. конф., Минск, 23-24 окт. 2014 г. / Гос. ком. судебных экспертиз Респ. Беларусь; под ред. А.И. Швед [и др.]. – Минск : ГКСЭ, 2014. – С. 61–63.

22. Короневич, М. А. Противодействие фальсификация дактилоскопических и биологических следов / М. А. Короневич // Сборник статей студентов Академии управления при Президенте Республики Беларусь : сб. ст. / Акад. упр. при Президенте Респ. Беларусь; под. ред. канд. юрид. наук Н. И. Рудовича, Л. Р. Миронович, Е. В. Олехника. – 2-е изд. – Минск, 2022. – С. 62–69.

ПРЕВЕНЦИЯ СЛЕДСТВЕННЫХ ОШИБОК В КОММУНИКАТИВНОЙ ДЕЯТЕЛЬНОСТИ СЛЕДОВАТЕЛЯ, ВОЗНИКАЮЩИХ ПРИ ДОПРОСЕ ЛИЦ, НЕ ДОСТИГШИХ СОВЕРШЕННОЛЕТИЯ

Крамаренко В. П.

«Институт высоких технологий» Балтийского федерального университета имени Иммануила Канта,
ул. Фрунзе 6, 236040 Калининград, Россия, vkram39@mail.ru

«Беседу следует вести так, чтобы собеседников из врагов сделать друзьями, а не друзей – врагами»
Пифагор

В статье в качестве ее целей ставиться исследование коммуникативной деятельности следователя, направленной на получение и закрепление релевантной, криминалистически значимой информации от лиц, не достигших совершеннолетия, выявление типовых ошибок при ее подготовке и построению, обозначение путей преодоления последних. Примененные диалектический метод, анализ, синтез, дедукция, формально-юридический метод, системный метод, метод межотраслевых научных исследований, составили Методологию исследования, что позволило определить главные, системные элементы коммуникации. Предложить определение криминалистической коммуникации. Дать криминалистическое понятие ее основного инструмента – вопроса и техники их построения. Установить, что серьезную опасность, для качественной составляющей предварительного следствия, представляют, выявленные во время исследования факты низкого уровня