ИНФОРМАЦИЯ ИЗ МОБИЛЬНЫХ УСТРОЙСТВ КАК ИСТОЧНИК ДОКАЗАТЕЛЬСТВ ПРИ РАССЛЕДОВАНИИ УЧАСТИЯ ГРАЖДАН РОССИЙСКОЙ ФЕДЕРАЦИИ В НЕЗАКОННЫХ ВООРУЖЕННЫХ ФОРМИРОВАНИЯХ НА ТЕРРИТОРИИ ИНОСТРАННОГО ГОСУДАРСТВА

Цахуев А.В., Следственное управление Следственного комитета Российской Федерации по Республике Дагестан, Дагестанский государственный университет, г. Махачкала, Российская Федерация, *Albert05ck@mail.ru*

В статье представлены современные аппаратно-программные комплексы и программы извлечения судебной информации из мобильных устройств, позволяющие в кратчайшие сроки получить криминалистически значимую информацию из мобильных устройств, изъятых по уголовным делам, возбужденным по фактам участия граждан Российской Федерации в незаконных вооруженных формированиях на территории иностранного государства. Автором изложен перечень различного рода сведений, содержащихся в памяти мобильных устройств, затрагиваются проблемные вопросы, возникающие при процессуальном оформлении результатов, полученных в ходе извлечения данных из мобильных устройств. По мнению автора, применение аппаратно-программных комплексов и программ извлечения судебной информации позволит успешно получать из мобильных устройств важную доказательственную информацию, способствующую скорейшему раскрытию и расследованию преступлений.

Ключевые слова: незаконные вооруженные формирования, мобильные устройства, извлечение данных, аппаратно-программные комплексы и программы извлечения судебной информации, осмотр предметов, судебная компьютерно-техническая экспертиза.

DOI: 10.21779/2224-0241-2019-30-2-151-155

UDC 343.985.2

INFORMATION FROM MOBILE DEVICES, AS A SOURCE OF EVIDENCE IN THE INVESTIGATION RELATED TO PARTICIPATION IN ILLEGAL ARMED FORMATIONS ON THE TERRITORY OF A FOREIGN STATE

Tsakhuev A.V., Investigative Directorates of the Russian Federation Investigative Committee for the Dagestan Republic, Dagestan State University, Makhachkala, Russian Federation, *Albert05ck@mail.ru*

The article presents modern hardware-software complexes and programmes of forensic information extraction from mobile devices, allowing quickly obtain forensic information from mobile devices seized in criminal cases initiated on the facts of participation of citizens of the Russian Federation in illegal armed formations on the territory of a foreign state. The author presents a list of various kinds of information contained in the memory of mobile devices, touches on the problematic issues arising in the procedural design of the results obtained during the extraction of data from mobile devices. The author is of the opinion that the use of hardware-software complexes and programmes of forensic information extraction will successfully obtain from mobile devices important evidentiary information that contributes to the early detection and investigation of crimes.

Key words: illegal armed formations, mobile devices, extract data, hardware-software complexes and programs of forensic information extraction, inspection of items, forensic computer-technical examination.

DOI: 10.21779/2224-0241-2019-30-2-151-155

В последние годы на территории Российской Федерации сохраняется большое количество преступлений террористической направленности, которые на современном этапе представляют наибольшую угрозу национальной безопасности нашей страны.

По данным Главного информационно-аналитического центра (ГИАЦ) МВД России на территории России в 2014 году зарегистрировано 1 128 преступлений террористической направленности

(АППГ +70,5%), в 2015 году – 1 538 (АППГ +35,8%), в 2016 году – 2 227 (АППГ +44,8%), в 2017 году – 1 871 (АППГ –16,0%), а за 2018 год – 1 679 (АППГ –10,3%) [1].

Участие граждан России в незаконных вооруженных формированиях (далее – НВФ) занимают значительную долю и составляют 65,8% от общего количества преступлений террористической направленности [2, с. 292]. Наибольшую угрозу представляет участие граждан России в НВФ на

территории иностранного государства. В качестве наглядного примера участия российских граждан в НВФ на территории иностранного государства приведем военный конфликт в Сирийской Арабской Республике (далее – САР), на территории которой в настоящее время действуют многочисленные НВФ, такие как «Джейш аль-Ислам», «Сабрий Джамаат», «Исламское государство», Хайят Тахрир аш-Шам и др., признанные террористическими и деятельность которых запрещена Решением Верховного Суда Российской Федерации на территории нашей страны [3]. Выезд российских граждан в САР и их участие в составе НВФ давно приобрела серьезный масштаб, что подтверждают данные Генерального штаба ГРУ, ФСБ и других специальных служб Российской Федерации, согласно которым в САР на стороне боевиков в составе НВФ сражается около четырех тысяч выходцев из России [4]. Боевики, возвращаясь на территорию России, продолжают свою преступную деятельность, в связи с чем основным направлением деятельности правоохранительных органов является пресечение их деятельности, фактов вербовки новых членов в ряды НВФ, а также перекрытие каналов их финансирования [5, с. 295].

В настоящее время в правоприменительной практике имеются проблемы доказывания преступной деятельности граждан России, выехавших для участия в составе НВФ на территорию иностранного государства. При проведении проверок сообщений о преступлениях в порядке ст. 144 и 145 УПК РФ и расследовании уголовных дел указанной категории все чаще возникает необходимость в изъятии и извлечении данных из различного рода мобильных устройств, к которым относятся мобильные телефоны, а также любой цифровой прибор, имеющий внутреннюю память и средства коммуникации, в том числе КПК-устройства, GPS-устройства, планшетные компьютеры, видеорегистраторы и т.д. [6, с. 13]. На любом мобильном устройстве, находящемся в пользовании преступника и других участников судопроизводства, хранятся электронные следы совершенного или готовящегося преступления [7, с. 43]. К таким следам относятся: контакты, сведения об устройстве, о соединениях между абонентами (исходящие, входящие, пропущенные звонки), переписка в виде SMS-сообщений, сообщений в социальных сетях и мессенджерах, фотоизображения, видео и аудиофайлы, геопозиционная информация, журнал использования интернет-браузеров, сведения о владельце устройства (пароли, логины, имена) и др. Указанные следы могут являться единственным доказательством по делу, в связи с чем возрастает их криминалистическая значимость [8, с. 156].

По результатам исследования, проведенного сотрудниками Института повышения квалификации Следственного комитета Российской Федерации, наиболее частыми объектами изъятия и извлечения электронной информации выступают мо-

бильные телефоны (67%), SIM-карты (29%) и планшетные компьютеры (4%) [9, с. 10].

Полноценная работа с мобильными устройствами возможна только при хорошей оснащенности правоохранительных органов современной высокотехнологичной криминалистической техникой, позволяющей извлекать полную (включая удаленную) информацию из памяти мобильных устройств, а также различного рода накопителей данных (карт памяти, SIM-карт и др.). К такой технике относятся аппаратно-программные комплексы «UFED», разработанный израильской компанией «Cellebrite», «XRY» (разработчик – шведская компания «Micro Systemation»), программный комплекс «Мобильный криминалист» (разработчик – российская компания «Oxygen Software») и др. [10, с. 12].

Исследование практики применения программных комплексов при извлечении данных из мобильных устройств при расследовании уголовных дел указанной категории показало, что в 83% случаев была получена информация, имеющая значение для дела. К сожалению, как показывает практика, не все следователи используют возможности таких комплексов.

На сегодняшний день в правоприменительной практике сложились различные мнения по поводу процессуального оформления результатов, полученных при извлечении данных из мобильных устройств. Из положений действующего законодательства следует, что извлечение данных из мобильных устройств возможно при производстве следственных действий (осмотр предметов), судебных экспертиз (компьютерно-технических) либо в ходе оперативно-розыскных мероприятий (исследование предметов и документов) [11, с. 22].

Изучение следственной и судебной практики расследования уголовных дел указанной категории показывает, что извлечение данных из мобильных устройств в ходе осмотра предметов занимает значительную долю и составляет 92% от общего количества извлечений, при производстве судебной компьютерно-технической экспертизы – 6,5%, в ходе оперативно-розыскных мероприятий – 1,5%.

Мы считаем, что осмотр предметов, в рамках которого производится извлечение данных из мобильных устройств, является наиболее оптимальным в связи с тем, что возникают обстоятельства, когда такое извлечение, в оперативно-тактическом смысле, необходимо произвести в кратчайшие сроки, а загруженность экспертов-компьютерщиков зачастую затягивает сроки проведения компьютерно-технической экспертизы до нескольких месяцев.

Результаты проведенного анкетирования следователей, в производстве которых находились уголовные дела рассматриваемой категории, свидетельствует о сложившемся у них мнении в части нарушения конституционных прав владельцев мобильных устройств, из которых осуществляется

извлечение данных. Однако оно является неверным, так как в Определении Конституционного Суда Российской Федерации от 25.01.2018 № 189-О сказано, что «проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения, и они не могут расцениваться как нарушающие его конституционные права» [12].

Безусловно, при извлечении данных из мобильных устройств в рамках осмотра предметов, обязательным является участие специалиста, применение специальной криминалистической техники или программ, фиксация хода извлечения данных из мобильных устройств с помощью фото- или видеосъемки, исключение возможности внесения каких-либо изменений либо потери каких-либо данных с памяти мобильных устройств [13, с. 15; 14, с. 254].

Хочется отметить, что успех расследования уголовных дел указанной категории во многих случаях зависит от соблюдения следователями и другими сотрудниками правоохранительных органов требований, предъявляемых к фиксации, изъятию, упаковке и осмотру любых электронных носителей информации [15; 16, с. 51].

В качестве положительного примера применения современных средств извлечения данных из мобильных устройств при расследовании уголовных дел рассматриваемой категории, с помощью которых получены сведения, имеющие важное доказательственное значение, можно привести уголовное дело, возбужденное по факту участия жителя Республики Дагестан в НВФ на территории иностранного государства. Расследованием установлено, что гражданин Г., 23.09.2017 г. вступил в НВФ, действующее на территории САР, принимал участие в боевых действиях, а также выполнял иные возложенные на него функциональные обязанности. В феврале 2017 года гражданин Г. покинул САР и вернулся на территорию России в Республику Дагестан, свою причастность к НВФ он отрицал. В результате проведенного в его домовладении обыска был обнаружен мобильный телефон «Samsung» с картой памяти, которые были изъяты

и незамедлительно осмотрены с применением аппаратно-программных комплексов. В ходе осмотра были получены фотоизображения, в том числе удаленные, на которых запечатлен гражданин Г. с оружием различных систем и моделей. На допросе гражданин Г. дал признательные показания, что на фотографиях изображен он с другими участниками НВФ, действующими на территории САР, в руках у него выданные для участия в боевых действиях автомат Калашникова и другие модели огнестрельного оружия [17].

В результате можно прийти к следующим выводам:

1) при расследовании участия граждан Российской Федерации в НВФ на территории иностранного государства изымается и осматривается большое количество мобильных устройств, содержащих в себе различные виды электронных следов, порой, являющихся единственными доказательствами по делу, в связи с чем возрастает их криминалистическая значимость;

2) имеющиеся на сегодняшний день в распоряжении криминалистических подразделений программные комплексы извлечения судебной информации из мобильных устройств заметно увеличили процент раскрываемости при расследовании участия граждан Российской Федерации в НВФ на территории иностранного государства;

3) извлечение данных из мобильных устройств при расследовании уголовных дел рассматриваемой категории может осуществляться в ходе следственных действий (осмотр предметов), при производстве судебных экспертиз (компьютерно-технических) либо в ходе оперативно-розыскных мероприятий (исследование предметов и документов), при этом способ получения данных определяет следователь с учетом складывающейся по делу оперативно-тактической ситуации;

4) применение современных программных комплексов извлечения судебной информации позволит в кратчайшие сроки успешно получать из мобильных устройств важную доказательственную информацию, способствующую скорейшему раскрытию и расследованию участия граждан Российской Федерации в НВФ на территории иностранного государства.

Литература

1. Состояние преступности в Российской Федерации за 2014–2018 гг. М.: ГИАЦ МВД России, 2018.
2. Меркурьев В.В., Агапов П.В. Уголовная политика в сфере противодействия преступлениям, связанным с участием российских граждан в незаконных вооруженных формированиях на территориях иностранных государств // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 4 (36). С. 292–295.
3. Решение Верховного Суда Российской Федерации от 29.12.2014 г. по делу № АКПИ 14-1424С [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru> (дата обращения: 01.03.2019).

4. Путин: в Сирии на стороне боевиков сражаются до четырех тысяч выходцев из РФ [Электронный ресурс]. URL: <http://tass.ru/politika/4047882> (дата обращения: 28.02.2019).
5. *Цахуев А.В., Юсупкадиева С.Н.* Участие граждан Российской Федерации в незаконных вооруженных формированиях на территории иностранного государства в целях, противоречащим интересам Российской Федерации // Евразийский юридический журнал. 2017. № 5 (108). С. 294–296.
6. *Олиндер Н.В.* Типичные способы совершения преступлений с использованием электронных платежных средств и систем // Эксперт-криминалист. 2014. № 1. С. 13–15.
7. *Смушкин А.Б.* Виртуальные следы в криминалистике // Законность. 2012. № 8. С. 43–45.
8. *Вехов В.Б.* Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения: сб. науч.-практ. тр. М.: Акад. Следственного комитета Российской Федерации, 2015. № 2. С. 155–158.
9. *Багмет А.М., Скобелин С.Ю.* Актуальные вопросы применения криминалистической техники для получения информации, содержащейся в мобильных электронных устройствах // Вестник криминалистики. М.: Спарк, 2013. Вып. 4 (48). С. 9–14.
10. *Хмелева А.В.* Тактические особенности назначения судебных экспертиз // Эксперт-криминалист. 2014. № 4. С. 12–15.
11. *Зуев С.В.* Электронное копирование информации – регламентация в УПК // Законность. 2013. № 8. С. 22–23.
12. Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации: определение Конституционного Суда Рос. Федерации от 25 янв. 2018 г. № 189-О [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru> (дата обращения: 05.03.2019).
13. *Багмет А.М., Скобелин С.Ю.* Особенности применения криминалистической техники для извлечения и анализа данных мобильных устройств // Совершенствование деятельности правоохранительных органов по борьбе с преступностью в современных условиях: материалы междунар. науч.-практ. конф. (1–2 ноября 2013 г.). Вып. 10: в 2 ч. Ч. 2. Тюмень: ТГАМЭУП, 2013. С. 13–17.
14. *Савицкая И.Г.* Участие специалиста в следственных действиях, связанных с изъятием электронных носителей информации // Судебная власть и уголовный процесс. 2016. № 2. С. 250–254.
15. *Салихов Т.Ю.* Поиск и изъятие электронных носителей информации // Вестник криминалистики. М.: Спарк, 2018. Вып. 3 (24). С. 25–29.
16. *Шибанова Е.В.* Особенности реализации следственных действий, проводимых с использованием кибернетических систем // Право и кибербезопасность. 2014. № 1. С. 51–54.
17. Дело № 1-42/2018. Архив Буйнакского районного суда Республики Дагестан.

References

1. *Sostoyanie prestupnosti v Rossiiskoi Federatsii za 2014–2018 gg.* М.: GIATs MVD Rossii, 2018.
2. *Merkur'ev V.V., Agapov P.V.* Ugolovnaya politika v sfere protivodeistviya prestupleniyam, svyazannym s uchastiem rossiiskikh grazhdan v nezakonnykh vooruzhennykh formirovaniyakh na territoriyakh inostrannykh gosudarstv // Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii. 2016. № 4 (36). С. 292–295.
3. Reshenie Verkhovnogo Suda Rossiiskoi Federatsii ot 29.12.2014 g. po delu № AKPI 14-1424S [Elektronnyi resurs] // Ofitsial'nyi internet-portal pravovoi informatsii. URL: <http://www.pravo.gov.ru> (data obrashcheniya: 01.03.2019).
4. Putin: v Sirii na storone boevikov srazhayutsya do chetyrekh tysyach vykhodtsev iz RF [Elektronnyi resurs]. URL: <http://tass.ru/politika/4047882> (data obrashcheniya: 28.02.2019).
5. *Tsakhuev A.V., Yusupkadiyeva S.N.* Uchastie grazhdan Rossiiskoi Federatsii v nezakonnykh vooruzhennykh formirovaniyakh na territorii inostrannogo gosudarstva v tselyakh, protivorechashchim interesam Rossiiskoi Federatsii // Evraziiskii yuridicheskii zhurnal. 2017. № 5 (108). С. 294–296.
6. *Olinder N.V.* Tipichnye sposoby soversheniya prestuplenii s ispol'zovaniem elektronnykh platezhnykh sredstv i sistem // Ekspert-kriminalist. 2014. № 1. С. 13–15.
7. *Smushkin A.B.* Virtual'nye sledy v kriminalistike // Zakonnost'. 2012. № 8. С. 43–45.
8. *Vekhov V.B.* Ponyatie, vidy i osobennosti fiksatsii elektronnykh dokazatel'stv // Rassledovanie prestuplenii: problemy i puti ikh resheniya: sb. nauch.-prakt. tr. М.: Akad. Sledstvennogo komiteta Rossiiskoi Federatsii, 2015. № 2. С. 155–158.
9. *Bagmet A.M., Skobelin S.Yu.* Aktual'nye voprosy primeneniya kriminalisticheskoi tekhniki dlya polucheniya informatsii, soderzhashcheysya v mobil'nykh elektronnykh ustroystvakh // Vestnik kriminalistiki. М.: Spark, 2013. Vyp. 4 (48). С. 9–14.
10. *Khmeleva A.V.* Takticheskie osobennosti naznacheniya sudebnykh ekspertiz // Ekspert-kriminalist. 2014. № 4. С. 12–15.

11. Zuev S.V. Elektronnoe kopirovanie informatsii – reglamentatsiya v UPK// Zakonnost'. 2013. № 8. S. 22–23.
12. Ob otkaze v prinyatii k rassmotreniyu zhaloby grazhdanina Prozorovskogo Dmitriya Aleksandrovicha na narushenie ego konstitutsionnykh prav stat'yami 176, 177 i 195 Ugolovno-protsessual'nogo kodeksa Rossiiskoi Federatsii: opredelenie Konstitutsionnogo Suda Ros. Federatsii ot 25 yanv. 2018 g. № 189-O [Elektronnyi resurs] // Ofitsial'nyi internet-portal pravovoi informatsii. URL: <http://www.pravo.gov.ru> (data obrashcheniya: 05.03.2019).
13. Bagmet A.M., Skobelin S.Yu. Osobennosti primeneniya kriminalisticheskoi tekhniki dlya izvlecheniya i analiza dannykh mobil'nykh ustroystv // Sovershenstvovanie deyatel'nosti pravookhranitel'nykh organov po bor'be s prestupnost'yu v sovremennykh usloviyakh: materialy mezhdunar. nauch.-prakt. konf. (1–2 noyabrya 2013 g.). Vyp. 10: v 2 ch. Ch. 2. Tyumen': TGAMEUP, 2013. S. 13–17.
14. Savitskaya I.G. Uchastie spetsialista v sledstvennykh deistviyakh, svyazannykh s iz'yatiem elektronnykh nositelei informatsii // Sudebnaya vlast' i ugolovnyi protsess. 2016. № 2. S. 250–254.
15. Salikhov T.Yu. Poisk i iz'yatie elektronnykh nositelei informatsii // Vestnik kriminalistiki. M.: Spark, 2018, Vyp. 3 (24). S. 25–29.
16. Shibanova E.V. Osobennosti realizatsii sledstvennykh deistvii, provodimykh s ispol'zovaniem kiberneticheskikh sistem // Pravo i kiberbezopasnost'. 2014. № 1. S. 51–54.
17. Delo № 1-42/2018. Arkhiv Buinakskogo raionnogo suda Respubliki Dagestan.

*Поступила в редакцию 9 апреля 2019 г.
Received 9 April, 2019*