Научная статья
УДК 343.985.2
EDN NTIQZQ
DOI 10.17150/2411-6122.2022.3.39-48

Некоторые вопросы обнаружения и исследования компьютерной информации при раскрытии и расследовании преступлений

А.А. Титов
Следственный департамент МВД России, г. Москва, Российская Федерация,
titov-aa@yandex.ru

Аннотация. В содержании статьи рассматриваются вопросы обнаружения и исследования компьютерной информации при проведении следственных действий и оперативно-розыскных мероприятий. Автором обозначаются проблемы недостаточной оснащенности оперативных, следственных и криминалистических подразделений техникой и программным обеспечением, при этом обозначается вывод о том, что современные возможности использования программно-аппаратных комплексов позволяют проводить качественный осмотр компьютерных и иных электронных устройств и безопасно извлекать необходимую информацию. Определяется специфика получения компьютерной информации с использованием аппаратно-программных комплексов. Также в статье выделяются отдельные характерные особенности деятельности специалиста при осмотре компьютерных устройств. Автором постулируется, что специалист в области компьютерных технологий является лицом, обладающим специальными знаниями, и содействующим следователю при осмотре электронных устройств. Он обладает знаниями и умениями пользования специальным аппаратным комплексом. При этом подчеркивается, что при производстве следственного действия следователь самостоятельно направляет ход производства следственного действия, именно он несет ответственность за результаты осмотра.

Ключевые слова: компьютерная информация, следственные действия, оперативно-розыскные мероприятия, осмотр компьютерных устройств, извлечение данных, следователь, оперативный сотрудник, информационные технологии.

Для цитирования: Титов А.А. Некоторые вопросы обнаружения и исследования компьютерной информации при раскрытии и расследовании преступлений / А.А. Титов. — DOI 10.17150/2411-6122.2022.3.39-48 — EDN NTIQZQ // Сибирские уголовно-процессуальные и криминалистические чтения. — 2022. — № 3. — С. 39–48.

Original article

Some Questions of Detecting and Researching Computer Information in Solving and Investigating Crimes

A.A. Titov
Investigations Department of the Ministry of Internal Affairs of Russia, Moscow, the Russian Federation,
titov-aa@yandex.ru

Abstract. The author examines the questions of detecting and researching computer information as part of investigative actions and operative search activities. The author also discusses the problems of insufficient availability of equipment

and software in operative, investigation and criminalistics divisions, and concludes that modern program-apparatus complexes make it possible to conduct a high-quality examination of computer and other electronic devices and to safely extract the necessary information. The specific features of obtaining computer information with the help of program-apparatus complexes are determined. The author also outlines some typical characteristics of the actions of a specialist during the examination of computer devices. It is stated that the computer technology specialist is a person with specialized knowledge who helps the investigator in the examination of electronic devices. This person has the knowledge and skills of using special apparatus complexes. It is also stressed that the investigator independently directs the course of investigative actions and is responsible for the results of the examination.

Keywords: computer information, investigative actions, operative search activities, examination of computer devices, extraction of data, investigator, operative employee, information technologies.

For citation: Titov A.A. Some Questions of Detecting and Researching Computer Information in Solving and Investigating Crimes. *Sibirskie Ugolovno-Processual'nye i Kriminalisticheskie Chteniya = Siberian Criminal Procedure and Criminalistic Readings,* 2022, no. 3, pp. 39–48. (In Russian). EDN: NTIQZQ. DOI: 10.17150/2411-6122.2022.3.39-48.

Повсеместная цифровизация и компьютеризация общества коснулись не только административной деятельности государства, но и его правоохранительной сферы. Так, принятое Распоряжение МВД России от 29.12.2020 г. № 1/15065 «Об утверждении Ведомственной программы цифровой трансформации МВД России на 2021–2023 годы»[1] наглядно демонстрирует активное влияние информационно-телекоммуникационных технологий на деятельность правоохранителей.

Необходимость внедрения цифровых технологий вызвана требованиями времени. Достаточно упомянуть количество краж с банковских карт, совершенных дистанционным способом, или количество преступлений в сфере компьютерной информации.

Так, в период с января по март 2022 г. удельный вес преступлений, совершенных с использованием информационно-телекоммуникационных технологий, составил 25, 7 % от общего числа зарегистрированных преступлений[2]. Иными словами, каждое четвертое преступление было совершено в сфере информационно-телекоммуникационных технологий или компьютерной информации. Как видно, статистические показатели объединяют указанные виды преступлений в единую группу. Такой подход обоснован тем, что по механизму, способу совершения и сокрытия обозначенных преступлений можно выделить их общую специфику. Она определяется в зависимости от свойств и структуры используемых информационных технологий и технических средств. Например, из 89 494 преступлений, совершенных с использованием сети «Интернет», 49 264 совершены с помощью средств мобильной связи, 8 274 — компьютерной техники[3].

Однако деятельность по предупреждению, раскрытию и расследованию преступлений такого рода не является «традиционной» для должностных лиц,

[1] Об утверждении Ведомственной программы цифровой трансформации МВД России на 2021–2023 годы : Распоряжение МВД России от 29 дек. 2020 г. № 1/15065 : (ред. от 8 сент. 2021) // СПС «КонсультантПлюс».

[2] Состояние преступности в Российской Федерации за январь-март 2022 г. // Портал правовой статистики. URL: http://crimestat.ru/analytics.

[3] Там же.

ведущих предварительное расследование. Данный аспект создает определенные сложности для выявления и раскрытия указанных видов преступлений. Динамика развития информационных технологий требует от правоохранительных органов столь же стремительной реакции.

Основываясь на результатах опроса, проведенного Л.Б. Красновой, 63 опрошенных следователя, что составляет 41,7 % от общего числа опрошенных, зачастую испытывают трудности при исследовании электронных следов при проведении следственных действий, связанных с компьютерной техникой и информационными технологиями [1, с. 5]. Это означает, что большинство трудностей возникает в связи с необходимостью обнаружения, фиксации и исследования электронных следов. Основной причиной возникающих сложностей является многообразие объектов, которые относятся к компьютерным устройствам, требующим применение специальных приемов и методов собирания и исследования информации. Несмотря на то, что в последнее время эта тема становится предметом изучения большого числа научных работ, а с каждым годом вырабатывается определенный практический опыт, проблема исследования электронных следов остается малоизученной и актуальной.

Анализ научной литературы и показателей практической деятельности позволяет автору настоящей статьи сформулировать следующие проблемные вопросы, влекущие сложности работы с электронными следами.

Первая проблема обуславливается недостаточной оснащенностью оперативных, следственных и криминалистических подразделений техникой и программным обеспечением, как минимум соответствующим тому, которое используют злоумышленники. Опыт показывает, что мир преступности уже давно опередил стражей правопорядка в вопросе технической оснащенности. Так, по данным МВД России, только за 2021 г. ущерб от дистанционного мошенничества составил 45 млрд р.[4] Стоит отметить, что от общего числа зарегистрированных преступлений за указанный период времени было раскрыто лишь 25,3 %[5], что не соответствует даже половине удельного веса. Данное обстоятельство непосредственно свидетельствует о том, что злоумышленники идут «на шаг впереди» правоохранителей в вопросе цифровизации, что, в свою очередь, негативно влияет на результаты деятельности органов правопорядка.

Вторая проблема связана с отсутствием соответствующей подготовки сотрудников оперативных и следственных подразделений. Дело в том, что в настоящее время не многие ведомственные вузы ведут подготовку узких специалистов по расследованию преступлений в области информационной безопасности или по расследованию иных преступлений, совершенных с применением информационно-телекоммуникационных средств. Безусловно, ведется постепенная интеграция результатов цифровизации в образовательный процесс, однако, обучить всех действующих сотрудников — процедура весьма затруднительная. Представляется, что в таком случае в следственных, оперативных и криминалистических подразделениях должен происходить взаимный обмен опытом и знаниями.

[4] МВД оценило ущерб от телефонного и интернет-мошенничества // Риа новости. URL: https://ria.ru/20211214/moshennichestvo-1763651565.html.

[5] Министерство внутренних дел Российской Федерации. М., 2022. URL: https://мвд.рф/reports/item/28021552/.

Перечисленные проблемы, безусловно, не носят исчерпывающий характер, однако выявлены нами в качестве основополагающих.

Современные возможности использования программно-аппаратных комплексов позволяют проводить качественный осмотр компьютерных и иных электронных устройств и безопасно извлекать необходимую информацию. Однако каково место программно-аппаратных комплексов в системе криминалистических средств при изъятии компьютерной информации? Заслуживает внимания позиция, выраженная А.М. Багметом и С.Ю. Скобелиным, которые указывают на необходимость выделения двух самостоятельных действий [2, с. 6]:

– изъятие электронного устройства;

– изъятие информации из устройства.

Анализируя указанную точку зрения, отметим, что действующий Уголовно-процессуальный кодекс РФ (далее — УПК РФ) не предусматривает специальную процедуру для извлечения информации из электронного устройства и ее последующего анализа. Изучение материалов уголовных дел показало, что подобное «извлечение» происходит в рамках производства следующих следственных действий: осмотр предметов; назначение и производство компьютерной экспертизы; выемка электронных носителей информации.

Указанные следственные действия активно используются в качестве инструмента обнаружения, изъятия или осмотра компьютерных устройств. Однако процедуры по изъятию самого устройства и информации с него зачастую смешиваются либо сливаются воедино. Следует отметить, что осмотр самого компьютерного устройства — процесс не простой и вряд ли можно его сравнить с осмотром другого предмета материального мира. При осмотре компьютерного устройства необходимо проделывать длительный цифровой путь к нужной информации. В связи с чем такое действие сложно назвать осмотром.

Необходимо дополнить, что обнаружить криминалистически значимую информацию можно и в ходе производства оперативно-розыскной деятельности (далее — ОРД). Так, в 2016 г. перечень оперативно-розыскных мероприятий (далее — ОРМ) был дополнен новым пунктом в виде получения компьютерной информации[6]. Безусловно, данное ОРМ позволяет оперативным сотрудникам получать сведения с электронных устройств. С принятием указанных изменений законодатель преодолел многолетнюю «путаницу», когда компьютерную информацию получали в ходе снятия информации с технических каналов связи, в ходе обследования помещений, зданий и сооружений и т.д. [3, с. 171].

Однако вернемся к процессуальной части извлечения компьютерной информации. Ранее мы определились с тем, что понятие «осмотр компьютерных устройств» в действительности не означает только их визуальное изучение и описание внешних характеристик. Однако в настоящее время извлечение такой информации происходит в процессе производства осмотра предметов, в связи с чем далее предлагаем перейти к рассмотрению самого процесса осмотра компьютерных устройств. Здесь же следует пояснить, что понятие «компьютерное устройство» в данном случае автором будет рассмотрено расширительно, поскольку в современном

[6] О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» : Федер. закон от 06 июля 2016 г. № 374-ФЗ // СПС «КонсультантПлюс».

мире к числу устройств, способных автоматически выполнять заданную последовательность операций относятся не только стационарные компьютеры или ноутбуки, но и мобильные телефоны, планшеты и многие другие гаджеты.

Стоит обратить внимание на результаты опроса, проведенного Н.А. Архиповой, согласно которому, 52 % следователей уделяют особое внимание средствам мобильной связи и принимают меры для получения информации именно с таких устройств [4, с. 16]. Таким образом, информация, содержащаяся во всех перечисленных устройствах, может обладать высокой значимостью и ценностью для раскрытия и расследования преступлений.

По этому поводу справедливо отмечает в своей работе С.Ю. Скобелин: «…с помощью данной информации следователь может получить криминалистически важную доказательственную или ориентирующую информацию: определить местонахождение субъекта преступления, его соучастников, свидетелей, потерпевших в определенное время, ознакомиться с журналом звонков, содержанием СМС-переписок, чатов, изучить журнал браузеров — страниц Интернета, на которые заходило лицо, и т.д.» [5, с. 26].

Однако самостоятельное обнаружение изъятие и фиксация информации, выраженной в электронной форме, зачастую вызывает сложности у следователей [6, с. 52]. Кроме того, для получения такой информации требуется осмотр устройств, на которых данная информация содержится, и уже на этом этапе должностные лица сталкиваются со сложностями, а допущенные ошибки могут повлечь частичную утрату или полное уничтожение данных.

Осмотр компьютерных устройств, а также содержащейся на них информации, обладает признаками не сколько следственного действия, столько технического исследования, для проведения которого необходимы специальные знания, методы и навыки.

Отдельные ученые, придерживаются мнения, согласно которого, любые компьютерные устройства должны направляться на судебную компьютерно-техническую экспертизу. Однако количество экспертов, обладающих допуском к проведению данных экспертиз, не позволяет их проводить по каждому компьютерному устройству. Более того, как отмечает О.С. Бутенко, в некоторых регионах для проведения экспертизы требуется от 4 до 6 месяцев [7, с. 60]. Поэтому именно осмотр позволяет выявить и зафиксировать криминалистическую значимую информацию, имеющую значение для расследования уголовного дела, в максимально короткие сроки.

В связи с этим для осмотра электронных устройств могут использоваться программно-аппаратные комплексы, которые призваны облегчить работу по получению компьютерной информации и сделать ее более надежной и качественной. С помощью таких комплексов как UFED, Мобильный криминалист, XRY, MOBILedit и т.д. информацию можно извлекать, декодировать, анализировать, автоматически создавая определенные отчеты.

Анализ спецификации данного оборудования позволяет утверждать, что подобные комплексы представляют собой портативные мобильные системы, позволяющие провести криминалистическое исследование по извлечению, декодированию и анализу данных, содержащихся в памяти мобильных устройств различных моделей.

В качестве объекта исследования комплексов могут выступать мобиль-

ные телефоны, смартфоны, планшеты, сим-карты и карты памяти, а также некоторые модели навигаторов.

Одним из наиболее успешно используемых в практике аппаратно-программных комплексов является отечественный комплекс — «Мобильный криминалист». Его использование возможно, как для проведения исследования мобильных устройств, так и облачных сервисов, дронов и персональных компьютеров. Программное обеспечение комплекса позволяет извлекать полную информацию об исследуемом мобильном устройстве, контактах пользователя, всех звонков, сообщениях, заметках, календарных событиях, учетных данных и паролях и т.д.

Мобильный криминалист имеет несколько версий, в зависимости от назначения применения и может представлять собой: специальное программное обеспечение в виде приложения (предоставляться USB-ключом, используемого для криминалистических исследований); переносной комплект — рабочее место; сетевая версия, предназначенная для одновременной работы большого числе пользователей; специальная сетевая версия для использования в учебных заведениях.

Использование указанного комплекса значительно повышает эффективность работы правоохранительных органов по получению и исследованию компьютерной информации. Однако интересным представляется вопрос, имеется ли необходимость привлечения специалиста к осмотру компьютерных устройств при применении подобных комплексов.

На сегодняшний день вопрос участия специалиста в ходе производства следственного действия регулируется положениями ст. 164 УПК РФ «Общие правила производства следственных действий» и ст. 168 УПК РФ «Участие специалиста». Из положений данных норм следует, что следователь вправе самостоятельно решать вопрос о привлечении специалиста. Однако в данном случае необходимо помнить, что специалистом является «лицо, обладающее специальными знаниями» и привлекаемым следователем к участию в следственном действии для содействия в применении технических средств и помощи в обнаружении и изъятии предметов и документов.

Представляется, что существующая формулировка ч. 1 ст. 58 УПК РФ нуждается в расширительной трактовке либо ее модификации, поскольку она не содержит положений об изъятии информации. Сложно отнести информацию к предметам или документам, о которых говорит законодатель. Кроме того, в литературе обращается внимание на то обстоятельство, что компьютерная информация может быть получена и в ходе ОРД, которая не является процессуальной [8, с. 85; 9, с. 118; 10, с. 62; 11].

При этом положения ст. 6 Федерального закона от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»[7] закрепляют возможность использования помощи специалистов при осуществлении ОРД. Поэтому представить положение ст. 58 УПК РФ следует в следующем виде: «Специалист — лицо, обладающее специальными знаниями, привлекаемое к участию в процессуальных и непроцессуальных действиях в порядке, установленном настоящим Кодексом, для содействия в обнаружении, закреплении и изъятии предметов, документов и информации, применении технических средств ...».

[7] Об оперативно-розыскной деятельности : Федер. закон от 12 авг. 1995 г. № 144-ФЗ : (ред. от 1 апр. 2022) // Российская газета. 1995. 18 авг. (№ 160).

Нами усматривается необходимость привлечения специалиста для осмотра компьютерных устройств ввиду сложности самого процесса и объекта осмотра. Нет сомнений, что в ходе производства такого следственного действия необходимы специальные знания.

Можно выделить некоторые характерные особенности деятельности специалиста при осмотре компьютерных устройств:

– обеспечение объективности отраженных в протоколе сведений (характеристики компьютерного устройства; его взаимосвязи с другими объектами и устройствами; принадлежности устройства к конкретной организации и (или) физическому лицу) [12, с. 17];

– обеспечение объективности оценки и анализа полученной информации (для формулирования (корректировки) следственных версий; возможного механизма совершения преступления).

Необходимость осмотра компьютерных устройств может возникать в ходе различных следственных и оперативно-розыскных ситуаций, которые могут отличаться как по времени (в ходе проверки сообщения о преступлении или после возбуждения уголовного дела, так и по месту извлечения информации (на месте преступления, в служебном кабинете).

Однако в любом случае правоприменитель должен фиксировать информацию в протоколе следственного действия или оперативно-розыскного мероприятия. Задача специалиста в данном случае заключается в правильном использовании АПК и разъяснения информации, содержащейся в устройстве. Протокол должен отражать всю последовательность действий следователя (оперативного сотрудника) и специалиста с подробным указанием обнаруженных сведений. Более того представляется целесообразным привлечение понятых или использования видеозаписи для обеспечения надежности фиксируемой информации. Поскольку из цифрового устройства невозможно извлечь информацию простым визуальным способом, в протоколе необходимо указывать наименование технического средства и все манипуляции, которые совершаются с целью извлечения и последующего детального осмотра информации.

Специалист, безусловно, является лицом, обладающим специальными знаниями, и содействующим следователю при осмотре электронных устройств. Он обладает знаниями и умениями пользования специальным аппаратным комплексом. Однако при производстве следственного действия следователь самостоятельно направляет ход производства следственного действия, именно он несет ответственность за результаты осмотра.

Следователь должен обладать определенным уровнем технических знаний, чтобы грамотно направлять ход осмотра и осуществлять правильный поиск доказательств. При отсутствии таких знаний специалист может неумышленно «затянуть» процесс осмотра, обратившись к тем системным элементам устройства, которые не имеют значения для расследования уголовного дела. Однако даже в таком случае на этапе подготовки к осмотру компьютерного устройства следователь может провести беседу со специалистом, чтобы объяснить, какие следы ему необходимо обнаружить в ходе осмотра. Тем самым следователь может выяснить у специалиста некоторые технические особенности изъятия компьютерной информации и осведомить его об объеме предстоящей работы. Указанные рекомендации применимы и к деятельно-

сти оперуполномоченных, проводящих оперативно-розыскные мероприятия, в ходе которых обнаруживается и исследуется компьютерная информация.

Следует констатировать, что в настоящее время использование программно-аппаратных комплексов не так широко распространено на районном уровне следственных подразделений, что негативно сказывается на общем показателе расследования преступлений. Представляется, что в условиях цифровизации и информатизации общества каждый территориальный орган должен обладать указанными программно-аппаратными комплексами. Вместе с тем стоит отметить, что Ведомственная программа цифровой трансформации МВД России на 2021–2023 гг. устанавливает задачу по переходу подразделениями МВД России на использование отечественного программного обеспечения и оборудования. Каким образом будет осуществляться данный переход и коснется ли он иных ведомственных подразделений — покажет время.

Резюмируя сказанное, следует отметить, что исследование компьютерной информации с использованием аппаратно-программных комплексов представляет собой сложное процессуальное или непроцессуальное действие с применением технических средств и привлечением специалиста, которое имеет следующие особенности:

– комплексность технического действия, которое подразумевает не только визуальное изучение устройства, но и исследование его «изнутри». Такая особенность обусловлена спецификой фиксации цифровой информации в виде электронных сигналов, которая не может быть выявлена без специального внешнего воздействия;

– осмотр технического устройства зачастую влечет за собой извлечение соответствующей информации из памяти компьютера и ее анализ;

– для его производства необходимо привлечение специалиста ввиду необходимости использования специальных знаний и навыков;

– использование аппаратно-программного комплекса повышает эффективность производства исследования.

Список источников

1. Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике : дис. … канд. юрид. наук : 12.00.09 / Л.Б. Краснова. — Воронеж, 2005. — 202 с. — EDN NNDXQV.

2. Багмет А.М. Получение информации, содержащейся в электронных мобильных устройствах, с применением универсального устройства извлечения судебной информации (UFED) : метод. указания / А.М. Багмет, С.Ю. Скобелин. — Москва : Московская акад. Следственного комитета Российской Федерации, 2013. — 52 с. — EDN YUOJNJ.

3. Серов А.В. Получение компьютерной информации как самостоятельное оперативно-розыскное мероприятие / А.В. Серов, А.С. Дубинин. — EDN XZHWEH // Вестник Воронежского института МВД России. — 2018. — № 3. — С. 170–176.

4. Архипова Н.А. К вопросу об использовании возможностей средств мобильной связи в раскрытии расследовании преступлений / Н.А. Архипова. — EDN SNKZSZ // Сборник материалов криминалистических чтений. — 2014. — № 10. — С. 16–21.

5. Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности / С.Ю. Скобелин. — EDN ZANFQT // Российский следователь. — 2019. — № 3. — С. 26–28.

6. Федоров Н.Н. Форензика — компьютерная криминалистика / Н.Н. Федоров. — Москва : Юрид. мир, 2007. — 359 с. — EDN OZENIX.

7. Бутенко О.С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия / О.С. Бутенко. — DOI 10.17803/1729-5920.2016.113.4.049-060. — EDN VXIZLV // Lex Russica. — 2016. — № 4 (113). — С. 49–60.

8. Ерахтина Е.А. Современные аппаратно-программные комплексы логического извлечения информации / Е.А. Ерахтина. — EDN TYOFIG // Высокотехнологичное право: генезис и перспективы : материалы III Междунар. межвуз. науч.-практ. конф., Красноярск, 24–25 февр. 2022 г. — Красноярск, 2022. — С. 84–88.

9. Семикаленкова А.И. Цифровые следы: назначение и производство экспертиз / А.И. Семикаленкова. — DOI 10.17803/2311-5998.2019.57.5.115-120. — EDN UIYDWP // Вестник Университета имени О.Е. Кутафина. — 2019. — № 5 (57). — С. 118–124.

10. Бахтеев Д.В. Криминалистические особенности производства процессуадьных действий с цифровыми следами / Д.В. Бахтеев, Е.В. Смахтин. — EDN TCQSFV // Российский юридический журнал. — 2019. — № 6 (129). — С. 61–68.

11. Давыдов В.О. Цифровые следы в расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий / В.О. Давыдов, И.В. Тишутина. — EDN AITQTT // Современное уголовно-процессуальное право — уроки истории и проблемы дальнейшего реформирования. — 2020. — Т. 1, № 1 (2). — С. 180–188.

12. Следственный осмотр. Понятие, виды и доказательственное значение : учеб.-практ. пособие / отв. ред. О.А. Луценко. — Элиста, 2007. — 121 с.

References

1. Krasnova L.B. *Computer Objects in Criminal Procedure and Forensics. Cand. Diss.* Voronezh, 2005. 202 p. EDN: NNDXQV.

2. Bagmet A.M., Skobelin S.Yu. *Obtaining information from mobile electronic devices using the universal forensic extraction device (UFED).* Moscow Academy of the Investigative Committee of the Russian Federation Publ., 2013. 52 p. EDN: YUOJNJ.

3. Serov A.V., Dubinin A.S. Obtaining of Computer-Based Data as an Particular OperationaL-Investigative Measure. *Vestnik Voronezhskogo instituta MVD Rossii = The Bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2018, no. 3, pp. 170–176. (In Russian). EDN: XZHWEH.

4. Arkhipova N.A. On the Issue of Using the Capabilities of Mobile Communications in Solving the Investigation of a Crime. *Sbornik materialov kriminalisticheskikh chteniĭ = Collection of Materials of Forensic Readings,* 2014, no. 10, pp. 16–21. (In Russian). EDN: SNKZSZ.

5. Skobelin S.Yu. Use of Digital Technologies in Proving of Criminal Activities. *Rossiiskii sledovatel' = Russian Investigator,* 2019, no. 3, pp. 26–28. (In Russian). EDN: ZANFQT.

6. Fedorov N.N. *Forensics — Computer Forensics.* Moscow, Yuridicheskii Mir Publ., 2007. 359 p. EDN: OZENIX.

7. Butenko O.S. Forensic and Procedural Aspects of Examining Mobile Phones during Preliminary Investigation. *Lex Russica,* 2016, no. 4, pp. 50–60. (In Russian). EDN: VXIZLV. DOI: 10.17803/1729-5920.2016.113.4.049-060.

8. Erakhtina E.A. Modern Hardware and Software Complexes of Logical Information Extraction. *High-Tech Law: Genesis and Prospects*. *Materials of the 3rd Inter-University Research Conference, Krasnoyarsk, February 24–25, 2022.* Krasnoyarsk, 2022, pp. 84–88. (In Russian). EDN: TYOFIG.

9. Semikalenova A.I. Digital Footprints: Purpose and Production of Expertise. *Vestnik Universiteta imeni O.E. Kutafina = Courier of the Kutafin Moscow State Law University*, 2019, no. 5, pp. 118–124. (In Russian). EDN: UIYDWP. DOI: 10.17803/2311-5998.2019.57.5.115-120.

10. Bakhteev D.V., Smakhtin E.V. Forensic Features of Procedural Actions with Digital Traces. *Rossiiskii yuridicheskii zhurnal = Russian Law Journal*, 2019, no. 6, pp. 61–68. (In Russian). EDN: TCQSFV.

11. Davydov V.O., Tishutina I.V. Digital Tracks in the Investigation of Crimes Committed with the Use of Information and Telecommunication Technologies. *Sovremennoe ugolovno-protsessual'noe pravo — uroki istorii i problemy dal'neishego reformirovaniya = Modern Criminal Procedure Law — Lessons of History and Problems of Further Reform* 2020, vol. 1, no. 1, pp. 180–188. (In Russian). EDN: AITQTT.

12. Lutsenko O.A. (ed.). *Investigative Examination. The Concept, Types and Evidentiary Value.* Elista, 2007. 121 p.

Информация об авторе

Титов Андрей Александрович — заместитель начальника 3 отдела управления по расследованию организованной преступной деятельности, Следственный департамент МВД России, г. Москва, Российская Федерация, titov-aa@yandex.ru.

Information about the Author

Titov, Andrey A. — Deputy Head of the 3 Division, Directorate for the Investigation of Organized Crime, Investigations Department of the Ministry of Internal Affairs of Russia, Moscow, the Russian Federation, titov-aa@yandex.ru.

Поступила в редакцию / Received 25.07.2022
Одобрена после рецензирования / Approved after reviewing 10.08.2022
Принята к публикации / Accepted 30.08.2022
Дата онлайн-размещения / Available online 13.09.2022