УДК 343.98:004
DOI 10.34822/2312-3419-2021-81-87

КРИМИНАЛИСТИЧЕСКИЕ ТЕХНОЛОГИИ ОБНАРУЖЕНИЯ, ФИКСАЦИИ, ИЗЪЯТИЯ ЦИФРОВЫХ СЛЕДОВ ПРЕСТУПЛЕНИЯ И ИНОЙ ДОКАЗАТЕЛЬНОЙ ИНФОРМАЦИИ

Я. Г. Варакин [1, 2]
[1] *Санкт-Петербургская академия Следственного комитета Российской Федерации, Санкт-Петербург, Россия*
[2] *Следственное управление Следственного комитета Российской Федерации по Ханты-Мансийскому автономному округу – Югре, Ханты-Мансийск, Россия*
E-mail: Yarik711@mail.ru

В исследовании уделяется внимание современным технологиям изъятия цифровых следов на примере деятельности следователей-криминалистов Следственного комитета России, рассматриваются имеющиеся на вооружении аппаратно-программные комплексы, а также описывается методика обнаружения, фиксации и изъятия цифровых следов. В статье анализируется такой информационный сегмент, как Интернет, а также его скрытая часть (в непривычных нам доменах получения информации). Кроме того, обсуждается проблема оперативного получения цифровых следов с учетом современных средств коммуникации, таких как мессенджеры и системы видеосвязи. Автором предпринимается попытка обобщить и проанализировать понятие «цифровой след» в криминалистике, не умаляя важности классического понятия следообразования.

В заключение автор присоединяется к идее создания специальных подразделений по расследованию киберпреступлений в силовых структурах страны, приходит к выводу о необходимости постоянного межведомственного взаимодействия и обмена опытом между специалистами в различных областях, часто на стыке юридических и технических дисциплин, а также наук информационного цикла.

Ключевые слова: криминалистика, способы обнаружения, Интернет, криптовалюта, киберпреступления, технические средства изъятия, домен, мессенджер, аппаратно-программный комплекс, дистанционное зондирование земли, снятие радиоэлектронной обстановки.

Для цитирования: Варакин Я. Г. Криминалистические технологии обнаружения, фиксации, изъятия цифровых следов преступления и иной доказательной информации // Вестник Сургутского государственного университета. 2021. № 4. С. 81–87. DOI 10.34822/2312-3419-2021-81-87.

FORENSIC TECHNOLOGIES FOR DETECTING, FIXING, AND SEIZING DIGITAL TRACES OF CRIME AND OTHER EVIDENCES

Ya. G. Varakin [1, 2]
[1] *Saint Petersburg Academy of the Investigative Committee of Russia*
[2] *Criminal Investigation Division, Investigative Committee of the Khanty-Mansi Autonomous Okrug – Ugra, Khanty-Mansiysk, Russia*
E-mail: Yarik711@mail.ru

The article emphasizes modern technologies for seizing digital traces on the example of the activity of forensic investigators of the Investigative Committee of Russia, considers hardware and software complexes available in service, and describes the methodology of detecting, fixing and seizing of digital traces. The article analyzes such informational segment as the Internet, as well as its hidden part (in the unknown domains of receiving information). Moreover, the problem of obtaining digital traces in a fast way, considering modern means of communication, such as messengers and video communication systems, is discussed. The author attempts to generalize and analyze the concept “digital trace” in forensics, taking into account the importance of classical concept of trace formation.

In conclusion, the author supports the idea of creating special divisions for investigation of cybercrimes in the country’s law enforcement agencies, makes a conclusion about constant interdivisional interac-

tion and experience exchange among experts from various fields, which are often at the intersection of legal and technical disciplines, and sciences of the informational cycle.

Keywords: forensics, methods for detecting, Internet, cryptocurrency, cybercrimes, technical means of seizing, domain, messenger, hardware and software complex, Earth remote probing, electronic environment imaging.

For citation: Varakin Ya. G. Forensic Technologies for Detecting, Fixing, and Seizing Digital Traces of Crime and Other Evidences // Surgut State University Journal. 2021. No. 4. P. 81–87. DOI 10.34822/2312-3419-2021-81-87.

ВВЕДЕНИЕ

В XXI в. основную ценность представляет информация, а ее главным способом передачи, обмена и хранения стала «цифра» с практически повсеместным применением систем беспроводной передачи данных Wi-Fi и Bluetooth, а также собственных систем отдельных компаний IT-сектора. Данный факт отразился на всех сферах жизнедеятельности человека: от бытовых (телевидение, Интернет, мобильная связь с ее множеством дополнительных функций) и профессиональных (электронный документооборот, цифровые подписи, дистанционное образование) до финансово-экономических (бесконтактные способы оплаты на основе биометрических данных, появление новых средств расчетов (криптовалюты) и т. д.). Кроме того, с развитием цифровых технологий появились нестандартные способы получения орудий преступления, например печать оружия на 3D-принтере. Пистолет, изготовленный таким способом, вполне способен произвести 1–3 выстрела боевыми патронами до того, как придет в неисправное состояние. Наряду с этим преступные сообщества и криминальные субъекты, осуществляющие противозаконную деятельность в одиночку, стали более профессиональными, изменили свой привычный облик и перенесли свою деятельность в виртуальное пространство, что ставит перед криминалистами концептуально новые задачи и требует поиска новых путей их решения [1].

Так, классический взгляд на образование следов преступления в криминалистике в виде взаимодействия двух материальных объектов с последующим наложением следа от одного объекта на другой, с учетом современных (цифровых) средств коммуникации, претерпел вынужденную трансформацию. В виртуальном пространстве след не выглядит как материальный объект и более не представляет собой материальный объект, а методика его обнаружения и изъятия является рядом действий с использованием технических средств, к которым часто относится применение компьютерных систем. На вооружении Следственного комитета России имеется несколько таких программ и программно-аналитических комплексов: «Мобильный криминалист» (программа российского производства), UFED Touch (израильского производства), система считывания и анализа информации с мобильных телефонов и сим-карт XRY (швейцарского производства).

Стоит отметить, что по-прежнему носителями «цифровых электронных» следов остаются материальные объекты: CD/DVD-диски, жесткие диски (HDD), flash-накопители, встроенная память персональных компьютеров (ноутбуков, планшетов), всевозможные пластиковые карты с микрочипами и магнитными лентами по типу банковских, скидочных, профсоюзных и проч., но уже не в императивной форме, как это было 10-15 лет назад [2]. Сегодня, в 20-е годы XXI в., появились облачные сервисы, которые позволяют хранить информацию без физических средств на руках; широко представлены средства обмена информацией через видеосвязь, различного рода онлайн- и офлайн-мессенджеры, базы данных (серверы) которых хранятся за пределами Российской Федерации, что существенно осложняет получение доказательной информации по уголовному делу. Социальные сети стали инструментом массовой манипуляции в плане создания положительного восприятия отрицательных мотивов (всем известные группы смерти «Синий Кит» и им подобные). Также в виртуальном (цифровом) пространстве получили широкое распространение акты пропаганды и непосредственно совершения преступлений, касающихся поло-

вой неприкосновенности несовершеннолетних, путем демонстрации видео- и фотоматериалов порнографического содержания либо путем принуждения к демонстрации собственных интимных частей тела как самих несовершеннолетних, так и лиц, склоняющих их к этому через сеть Интернет и мобильные приложения (мессенджеры). Массовой и бесконтрольной рекламной атаке в виде пропаганды наркотиков подверглись многие абоненты сотовых операторов [3].

МАТЕРИАЛ И МЕТОДЫ

В качестве предмета исследования выступает скрытый сегмент интернет-пространства в непривычных для обычных пользователей доменах. Изучается техническая возможность следователей-криминалистов противостоять современным вызовам в сфере киберпреступлений. Рамки исследования ограничиваются периодом с 2015 по 2020 г., что дает возможность понять потенциал современной криминалистики, ее технические возможности, а также проследить динамику развития.

В работе использованы теоретические методы научного познания, такие как анализ, синтез и дедукция. Анализ показателей отчетности Следственного комитета дает возможность отметить явный рост количества преступлений в цифровой сфере; анализ технического оснащения криминалистической базы позволяет изучить возможности правоохранительной системы и выяснить, какие пробелы в данной области требуют восполнения; анализ процессуальных документов и научной литературы позволяет сформировать социальный и психологический портрет киберпреступника для внесения дополнений в теорию личности преступника и криминальную психологию.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Для борьбы с описанными выше криминальными проявлениями специалистами выработаны методики обнаружения, фиксации и изъятия следов и сведений, представляющих интерес для следствия, которые в дальнейшем, путем проведения осмотра предметов и документов, признаются вещественными доказательствами по уголовному делу и представляются в суде стороной обвинения в виде доказательств вины подсудимого.

С этими задачами хорошо справляются программные комплексы «Мобильный криминалист», UFED Touch, XRY. Их применение на практике не требует от специалиста глубоких познаний в программировании, что, несомненно, является плюсом. После проведения исследования информация предоставляется на бумажных и электронных носителях в качестве отчетов, которые не требуют расшифровки и доступны для понимания и изучения всем участникам предварительного следствия при ознакомлении с материалами уголовного дела. Стоит отметить что эффективное использование данных систем обнаружения, фиксации и извлечения цифровых следов требует соблюдения определенных условий, например наличия пароля пользователя для разблокировки исследуемого объекта или полного заряда батареи. Также для извлечения информации из новейших моделей телефонов, операционные системы которых были обновлены до последних версий, необходим постоянный апгрейд систем самих программных комплексов [4].

Останавливаясь более подробно на функционале описанных программных комплексов, необходимо подчеркнуть, что каждый из них направлен в первую очередь на поиск явных и обнаружение скрытых, ранее удаленных данных на электронных носителях, но при этом каждая из систем обладает индивидуальными особенностями. Например, «Мобильный криминалист», помимо извлечения данных, предлагает их анализ, в том числе в хронологическом порядке, с составлением визуализированной схемы. Кроме того, программа позволяет проводить исследования в облачных сервисах. UFED Touch в некоторых случаях предлагает обход блокировок исследуемого объекта, то есть декодирование, а система XRY предполагает более глубокий анализ данных на сим-картах мобильных телефонов и в их встроенной памяти, вплоть до восстановления ранее удаленных данных.

Но к цифровым следам преступления, на наш взгляд, относится не только явная или неявная информация в виде платежных операций, передачи запрещенной информации

(экстремизм, терроризм и т. д.) посредством мессенджеров или социальных сетей, которые, как правило, обнаруживаются на цифровых носителях информации, таких как мобильные телефоны и планшеты, но и более классические примеры в формате видеоизображений, так как в результате видеофайл в конечном месте его хранения – на сервере – находится в цифровом виде и подлежит изъятию на электронный носитель. То же стоит сказать и о цифровой фотографии. Так, к криминалистической технологии обнаружения стоит отнести стоящий на вооружении следователей-криминалистов Следственного комитета России профессиональный обнаружитель скрытых видеокамер «ОПТИК-2». Данный инструмент позволяет обнаружить работающие явные, а главное – скрытые системы видеонаблюдения путем отражения луча от линзы объектива системы видеонаблюдения. Данная разработка не является прибором, предназначенным для непосредственного обнаружения цифрового следа, но позволяет обнаружить систему, которая этот цифровой след создает путем записи на сервере видеофайла, который сам по себе является цифровым следом и подлежит изъятию. К тому же привычное нам определение геопозиции сегодня приобрело принципиально новое значение, в связи с тем что в настоящее время появилась возможность получать снимки точностью от 1 до 400 м относительно размера поверхности Земли. При этом все данные хранятся и передаются в цифровом формате. Сотрудниками Роскосмоса предоставляются снимки интересующих следствие участков Земли, при этом есть возможность запросить архивные снимки. Также на сегодняшний день следователями-криминалистами Следственного комитета России при взаимодействии со специалистами радиочастотных центров городов часто используется такой метод, как снятие радиоэлектронной обстановки определенного участка местности при помощи аппаратно-программных комплексов «Сигмент-С» и «Следопыт-М» (как в городах, так и на открытых протяженных участках местности), что в комплексе с анализом данных, полученных от сотовых операторов, вносит ощутимый вклад в доказывание вины не только по преступлениям экологической направленности, но и по экономическим составам. В системе Следственного комитета России в 2020 г. рост показателей применения специальных технических средств, по сравнению с аналогичным периодом 2019 г., составил 83 % по дистанционному зондированию Земли (ДДЗ) и 13 % по снятию радиоэлектронной обстановки (РЭО) в местах, интересующих следствие в комплексе с анализом данных, полученных от сотовых операторов. Кроме того, широко используются экспертные возможности, применяются сложные компьютерные модели, позволяющие улучшать изображение и тем самым выявлять лица и предметы, менять угол исследуемого изображения так, чтобы надписи становились читаемыми. Эти примеры отражают положительный опыт межведомственного взаимодействия, которое, на наш взгляд, необходимо поддерживать и развивать. В частности, в обозримом будущем возможно расширение перечня ведомств, с которыми будут осуществляться совместные мероприятия по проведению следственных действий. Междисциплинарное взаимодействие специалистов на местах позволяет получить данные, которые впоследствии лягут в основу обвинительных заключений. Примером может служить дистанционное зондирование Земли, ведь изначально эта технология применялась в сельском хозяйстве и геодезии.

Методики обнаружения подразумевают под собой применение различных криминалистических технологий к одному объекту исследования, т. е. при проведении исследования, например, одного мобильного телефона следователь применяет не один программный комплекс, а все имеющиеся по очереди. Практика показывает, что данный метод является эффективным, так как программное обеспечение написано разными разработчиками, а следовательно, методы извлечения данных отличаются. Информация, которую не может извлечь UFED Touch, становится доступной для следствия после применения «Мобильного криминалиста» и наоборот. При синтезе извлеченной информации следствие имеет более полную картину произошедшего и в результате получает больше доказательств.

Однако в настоящее время у российских следователей-криминалистов появились сложности, которые не находятся в правовой плоскости или плоскости личных взаимоотношений сторон. Так, санкционная политика коллективного Запада привела к тому, что компания Cellebrite (производитель системы UFED Touch) отказалась предоставлять обновление программного комплекса российской стороне. Более того, правозащитники обнаружили уязвимость в программном обеспечении UFED Touch. Выявлена возможность внесения изменений не только в интересующий (проводимый) в настоящее время отчет, но и во все последующие (без оставления каких-либо электронных меток о данном противоправном действии) [5].

Вместе с тем сегодня не существует универсального способа извлечения информации и ее анализа, каждый разработчик представляет свой продукт и заявляет о его плюсах в сравнении с другими. Но если говорить о такой части информационного сегмента как Интернет, все описанные информационно-программные комплексы являются эффективными только при физическом изъятии носителя информации, только при обнаружении цифровых следов которые были сформированы в так называемом «видимом» Интернете (в доменах типа .ru, .com, .рф и т. д.), то есть там, где мы привыкли к «серфингу» знакомых нам страниц сайтов, поисковых систем, социальных сетей, аудио- и видеохостингов и т. п., что составляет всего 5–6 % от общего объема информации в сети Интернет [6]. Что же можно противопоставить сегменту DarkNet, работа с которым требует специальных программ, например браузера Tor, позволяющего работать с доменами .union, которые, в свою очередь, являются полем действия криминальных структур, занимающихся торговлей людьми и их органами, распространением наркотиков, оружия, предоставлением услуг физической расправы, вплоть до физического устранения (убийства за вознаграждение), а также всевозможным «мессенджерам», посредством которых в борьбе за так называемую свободу слова в отдельно взятых государствах утраиваются несанкционированные акции протеста, попытки «цветных» революций и которые не предоставляют государственным органам безопасности исходный код, что не позволяет декодировать трафик, а также не отвечают на официальные запросы, даже при наличии судебных решений о предоставлении информации, в связи с тем, что создатели этих мессенджеров и их серверы находятся на территории иностранных государств [7]?

В настоящее время в контексте именно криминалистической техники имеется очень малый спектр возможностей, не существует никаких эффективных способов противодействия, кроме ограничения трафика (работы) на территории страны путем блокировки сервиса или замедления его работы, но и здесь используются специальные VPN-сервисы, которые позволяют обходить блокировки Роскомнадзора. Также спецслужбами может контролироваться исходящий трафик, но трафик из-за рубежа не контролируется. То есть оперативно получить цифровые следы невозможно. Сделать какие-либо выводы можно будет только после проведения судебной экспертизы, при наличии изъятых объектов. Дополнительную сложность формируют повсеместно используемые злоумышленниками средства расчетов в виде не так давно появившихся криптовалют, уже достигнувших объемов капитализации в размере 2,1 трлн долларов по состоянию на апрель 2021 г. Более половины этого объема составляет биткоин – основное средство расчета в киберсреде. В данный момент нет каких-либо действенных механизмов выявления расчетов в криптовалюте, как и нет эффективных способов выявления происхождения данных капиталов, места их хранения. Эти факторы создают пространство для принципиально новой деятельности следователей, для появления новых частных теорий в криминалистике и дальнейшего их развития.

Одним из способов уравновесить силы, нивелировать данную проблему (отсутствие выработанных методик, механизмов и наличие квалифицированных кадров) является недавно принятое решение о создании в системе следственного комитета России специализированного подразделения – отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий. Данное решение при наполнении штата следователей и специалистов квалифицированными кадрами поз-

волит существенно расширить видимую часть совершаемых преступлений, так как следователь, обладающий специальными познаниями в области цифровых технологий, будет видеть более полную картину криминального события, а значит, сможет представить более структурный анализ, сумеет эффективнее спланировать следствие, что позволит избежать проведения ненужных следственных действий, выдвижения нерабочих версий, бессмысленных изъятий предметов и документов, назначения непрофильных экспертиз [8]. Представляется, что в каждом ведомстве (будь то СК, МВД или ФСБ) необходимо создать такое подразделение в соответствии со статьями подследственности. Кроме того, в данной области требуется постоянное проведение комплекса междисциплинарных исследований для решения криминалистических задач. Следует уделять внимание межведомственному взаимодействию, в частности проведению учебных семинаров, направленных на обмен опытом и установление связей между специалистами разных ведомств. Важность данных мероприятий обусловлена разницей в опыте при производстве предварительного следствия по различным категориям преступлений, а также индивидуальными особенностями мышления каждого специалиста. В ходе проведения подобных семинаров необходимо привлекать специалистов из городских служб и экспертных подразделений, чтобы инспектировать актуальность применяемых средств и методик.

ЗАКЛЮЧЕНИЕ

В настоящее время правоохранительными органами предпринимаются попытки активного противодействия киберпреступлениям. Кроме того, развивается частная теория цифровой криминалистики. Вместе с тем имеются отдельные информационные сегменты, где образ злоумышленника представляет собой высокоинтеллектуальный, идущий в ногу со временем криминальный субъект, обладающий специальными познаниями в области цифровых технологий, глобальных экономических процессов и т. д. По итогам исследования криминологической характеристики личности, основанного на изучении текстов более 200 судебных решений за 2015–2020 гг., можно составить усредненный портрет киберпреступника: в большинстве своем это мужчина, житель районного центра или мегаполиса в возрасте от 22 до 35 лет, не состоящий в брачных отношениях, не имеющий на иждивении несовершеннолетних детей, без проблем со здоровьем, ранее не судимый [9].

Сегодня задача правоохранительного блока – сформировать в своих рядах кадровый резерв, способный противостоять современным вызовам в области киберпреступлений, а впоследствии разработать методики эффективных способов борьбы с такими преступлениями. Для решения данной задачи необходимо наполнить кадровый резерв специалистами не только в области права, но и в области программирования и кибербезопасности.

ЛИТЕРАТУРА

1. Оконенко Р. И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права // Актуальные проблемы российского права. 2015. № 3. С. 120–124.
2. Дубоносов Е. С. Оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и проблемы проведения // Известия Тул. гос. ун-та. Экономические и юридические науки. 2017. С. 24–30.
3. Батоев В. Б. Использование мессенджеров в преступной деятельности: проблемы деанонимизации пользователей и дешифрования информации // Оперативник (сыщик). 2017. № 2. С. 15–20.
4. Зуев С. В., Никитин Е. В. Информационные технологии в решении уголовно-процессуальных проблем // Всерос. криминолог. журнал. 2017. № 3. С. 587–595.

REFERENCES

1. Okonenko R. I. Digital Evidence as a New Direction for the Improvement of the Russian Criminal Procedural Law // Actual Problems of Russian Law. 2015. No. 3. P. 120–124. (In Russian).
2. Dubonosov E. S. Operational-Pink Activity “Obtaining Computer Information”: Content and Problems of Carrying Out // Izvestiya Tula State University. Economic and Legal Sciences. 2017. P. 24–30. (In Russia).
3. Batoev V. B. Using “Messengers” in Criminal Activity: Problems of Disclosing Anonymous Users and Information Decyphing // The Field Investigator (Sleuth) Journal. 2017. No. 2. P. 15–20. (In Russian).
4. Zuev S. V., Nikitin E. V. Information Technologies in Solving Criminal Procedure Problems // Russian Journal of Criminology. 2017. No. 3. P. 587–595. (In Russian).

5. Васюков В. Ф. Некоторые вопросы проведения следственных действий, направленных на обнаружение, фиксацию и изъятие электронных сообщений, переданных посредством мобильных абонентских устройств сотовой связи // Российский следователь. 2016. № 23. С. 15–18.
6. Павлов В. В., Золотов М. А., Калентьева Т. А. Проблема получения и фиксации информации, содержащейся на электронных устройствах лиц, задержанных по делам о незаконном обороте наркотических средств с использованием ресурсов сети Интернет // Вестн. Волж. ун-та им. В. Н. Татищева. 2019. № 2. С. 216–225.
7. Карпов А. Л., Пахорукова Ю. Е. Процессуальная фиксация интернет-переписки в качестве доказательств по уголовным делам о преступлениях в сфере незаконного оборота наркотиков // Вестн. Сибир. юрид. ин-та МВД России. 2016. № 4. С. 111–117.
8. Осипенко А. Л. Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления // Вестн. Воронеж. ин-та МВД России. 2016. № 3. С. 86–87.
9. Абдулвалиев А. Ф., Белоусов А. В., Вассалатий Ж. В. и др. Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования : монография. Тюмень : Изд-во ТюмГУ, 2021 С. 230–231.

5. Vasyukov V. F. Several Aspects of Investigative Actions Aimed at Detection, Fixation and Caption of Electronic Messages Transmitted via User Mobile Devices // Russian Investigator. 2016. No. 23. P. 15–18. (In Russian).
6. Pavlov V. V., Zolotov M. A., Kalentyeva T. A. The Problem of Obtaining and Fixation of Information Contained on the Electronic Devices of Persons Detained in Cases of Illegal Turnover of Narcotic Drugs with the Use of the Resources of the Internet // Vestnik of Volzhsky University after V. N. Tatischev. 2019. No. 2. P. 216–225. (In Russian).
7. Karpov A. L., Pakhorukova Yu. E. Procedural Fixation of Internet Correspondence as Evidence in Criminal Cases Involving Crimes in the Sphere of Illicit Drugs Trafficking // Vestnik of Siberian Law Institute of the MIA of Russia. 2016. No. 4. P. 111–117. (In Russian).
8. Osipenko A. L. New Operational-Investigative Action “Getting Computer-Baseddata”: Content and the Basics of Implementation // Vestnik of Voronezh Institute of the Ministry of Interior of Russia. 2016. No. 3. P. 86–87. (In Russian).
9. Abdulvaliev A. F., Belousov A. V., Vassalaty Zh. V. et al. Prestupleniia, sovershaemye s ispolzovaniem informatsionnykh tekhnologii: problemy kvalifikatsii i osobennosti rassledovaniia : Monograph. Tyumen : Izd-vo TyumGU, 2021. P. 230–231. (In Russian).

СВЕДЕНИЯ ОБ АВТОРЕ

Варакин Ярослав Геннадьевич – аспирант, Санкт-Петербургская академия Следственного комитета Российской Федерации, Санкт-Петербург, Россия; капитан юстиции, следователь-криминалист отдела криминалистики, Следственное управление Следственного комитета Российской Федерации по Ханты-Мансийскому автономному округу – Югре, Ханты-Мансийск, Россия.

E-mail: Yarik711@mail.ru

ABOUT THE AUTHOR

Yaroslav G. Varakin – Postgraduate, Saint Petersburg Academy of the Investigative Committee of Russia, Saint Petersburg, Russia; Capitan of Justice Department, Forensic Investigator, Forensic Division, Criminal Investigation Division, Investigative Committee of the Khanty-Mansi Autonomous Okrug – Ugra, Khanty-Mansiysk, Russia.

E-mail: Yarik711@mail.ru