УДК 34

Понятие технико-криминалистического обеспечения выявления и закрепления электронных доказательств

Пономарев Виталий Евгеньевич

Старший преподаватель,
кафедр криминалистики и правовой информатики,
Кубанский государственный университет,
350040, Российская Федерация, Краснодар, ул. Октябрьская, 25;
e-mail: 9529788272@mail.ru

Аннотация

Статья посвящена исследованию понятия и содержания технико-криминалистического обеспечения выявления и закрепления электронных доказательств в условиях цифровизации. Анализируются различные научные подходы к определению сущности данной категории, рассматривается соотношение технических средств, программного обеспечения и аппаратно-программных комплексов. Отдельное внимание уделено проблеме отнесения программных продуктов к числу криминалистических средств и роли методов их применения в доказательственной деятельности. Обосновывается необходимость комплексного подхода, а также разработка федерального стандарта, который закрепит перечень используемых средств и методов с указанием их возможностей и ограничений. Делается вывод о том, что технико-криминалистическое обеспечение электронных доказательств представляет собой целостную систему традиционных и современных средств, призванную повысить эффективность и надежность раскрытия и расследования преступлений.

Для цитирования в научных исследованиях

Пономарев В.Е. Понятие технико-криминалистического обеспечения выявления и закрепления электронных доказательств // Вопросы российского и международного права. 2025. Том 15. № 7А. С. 171-179.

Ключевые слова

Криминалистика; технико-криминалистическое обеспечение; электронные доказательства; технические средства; программное обеспечение; аппаратно-программные комплексы.

Введение

Поступательное развитие криминалистической техники и её применение в процессе раскрытия и расследования преступлений обусловлен с одной стороны потребностью практики в получении новых технических инструментов, а с другой стороны появления новых достижений науки и техники, которые могут найти свое место и применение в криминалистике. Свой отпечаток на этот процесс неизбежно накладывают процессы всеобщей цифровизации, повсеместного распространения технических устройств, распространение процессов обмена информацией.

Сложно говорить о выявлении и закреплении электронных доказательств без применения соответствующих технических средств, что в свою очередь требует также описания методики их применения для целей раскрытия и расследования преступлений, а также правовых и организационных основ применения таких средств. Без комплексного подхода к исследованию технико-криминалистического обеспечения невозможно определить рамки применения его в деятельности субъектов расследования. Это обусловлено характером науки криминалистики, все теоретические исследования так или иначе направлены на совершенствование практики раскрытия и расследования преступлений.

Основная часть

Исходя из определения, данного А.Ф. Волынским технико-криминалистическое обеспечение — это деятельность, направленная на совершенствование собственно криминалистических методов и средств (техники), организации и правового регулирования их применения в целях раскрытия, расследования и предупреждения преступлений [Волынский, 1999, с.14].

В свою очередь Р.С. Белкин под технико-криминалистическим обеспечением понимает систему криминалистических знаний и основанных на них навыков и умений сотрудников использовать научные криминалистические рекомендации, применять криминалистические средства, методы и технологии их использования в целях предотвращения, выявления и расследования преступлений [Аверьянова, Белкин, 1997, с.64].

С точки зрения А.С. Шаталова технико-криминалистическое обеспечение представляет собой деятельность, направленную на создание и практическую реализацию условий постоянной готовности органов внутренних дел к решению технико-криминалистических задач в процессе раскрытия и расследования преступлений [Шаталов, 1993, с.12].

И.Л. Ландау формулирует определение технико-криминалистического обеспечения в широком смысле как систему правовых, научных, организационных и дидактических мер по разработке, внедрению и практическому использованию технико-криминалистических средств и научных методов, применяемых органами предварительного расследования и суда для наиболее эффективного решения задач, стоящих перед ними [Ландау, 2003, с.12].

Необходимо отметить мнение В.И. Шелудченко, рассматривающего технико-криминалистическое обеспечение расследования преступлений в качестве одной из частных криминалистических теорий, важной функцией которой является исследование закономерностей в вопросах использования криминалистических средств и методов в раскрытии преступлений [Шелудченко, 2002, с.32].

На наш взгляд технико-криминалистическое обеспечения деятельности оп выявлению и

закреплению электронных доказательств является соотносится с информационно-компьютерным обеспечением, как целое и часть, поскольку технико-криминалистическое обеспечение рассматриваемого вида деятельности гораздо шире и включает в себя не только информацию и компьютерные продукты, а также и традиционные методы криминалистики.

Определение технико-криминалистического обеспечения строится вокруг понятия технико-криминалистического средства или средства криминалистической техники.

Так, П.Т. Скорченко предлагает отличать технико-криминалистические средства от просто технических средств опираясь на два критерия: цели применения таких средств и субъекта их применения [Скорченко, 1999].

Если исходить из целей применения технико-криминалистических средств, то они всегда служат задачам раскрытия и расследования преступлений. При этом с точки зрения субъектного состава их использование может осуществляться как следователем или дознавателем, так и экспертом, что представляется вполне логичным и не содержит противоречий.

Безусловно, встает и вопрос о целесообразности отнесения к данному кругу субъектов оперативных сотрудников, как лиц, уполномоченных на проведение оперативно-розыскных мероприятий. Нам представляется, что их надо рассматривать вместе с другими субъектами при условии учёта специфики оперативно-розыскной деятельности, отталкиваясь от её задач. Ввиду того, что одной из важных задач ОРД является выявления источников информации, значит и используются технико-криминалистические средства, нацеленные на решение данной задачи. При этом необходимо иметь ввиду, что для целей ОРД могут применяться оперативно-розыскные технические средства, не пригодные для использования иными субъектами расследования, ввиду, например, нацеленности средства на негласное получение информации. Но это не означает принципиальную невозможность использования таких средств иными субъектами, в том случае, если такое применение не запрещено законом.

В этой связи мы опираемся на мнение Р.С. Белкина: «выделение и развитие в составе криминалистической техники, единой по своей принадлежности к криминалистике, средств и приемов для следователей, для экспертов и т. п. вовсе не означает двух (или более) техник. Группы этих средств и приемов не отделены друг от друга барьером принципиальной невозможности их использования лицами с различными процессуальными функциями. Следователь, оперативный работник, эксперт, судья в пределах своих возможностей и полномочий могут применять любое технико-криминалистическое средство или прием. С этой точки зрения, деление средств и приемов на группы не имеет значения, и в этом аспекте криминалистическая техника так же едина, как и в смысле ее научной принадлежности (несмотря на источник возникновения)» [Аверьянова и др., 2001, с.150-151]. Аналогичный подход отмечен ученым применительно к «полевой криминалистике», рассматривая возможности использования оборудования Р.С. Белкин указывал, что технику на месте происшествия с равным успехом может применять, как следователь, так и эксперт [Белкин, 1997, с.8].

При этом следует согласиться с мнение Р.С. Белкина о том, что пределы использования технико-криминалистических средств определяются процессуальными функциями субъектов расследования, объемом их профессиональных познаний в области применения технико-криминалистических средств и реальными возможностями доставки и развертывания необходимого оборудования по месту его использования [Белкин, 1997, с.10]. Так, следователь, не обладая специальными техническим познаниями в области компьютерной техники не может в полной мере воспользоваться тем программным и аппаратным обеспечением, насколько это

доступно эксперту, обладающему специальными познаниями в соответствующей области.

На наш взгляд требуется дополнить перечень критериев еще одним. Необходимо определить, что относится к техническим средствам. Существует тенденция трактовать понятие технического средства максимально широко, включая, в число технических средств осветительные приборы, оптические приборы и даже химические вещества-реагенты [Дёмин, 2017, с.16-20]. Л.Я. Драпкин определял технические средства, как приборы, устройства, инструменты и вещества, специально разработанные, приспособленные или позаимствованные криминалистикой [Драпкин, Карагодин, 2012, с.87]. Р.С. Белкин рассматривал технические средства, как устройство, приспособление или материал, используемые для собирания и исследования доказательств [Белкин, 1997].

При выявлении и закреплении электронных доказательств используются не только устройства, приспособления или материалы. Также могут применятся и компьютерные программы. Под компьютерной программой принято понимать упорядоченные последовательности команд, при этом конечная цель любой программы – управление аппаратными средствами [Щапова, 2008, с.12-14]. В законодательстве программа для ЭВМ определена в ст.1261 Гражданского кодекса РФ, как: «представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения» [Волеводз, 2008].

Выделение в среде аппаратных средств (Hard Ware) и программных средств (Soft Ware), разделяя их на этом основании далеко не нова в криминалистике и возникла достаточно давно [ГОСТ Р 52980-2008, www]. Однако, мы считаем, что считать программу техническим средством, неправильно, ввиду того, что она выполняется на другом техническом средстве общего назначения – ЭВМ (имеющим различные форм-факторы: ноутбук, смартфон, персональный компьютер и тд.). То есть наряду с программными средствами существуют аппаратные.

Аппаратное средство применительно к сфере компьютерных средств это то устройство (персональный компьютер, смартфон, микроконтроллер или иное), которое осуществляет выполнение программы. Аппаратное средство требует установки программного обеспечения, поэтому часто говорят об аппаратно-программном комплексе (АПК) — это комплекс из аппаратного и программного обеспечений, который обеспечивает сбор, обработку, хранение и отображение информации. Формально такое определение закреплено в ГОСТ Р 52980-2008 [Глимейда, 2024]. Суть аппаратно-программного комплекса в том, что он состоит из программной и аппаратной части, которые настроены на совместную работу для достижения тех целей, для которых такой комплекс был создан.

Аппаратное обеспечение при этом бывает общего назначения – например персональный компьютер позволяет установить большой перечень различных программ и узкоспециализированное, где аппаратная часть заточена под установку конкретной программы, которая часто именуются прошивкой, именно такое оборудование часто и называют аппаратно-программными комплексами.

Заслуживает внимания позиция В.В. Галимейды, указывающего на то, что программа является лишь методом работы с информацией [Аверьянова и др., 2000, с.31]. На наш взгляд необходимо расширить эту позицию: существует две ситуации.

Программа может носить специализированный характер, то есть быть заточенной на

выполнение одной узкой задачи и пригодная только для этой цели, но также быть и универсальной, то есть позволять выполнять совершенно разнообразные задачи. Так, примером универсальной программы может служить операционная система.

В первом случае, мы говорим о применении субъектом расследования программного обеспечения специализированного назначения, которое используется им вместе с собственной ЭВМ (обычно такое использование принято называть Аппаратно-программным комплексом) либо загруженного на исследуемую ЭВМ. Такое программное обеспечение отвечает введенному нами критерию целей, то есть оно создано и/или используется для целей раскрытия и расследования преступлений.

Для выявления и закрепления электронных доказательств часто необходимо взаимодействовать с операционной системой, соответственно нужно говорить о методах взаимодействия с программой и в зависимости от выбранных методов можно получить различные информационные результаты. В этом случае мы не можем говорить, что программа операционной системы (или иная программа), установленная на компьютере подозреваемого, была создана с целью раскрытия и расследования преступлений, то есть такое программное обеспечение не может быть признано техническим средством.

Однако при использовании подобных программ задействуются определённые методы, разрабатываемые криминалистической наукой. Именно они направлены на обеспечение максимально эффективного получения электронных (цифровых) доказательств, а их конечной целью выступает раскрытие и расследование преступлений. Хотя сами методы не относятся к техническим средствам, они занимают равное с ними место в системе технико-криминалистического обеспечения.

Следовательно, представляется оправданным рассматривать в структуре технико-криминалистического обеспечения не только технические средства, но и технико-криминалистические методы (способы). Они ориентированы на достижение тех же целей — раскрытие и расследование преступлений, используются теми же субъектами, однако не связаны непосредственно с каким-либо материальным носителем, устройством или веществом. Также в систему технических средств подлежат включению программы и иное программное обеспечение, а также аппаратно-программные комплексы.

В практическом смысле удобно ввести следующий критерий: программа становится технико-криминалистическим средством, когда, во-первых, её функциональность направлена на решение криминалистических задач, а во-вторых, у неё есть апробированная процедура применения с известными пределами использования и известными погрешностями и ошибками. Универсальные программные продукты, такие как операционные системы или офисные пакеты программ сами по себе не становятся технико-криминалистическими средствами, средствами становятся методы их использования, описанные в определенных процедурах.

Технико-криминалистические средства принято классифицировать не только по субъектам применения, но и по другим основаниям, так в зависимости от источника происхождения выделяют:

– Технические средства, заимствованные криминалистикой без конструктивных изменений;
– Средства и методы, которые заимствованы криминалистикой из других отраслей науки и техники, но приспособленные для раскрытия и расследования преступлений;
– Собственные разработки криминалистической науки и ученых-криминалистов [Аверьянова и др., 2000].

Такое деление применимо на наш взгляд и к программному обеспечению:

– без изменений: стандартные системные утилиты, копирование средствами операционной системы, веб-браузеры для осмотра страниц, инструменты для записи экрана и др.
– заимствованные и адаптированные: сетевые анализаторы, средства резервного копирования и др.
– собственные разработки: специализированные пакеты мобильной, компьютерной, облачной криминалистики.

Мы солидарны с мнением авторов о том, что некоторые средства криминалистической техники могут носить универсальный характер, то есть применяться как для поисковых целей, так и для закрепления. В качестве примера приводится персональный компьютер [Бурцева и др., 2006, с.127], другой пример операционная система или любые программы общего, а не узкоспециального назначения.

В практических целях выявления и закрепления электронных доказательств можно дополнить классификации делением с точки зрения глубины вмешательства в исследуемый объект. Так, можно выделить средства исходя из трех режимов работы:

– Технико-криминалистические средства наблюдения. Обеспечивают выявление и закрепление электронных доказательств пассивно – без вмешательства в содержимое. Например, оборудование для фото или видеосъемки экрана.
– Технико-криминалистические средства минимального воздействия, обеспечивающие выявление и закрепление электронных доказательств при условии сохранения их содержания, без вмешательства во внутреннюю структуру. Сюда можно отнести средства, обеспечивающие изъятие носителей электронной информации, технические средства и оборудование для поиск электронных носителей информации и многие другие.
– Технико-криминалистические средства активного воздействия. В эту группу входят любые аппаратные, программные и аппаратно-программные продукты, обеспечивающие выявление и закрепление электронных доказательств, при условии их прямой работы с электронными носителями. К таковым относятся средства для вскрытия корпусов техники, извлечения носителей информации и другие.

Для целей выявления и закрепления электронных доказательств возможно использование как универсальных средств, приёмов и методов технико-криминалистического обеспечения, так и специализированных, применимых исключительно в электронной среде. В этой связи представляется обоснованным разграничение следующих категорий:

– Группу средств и методов технико-криминалистического обеспечения, которые используются, как для выявления и закрепления электронных доказательств, так и в других сферах криминалистической науки и практики. Например, оборудование и материалы, предназначенные для обнаружения и изъятия электронных носителей информации.
– Группа средств и методов, используемых только в целях выявления и закрепления электронных доказательств. Как пример можно назвать различное программное обеспечение.

Заключение

На сегодняшний день отсутствует единое понимание и оформленные требования к техническим средствам, программному обеспечению, аппаратно-программным комплексам, используемым как в криминалистике, так и в экспертной практике.

На современном этапе одной из ключевых задач технико-криминалистического обеспечения в цифровой сфере следует признать разработку и утверждение на уровне государственного федерального стандарта перечня технических средств и методов выявления, закрепления и исследования электронных доказательств. Такой стандарт позволил перечислить применяемые средства и методы, представить их в систематизированной форме с указанием преимуществ и ограничений каждого, возможных ошибок и рисков при использовании, а также регламентировать порядок их применения и определять цели, ради которых они создаются и используются.

В обобщённом виде технико-криминалистическое обеспечение выявления и закрепления электронных доказательств можно определить как целостную систему технических средств, программного обеспечения, методов и приёмов, направленных на поиск, фиксацию и исследование цифровой информации, обладающей доказательственным значением. Данная система должна включать как современные электронные, так и традиционные криминалистические средства, но быть унифицированной и закреплённой в государственном федеральном стандарте, что обеспечит единообразие практики и повысит надёжность результатов в процессе раскрытия и расследования преступлений.

Наряду с техническими средствами, под которыми понимаются любое оборудование или материалы в систему технико-криминалистического обеспечения выявления и закрепления электронных доказательств входят программные и аппаратно-программные комплексы. При этом если программное обеспечение или комплекс создан или приспособлен для целей выявление и закрепления электронных доказательств, то такой комплекс является самостоятельным средством в системе технико-криминалистического обеспечения.

В тех случаях, когда программное обеспечение имеет универсальный характер и не ориентировано специально на криминалистические задачи, в систему технико-криминалистических средств включается не сама программа, а разработанный комплекс приёмов и методика её применения для целей раскрытия и расследования преступлений.

Библиография

1. Волынский, А.Ф. Концептуальные основы технико-криминалистического обеспечения раскрытия и расследования преступлений: дис. … д-ра юрид. наук: 12.00.09. М., 1999.
2. Криминалистическое обеспечение деятельности криминальной милиции и органов предварительного расследования / под ред. проф. Т.В. Аверьяновой и проф. Р.С. Белкина. – М., 1997.
3. Шаталов А.С. Технико-криминалистическое обеспечение раскрытия и расследования преступлений, совершаемых в условиях массовых беспорядков: автореф. дис. … канд. юрид. наук: 12.00.09. Москва: ВЮЗШ МВД РФ, 1993.
4. Ландау И.Л. Ситуационный подход в технико-криминалистическом обеспечении предварительного расследования и судебного следствия: дис. … канд. юрид. наук: 12.00.09 / И.Л. Ландау. – М.: РГБ, 2003.
5. Шелудченко В. И. Проблемы технико-криминалистического обеспечения расследования убийств: автореф. дис. … канд. юридических наук : 12.00.09. 2002. Краснодар.
6. Скорченко, П.Т. Криминалистика. Технико-криминалистическое обеспечение расследования преступлений: учеб. пособие для вузов / П.Т. Скорченко. – М. : Былина, 1999. 272 с.
7. Криминалистика : учебник для вузов / Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р. и др. ; под ред. Р. С. Белкина. 3-е изд., доп. Москва : ЮНИТИ-ДАНА ; Закон и право, 2001.
8. Белкин Р. С. Курс советской криминалистики : в 3 т. Т. 3. Москва : Юристъ, 1997
9. Криминалистическая техника: учебник / под ред. К. Е. Дёмина. — М.: Юридический институт МИИТ, 2017.
10. Драпкин Л.Я., Карагодин В. Н. Криминалистика: учебник. М. : Проспект, 2012.
11. Белкин, Р. С. Курс криминалистики : в 3 т. Т. 3: Криминалистические средства, приёмы и рекомендации. — М. : Юристъ, 1997.
12. Щапова И. Н. Информатика: учебное пособие. Пермь, Изд-во Пермского государственного технического университета, 2008. 115 с.

13. Волеводз А.Г. Компьютерная информация как объект криминалистического следоведения / А.Г.Волеводз // Криминалистическая техника: Учебник / Отв. ред. И.М. Балашов, рук. колл. С.В. Маликов. - М.: Юрлитинформ, 2008.
14. ГОСТ Р 52980-2008 Системы промышленной автоматизации и их интеграция. Системы программируемые электронные железнодорожного применения. Требования к программному обеспечению. Москва Стандартинформ 2009 23 с. П. 3.2 «Аппаратно-программный комплекс». URL: meganorm.ru/Data/482/48291.pdf (дата обращения: 29.08.2025).
15. Глимейда В. В. Применение технических средств и цифровых технологий при производстве следственных действий : дис. … канд. юрид. наук : 5.1.4. Краснодар, 2024.
16. Аверьянова, Т. В., Белкин, Р. С., Корухов, Ю. Г., Россинская, Е. Р. Криминалистика: учебник для вузов / под ред. Р. С. Белкина. М.: Норма, 2000. С. 59–60., Криминалистическая техника: учебник / под ред. К. Е. Дёмина. М.: Юридический институт МИИТ, 2017.
17. Бурцева, Е.В., Рак, И.П., Селезнев, А. В., Сысоев, Э. В. Криминалистика. Часть I: Общая теория криминалистики и криминалистическая техника: учебное пособие. Тамбов: Изд-во ТГТУ, 2006.

The Concept of Forensic Technical Support for the Detection and Preservation of Digital Evidence

Vitalii E. Ponomarev

Senior Lecturer,
Department of Forensics and Legal Informatics,
Kuban State University,
350040, 25 Oktyabrskaya str., Krasnodar, Russian Federation;
e-mail: 9529788272@mail.ru

Abstract

The article investigates the concept and content of forensic technical support for the detection and preservation of digital evidence in the context of digitalization. Various scientific approaches to defining the essence of this category are analyzed, and the relationship between technical means, software, and hardware-software complexes is examined. Special attention is paid to the problem of classifying software products as forensic tools and the role of their application methods in evidence activities. The necessity of a comprehensive approach is substantiated, along with the development of a federal standard that would establish a list of used tools and methods, specifying their capabilities and limitations. It is concluded that forensic technical support for digital evidence represents an integrated system of traditional and modern means designed to enhance the efficiency and reliability of crime detection and investigation.

For citation

Ponomarev V.E. (2025) Ponyatiye tekhniko-kriminalisticheskogo obespecheniya vyyavleniya i zakrepleniya elektronnykh dokazatel'stv [The Concept of Forensic Technical Support for the Detection and Preservation of Digital Evidence]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (7A), pp. 171-179.

Keywords

Forensics; forensic technical support; digital evidence; technical means; software; hardware-software complexes.

References

1. Volynsky, A. F. Conceptual Foundations of Technical and Forensic Support for Crime Detection and Investigation: Doctor of Law Dissertation (12.00.09). Moscow, 1999.
2. Forensic Support of the Activities of the Criminal Police and Preliminary Investigation Bodies / ed. by Prof. T. V. Averyanova and Prof. R. S. Belkin. Moscow, 1997.
3. Shatalov, A. S. Technical and Forensic Support for the Detection and Investigation of Crimes Committed in Conditions of Mass Disorders: Abstract of PhD Dissertation (12.00.09). Moscow: VYUZSh MVD RF, 1993.
4. Landau, I. L. Situational Approach in Technical and Forensic Support of Preliminary and Judicial Investigation: PhD Dissertation (12.00.09). Moscow: Russian State Library, 2003.
5. Sheludchenko, V. I. Problems of Technical and Forensic Support in the Investigation of Murders: Abstract of PhD Dissertation (12.00.09). Krasnodar, 2002.
6. Skorchenko, P. T. Criminalistics. Technical and Forensic Support for Crime Investigation: Textbook for Universities. Moscow: Bylina, 1999. 272 p.
7. Criminalistics: Textbook for Universities / T. V. Averyanova, R. S. Belkin, Yu. G. Korukhov, E. R. Rossinskaya et al.; ed. by R. S. Belkin. 3rd ed., rev. Moscow: UNITY-DANA; Zakon i Pravo, 2001.
8. Belkin, R. S. Course of Soviet Criminalistics: In 3 vols. Vol. 3. Moscow: Yurist, 1997.
9. Forensic Technology: Textbook / ed. by K. E. Dyomin. Moscow: Law Institute of MIIT, 2017.
10. Drapkin, L. Ya., Karagodin, V. N. Criminalistics: Textbook. Moscow: Prospekt, 2012.
11. Belkin, R. S. Course of Criminalistics: In 3 vols. Vol. 3: Forensic Means, Techniques and Recommendations. Moscow: Yurist, 1997.
12. Shchapova, I. N. Informatics: Study Guide. Perm: Perm State Technical University Press, 2008. 115 p.
13. Volevodz, A. G. Computer Information as an Object of Forensic Research // In: Forensic Technology: Textbook / ed. by I. M. Balashov, research team led by S. V. Malikov. Moscow: Yurlitinform, 2008.
14. GOST R 52980-2008. Industrial Automation Systems and Their Integration. Programmable Electronic Systems for Railway Applications. Software Requirements. Moscow: Standartinform, 2009. 23 p. § 3.2 “Hardware-Software Complex.” Available at: meganorm.ru/Data/482/48291.pdf (accessed 29.08.2025).
15. Glimeyda, V. V. Application of Technical Means and Digital Technologies in the Conduct of Investigative Actions: PhD Dissertation (5.1.4). Krasnodar, 2024.
16. Averyanova, T. V., Belkin, R. S., Korukhov, Yu. G., Rossinskaya, E. R. Criminalistics: Textbook for Universities / ed. by R. S. Belkin. Moscow: Norma, 2000, pp. 59–60; Forensic Technology: Textbook / ed. by K. E. Dyomin. Moscow: Law Institute of MIIT, 2017.
17. Burtseva, E. V., Rak, I. P., Seleznev, A. V., Sysoev, E. V. Criminalistics. Part I: General Theory of Criminalistics and Forensic Technology: Study Guide. Tambov: Tambov State Technical University Press, 2006.