

МЕХАНИЗМ СЛЕДООБРАЗОВАНИЯ В КОМПЬЮТЕРНЫХ СИСТЕМАХ С ТОЧКИ ЗРЕНИЯ ТЕОРИИ ОТРАЖЕНИЯ

В статье поднимается проблема отсутствия единого понятийного аппарата в отношении следов, образующихся в информационно-телекоммуникационной среде. Предлагается рассмотрение механизма образования указанных следов с применением криминалистической теории отражения. В процессе анализа выявляются ошибки, связанные с отождествлением некоторых понятий и приводящие к терминологическим коллизиям. Результатом проведённого анализа является определение основных понятий теории отражения: отражение, отображение следа, отражаемый объект, отражающий объект, следообразующий объект следовоспринимающий объект, применительно к компьютерным системам. Также в статье рассматривается проблема наименования и определения следов, образующихся в компьютерных системах, предлагается классификация рассматриваемых следов по степени опосредованности воздействия пользователя на компьютерную систему.

Ключевые слова: теория отражения, следообразующий объект, следовоспринимающий объект, электронно-цифровой след, компьютерная система, механизм следообразования.

A.G. Sebyakin

THE MECHANISM OF TRACE FORMATION IN COMPUTER SYSTEMS FROM THE STANDPOINT OF THE REFLECTION THEORY

The author raises the problem of the absence of a common conceptual framework for traces in the information-telecommunications environment. It is suggested that the mechanism of their formation should be examined with the use of a criminalistic theory of reflection. The conducted analysis highlights mistakes connected with the equating of some concepts, which leads to terminological collisions. The analysis allowed the author to define key concepts of the theory of reflection as applied to computer systems: reflection, display of a trace, a reflected object, a trace-forming object, a trace-perceiving object. The author also discusses the problem of naming and defining traces formed in computer systems and presents a classification of the examined traces based on how indirect a user's impact on the computer system is.

Keywords: reflection theory, trace-forming object, trace-perceiving object, electronic-digital trace, computer system, mechanism of trace formation.

Цифровизация человеческой деятельности, экспоненциально растущая с начала 21 века, неизбежно повышает интерес учёных к различным аспектам исследования компьютерных систем с целью получения криминалистически значимой информации. В информационной среде, которая образуется в результате

работы компьютерных устройств и их взаимодействия посредством телекоммуникационных каналов связи, как пишет Е.П. Ищенко, «отражаются, фиксируются и сохраняются специфические следы самой различной человеческой деятельности» [1, с. 58], в том числе, преступной. Специфичность такого следа обуславливается его природой, поскольку соотнесение смысла криминалистической категории «след» с особенностями функционирования компьютерных систем является дискуссионной задачей, обсуждение которой до сих пор актуально.

За последние пятнадцать лет в научной литературе опубликовано множество научных работ, в которых авторы обсуждают значение криминалистически значимых следов, образующихся в компьютерных системах. Вопросы механизма возникновения, формирования, фиксации следов в компьютерных системах, их структуры, места в классификации следов подробно исследовались В.А. Мещеряковым [2], В.Б. Веховым [3]. Большой спектр вопросов, касающихся «электронных следов», рассмотрен в работе Ю.В. Гаврилина [4]. Тем не менее, понятийный аппарат следов, образующихся в информационно-коммуникационной среде, так и не был приведён к единообразию. Это наглядно продемонстрировано в анализе, проведённом А.Н. Колычевой [5, с. 41–42], и свидетельствует об отсутствии среди ученых единого мнения по поводу ключевых вопросов, связанных со следообразованием в компьютерных системах: определение следов, механизм возникновения следов, их природа, классификация и пр. Ниже указанные вопросы будут рассмотрены с точки зрения существующей нормативной базы в криминалистической теории отражения.

С целью дальнейшего анализа природы информационно-коммуникационной среды и следов, образующихся в ней, необходимо единообразно определить источник возникновения следа. Для этого обратимся к ГОСТ 15971-90, который определяет вычислительную машину (компьютер) как совокупность технических средств, создающую возможность проведения обработки информации и получение результата в необходимой форме¹. В статье 1 конвенции Совета Европы «О преступности в сфере компьютерной информации», указывается, что: «компьютерная система означает любое устройство или группу взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных»². Приведённые определения компьютера и компьютерной системы одновременно обширны и лаконичны, поскольку описывают всё многообразие устройств, функционирующих на основе процессора, а также вычислительных сетей, как локальных, так и глобальных. С указанным определением согласуется и точка зрения А.И. Семикаленовой, которая отмечает, что «информационно-компьютерная система является комплексным объектом, вклю-

¹ ГОСТ 15971-90 Системы обработки информации. Термины и определения : утв. и введен в действие Постановлением Госстандарта СССР от 26 окт. 1990 г. № 2698 // СПС «КонсультантПлюс».

² Конвенция Совета Европы о преступности в сфере компьютерной информации ETS № 185 : заключена в г. Будапеште 23 нояб. 2001 г. (в ред. от 28 янв. 2003)// СПС «КонсультантПлюс».

чающим аппаратные, программные, информационные... и сетевые компоненты» [6, с. 113]. Таким образом, любое локальное устройство, функционирующее на основе процессора, а также любые вычислительные сети предлагается именовать термином «компьютерная система». Соответственно, для обозначения криминалистически значимых следов, возникающих в процессе функционирования различных компьютерных систем, предлагается использовать термин «следы в компьютерных системах».

За основу рассмотрения механизма следообразования в компьютерных системах возьмём два постулата криминалистической теории отражения:

- отражение является результатом воздействия отражаемого объекта на отражающий;

- след является результатом взаимодействия объекта следообразующего и объекта следовоспринимающего.

В литературных источниках встречается, на наш взгляд, ошибочное смешение приведённых понятий: отражение отождествляется со следом, воздействие - с взаимодействием, отражаемый объект - со следообразующим объектом, отражающий объект - со следовоспринимающим объектом. Так, В.Б. Вехов пишет, что «Отражением преступных действий являются следы... Отражение присутствует всегда, когда происходит взаимодействие двух и более материальных объектов — объектов следообразования... Следообразующий (отражаемый) объект является носителем непосредственной, первичной информации...» [7, с. 12]. По нашему мнению, в процессе следообразования в компьютерных системах отражающим объектом является компьютерная система, на которую воздействует пользователь (отражаемый объект). При таком рассмотрении отражение, как результат воздействия, является процессом, приводящим к изменениям, а след – это изменения, зафиксированные в материальной или идеальной среде. Соответственно, след не может являться процессом, о чём писал Р.С. Белкин, подразумевая под механизмом следообразования «специфическую конкретную форму протекания процесса, конечная фаза которого представляет собой образование следа-отображения» [8, с. 61].

Ряд авторов, анализируя механизм образования следов в информационно-коммуникационной среде, определяют в качестве следовоспринимающего объекта различные разновидности памяти компьютерной системы. Например, Ж.Ю. Кабанова указывает, что следовоспринимающим объектом выступает цифровой носитель [9, с. 123]. С.Д. Долгинов пишет, что «любые действия с компьютерными или иными программными устройствами получают свое непосредственное отражение в их памяти» [10, с. 266]. Рассматривая данный вопрос с точки зрения современной логической архитектуры вычислительных машин, можно представить компьютерную систему как совокупность элементов памяти, каналов передачи информации, арифметико-логических устройств и устройств ввода/вывода информации. Так как под следом стоит понимать изменения, зафиксированные в материальной или идеальной среде, то применительно к компьютерным системам, устройство хранения цифровых данных и является той средой в которой фиксируются изменения. Мы разделяем точку зрения авторов, по мнению которых следовоспринимающим объектом при воз-

действии пользователя на компьютерную систему является массив памяти компьютерной системы. При этом тип, вид и локализация массива памяти не имеет принципиального значения с точки зрения механизма слеодообразования, поэтому массив памяти будем в дальнейшем обозначать термином «запоминающее устройство».

В процессе функционирования компьютерной системы изменения в массиве памяти происходят с помощью программного обеспечения, именно оно непосредственно взаимодействует с запоминающим устройством. Соответственно, в рассматриваемой модели слеодообразования программное обеспечение компьютерной системы является слеодообразующим объектом. Стоит согласиться с мнением Б.К. Давлетова, который в качестве слеодообразующего объекта указывает «программное обеспечение компьютерной системы, которое и находит свое отображение в системе файлов» [11, с. 44]. Однако, для наиболее чёткого представления механизма слеодообразования в компьютерных системах необходимо условно дифференцировать программное обеспечение на системное и прикладное, поскольку функциональное предназначение у них разное. К системному программному обеспечению мы будем относить совокупность программ, предназначенных для обеспечения функционирования компьютерной системы: программы, осуществляющие взаимодействие с аппаратными компонентами компьютерной системы, операционная система, программы, обеспечивающие ввод/вывод и передачу данных. Под прикладным программным обеспечением будут подразумеваться программные средства, обеспечивающие возможность выполнения пользователем практических задач. Поскольку именно системное программное обеспечение осуществляет взаимодействие с запоминающим устройством как с аппаратным компонентом компьютерной системы, то именно оно является слеодообразующим объектом при формировании следа. Прикладное же программное обеспечение является элементом средства отражения, характеризующим средства и способы действия отражаемого объекта (пользователя).

Обобщая вышеизложенные понятия криминалистической теории отражения применительно к механизму образования следов в компьютерных системах, можно обозначить модель слеодообразования, согласно которой: пользователь, являющийся как отражаемый объект, опосредованно воздействует на компьютерную систему, являющуюся отражающим объектом. Средством отражения является совокупность команд, сигналов электромагнитной природы. Компьютерные команды могут быть инициированы как самим объектом отражения (пользователем), так и транслированы посредством прикладного программного обеспечения, являющегося элементом средства отражения. В качестве слеодообразующего объекта выступает системное программное обеспечение, следовоспринимающим объектом является запоминающее устройство компьютерной системы.

Определённая дискуссия присутствует в кругу учёных относительно определения следа в компьютерных системах и его именовании. Так, инициатором введения термина «виртуальный след» является В.В. Мещеряков, определяя его как «любое изменение состояния автоматизированной информационной

системы, связанное с событием преступления и зафиксированное в виде компьютерной информации [12, с. 43]. Поддерживая предложенное именование следа, А.Б. Смушкин, предлагает иное определение, считая, что «виртуальные следы» представляют собой следы совершения любых действий (включения, создания, открывания, активации, внесения изменений, удаления) в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей [13, с. 43]. В. А. Милашев предложил использовать термин «бинарные следы», определив их как «результаты логических и математических операций с двоичным кодом» [14, с. 18]. Н.Н. Лыткин предлагает называть такие следы компьютерно-техническими следами, обосновывая свою позицию, в противовес мнению В.А. Милашева, тем, что изменения в компьютерной информации, являющиеся следами преступления, в подавляющем большинстве случаев доступны восприятию не в двоичном виде, а в преобразованном виде: записи в файле реестра, изменении атрибута файла, электронном почтовом сообщении [15, с. 10]. Г.М. Шаповалова определяет рассматриваемый вид следов как «изменение информационной среды в виде сигналов и кодов на электронных и иных физических носителях [16, с. 34]», и называет их информационными. Е.Р. Россинская в ранних публикациях считает, что такие следы необходимо именовать информационно-технологическими, «поскольку формирование данных следов обусловлено спецификой реализации информационных технологий, и для их преобразования в доступную для восприятия форму информационные технологии также используются» [17, с. 112]. Позже она корректирует свою точку зрения, предлагая следующее определение: «Цифровой след представляет собой криминалистически значимую компьютерную информацию о событиях или действиях, отражённую в материальной среде, в процессе её возникновения, обработки, хранения и передачи» [18, с. 658]. В.Б. Вехов под «электронно-цифровым следом» понимает «любую криминалистически значимую компьютерную информацию, т.е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов» [3, с. 71].

По нашему мнению максимально точно описывает особенность следообразования следов в компьютерных системах наименование «электронно-цифровой след», данное В.Б. Веховым. Применительно к обсуждаемому термину характеристика «электронный» не относится к технологической стороне процесса следообразования, как указывают некоторые авторы [19, с. 163], а соотносится с определением ЭВМ, содержащимся в ГОСТ 15971-90: «Электронная вычислительная машина – вычислительная машина, основные функциональные устройства которой выполнены на электронных компонентах»³. Характеристика «цифровой» обозначает тип ЭВМ – цифровая, дискретная (в от-

³ ГОСТ 15971-90 Системы обработки информации. Термины и определения : утв. и введен в действие Постановлением Госстандарта СССР от 26 окт. 1990 г. № 2698 // СПС «КонсультантПлюс».

личие от аналоговых). Таким образом, «электронно-цифровой след» означает след, зафиксированный в цифровых ЭВМ (компьютерных системах).

Определение электронно-цифрового следа более точно сформулировано Е.Р. Россинской, Однако, на наш взгляд, определять след как информацию, не совсем корректно по следующим причинам:

- информация становится таковой только при её восприятии субъектом познания, или, иначе говоря, информация является субъективным отражением объективных данных [20, с. 73].

- информативность следа является одним из его свойств, заключающихся в способности следа «сохранять и передавать содержащуюся в нем информацию о следообразующем объекте и механизме следообразования» [21, с. 93]. Следовательно, информативность является свойством объективных данных, так как не может являться свойством информации.

С учётом вышеизложенного, след в компьютерной системе предлагаем именовать как электронно-цифровой след и определять его как, компьютерные данные, содержащие криминалистически значимую информацию о событиях или действиях, отражённые в материальной среде.

Учёными на настоящий момент предложены различные классификации электронно-цифровых следов. Основными основаниями классификации являются физический носитель виртуального следа [22, с. 159–160], место обнаружения следа [23, с. 264]. Достаточно взвешенной является классификация следов, предложенная Л.Б. Красновой: в зависимости от механизма следообразования следы подразделяются на первичные и вторичные. Первичные следы – следствие непосредственного воздействия пользователя с использованием какой-либо информационной технологии, а вторичные – следствие воздействия технологических процессов без участия человека и вне его желания [24, с. 17]. Однако, если рассматривать отражение как результат воздействия пользователя на компьютерную систему, то, строго говоря, любое воздействие в той или иной степени связано с пользователем, Разница определяется лишь глубиной опосредованности данного воздействия. Соответственно, помимо проблемы разграничения первичных и вторичных следов, возникает вопрос возможности существования следов, возникших без участия пользователя, помимо его желания.

Ю.В. Гаврилин, предлагает схожую классификацию, предлагая дифференцировать следы по механизму инициации изменений: следы, инициированные пользователем и следы, инициированные программой [4, с. 39]. Классификация по указанному основанию получила дальнейшее развитие у Б.К. Давлетова, который высказал идею под первичными следами понимать следы, «образующиеся непосредственно при воздействии на предмет посягательства – компьютерную информацию, а под вторичными следами – следы, образующиеся не на предмете посягательства, а на других, не являющихся предметами посягательства, объектах, вследствие этого воздействия» [11, с. 46]. Целесообразность смещения понятий следа и предмета посягательства вызывает определённое сомнение, поскольку при таком подходе возникает зависимость вида следа от квалификации деяния.

Развивая основание классификации, предложенное Л.Б. Красновой, и основываясь на результатах анализа механизма следообразования в компьютерных системах, нами предложена классификация электронно-цифровых следов по степени опосредованности воздействия пользователя на компьютерную систему: следы непосредственные и опосредованные.

Непосредственные следы – электронно-цифровые следы, имеющие прямую связь с причиной (целью) воздействия пользователя на компьютерную систему. В качестве таких следов выступают компьютерные данные, образованные пользователем посредством устройств ввода (так называемые, «пользовательские файлы»: документы, фотографии, видеоизображения и т. п.), почтовые отправления, переписка с использованием мессенджеров, история запросов Интернет-браузера, журнал вызовов мобильного средства связи, записи в прикладных базах данных и пр. Указанные следы могут находиться как непосредственно на локальном запоминающем устройстве, так и на запоминающем устройстве, доступ к которому обеспечивается с применением средств телекоммуникации (так называемый «удалённый ресурс»).

Под опосредованными следами будут подразумеваться электронно-цифровые следы, не имеющие прямой связи с причиной (целью) воздействия пользователя на компьютерную систему, но инициированные этим воздействием, обусловленные особенностями функционирования системного программного обеспечения, стандартами форматов файлов и протоколов передачи данных. К таким следам стоит отнести записи в файлах журналирования системных событий, файлах реестра операционной системы, метаданные пользовательских файлов, записи служебных баз данных, таблиц размещения файлов и пр.

Предложенная классификация содержит в себе, прежде всего, аспект практический, поскольку дифференциация электронно-цифровых следов по указанному основанию может определять уровень применения специальных знаний и криминалистической техники, необходимых для его обнаружения и фиксации.

Список использованной литературы

1. Ищенко Е.П. Современный этап развития российской криминалистики / Е.П. Ищенко // Криминалистические чтения на Байкале – 2015 : материалы Междунар. науч.-практ. конф. / отв. ред. Д.А. Степаненко. – Иркутск, 2015. – С. 57–61.
2. Мещеряков В.А. Следы преступлений в сфере высоких технологий / В.А. Мещеряков // Библиотека криминалиста. – 2013. – № 5 (10). – С. 265–270.
3. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки / В.Б. Вехов. – Волгоград : Изд-во Волгогр. акад. МВД России, 2008. – 407 с.
4. Гаврилин Ю.В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы : автореф. дис. ... д-ра юрид. наук : 12.00.09 / Ю.В. Гаврилин. – Москва, 2010. – 56 с.

5. Колычева А.Н. Анализ понятийного аппарата следов, образующихся в информационно-коммуникационной среде / А.Н. Колычева // Научный вестник Орловского юридического института МВД им. В.В. Лукьянова. – 2019. – № 2. – (79). – С. 41–43.
6. Семикаленова А.И. Современные проблемы определения объекта судебной компьютерно-технической экспертизы / А.И. Семикаленова // Вестник Университета имени О.Е. Кутафина. – 2018. – № 7. – С. 111–115.
7. Вехов В.Б. Электронные следы в системе криминалистики / В.Б. Вехов, Б.П. Смагоринский, С.А. Ковалев // Судебная экспертиза. – 2016. – № 2. (46). – С. 10–19.
8. Белкин Р.С. Курс криминалистики. В 3 т. / Р.С. Белкин. – Москва : Юристъ, 1997. – Т. 2 : Частные криминалистические теории. – 521 с.
9. Кабанова Ж.Ю. Электронный след в уголовно-исполнительной системе / Ж.Ю. Кабанова // Уголовно-исполнительная система сегодня: взаимодействие науки и практики : материалы науч.-практ. конф. – Новокузнецк, 2016. – С. 123–124.
10. Долгинов С.Д. Следы электронных устройств в криминалистике / С.Д. Долгинов // Шестой пермский конгресс ученых-юристов: Российская национальная правовая система: современное состояние, тенденции и перспективы развития. – Пермь, 2015. – С. 266–267.
11. Давлетов Б.К. Виртуальный след в генезисе научных представлений о механизмах слеодообразования / Б.К. Давлетов // Вестник КРСУ. – 2008. – Т. 8, № 1. – С. 43–46.
12. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В.А. Мещеряков. – Воронеж : Изд-во Воронеж. гос. ун-та, 2002. – 407 с.
13. Смушкин А.Б. Виртуальные следы в криминалистике / А.Б. Смушкин // Законность. – 2012. – № 8 (934). – С. 43–45.
14. Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : автореф. дис. ... канд. юрид. наук / В.А. Милашев. – Москва, 2004. – 22 с.
15. Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности : автореф. дис. ... канд. юрид. наук : 12.00.09 / Н.Н. Лыткин. – Москва, 2007. – 24 с.
16. Шаповалова Г.М. Возможность использования информационных следов в криминалистике (вопросы теории и практики) : дис. ... канд. юрид. наук : 12.00.09 / Г.М. Шаповалова. – Владивосток, 2005. – 198 с.
17. Россинская Е.Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности / Е.Р. Россинская // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – № 3-2 – С. 109–117.
18. Россинская Е.Р. Концепция цифровых следов в криминалистике / Е.Р. Россинская. – Москва : Норма. 2019. – 680 с.

19. Лушин Е.А. О термине «электронно-цифровые следы» / Е.А. Лушин // Расследование преступлений: проблемы и пути их решения. – 2017. – № 4 (18). – С. 161–163.

20. Тисов В.В. Онтологические различия информации и данных / В.В. Тисов // Философские проблемы информационных технологий и киберпространства. – 2016. – № 2 (12). – С. 63–73.

21. Белкин Р.С. Криминалистическая энциклопедия / Р.С. Белкин. – Москва : Мегатрон XXI, 2000. – 334 с.

22. Волеводз А.Г. Противодействие компьютерным преступлениям / А.Г. Волеводз. – Москва : Юрлитинформ, 2002. – 485 с.

23. Леонтьев В.П. Большая энциклопедия компьютера и Интернета / В.П. Леонтьев. – Москва : Просвещение, 2006. – 1121 с.

24. Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике : автореф. дис. ... канд. юрид. наук : 12.00.09 / Л.Б. Краснова. – Воронеж, 2005. – 24 с.

References

1. Ishchenko E.P. The Current Stage in the Development of Russian Forensics. In Stepanenko D.A. (ed.). *Kriminalisticheskie chteniya na Baikale - 2015. Materialy Mezhdunarodnoi nauchno-prakticheskoi konferentsii, Irkutsk, 18-19 iyunya 2015 g.* [Baikal Criminalistic Readings - 2015. Materials of International Research Conference, Irkutsk, June 18-19, 2015]. Irkutsk, 2015, pp. 57–61. (In Russian).

2. Meshcheryakov V.A. Traces of Crime in the Field of High Technologies. *Biblioteka kriminalista = Library of a Criminalist*, 2013, no. 5 (10), pp. 265–270. (In Russian).

3. Vekhov V.B. *Osnovy kriminalisticheskogo ucheniya ob issledovanii i ispol'zovanii komp'yuternoi informatsii i sredstv ee obrabotki* [Fundamentals of Forensic Science on the Study and Use of Computer Information and its Processing Tools]. Volgograd Academy of the Ministry of Internal Affairs of Russia Publ., 2008. 407 p.

4. Gavrilin Yu.V. *Rassledovanie prestuplenii, posyagayushchikh na informatsionnyu bezopasnost' v sfere ekonomiki: teoreticheskie, organizatsionno-takticheskie i metodicheskie osnovy. Avtoref. Dokt. Diss.* [Investigation of Crimes that Infringe on Information Security in the Economic Sphere: Theoretical, Tactical and Organizational and Methodological Principles. Doct. Diss. Thesis]. Moscow, 2010. 56 p.

5. Kolycheva A.N. Analysis of the Conceptual Apparatus for Traces Formed in the Information and Communication Environment. *Nauchnyi vestnik Orlovskogo yuridicheskogo instituta MVD im. V.V. Luk'yanova = Scientific Bulletin of the Oryol Law Institute of the Ministry of Internal Affairs of Russia named after V.V. Lukyanov*, 2019, no. 2 (79), pp. 41–43. (In Russian).

6. Semikalenova A.I. Actual Problems of Determining the Object of the Court Computer Technical Expertise. *Vestnik Universiteta imeni O.E. Kutafina = Courier of the Kutafin Moscow State Law University*, 2018, no. 7, pp. 111–115. (In Russian).

7. Vekhov V.B. Electronic Traces in the Forensic System. *Sudebnaya ekspertiza = Forensic Examination*, 2016, no. 2 (46), pp. 10–19. (In Russian).

8. Belkin R.S. *Kurs kriminalistiki* [A Course in Criminalistics]. Moscow, Yurist Publ., 1997. Vol. 2. 837 p.

9. Kabanova Zh.Yu. Electronic Trace in the Penal System. *Ugolovno-ispolnitel'naya sistema segodnya: vzaimodeistvie nauki i praktiki. Materialy mezhdunarodnoi nauchno-prakticheskoi konferentsii* [The penal system today: interaction of science and practice. Materials of International Research Conference]. Novokuznetsk, 2016, pp. 123–124. (In Russian).

10. Dolginov S.D. Traces of Electronic Devices in Forensic Science. *Shestoi permskii kongress uchenykh-yuristov: Rossiiskaya natsional'naya pravovaya sistema: sovremennoe sostoyanie, tendentsii i perspektivy razvitiya* [Sixth Perm Congress of Legal Scholars: Russian National Legal System: Current State, Trends and Prospects of Development]. Perm, 2015, pp. 266–267. (In Russian).

11. Davletov B.K. Virtual Footprint in the Genesis of Scientific Ideas about the Mechanisms of Trace Formation. *Vestnik KRSU = Herald of KRSU*, 2008, vol. 8, no. 1, pp. 43–46. (In Russian).

12. Meshcheryakov V.A. *Prestupleniya v sfere komp'yuterno informatsii: osnovy teorii i praktiki rassledovaniya* [Crimes in the Field of Computer Information: the Basics of the Theory and Practice of Investigation]. Voronezh State University, 2002. 407 p.

13. Smushkin A.B. Virtual Traces in Criminalistics. *Zakonnost' = Legality*, 2012, no. 8 (934), pp. 43–48. (In Russian).

14. Milashev V.A. *Problemy taktiki poiska, fiksatsii i iz'yatiya sledov pri nepravomernom dostupe k komp'yuterno informatsii v setyakh EVM. Avtoref. Kand. Diss.* [Problems of Tactics of Search, Fixation and Removal of Traces in Case of Illegal Access to Computer Information in Computer Networks. Cand. Diss. Thesis]. Moscow, 2004. 22 p.

15. Lytkin N.N. *Ispol'zovanie komp'yuterno-tekhnicheskikh sledov v rassledovanii prestuplenii protiv sobstvennosti. Avtoref. Kand. Diss.* [The Use of Computer-technical Traces in the Investigation of Crimes against Property. Cand. Diss. Thesis]. Moscow, 2007. 24 p.

16. Shapovalova G.M. *Vozmozhnost' ispol'zovaniya informatsionnykh sledov v kriminalistike (voprosy teorii i praktiki). Avtoref. Kand. Diss.* [The Possibility of Using Information Traces in Criminalistics (Issues of Theory and Practice). Cand. Diss. Thesis]. Vladivostok, 2006. 21 p.

17. Rossinskaya E.R. The Issue of Private Theory of Information and Computer Software Criminalistics Operations. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki = Izvestiya of the Tula State University. Economic and Legal Sciences*, 2016, no. 3-2, pp. 109–117. (In Russian).

18. Rossinskaya E.R. *Kontseptsiya tsifrovyykh sledov v kriminalistike* [Concept of Digital Traces in Criminalistics]. Moscow, Norma Publ., 2019. 680 p.

19. Lushin E.A. About the Term «Digital Footprints». *Rassledovanie prestuplenii: problemy i puti ikh resheniya = Criminal Investigation: Problems and Ways of Their Solution*, 2017, no. 4 (18), pp. 161–163. (In Russian).

20. Tisov V.V. Ontological Differences of Information and Data. *Filosofskie problemy informatsionnykh tekhnologii i kiberprostranstva = Philosophical Problems of Information Technology and Cyberspace*, 2016, no. 2 (12), pp. 63–73. (In Russian).

21. Belkin R.S. *Kriminalisticheskaya entsiklopediya* [Forensic Encyclopedia]. Moscow, Megatron XXI Publ., 2000. 334 p.

22. Volevodz A.G. *Protivodeistvie komp'yuternym prestupleniyam* [Counteraction to Computer Crimes]. Moscow, Yurlitinform Publ., 2002. 485 p.

23. Leontev V.P. *Bol'shaya entsiklopediya komp'yutera i Interneta* [Great Encyclopedia of Computer and Internet]. Moscow, Prosveshchenie Publ., 2006. 1121 p.

24. Krasnova L. B. *Komp'yuternye ob'ekty v ugolovnom protsesse i kriminalistike. Avtoref. Kand. Diss.* [Computer Objects in Criminal Procedure and Criminalistics. Cand. Diss. Thesis]. Voronezh, 2005. 24 p.

Информация об авторе

Себякин Алексей Геннадьевич – руководитель второго экспертного отдела (с дислокацией в городе Иркутск) Сибирского филиала (с дислокацией в городе Новосибирск) ФГКУ «Судебно-экспертный центр Следственного комитета Российской Федерации», г. Иркутск, Российская Федерация, e-mail: quattro.sa@yandex.ru.

Information about author

Sebyakin, Alexey G. – Head, 2nd Expert Division (based in Irkutsk), Siberian Branch (based in Novosibirsk) of the Forensic Expert Center, the Investigative Committee of the Russian Federation, Irkutsk, the Russian Federation, e-mail: quattro.sa@yandex.ru.