КРИМИНАЛИСТИКА

УДК 343.9+340.6

Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности*

Е. Р. Россинская, А. И. Семикаленова

Московский государственный юридический университет им. О. Е. Кутафина,
Российская Федерация, 125993, Москва, ул. Садовая-Кудринская, 9

Для цитирования: Россинская, Елена Р., Анастасия И. Семикаленова. 2020. «Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности». *Вестник Санкт-Петербургского университета. Право* 3: 745–759. https://doi.org/10.21638/spbu14.2020.315

В статье рассмотрены проблемы создания учения о криминалистическом исследовании компьютерных средств и систем. Обозначена негативная позиция авторов, касающаяся добавления к наименованию криминалистической науки определений, связанных с появлением новых объектов судебных экспертиз: «электронная криминалистика», «лингвистическая криминалистика», «цифровая криминалистика» и др. Декларируется единство криминалистики как науки, имеющей свой предмет, систему, задачи, объекты. Предмет учения о криминалистическом исследовании компьютерных средств и систем составляют основные закономерности выявления, фиксации, изъятия и исследования криминалистически значимой компьютерной информации и разрабатываемые на основе познания этих закономерностей технико-криминалистические методы, средства, приемы и методики собирания криминалистически значимой информации о компьютерных средствах и системах, имеющей доказательственное значение и используемой в уголовном, гражданском и административном судопроизводстве. Показана роль данного учения в получении информации ориентирующего характера для обеспечения иных мер раскрытия и предупреждения преступлений. Обозначено его место в теории информационно-компьютерного обеспечения криминалистической деятельности. Объектами этого учения выступают компьютерные средства и системы,

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16003.

рассматриваемые в широком смысле, и содержащаяся в них разыскная и доказательственная криминалистически значимая компьютерная информация. Учение о криминалистическом исследовании компьютерных средств и систем является основой нового раздела криминалистической техники и технологии как системы научных положений и базирующихся на них рекомендаций, средств, приемов и методик, предназначенных для собирания и исследования информации о компьютерных средствах и системах, в том числе цифровых следах и процессах их возникновения, для передачи и трансформации в целях получения доказательств в судопроизводстве, раскрытия и предупреждения преступлений. Подчеркивается двуединство существования цифровых следов: следы способны существовать на конкретном материальном носителе в виде зафиксированной различными физическими методами информации, а также способны перемещаться с этих физических носителей практически без изменения на другие носители, зачастую сохраняясь на них с помощью совершенно других технологий.

Ключевые слова: компьютерные преступления, криминалистически значимая информация, цифровизация, цифровые следы, носитель компьютерной информации, информационно-компьютерное обеспечение, криминалистическая деятельность, устройства ввода/вывода, устройства хранения информации, устройства передачи информации.

1. Введение

Одним из основных векторов научно-технического прогресса в современном обществе является глобальный процесс цифровизации, внедрение компьютерных технологий во все сферы человеческой деятельности — социальную, экономическую, управленческую, культурную и др. Этот процесс оказал огромное влияние на жизнь социума, в том числе серьезно затронул уголовное, гражданское и административное судопроизводство. Прежде всего произошло радикальное видоизменение преступной деятельности в целом. Использование в противоправных целях информационных компьютерных технологий не только породило новые виды преступлений — преступления в сфере компьютерной информации. Наряду с этим практически любые преступления (кражи, мошенничества, преступления в финансовой и банковской сфере, фальшивомонетничество, лжепредпринимательство, фальсификации платежных документов, хищения наличных и безналичных денежных средств путем перечисления на фиктивные счета, отмывания денег, вторичного получения уже произведенных выплат, совершения покупок с использованием фальсифицированных или похищенных электронных платежных средств, продажи секретной информации и пр.) совершаются теперь с использованием компьютерных средств и систем.

Развитие цифровизации постоянно порождает все новые и новые способы преступлений, изменения механизма их совершения и сокрытия. Например, повсеместное распространение мобильных коммуникаторов привело к реализации таких новых способов преступлений, как создание и распространение вредоносных программ для мобильных телефонов, использование средств мобильной коммуникации для совершения террористических актов, взрывов, поджогов, инициализации массовых беспорядков, вымогательств, мошенничеств и др. Проблема борьбы с подобными преступлениями в силу их транснационального характера за счет использования компьютерных сетей актуальна для всех стран независимо от их географического положения.

Поскольку указанные преступления выходят далеко за рамки преступлений в сфере компьютерной информации, регламентированных гл. 28 Уголовного кодекса РФ от 13.06.1996 № 63-ФЗ (СПС «КонсультантПлюс». Дата обращения 10 февраля, 2020. http://www.consultant.ru), в наших работах мы неоднократно предлагали именовать их «компьютерными преступлениями», причем понятие «компьютерное преступление», по нашему мнению, должно употребляться в криминалистическом, а не в уголовно-правовом аспекте, где это только затрудняет квалификацию деяния, так как определяется не квалификацией, а способом преступления, следовательно, методикой его раскрытия и расследования. Компьютерные преступления имеют общую родовую криминалистическую характеристику, которая включает информацию о способах преступлений, совершивших их лицах, потерпевшей стороне, обстоятельствах, способствовавших и препятствовавших данным преступлениям.

До недавнего времени в России вообще отсутствовали какие-либо системные разработки, касающиеся юридической оценки исследуемой проблемы, информационно-компьютерных технологий для получения достоверной доказательственной информации, позволяющей однозначно инкриминировать фигурантам конкретное уголовно-наказуемое деяние. И это несмотря на то, что первая информация о совершении хищения денежных средств с применением средств электронно-вычислительной техники относится еще к 1979 г., когда в Вильнюсе было похищено 78 584 руб. путем манипуляции данными на входе в компьютерную систему (Батурин 1991, 126). Хотя теме преступлений в сфере компьютерной информации в настоящее время посвящен целый ряд литературных источников, эти работы носят в целом неупорядоченный фрагментарный характер и затрагивают в основном элементы методики расследования.

Процессы цифровизации в раскрытии и расследовании преступлений проявляются через широкое использование цифровых средств фиксации, сохранения, автоматизированной обработки и исследования доказательственной и ориентирующей информации, а также через новые виды криминалистически значимой информации, фиксируемой на компьютерных носителях. Данная статья логически продолжает ряд наших публикаций, где отмечалось, что для исследования компьютерных систем и средств необходим особый комплекс специальных знаний, сформированный на основе разработки частной криминалистической теории информационно-компьютерного обеспечения криминалистической деятельности.

2. Основное исследование

Ряд авторов полагает, что разработка криминалистического обеспечения расследования преступлений, совершаемых с использованием компьютерных средств и систем, осуществляется новой наукой — «электронной криминалистикой», или «цифровой криминалистикой» (Вехов 2017; Яковлев 2018). К сожалению, подобные новации вводятся специалистами и других отраслей знания при появлении новых объектов или задач, требующих комплексного исследования (например, «медицинская криминалистика», «лингвокриминалистика» (Грачев, Грачев 2015), «экономическая криминалистика» (Голубятников 2017) и др.). Полагаем, что такие наименования связаны, как правило, с возникновением новых родов или видов судебных экспертиз, а авторы этих новаций не имеют четкого представления

о криминалистической науке, зачастую смешивая понятия криминалистики и родов судебных экспертиз. По нашему мнению, это приводит к размыванию предмета криминалистической науки. Криминалистика едина! Это наука, имеющая свой предмет, систему, задачи, объекты и изучаемые закономерности (Белкин 2001, 51; и др.). Криминалистика может быть обосновывающим знанием для новых родов и видов судебных экспертиз, поэтому нет никакой необходимости менять название науки. Развитие криминалистики идет за счет изучения новых закономерностей, новых механизмов следообразования, новых технологий собирания (выявления, фиксации, изъятия), исследования, оценки и использования криминалистически значимой информации, новаций в области криминалистической тактики и методики.

Нами разработана частная теория информационно-компьютерного обеспечения криминалистической деятельности, предметом которой выступают закономерности возникновения, движения, собирания и исследования компьютерной информации при расследовании преступлений и судебном рассмотрении уголовных дел. Криминалистические методы и средства как в России, так и за рубежом широко востребованы гражданским и административным судопроизводством, поскольку в процесс доказывания вовлечены компьютерные средства и системы. В связи с этим полагаем необходимым включить в предмет рассматриваемой теории закономерности, связанные с рассмотрением дел в гражданском, арбитражном, административном процессе. Однако, поскольку общая и главная задача криминалистической науки — борьба с преступностью, раскрытие и расследование преступлений приоритетны.

Объектами частной теории информационно-компьютерного обеспечения криминалистической деятельности являются, с одной стороны, сами компьютерные средства и системы как носители разыскной и доказательственной, криминалистически значимой информации, а с другой — система действий и отношений в механизмах преступлений с использованием компьютерных средств и систем, а также криминалистических компьютерных технологий обнаружения, фиксации, изъятия, сохранения, исследования и использования криминалистически значимой доказательственной и ориентирующей информации (Россинская 2019b).

Мы создали систему частной теории информационно-компьютерного обеспечения криминалистической деятельности (Россинская 2019a, 184–191), состоящую из ряда учений. Задача данного исследования — разработка основ учения о криминалистическом исследовании компьютерных средств и систем как части теории информационно-компьютерного обеспечения криминалистической деятельности.

Данное учение с точки зрения системы криминалистики должно относиться к криминалистической технике и технологии. В настоящее время это один из разделов криминалистики, в котором дается система «научных положений и основанных на них технических (в широком смысле. — *Авт.*) средств, приемов и методов, предназначенных для собирания и исследования доказательств в процессе судопроизводства по уголовным (гражданским, административным) делам, иных мер раскрытия и предупреждения преступлений» (Белкин 2000, 102). Термином «криминалистическая техника» обозначается, во-первых, раздел криминалистической науки, а во-вторых, совокупность технических средств, т. е. приборов, аппаратуры, оборудования, инструментов, приспособлений, принадлежностей и материалов,

применяемых для собирания и исследования доказательств в процессе судопроизводства. Отсюда изучение возможностей интеграции в криминалистику новых научных методов и разработка на этой основе новых криминалистических технологий, а также разработка частных криминалистических теорий за счет творческого использования ею достижений фундаментальных и прикладных наук неразрывно связаны с развитием новых направлений криминалистической техники.

Попытки включения в криминалистическую технику новых разделов вызывают обычно бурные споры о том, является ли это направление криминалистическим или отнесено к ним искусственно, не существуя в реальности. Криминалистическая техника не беспредельна, поэтому включение в нее новых разделов возможно, только если необходимость их включения обоснованна и реально существует, а добавление слова «криминалистическая» к какому-то разделу науки, как нередко случается, еще не означает, что такое направление уже имеется. Именно поэтому, как мы ранее указывали в своих работах, направление криминалистической техники можно считать сформировавшимся только в том случае, если оно отвечает следующим критериям:

— специфика объектов исследования — вещественных доказательств и в то же время их распространенность, частая встречаемость в уголовном и гражданском судопроизводстве;
— решение специфических криминалистических задач, которые не ставятся при исследовании подобных объектов в других сферах человеческой деятельности;
— методологическая и методическая разработанность данного направления.

Попробуем обосновать выполнение этих критериев в настоящий момент. Для этого необходимо сформировать в рамках криминалистической техники новое учение, затрагивающее область интеграции в криминалистику компьютерно-цифровых технологий.

«Компьютерная преступность» как особая категория уголовно наказуемых деяний, при совершении которых так или иначе использовалась компьютерная техника, признана уже с конца 1990-х годов, а с начала 2000-х в Российской Федерации предпринимаются попытки (в том числе авторами настоящей статьи) определения специфических объектов и криминалистических задач, возникающих при их исследовании (Усов 2002; Вехов 2008; и др.). В экспертно-криминалистических подразделениях МВД России, ФСБ России, судебно-экспертных учреждениях Минюста России, а сейчас и Следственного комитета России открываются отделы по исследованию компьютерных средств, где начинаются разработки методического обеспечения по собиранию и исследованию криминалистически значимой компьютерной информации. Однако проводимые исследования разрозненны, связаны главным образом с разработкой методического обеспечения некоторых отдельных видов судебных компьютерных экспертиз.

Задачи определения специальных знаний, методов и средств, необходимых для выявления, фиксации, изъятия криминалистически значимой информации, содержащейся в компьютерных средствах и системах, разработки соответствующих информационно-компьютерных технологий, могут быть решены только в рамках учения «Криминалистическое исследование компьютерных средств и систем»,

на базе которого будет основан соответствующий прикладной раздел криминалистической техники, включенный в учебники криминалистики.

Попытки введения похожих разделов криминалистической техники предпринимались различными авторами (Колдин 2007, 389–414). Однако эти попытки охватывали только вопросы, связанные с получением и анализом компьютерной информации, т. е. лишь небольшую часть вопросов, возникающих при решении технико-криминалистических задач в ходе расследования компьютерных преступлений и не получивших пока должного дальнейшего распространения и развития.

Предмет учения о криминалистическом исследовании компьютерных средств и систем можно определить как систему закономерностей собирания криминалистически значимой компьютерной информации, на основе познания которых разрабатываются технико-криминалистические методы, средства, приемы и методики выявления, фиксации и изъятия доказательственной и ориентирующей криминалистической информации, содержащейся в компьютерных средствах и системах, в процессе судопроизводства по уголовным, гражданским и административным делам и для осуществления иных мер раскрытия и предупреждения преступлений.

Объектами учения о криминалистическом исследовании компьютерных средств и систем выступают компьютерные средства и системы, рассматриваемые в широком смысле, и содержащаяся в них разыскная и доказательственная криминалистически значимая компьютерная информация.

Предлагаемый новый раздел криминалистической техники, на наш взгляд, должен содержать описание объектов криминалистического исследования, особенностей собирания (выявления, фиксации, изъятия) криминалистически значимой информации, возможностей судебно-экспертного исследования этих объектов.

Криминалистически значимая компьютерная информация содержится как в стационарных компьютерах, серверах, средствах их коммуникации, внешних и внутренних носителях данных, периферийных устройствах и т. д., так и в мобильных устройствах сотовой связи (смартфонах, планшетных компьютерах и т. д.), микропроцессорных устройствах. Компьютерные средства и системы приобщаются к материалам дела в качестве вещественных доказательств, но доказательственное значение, как правило, имеет именно компьютерная информация, содержащаяся в памяти данных устройств, которая и является основным объектом криминалистического исследования. Поэтому следует изучать в совокупности как особенности создания, хранения и распространения информации в компьютерных системах, так и материальную форму ее хранения и обеспечения возможности ее восприятия.

Поскольку компьютерная информация на материальных носителях представлена в неявном виде, а для ее восприятия необходимо использовать специальные средства, особое внимание нужно уделить созданию и использованию данных средств. Анализ российской следственной и экспертной практики, имеющихся на эту тему научных исследований за последние пять лет показал, что этот вопрос остается непроработанным, что влечет за собой снижение доказательственного значения обнаруженной криминалистически значимой информации, а зачастую и вообще ее утрату.

Повсеместное проникновение компьютерных средств и систем, их использование в преступной деятельности послужили причиной того, что в зарубежной

практике выделен особый класс цифровых доказательств, описаны методы и приемы работы с ними (Sammons 2015; Horsman 2019), разработаны методические рекомендации. Анализ зарубежной литературы в области цифровых доказательств (Daniel et al. 2012), современной следственной и экспертной практики, состояния научной мысли в области IT-технологий показал необходимость установить различие между оригиналом цифрового доказательства, его дубликатом и копией.

Оригиналами цифровых доказательств выступают материальные носители и такие информационные объекты, которые связаны с этими носителями на момент изъятия (получения). *Дубликаты* цифровых доказательств — точные цифровые репродукции всех информационных объектов, хранящихся на оригинальном материальном носителе, в то время как копия — это точная репродукция информации, содержащейся в информационных объектах, независимая от материального носителя.

Необходимость такого различения возникла вследствие особенности природы цифрового доказательства, которая, с одной стороны, позволяет неоднократно исследовать его разными методами, в том числе уничтожающими, а с другой — внести фатальные изменения в его структуру, способные увести ход расследования в сторону и вывести криминалистически значимую информацию из доказательственного поля.

Данные манипуляции с доказательствами, создаваемыми, распространяемыми, хранимыми в компьютерных средствах и системах, возможны в силу того, что к ним, как и к интеллектуальной собственности, применимо понятие двуединства существования: одно — это существование следов на конкретном материальном носителе в виде зафиксированной различными физическими методами информации, а другое — их способность перемещаться с этих физических носителей практически без изменения на другие носители, зачастую сохраняясь на них с помощью совершенно других технологий. Например, изначально информация возникла и хранилась на твердотельном носителе информации (так называемом SSD или флеш-носителе) посредством сохраненного электрического заряда в электронной схеме, далее была перенесена с использованием электромагнитных импульсов на жесткий магнитный диск (HDD) или магнитную ленту (кассеты резервного копирования), где хранилась на магнитных носителях (лентах, дисках) с помощью нанесенных на них векторов намагниченности и т. д. Подобные трансформации криминалистически значимой компьютерной информации возможны многократно и с участием не только электрических и магнитных свойств вещества, но и оптических, механических и даже биологических (запись информации в геном) (Семикаленова 2019), при этом информативность не теряется, а зачастую даже возрастает. Необходимость анализа такого рода следов и их исследования остро поставила перед криминалистической наукой вопрос: к какой группе уже известных следов их следует отнести? Достаточно долгое время этот вопрос оставался открытым.

В отечественной литературе неоднократно высказывались предложения ввести для исследования компьютерных средств и систем новый вид следов. Так, рядом авторов обосновывался термин «виртуальные следы» (Агибалов 2012, 13; Волеводз 2002, 6; Краснова 2005, 15–17; Мещеряков 2001, 112–113; Смушкин 2012, 43–45), что, однако, не нашло единодушной поддержки. Некоторые оппоненты указывали на несоответствие академического значения термина «виртуальный» тем

объектам, в отношении которых использовалось данное понятие (Милашев 2004, 63–65). Еще одним вариантом была замена слова «виртуальный» словами «бинарный» (Мещеряков 2001, 18) и «компьютерно-технический» (Колдин 2007, 11).

Мы, как и ряд других исследователей (см., напр.: Поляков, Шебалин 2013; Нехорошев 2004, 123–125), считаем, что с позиций общей теории криминалистики «виртуальных следов» не может быть в принципе, и полагаем, что данные следы являются материальными, поскольку зафиксированы на материальных носителях путем изменения с помощью физических, биологических или химических методов свойств или состояния отдельных их элементов. Относить их к идеальным на том основании, что они недоступны непосредственному наблюдению, как предлагает А. Г. Волеводз (Волеводз 2002, 4), полагаем нецелесообразным, поскольку ряд следов (например, пахнущие следы человека или животного, геномная информация, следы целого ряда веществ, невидимые следы рук и пр.) также недоступен непосредственному восприятию, но это не означает, что они являются идеальными. Идеальные следы запечатлеваются в памяти человека, и существенное влияние на них оказывают психофизиологические особенности личности и ее состояние на момент получения и фиксации следа, что никак не свойственно компьютерной информации.

Постараемся показать, что представляет собой компьютерная информация, и на основе этого предложить, на наш взгляд, оптимальный термин, описывающий следы данного рода. Компьютерная информация применительно к процессу доказывания (о чем мы уже неоднократно говорили) может быть определена как фактические данные, обработанные компьютерной системой и/или передающиеся по телекоммуникационным каналам, а также доступные для восприятия, на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения уголовного, гражданского или административного дела. Изъять и приобщить к материалам дела непосредственно информацию нельзя. Но, поскольку она неотделима от носителя, именно носители становятся особой категорией объектов криминалистического исследования. Важным моментом здесь будет сложная — двойственная — сущность объекта криминалистического исследования, в результате чего исследованию будут подвергнуты сразу два объекта: носитель и хранимая на нем информация.

Для рассмотрения феномена компьютерной информации коснемся принципов работы современных компьютеров. Согласно определению, данному профессором Э. Таненбаумом, «цифровой компьютер — это машина, которая может решать задачи, исполняя данные ей команды» (Таненбаум, Остин 2013). Для решения конкретных задач команды собираются в определенные последовательности, называемые программами. Для взаимодействия с аппаратными средствами компьютера и поддержания оптимальной работы микросхем эти программы должны состоять из команд базового уровня (сложить два числа, скопировать данные из одной микросхемы в другую, сравнить числа). Такой язык называется машинным, а программы — машинным кодом. Принимая во внимание, что аппаратные средства по своей природе оперируют данными, записанными в двухсимвольном алфавите, состоящем из 0 и 1, мы можем утверждать, что информация, хранящаяся и циркулирующая в компьютерах и компьютерных системах, является цифровой последовательностью. Это, в свою очередь, приводит нас к пониманию цифровой природы криминалистически значимых следов, образующихся в компьютерных системах.

Исходя из изложенного, мы приходим к подтверждению предложенного нами ранее понятия «цифровой след», выступающего объектом учения о цифровых следах как источниках криминалистически значимой компьютерной информации, входящего в систему теории информационно-компьютерного обеспечения криминалистической деятельности (см., напр.: Россинская 2019b). Цифровой след представляет собой криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи и не имеет аналогов в учении о следах и следообразовании (Белкин 2001, 304–322).

Можно с уверенностью утверждать, что цифровые следы являются объектами изучения нового раздела криминалистической техники — криминалистического исследования компьютерных средств и систем. Однако, говоря о цифровых следах, нельзя забывать о двойственной природе информационно-компьютерных объектов, которая включает в себя информационно-цифровую и материальную составляющие. Следовательно, наряду с цифровыми следами объектами криминалистического исследования компьютерных средств и систем будут носители цифровых следов, от правильного обнаружения, фиксации и изъятия которых, их судебно-экспертного исследования зависят целостность и полнота криминалистически значимой информации, положенной в основу доказательственной базы.

На сегодня можно выделить следующие категории объектов, которые могут быть *носителями криминалистически значимой компьютерной информации*:

— устройства хранения информации;
— устройства ввода/вывода информации;
— устройства обработки информации;
— устройства передачи информации по каналам связи;
— информационные комплексы и системы.

Все перечисленные виды объектов содержат цифровые следы, могут продуцировать собственные цифровые следы и участвуют в формировании криминалистически значимой компьютерной информации. В связи с этим уделим им более пристальное внимание.

Устройства хранения информации предназначены для записи и хранения информации. Запись информации (данных) — это процесс преобразования информационных сигналов в пространственное изменение физических характеристик (например, наличие или отсутствие заряда, ориентация вектора намагниченности и др.) или формы носителя записи (например, следы от прожигания на лазерном CD-диске) с целью сохранения и последующего воспроизведения записанной информации. Отсюда хранение информации характеризуется ее переносом с помощью цифрового кодирования и изменения физических или биологических свойств носителя на данный носитель, вспомогательное устройство для последующего использования компьютерной системой. Хранение — одна из основных операций, осуществляемых над информацией (или, как еще ее называют в IT-технологиях, данными), и служит главным способом обеспечения ее доступности в течение определенного времени.

Устройства хранения информации принято в основном разделять на внешние и внутренние. К внутренним относятся: устройства, обеспечивающие работо-

способность самой вычислительной системы (компьютера), — это оперативная память, кеш-память, BIOS. К внешним принято относить большинство запоминающих устройств, известных как винчестер, флеш-накопитель, карта памяти, CD-диск. До недавнего времени существовали только эти два вида памяти, разделенные по признаку расположения: в компьютерной системе или вне ее. Однако сегодня имеется еще один, можно сказать гибридный, вид устройства хранения информации — облачное хранилище, располагающееся в сети Интернет. Почему данный вид является гибридным? Ответ на данный вопрос вытекает из самой сути такого вида хранения. Данные, подготовленные и обработанные пользователем на своем компьютерном средстве и предназначенные для использования на нем или в других компьютерных системах, хранятся на внутренних носителях информации серверов, расположенных за пределами системы пользователя.

Классификация устройств хранения информации, имеющая существенное криминалистическое значение, может осуществляться и по другим основаниям. Немаловажно подразделение устройств хранения информации по принципу энергозависимости устройства, когда они могут быть разделены на два класса: энергозависимые (оперативная память) и энергонезависимые (жесткие магнитные диски, флеш-память, оптические и магнитооптические диски и др.). Энергозависимые устройства требуют постоянного использования электропитания для возможности удержания записанной на них информации и очищаются при снятии электропитания, в то время как энергонезависимые запоминающие устройства сохраняют информацию при отключении электропитания.

Еще одно значимое основание разделения устройств хранения информации — устойчивость записи. В соответствии ней выделяются постоянные запоминающие устройства (BIOS), записываемые (CD-R), многократно перезаписываемые (CD-RW, DVD-RW, жесткие магнитные диски, флеш-память), оперативные запоминающие устройства (ОЗУ).

Запоминающие устройства могут быть классифицированы и по иным основаниям, но именно эти на сегодняшний день определяют специфику криминалистического исследования данных объектов, применяемые к ним технические средства. При получении доступа к устройствам хранения и изъятии с них криминалистически значимой компьютерной информации наиболее важно определить порядок действий, позволяющий сохранить содержащиеся на устройствах данные в неизменном виде, а это зависит в первую очередь от отнесения устройства к тому или иному виду в соответствии с основаниями классификации, указанными нами выше.

Устройства ввода информации предназначены для преобразования поступающих от пользователя данных в доступную для обработки системой цифровую форму. К таковым относятся клавиатуры, манипуляторы (мыши, джойстики, трекболы), сенсорные графические планшеты (не путать с мобильными устройствами), интерактивные доски, сканеры, веб-камеры, устройства видеозахвата, звуковые карты с аудиовходом, считыватели смарт-карт, акселерометры и гироскопы, приемники спутниковой навигации, сканеры папиллярных узоров и узоров сетчатки глаз, разного рода датчики и измерительное оборудование, а также иные устройства.

Устройства вывода информации предназначены для преобразования информации из цифровой формы в форму, доступную для восприятия человеком, а также техническими средствами. К ним относятся индикаторы, мониторы, проекторы,

принтеры, звуковые карты, исполнительные механизмы и телемеханика (например, турникет или электронный замок) и т. д.

Устройства обработки информации предназначены для регистрации поступающей информации и формирования управляющих команд в соответствии с алгоритмом. Среди компонентов персонального компьютера примерами устройств обработки информации являются центральный процессор, графический контроллер (видеокарта), звуковой процессор (звуковая карта). В устройствах обработки информации также обычно присутствует оперативная память, используемая для хранения обрабатываемых объемов информации (кеш, буфер). Строго говоря, практически в каждом цифровом устройстве в том или ином виде имеется устройство обработки информации — микроконтроллер (преобразователь), осуществляющий обработку данных по алгоритму, заложенному в микропрограмме («прошивке») и хранящемуся в постоянном запоминающем устройстве.

Устройства передачи информации по каналам связи представляют собой устройства ввода/вывода информации, которые осуществляют преобразование поступающих данных в сигнал, пригодный для передачи по каналу связи (модуляцию), и его трансляцию, а также прием сигналов и их обратное преобразование в доступную для обработки форму (демодуляцию). К устройствам относятся Wi-Fi-роутеры, модемы, сетевые карты, GSM-модули, маршрутизаторы, bluetooth-модули, модули ИК-связи, коммутаторы и др.

Сегодня передачу и хранение криминалистически значимой информации следует рассматривать не только для компьютерных средств и систем, но и для мобильных телефонов сотовой связи, смартфонов, планшетов. Данные устройства в силу всеобщего распространения — это одни из самых часто встречающихся объектов криминалистического исследования компьютерных средств и систем, поскольку выступают в качестве не только носителей и средств передачи криминалистически значимой информации, но и орудий совершения преступлений. Означенные мобильные устройства не могут классифицироваться как электронно-вычислительные машины, поскольку имеют постоянное соединение с сетью и являются ее частью. Они представляют собой интегрированные устройства, в которые входят персональный компьютер (иногда с урезанными возможностями), устройство связи, коммутации; используют специфическое программное обеспечение; содержат носители информации (SIM-карты, карты памяти, USB-накопители); осуществляют функции глобальной системы позиционирования (GPS), оснащены фото- и видеокамерами (Семикаленова, Сергеева 2011).

Современная компьютерная система независимо от своих конструктивных особенностей (будь то сервер, ноутбук, смартфон или планшет), по сути, представляет собой единый информационный комплекс. Управление им и взаимодействие его составных частей осуществляются посредством программного обеспечения, которое, в свою очередь, является средством, продуцирующим цифровые следы, и в то же время само представляет собой цифровой след.

3. Выводы

Проведенное исследование позволяет сформулировать основные дефиниции учения о криминалистическом исследовании компьютерных средств и систем,

определить его предмет как систему криминалистических закономерностей собирания и исследования криминалистически значимой компьютерной информации доказательственного и ориентирующего характера. Объектами этого учения выступают компьютерные средства и системы, рассматриваемые в широком смысле, и содержащаяся в них разыскная и доказательственная криминалистически значимая компьютерная информации.

Это учение входит в систему теории информационно-компьютерного обеспечения криминалистической деятельности и служит базой для нового раздела криминалистической техники — «Криминалистического исследования компьютерных средств и систем». Данный раздел представляет собой систему научных положений и основанных на них рекомендаций, средств, приемов и методик, предназначенных для собирания и исследования информации о компьютерных средствах и системах, в том числе цифровых следах и процессах их возникновения, для передачи и трансформации в целях получения доказательств в судопроизводстве, раскрытия и предупреждения преступлений. К отличительным чертам вышеописанных объектов этого раздела криминалистической техники относятся:

— в основном цифровой вид информации, несущей доказательственное значение;
— сочетание явного и неявного вида получаемой криминалистически значимой информации;
— в случае неявного вида — необходимость использования специальных средств для обеспечения ее восприятия;
— возможность уничтожения или модификации в кратчайшие сроки и удаленно;
— наличие специальных средств IT-технологий, ограничивающих доступ к информации;
— постоянное видоизменение информации, в том числе в ходе выполнения различных операций пользователем;
— формирование взаимосвязанной информации на различных устройствах одновременно при передаче данных по каналам связи.

Библиография

Агибалов, Владимир Ю. 2012. *Виртуальные следы в криминалистике и уголовном процессе*. М.: Юрлитинформ.

Батурин, Юрий М. 1991. *Проблемы компьютерного права*. М.: Юридическая литература.

Белкин, Рафаил С. 2000. *Криминалистическая энциклопедия*. М.: Мегатрон XXI.

Белкин, Рафаил С. 2001. *Курс криминалистики*. М.: ЮНИТИ-ДАНА; Закон и право.

Вехов, Виталий Б. 2008. «Криминалистическое учение о компьютерной информации и средствах ее обработки». Дис. … д-ра юрид. наук, ВА МВД России.

Вехов, Виталий Б. 2017. «Электронная криминалистика: понятие и система». *Криминалистика: актуальные вопросы теории и практики: сб. трудов участников междунар. науч.-практ. конф.*, 40–46. Ростов-на-Дону.

Волеводз, Александр Г. 2002. «Следы преступлений, совершенных в компьютерных сетях». *Российский следователь* 1: 4–12.

Голубятников, Севир П. 2017. «Экономическая криминалистика: фантом или реальность». *Вестник Нижегородской академии МВД России* 4 (40): 118–121.

Грачев, Михаил А., Александр М. Грачев. 2015. «Современные проблемы лингвокриминалистики как науки». *Вестник Череповецкого госуниверситета* 1: 26–29.

Колдин, Валентин Я., ред. 2007. *Криминалистика: информационные технологии доказывания*. М.: Зерцало.

Краснова, Людмила Б. 2005. «Компьютерные объекты в уголовном процессе и криминалистике». Автореф. дис. … канд. юрид. наук, Воронежский государственный университет.

Мещеряков, Владимир А. 2001. «Основы методики расследования преступлений в сфере компьютерной информации». Дис. … д-ра юрид. наук, Воронежский государственный университет.

Милашев, Вадим А. 2004. «Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ». Автореф. дис. … канд. юрид. наук, Московский государственный университет им. М. В. Ломоносова.

Нехорошев, Александр Б. 2004. *Компьютерные преступления: квалификация, расследование, экспертиза*: в 2 ч. *Ч. 2. Расследование и экспертиза*. Саратов: СЮИ МВД России.

Поляков, Виталий В., Алексей В. Шебалин. 2013. «К вопросу об использовании понятий "виртуальные следы" и "электронно-цифровые следы" в криминалистике». *Актуальные проблемы борьбы с преступлениями и иными правонарушениями* 11–1: 123–125.

Россинская, Елена Р. 2019a. «Система частной теории информационно-компьютерного обеспечения криминалистической деятельности». *Современные проблемы цифровизации криминалистической и судебно-экспертной деятельности: материалы науч.-практ. конф. с междунар. участием*, 184–191. Москва.

Россинская, Елена Р. 2019b. «Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности». *Вестник Восточно-Сибирского института МВД России* 2 (99): 193–202.

Семикаленова, Анастасия И. 2019. «Цифровые следы и их носители как объекты судебно-экспертного исследования». *Современные проблемы цифровизации криминалистической и судебно-экспертной деятельности: материалы науч.-практ. конф. с междунар. участием*, 212–215. Москва.

Семикаленова, Анастасия И., Ксения А. Сергеева. 2011. «Мобильные телефоны сотовой связи — новые объекты судебной компьютерно-технической экспертизы». *Законы России, опыт, анализ, практика* 12: 89–94.

Смушкин, Александр Б. 2012. «Виртуальные следы в криминалистике». *Законность* 8: 43–48.

Таненбаум, Эндрю, Тод Остин. 2013. *Архитектура компьютера*. Пер. с англ. СПб.: Питер.

Усов, Александр И. 2002. «Концептуальные основы судебной компьютерно-технической экспертизы». Дис. … д-ра юрид. наук, Московский институт МВД России.

Яковлев, Алексей Н. 2018. «Цифровая криминалистика и ее значение для расследования преступлений в современном информационном обществе». *Совершенствование следственной деятельности в условиях информатизации: сб. материалов междунар. науч.-практ. конф.*, 357–362. Минск.

Daniel, Larry E., Lars E. Daniel, Robert Maxwell, Sue Spielman. 2012. *Digital Forensics for Legal Professionals. Understanding Digital Evidence from the Warrant to the Courtroom*. Waltham, MA: Syngress, Elsevier.

Horsman, Graeme. 2019. "Raiders of the lost artefacts: Championing the need for digital forensics research". *Forensic Science International Reports* 1. https://doi.org/10.1016/j.fsir.2019.100003.

Sammons, John. 2015. *The Basics of Digital Forensics. The Primer for Getting Started in Digital Forensics*. Waltham, MA: Syngress, Elsevier.

Статья поступила в редакцию 26 марта 2020 г.;
рекомендована в печать 19 июня 2020 г.

Контактная информация:

Россинская Елена Рафаиловна — д-р юрид. наук; elena.rossinskaya@gmail.com
Семикаленова Анастасия Игоревна — канд. юрид. наук; semiks@mail.ru

Fundamental doctrine of the criminalistics study of computer tools and systems as part of the theory of information and computer support for criminalistics activities*

E. R. Rossinskaya, A. I. Semikalenova

Kutafin Moscow State Law University,
9, Sadovaya-Kudrinskaya ul., Moscow, 125993, Russian Federation

For citation: Rossinskaya, Elena R., Anastasiya I. Semikalenova. 2020. "Fundamental doctrine of the criminalistics study of computer tools and systems as part of the theory of information and computer support for criminalistics activities". *Vestnik of Saint Petersburg University. Law* 3: 745–759. https://doi.org/10.21638/spbu14.2020.315 (In Russian)

The development of digitalization constantly generates new forms of crime, changes in the mechanisms of how they are committed, and concealment. The problem of combating such crimes is transnational in nature. This article considers the difficulties of creating the criminalistics study of computer tools and systems doctrine as part of the theory of information and computer support of criminalistics activities. The authors' negative stance on the issue is indicated as well as the addition of definitions to the name of criminalistics that are related to the emergence of new objects of expertise: "electronic criminalistics", "linguistic criminalistics", "digital criminalistics", and others. The unity of criminalistics as a science having its own subject, system, tasks, and objects is declared. The article substantiates the subject of the theory of criminalistics research of computer tools and systems as a system for gathering significant computer information on the basis of the knowledge of which technical and criminalistics methods, tools, techniques, and methods for identifying, fixing, and seizing evidence and orienting criminalistics information about computer tools are developed. In addition, the theory is based on systems in legal proceedings in criminal, civil, and administrative cases. The objects of this theory are computer tools and systems as well as the search and criminalistics evidence of information contained in them. Based on the doctrine of the criminalistics investigation of computer tools and systems, the foundations of a new area of criminalistics techniques and technology, as a system of scientific principles, are provided. This area centers around recommendations, tools, techniques, and methods designed to collect and study information about computer tools and systems. Digital footprints and the processes of their occurrence, transmission, and transformation in order to obtain evidence in legal proceedings, disclosure, and prevention of crimes, are included.

Keywords: computer crimes, criminally significant information digitalization, digital footprints, computer storage medium, computer information carrier, input/output devices, information transmission devices.

References

Agibalov, Vladimir Iu. 2012. *Virtual traces in criminalistics and criminal procedure.* Moscow, Iurlitinform Publ. (In Russian)

Baturin, Iurii M. 1991. *Problems of computer law*. Moscow, Iuridicheskaia literatura Publ. (In Russian)

Belkin, Rafail S. 2000. *Criminalistics Encyclopedia*. Moscow, Megatron XXI Publ. (In Russian)

Belkin, Rafail S. 2001. *Criminalistics course*. Moscow, IuNITI-DANA Publ., Zakon i parvo Publ. (In Russian)

Daniel, Larry E., Lars E. Daniel, Robert Maxwell, Sue Spielman. 2012. *Digital Forensics for Legal Professionals. Understanding Digital Evidence from the Warrant to the Courtroom*. Waltham, MA, Syngress, Elsevier.

Golubiatnikov, Sevir P. 2017. "Economic Criminalistics: phantom or reality". *Vestnik Nizhegorodskoi akademii MVD Rossii* 4 (40): 118–121. (In Russian)

* The reported study was funded by RFBR according to the research project No. 18-29-16003.

Grachev, Mikhail A., Aleksandr M. Grachev. 2015. "Modern problems of linguistic criminalistics s a science". *Vestnik Cherepovetskogo gosuniversiteta* 1: 26–29. (In Russian)
Horsman, Graeme. 2019. "Raiders of the lost artefacts: Championing the need for digital forensics research". *Forensic Science International Reports* 1. https://doi.org/10.1016/j.fsir.2019.100003.
Iakovlev, Aleksei N. 2018. "Digital criminalistics and its significance for the investigation of crimes in the modern information society". *Sovershenstvovanie sledstvennoi deiatel'nosti v usloviiakh informatizatsii: sbornik materialov mezhdunarodnoi nauchno-prakticheskoi konferentsii*, 357–362. Minsk. (In Russian)
Koldin, Valentin Ia., ed. 2007. *Criminalistics: information technology evidence.* Moscow, Zertsalo Publ. (In Russian)
Krasnova, Liudmila B. 2005. "Computer objects in criminal proceedings and criminalistics". PhD diss. abstract, Voronezhskii gosudarstvennyi universitet. (In Russian)
Meshcheriakov, Vladimir A. 2001. "Fundamentals of the method of investigation of crimes in the field of computer information". Dr. Sci. Diss., Voronezhskii gosudarstvennyi universitet. (In Russian)
Milashev, Vadim A. 2004. "Problems of tactics for searching, fixing and removing traces with unauthorized access to computer information in computer networks". PhD diss. abstract, Moskovskii gosudarstvennyi universitet im. M. V. Lomonosova. (In Russian)
Nekhoroshev, Aleksandr B. 2004. *Computer crimes: qualification, investigation, examination.* 2 parts. *Part 2. Investigation and examination.* Saratov, SIuI MVD Rossii Publ. (In Russian)
Poliakov, Vitalii V., Aleksei V. Shebalin. 2013. "On the use of the concepts of 'virtual traces' and 'electronic-digital traces' in forensics". *Aktual'nye problemy bor'by s prestupleniiami i inymi pravonarusheniiami* 11–1: 123–125. (In Russian)
Rossinskaia, Elena R. 2019a. "The system of a private theory of information and computer support of criminalistics activities". *Sovremennye problemy tsifrovizatsii kriminalisticheskoi i sudebno-ekspertnoi deiatel'nosti: materialy nauchno-prakticheskoi konferentsii s mezhdunarodnym uchastiem*, 184–191. Moscow. (In Russian)
Rossinskaia, Elena R. 2019b. "Theory of information and computer support for criminalistics activity: concept, system, basic laws". *Vestnik Vostochno-Sibirskogo instituta MVD Rossii* 2 (99): 193–202. (In Russian)
Sammons, John. 2015. *The Basics of Digital Forensics. The Primer for Getting Started in Digital Forensics.* Waltham, MA, Syngress, Elsevier.
Semikalenova, Anastasiia I. 2019. "Digital footprints and their carriers as objects of forensic research". *Sovremennye problemy tsifrovizatsii kriminalisticheskoi i sudebno-ekspertnoi deiatel'nosti: materialy nauchno-prakticheskoi konferentsii s mezhdunarodnym uchastiem*, 212–215. Moscow. (In Russian)
Semikalenova, Anastasiia I., Kseniya A. Sergeeva. 2011. "Mobile cellular phones — new objects of forensic computer-technical expertise". *Zakony Rossii, opyt, analiz, praktika* 12: 89–94. (In Russian)
Smushkin, Aleksandr B. 2012. "Virtual traces in criminalistics". *Zakonnost'* 8: 43–48. (In Russian)
Tanenbaum, Andrew, Todd Austin. 2013. *Computer architecture.* Rus. ed. St. Petersburg, Piter Publ. (In Russian)
Usov, Aleksandr I. 2002. "Conceptual foundations of forensic computer-technical examination". Dr. Sci. diss., Moskovskii institut MVD Rossii. (In Russian)
Vekhov, Vitalii B. 2008. "Forensic doctrine of computer information and means of its processing". Dr. Sci. diss., VA MVD Rossii. (In Russian)
Vekhov, Vitalii B. 2017. "Electronic Criminalistics: concept and system". *Kriminalistika: aktual'nye voprosy teorii i praktiki: sbornik trudov uchastnikov mezhdunarodnoi nauchno-prakticheskoi konferentsii*, 40–46. Rostov-on-Don. (In Russian)
Volevodz, Aleksandr G. 2002. "Traces of crimes committed in computer networks". *Rossiiskii sledovatel'* 1: 4–12. (In Russian)

Received: March 26, 2020
Accepted: June 19, 2020

Authors' information:

Elena R. Rossinskaya — Dr. Sci. in Law; elena.rossinskaya@gmail.com
Anastasiya I. Semikalenova — PhD in Law; semiks@mail.ru