УДК 343.148.6 DOI: 10.18698/2541-8009-2019-08-514

СУДЕБНАЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКАЯ ЭКСПЕРТИЗА В СИСТЕМЕ СУДЕБНЫХ ЭКСПЕРТИЗ

А.А. Баюш annabayush@mail.ru
SPIN-код: 3271-9054

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Рассмотрено одно из перспективных направлений судебной экспертизы — судебная компьютерно-техническая экспертиза (СКТЭ), назначаемая уполномоченными органами и должностными лицами. Дано определение СКТЭ как отдельного рода инженерно-технического класса экспертиз и предмета и СКТЭ, перечислены основные отрасли специальных знаний, применяемых экспертами данной области в процессе производства СКТЭ. Также приведена классификация объектов исследования СКТЭ, проанализированы как основные виды СКТЭ, так и их предметные объекты, цели исследования последних. Даны примеры определенных идентификационных и диагностических задач СКТЭ, определены основные перспективные направления СКТЭ.

Ключевые слова

Судебная экспертиза, судебный эксперт, заключение эксперта, судебная компьютерно-техническая экспертиза (СКТЭ), объекты СКТЭ, специальные знания, идентификационные задачи, диагностические задачи

Поступила в редакцию 18.06.2019

Компьютеризация почти всех существующих сфер человеческой жизнедеятельности в совокупности со свободным доступом к различного рода программам и ресурсам в течение продолжительного промежутка времени привели не только к положительным результатам, но и к отрицательным — так называемым компьютерным преступлениям. Ответственность за их совершение регламентирована законодателем в главе 28 Уголовного кодекса Российской федерации (УК РФ) под названием «Преступления в сфере компьютерной информации». Для изучения последствий таких преступлений назначают судебную компьютерно-техническую экспертизу (СКТЭ).

Определение СКТЭ и специальные знания, применяемые в СКТЭ. СКТЭ представляет собой отдельный род судебной экспертизы, относящейся к классу инженерно-технических экспертиз, целями которой являются получение доступа к информации, имеющей доказательственное значение для конкретного расследуемого дела, на представленных эксперту носителях (объектах), а также последующее изучение полученных в ходе такого доступа данных для выявления их роли в расследуемом деле. Ее объектами исследования являются компьютерная техника и (или) компьютерные (электронные) носители информации.

За рубежом существует судебная экспертиза цифровых устройств (*digital forensic*), в которую принято включать уже саму компьютерную экспертизу (*IT forensic, computer forensic*); туда же входят экспертизы мобильных устройств

(*mobile device forensic*), баз данных и компьютерных сетей [1, с. 57], при проведении которых также осуществляется изъятие носителей информации, создание их побитовой (либо посекторной) копии вместе со всем содержимым с последующим исследованием данного содержимого с помощью специализированных автоматизированных информационных систем и справочно-правовых систем, а также иных лицензионных программ, и составляется отчет (заключение эксперта, специалиста) о проделанной работе и собранных в процессе последней доказательствах.

Как известно, основной формой применения специальных знаний в судопроизводстве (конституционном, гражданском, административном и уголовном) является судебная экспертиза. Хотя законодатель не дает точного определения специальным знаниям, под ними следует понимать познания в области науки, техники, промышленного производства, искусства или других специальных отраслей человеческой деятельности [2, с. 9], т. е. это знания в определенных научных направлениях, а также в междисциплинарных областях науки, которые приобретаются после специальной подготовки и профессиональной практики (практических навыков). Так, известный ученый-криминалист А.А. Эйсман давал определение специальным знаниям как знаниям, не распространенным в общественной среде, доступ к которым ограничен [3, с. 91]. Для СКТЭ специальные знания содержатся в таких технических отраслях, как электротехника, программирование, электроника, радиотехника и др. Эти знания также заключаются в умении работать с вычислительной и автоматизированной техникой, информационными и телекоммуникационными системами, оконечным оборудованием[*] и т. п. Применение специальных знаний на практике приносит свои плоды: способствует повышению качества судебных экспертиз, уменьшению числа допущенных в ходе их проведения экспертных ошибок (неверная оценка и неправильные выводы, а в ряде случаев — осознанно недействительное отражение процесса (хода) и результатов исследования, умышленное искажение фактов, умолчание о них), как следствие, это приводит к сокращению решений, которые были вынесены судом ошибочно [4, с. 279].

На практике СКТЭ в целом и ее отдельные виды применяются совместно при проведении почти всех экспертных исследований либо в комплексе со специальными знаниями из других областей науки и техники [5, с. 7]. В условиях всеобъемлющего усложнения многих сфер человеческой деятельности в процессе возбуждения уголовных либо при рассмотрении гражданских и иных дел перед судебным экспертом на разрешение регулярно ставятся комплексные задачи, при анализе которых в качестве объектов фигурируют электронно-

[*] Оконечным оборудованием являются технические средства, предназначенные для передачи и приема сигналов электронной связи, а также управляющие различными пользовательскими линиям услуг связи. Такое оборудование может быть либо стационарным (контрольно-кассовая техника, различного рода терминалы, банкоматы, персональные компьютеры) либо мобильным (смартфоны, телефоны).

вычислительные машины [6, с. 34]. Примерами такого комплексного применения специальных знаний из различных отраслей вместе со специальными знаниями СКТЭ являются:

– применение методов криптографии при решении задач, связанных с получением доступа к зашифрованной информации, обходом установленных паролей, расшифровкой закодированных и частично поврежденных данных [7, с. 1];

– применение специальных знаний из экономической, кредитно-финансовой, бухгалтерской сферы (например, использование услуг онлайн-банка), поскольку сведения о текущем состоянии денежных средств на счетах и о статусе проведенных или готовящихся операциях над последними в электронном виде преобладают над задокументированной информацией;

– комплексное исследование совместно с судебно-технической экспертизой документов в процессе изучения денежных билетов и иных ценных бумаг, поддельных документов и оттисков печатей, расчетных банковских карт, изготовление которых сопряжено с использованием информационных технологий;

– применение специальных знаний судебной видеотехнической и фоноскопической экспертизы при разрешении вопросов о подлинности представленной на исследование видеозаписи, наличии монтажа и т. п. [8, с. 221].

Предмет, объекты СКТЭ и их классификация, виды СКТЭ. Прежде всего необходимо акцентировать внимание непосредственно на самих понятиях «информация» и «компьютерная информация», поскольку последние относятся как к предмету, так и к объекту СКТЭ. В соответствии с федеральным законом № 149 «Об информации, информационных технологиях и о защите информации», под информацией следует понимать любые сведения о ком-либо (лицах) либо о чем-либо (предметах, фактах, событиях, явлениях и процессах) из различных существующих источников такой информации независимо от формы их представления (письменной, устной, визуальной), т. е. информация представлена законодателем как универсальное понятие, отличающееся от привычной для всех дефиниции «информации» в философской интерпретации [9, ст. 2]. Согласно примечанию 1 к статье 272 УК РФ, под компьютерной информацией следует понимать те данные (фактические сведения), которые представляют собой по форме электронные сигналы в независимости от средств, на которых они содержатся (хранятся), обработки и передачи с использованием аппаратно-программных средств [10, п. 1 ст. 272]. В целом данное понятие можно трактовать как фактические данные, которые обрабатываются непосредственно самой информационной (компьютерной) системой либо перемещаются по каналам телекоммуникационной сети (либо в ее пределах) и представляются в доступном для восприятия человека виде, с помощью таких данных можно установить имеющие доказательственное значение для конкретного дела обстоятельства.

Предметом любой судебной экспертизы являются обстоятельства дела, которые исследуются и устанавливаются в уголовном, гражданском, административном и конституционном судопроизводстве с помощью профессиональных познаний, умений и навыков специального субъекта, т. е. эксперта либо специа-

листа, на основе изучения предоставленных материалов дела, а также вещественных доказательств[†] в строго регламентированном процессуальными законами порядке и иными соответствующими нормативными предписаниями законодателя. Стоит отметить, что предмет судебной экспертизы определяется непосредственно совокупностью как характеристик объекта экспертного исследования, так и задачами, методами такого исследования, проводимого в рамках назначенной судебной экспертизы, при этом целесообразно проведение их описания и структурного анализа в отдельности друг от друга, поскольку каждая вышеперечисленная категория обладает присущей только ей спецификой.

Предмет СКТЭ — это обстоятельства и фактические данные о создании, изменении, удалении и использовании информации, включая ее передачу, на материальных (компьютерных) носителях информации, необходимые для получения доказательств по уголовным, гражданским, арбитражным делам и делам об административных правонарушениях, которые устанавливаются с помощью аппаратно-программных средств исследования компьютерной информации и зафиксированных в материалах дела закономерностей (механизмов) ее возникновения и дальнейшего изменения, закономерностей эксплуатации компьютерных носителей такой информации [11, с. 473].

Общим (родовым) предметом судебных компьютерно-технических экспертиз являются все те фактические обстоятельства, которые можно установить на базе изучения отдельных закономерностей разработки и эксплуатации компьютерных средств, позволяющих реализовывать выполнение информационных процессов[‡], которые были описаны в материалах расследуемого дела.

В соответствии со статьей 10 Федерального закона № 73 «О государственной судебно-экспертной деятельности в Российской Федерации» объектами судебной экспертизы могут быть «вещественные доказательства, документы, предметы, животные, трупы и их части, образцы для сравнительного исследования, а также материалы дела, по которому производится судебная экспертиза» [12, ст. 10], а также живые лица, другими словами, таковыми объектами можно считать материальные предметы, которые в соответствии с процессуальным законодательством закреплены и описаны в материалах уголовного (или другого) дела, имеющие значение для данного уголовного дела, так как содержат информацию, необходимую для проведения экспертного исследования с помощью спе-

[†] Вещественные доказательства — это носители доказательственной информации в ее первоначальном состоянии, источники криминалистически значимой информации, которая извлекается экспертом, следователем и др., а также процессуально оформленные и приобщенные к материалам конкретного уголовного дела сведения, полученные из первоисточников и объектов материального мира.

[‡] Информационные процессы — это, в соответствии с ФЗ № 149, различного рода процессы, методы и способы поиска, получения, хранения и последующего проведения операций манипулирования (обработки), отображения и распространения информации, включая сами способы реализации таких процессов и методов.

циальных профессиональных знаний с целью дачи заключения путем решения поставленных перед экспертом задач. Более того, объекты судебной экспертизы принято подразделять по объему, их информативности, по типу носителя информации и по их процессуальному значению [13, с. 182].

Общим объектом СКТЭ является любая вычислительная техника в широком смысле данного слова, а также программные и информационные продукты. Данное понятие формализовано и используется для разграничения отдельных классов судебных экспертиз в системе их классификации.

На основании функционально обеспечивающих составляющих любого компьютерного средства и устройства, т. е. по родовому иначе предметному объекту, различают отдельные классификационные виды СКТЭ, в роли которых выступают следующие экспертизы:

– судебная информационно-компьютерная экспертиза (иначе — экспертиза компьютерных данных), на основе которой производится построение доказательственной базы;

– судебная программно-компьютерная экспертиза, выявляющая закономерности как разработки, так и функционирования определенного программного обеспечения, представляемого на экспертизу для установления фактов объективной действительности по конкретному делу;

– судебная аппаратно-компьютерная экспертиза, изучающая принципы функционирования собственно компьютерно-технических средств конкретной компьютерной системы;

– судебная компьютерно-сетевая экспертиза, с помощью которой исследуются, прежде всего, сетевые информационные технологии [14, с. 379].

Каждая из вышеперечисленных экспертиз обладает своими собственными предметными объектами. Так, объектами информационно-компьютерной экспертизы служит различного рода информация, введенная и функционирующая в вычислительных системах, на носителях и в сетях, а также представленная в виде данных, файлов, которые были предварительно созданы при помощи специально предназначенных для этого программных средств, в виде различных расширений текстового (*.doc*, *.docx*, *.pdf*, *.txt*, *.htm* и др.), графического форматов (*.cdr*, *.tif*, *.bmp*, *.jpeg*, *.gif* и др.), а также форматов электронных таблиц (*.cal*, *.xls* и др.), баз данных (*.db*, *.mdb*, *.dbf*, *.accdb* и др.), системных (*.sys*, *.dll*) и программных файлов (*.exe*, *.com*, *.cmd*, *.bat* и др.).

Объектами программно-компьютерной экспертизы являются, исходя уже из самого названия, отдельные программы и их блоки, целые программные комплексы: различного рода программное обеспечение (операционные системы от определенных производителей), утилиты (иначе — вспомогательные программы), прикладное программное обеспечение в виде приложений общего и специального назначения, служебные системные данные, средства разработки и отладки функционирующих программ.

В роли объектов аппаратно-компьютерной экспертизы выступают следующие материальные носители информации: персональные компьютеры, мобильные телефоны (включая также смартфоны), различного рода планшеты и пери-

ферийные устройства, аппаратно-сетевое оборудование, интегрированные системы, запоминающие устройства различного рода (жесткие диски или HDD/винчестеры, гибкие магнитные дискеты/Floppy-диски, оптические и магнитно-оптические диски, устройства flash-памяти и т. п.), комплектующие ранее перечисленных устройств, различные встроенные системы на базе контроллеров в виде микропроцессоров (иммобилайзер или *immobilizer*[§], транспондер или *transponder*[**], круиз-контроллер или *cruise control* и др.); и др. [15, с. 350].

Объектами судебной компьютерно-сетевой экспертизы являются интернет-технологии, сети связи либо коммуникационно-технические объекты. Более того, в науке об общей теории судебной экспертизы выделяют непосредственный (специальный) объект, предназначенный для внутривидовой классификации (например, системные блоки, пульты управления, носители информации и пр.), а также конкретный объект судебной экспертизы, необходимый для описания конкретного объекта, который характеризуется определенными признаками индивидуальности и неповторимости, экспертного анализа, проводимого в процессе данного исследования (например, системный блок с обозначенной маркой модели, серийным номером и индивидуализирующими признаками в виде каких-либо дефектов или следов эксплуатации).

Отметим, что в теории производства судебной компьютерно-технической экспертизы существует классификация объектов СКТЭ в зависимости от решаемых задач в процессе исследования последних (см. таблицу), исходя из того, что в СКТЭ решаются два типа основных задач — диагностические и идентификационные, которые будут подробно рассмотрены позднее в следующем разделе настоящей курсовой работы. В таблице наглядно отображены основные четыре типа объектов СКТЭ и восемь типов аналитических исследований, при этом диагностические задачи выдвинуты на первый план в виду своей многочисленности и преобладающего характера в области СКТЭ [14, с. 38].

Классификация объектов СКТЭ в зависимости от решаемых задач

Типы объектов		Типы задач	
		Диагностические задачи 1	Идентификационные задачи 2
A	Собственно компьютерно-технические объекты	A-1	A-2
B	Информационно-компьютерные объекты	B-1	B-2
C	Программно-компьютерные объекты	C-1	C-2
D	Коммуникационно-технические объекты	D-1	D-2

[§] Иммобилайзер (*immobilizer*) — электронное средство, обеспечивающее блокировку основных функциональных систем автомобиля (например, системы зажигания, системы подачи топлива и др.), а также предназначенное для предотвращения угона автомобиля.

[**] Транспондер или (*transponder*) — электронное устройство, обеспечивающее как передачу, так и прием входящего сигнала (например, автомобильные транспондеры на дорогах, спутниковые транспондеры).

Цели и задачи исследования СКТЭ и ее отдельных видов. Общей целью СКТЭ представляется исследование компьютерной техники, поиск, изучение и последующее закрепление доказательств по уголовному, гражданскому или арбитражным делам, в соответствии с которой и выделяются следующие общие (основные) задачи СКТЭ:

1) поиск, нахождение, диагностика, классификация информационных объектов либо их частей (установление статуса объекта как компьютерного средства, устройства с последующим получениям доступа к информации);

2) истолкование содержимого информационных объектов либо их фрагментов;

3) комплексный анализ, последующая оценка полученных данных, созданных непосредственно пользователями либо системными программами компьютерного средства;

4) установление функции назначения, определение каких-либо структурных особенностей, признаков (свойств) и иных характеристик, алгоритма и состояния на момент проведения исследования представленного на экспертизу информационного обеспечения;

5) выявление источников и фактов (фактических обстоятельств) создания информационных объектов либо их частей (выявление и изучение роли представленного на экспертизу объекта в расследуемом деле) [16, с. 7].

Целесообразно также определить цели отдельных видов СКТЭ. Так, целью судебной информационно-компьютерной экспертизы является поиск, выявление, исследование и оценка полученной информации (данных), которые были предварительно созданы с помощью специально предназначенных для этого программных средств самими пользователями либо программами и используются для управления информационными процессами в компьютерной системе. Более частные задачи данного вида СКТЭ представляют собой: определение наличия информации на конкретных носителях, представленных на экспертизу, технические и содержательные характеристики данных, степень их защищенности, наличие инфицированности (зараженности вирусами).

Цель программно-компьютерной экспертизы представляет собой исследование: функции назначения, параметров (отдельных особенностей), текущего состояния, логической структуры, требований к программному обеспечению конкретной представленной на такое изучение компьютерной системы, установление фактов объективной действительности по конкретному делу, например, исследование на соответствие выполненных работ по созданию автоматизированной системы требованиям контрактной и технической документации.

Целью аппаратно-компьютерной экспертизы является исследование аппаратной составляющей, а именно ее устройство, принцип работы, соответствие требованиям нормативных актов, а также причин сбоев в функционировании, причин возникновения различных дефектов в устройстве.

Цель компьютерно-сетевой экспертизы представляет собой изучение принципа работы и определение функции назначения средств, работающих на базе какой-либо информационно-сетевой технологии.

Отметим, что под задачей зачастую понимается сама цель, которая достигается лишь при соблюдении конкретных условий, а именно при соблюдении определенных правил решения поставленных задач, поэтому задачи бывают как частными, так и общими. В то время как частные задачи ставятся перед судебными экспертами при назначении конкретного вида экспертизы в виде определенных задач (вопросов), общие задачи относятся к самому классу и роду экспертизы. В СКТЭ решаются два типа основных задач: идентификационные и диагностические. Последние, в свою очередь, являются наиболее распространенными в СКТЭ, что наблюдается и в других родах судебной экспертизы, однако часто судебный эксперт применяет равноценный комплекс методов для решения и тех и других.

Любые идентификационные задачи подразумевают установление тождества представленного на судебную экспертизу объекта. На практике в любой судебной экспертизе, как и в СКТЭ, выделяют следующие виды идентификации:

1) установление источника происхождения самого объекта, представленного на изучение (например, определение установочной версии программного продукта и нахождение его копии в нескольких компьютерных системах, где общий источник происхождения — сам инсталляционный файл), т. е. определение как места, времени, обстоятельств изготовления и комплектации, так и условий эксплуатации, хранения объекта, представленного на исследование;

2) непосредственная (индивидуальная) идентификация объекта (например, установление автора программного продукта, установление наличия/отсутствия конкретного приложения) в системе как одна из наиболее значимых задач;

3) определение групповой принадлежности, т. е. применение метода классификации (например, причисление аппаратного средства, представленного на экспертизу, к классу вычислительных устройств и техники, отнесение исследуемого компьютера к конкретному поколению и модели);

4) идентификация целого по частям, т. е. определение факта принадлежности каких-либо элементов вычислительной техники единому целому и наоборот (например, установление факта относимости конкретного файла к исследуемой единой базе данных);

5) выделение группы по признакам объекта, представленного на исследование (например, классификация и описание характерных отклонений от предыдущих моделей представленного на экспертизу компьютера), т. е. иначе выделение и описание подмножества из множества по определенным признакам, характерным для конкретного объекта, представленного на экспертизу [17, с. 23].

В процессе решения не идентификационных задач, иначе диагностических, совпадающих по содержанию с криминалистической диагностикой, также выделяют следующие задачи:

1) непосредственно диагностические как наиболее распространенные (например, определение фактического состояния компьютерных средств, наличия их повреждений и отклонений от нормы функционирования, зараженности

системы вредоносными компьютерными программами[††], существования каких-либо неисправностей сетевой связи и т. д.);

2) оценочные задачи или ситуационные (например, проверка соответствия созданной программы либо приобретенных аппаратных средств поставленному перед экспертом техническому заданию для разрешения необходимых вопросов исследования);

3) реставрационные (например, восстановление какого-либо текста либо графического изображения на различного рода носителях информации, реконструкция поврежденного либо уничтоженного какого-либо аппаратного средства, представленного на экспертизу);

4) причинно-следственные (причинно-динамические) диагностические задачи (например, определение причин аварийных сбоев, а также отклонений в функционировании систем, устройств, средств программного обеспечения и др.) [17, с. 26].

В настоящее время выделяются несколько перспективных и набирающих обороты направлений СКТЭ, таких как поиск и извлечение интересующей судебного эксперта информации в области СКТЭ данных с твердотельных накопителей данных и устройств их хранения с архитектурой NAND (например, SSD-диски и др.); восстановление и анализ полученных в ходе такого исследования данных, содержащихся в мобильных устройствах (в том числе и поврежденных, не функционирующих, в разобранном виде и др.); поиск уязвимостей и способов защиты iOS устройств, а также изучение их специфических особенностей файловой системы; рассмотрение и изучение новейших объектов в области СКТЭ (например, «беспилотники», иначе дроны, всем известные GPS-навигатор, автоматизированные домашние системы «умный дом» и др.) [28, с. 121–122].

Дальнейшее развитие и внедрение новых открытий и изобретений микроэлектроники, нано- и нейротехнологий, расширение влияния информационных географических систем различного назначения, создание телекоммуникационных и информационных сетей нового уровня диктуют необходимость и условия последующей эволюции СКТЭ как отдельного рода инженерно-технического класса экспертиз. Для реализации успешного противодействия киберпреступности и иным преступлениям в сфере IT. Экспертам в данной области и правоохранительным органам необходимо осуществление как международного взаимодействия в обеспечении информационной безопасности государств, так и взаимного обмена практическим опытом и разработкой единого методического обеспечения (регламента) для производства СКТЭ.

[††] Вредоносная компьютерная программа — отдельный вид информационного программного оружия, предназначенный для реализации несанкционированного изменения, копирования, блокирования, уничтожения непосредственно компьютерной информации, а также осуществляющий обезвреживание средств, обеспечивающих защиту последней.

Литература

[1] Моисеева Т.Ф., ред. Компьютерные технологии в судебно-экспертной деятельности. М., РГУП, 2016.

[2] Безлепкин Б.Т., ред. Комментарий к Уголовно-процессуальному кодексу Российской Федерации (постатейный) с учетом ФЗ № 271-ФЗ, 272-ФЗ, 302-ФЗ. М., Проспект, 2016.

[3] Эйсман А.А., ред. Заключение эксперта (структура и научное обоснование). М., Юрид. лит., 1967.

[4] Чарыков А.В., Чарыков В.И. Электротехническая экспертиза, специальные знания: дискуссия на заданную тему. *Вестник КрасГАУ*, 2014, № 5, с. 278–281.

[5] Усов А.И., ред. Производство судебной компьютерно-технической экспертизы. Ч. V. Актуальные задачи исследования компьютерной информации. М., РФЦСЭ при Минюсте РФ, 2011.

[6] Галинская А.Е. Особенности использования специальных знаний в деятельности сторон и их представителей по делам о правонарушениях в сфере информационных технологий. *Теория и практика судебной экспертизы*, 2017, т. 12, № 1, с. 30–37. DOI: 10.30764/1819-2785-2017-12-1-30-37 URL: https://www.tipse.ru/jour/article/view/25

[7] Баюш А.А. Применение в судебной экспертизе математических методов криптографии и криптоанализа. IX Межд. студ. науч. конф. «Студенческий научный форум 2017». URL: https://scienceforum.ru/2017/article/2017040486 (дата обращения: 22.01.2018).

[8] Россинская Е.Р., ред. Экспертиза в судопроизводстве. М., Проспект, 2016.

[9] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». *Парламентская газета*, 03.08.2006, № 126-127.

[10] Уголовный кодекс РФ от 13.06.1996 № 63-ФЗ (ред. от 29.07.2017). Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954.

[11] Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. М., Норма, 2011.

[12] Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» (с изменениями и дополнениями). Собрание законодательства РФ, 04.06.2001, № 23, ст. 2291.

[13] Баюш А.А. Понятие, сущность и значение судебной экспертизы в условиях современного делопроизводства. *Студенческая научная весна, посвященная 165-летию со дня рождения В.Г. Шухова. Сб. тез. докл. всерос. студ. конф.* М., Изд-во МГТУ им. Н.Э. Баумана, 2018, с. 181–182.

[14] Усов А.И., ред. Производство судебной компьютерно-технической экспертизы. Ч. I. Общая часть II. Диагностические и идентификационные исследования аппаратных средств. М., РФЦСЭ при Минюсте РФ, 2009.

[15] Россинская Е.Р., ред. Судебная экспертиза в цивилистических процессах. М., Проспект, 2018.

[16] Зубаха В.С., Усов А.И., Саенко Г.В. и др. Общие положения по назначению и производству компьютерно-технической экспертизы. М., ГУ ЭКЦ МВД России, 2001.

[17] Усов А.И. Методы и средства решения задач компьютерно-технической экспертизы. М., ГУ ЭКЦ МВД России, 2002.

[18] Хатунцев Н.А. Актуальные направления судебной экспертизы информационных технологий. *Теория и практика судебной экспертизы*, 2018, т. 13, № 1, с. 121–124. DOI: 10.30764/1819-2785-2018-13-1-121-124 URL: https://www.tipse.ru/jour/ article/view/398

Баюш Анна Анатольевна — студентка кафедры «Юриспруденция, интеллектуальная собственность и судебная экспертиза», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Хайретдинов Дмитрий Александрович, старший преподаватель кафедры «Юриспруденция, интеллектуальная собственность и судебная экспертиза», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

FORENSIC COMPUTER TECHNICAL EXAMINATION IN THE SYSTEM OF FORENSIC EXAMINATION

A.A. Bayush
annabayush@mail.ru
SPIN-code: 3271-9054

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

This article considers one of the most promising areas of forensic examination — forensic computer-technical examination (FCTE), appointed by authorized bodies and officials. The definition is given of FCTE as a separate kind of engineering and technical class of examinations and subject and FCTE, the main branches of special knowledge used by experts in this field in the process of FCTE are listed. Also, the classification of research objects of FCTE is given, both the main types of FCTE and the objectives of the study of the latter are analyzed. Examples of specific identification and diagnostic tasks of FCTE are given, the main promising areas of FCTE are identified.

Keywords

Forensic examination, forensic expert, expert opinion, forensic computer-technical examination (FCTE), objects of FCTE, special knowledge, identification tasks, diagnostic tasks

Received 18.06.2019

References

[1] Moiseeva T.F., ed. Komp'yuternye tekhnologii v sudebno-ekspertnoy deyatel'nosti [Computer technologies in forensic activity]. Moscow, RGUP Publ., 2016 (in Russ.).

[2] Bezlepkin B.T., ed. Kommentariy k Ugolovno-protsessual'nomu kodeksu Rossiyskoy Federatsii (postateynyy) s uchetom FZ № 271-FZ, 272-FZ, 302-FZ [Comments to the Russian Federation Code of Criminal Procedure (clause by clause) taking into account FL no. 271-FZ, 272-FZ, 302-FZ]. Moscow, Prospekt Pybl., 2016 (in Russ.).

[3] Eysman A.A., ed. Zaklyuchenie eksperta (struktura i nauchnoe obosnovanie) [Expert report (structure and scientific rationale]. Moscow, Yurid. lit. Publ., 1967 (in Russ.).

[4] Charykov A.V., Charykov V.I. Electrotechnical expertise, special knowledge: the discussion on the given topic. *Vestnik KrasGAU* [The Bulletin of KrasGAU], 2014, no. 5, pp. 278–281 (in Russ.).

[5] Usov A.I., ed. Proizvodstvo sudebnoy komp'yuterno-tekhnicheskoy ekspertizy. Ch. V. Aktual'nye zadachi issledovaniya komp'yuternoy informatsii [Proceeding of computer forensic examination. P. V Actual problems of computer information study]. Moscow, RFTsSE pri Minyuste RF Publ., 2011 (in Russ.).

[6] Galinskaya A.E. The use of special knowledge by the parties and their representatives in cyber crime investigations. *Teoriya i praktika sudebnoy ekspertizy* [Theory and Practice of Forensic Science], 2017, vol. 12, no. 1, pp. 30–37. DOI: 10.30764/1819-2785-2017-12-1-30-37 URL: https://www.tipse.ru/jour/article/view/25 (in Russ.).

[7] Bayush A.A. [Forensic application of mathematical methods in cryptography and cryptoanalysis]. *IX Mezhd. stud. nauch. konf. "Studencheskiy nauchnyy forum 2017"* [IX Int. Student sci. conf. "Student scientific forum 2017"]. URL: https://scienceforum.ru/2017/article/2017040486 (accessed: 22.01.2018). (in Russ.).

[8] Rossinskaya E.R., ed. Ekspertiza v sudoproizvodstve [Expert evaluation in legal process]. Moscow, Prospekt Publ., 2016 (in Russ.).
[9] Federal'nyy zakon ot 27.07.2006 № 149-FZ "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii" [Federal law of 27.07.2006 no. 149-FZ "On information, information technologies and information protection"]. *Parlamentskaya gazeta*, 03.08.2006, no. 126-127 (in Russ.).
[10] Ugolovnyy kodeks RF ot 13.06.1996 № 63-FZ (red. ot 29.07.2017) [The Criminal Code of the Russian Federation of 13.06.1996 no. 63-FZ (ed. of 29.07.2017)]. *Sobranie zakonodatel'stva RF*, 17.06.1996, no. 25, art. 2954 (in Russ.).
[11] Rossinskaya E.R. Sudebnaya ekspertiza v grazhdanskom, arbitrazhnom, administrativnom i ugolovnom protsesse [Forensic enquiry in civil, arbitral, administrative and criminal process]. Moscow, Norma Publ., 2011 (in Russ.).
[12] Federal'nyy zakon ot 31.05.2001 № 73-FZ "O gosudarstvennoy sudebno-ekspertnoy deyatel'nosti v Rossiyskoy Federatsii" (s izmeneniyami i dopolneniyami) [Federal law of 31.05.2001 no. 73-FZ "On federal forensic activity in Russian Federation" (as amended)]. *Sobranie zakonodatel'stva RF*, 04.06.2001, no. 23, art. 2291 (in Russ.).
[13] Bayush A.A. [Conception, contents and meaning of forensic enquiry in conditions of nowdays clerical work]. *Studencheskaya nauchnaya vesna, posvyashchennaya 165-letiyu so dnya rozhdeniya V.G. Shukhova. Sb. tez. dokl. vseros. stud. konf.* [Students science spring dedicated to 165 anniversary of Shukhov V.G. Coll. Abs. Russ. Stud. Conf.]. Moscow, Bauman MSTU Publ., 2018, pp. 181–182 (in Russ.).
[14] Usov A.I., ed. Proizvodstvo sudebnoy komp'yuterno-tekhnicheskoy ekspertizy. Ch. I. Obshchaya chast' II. Diagnosticheskie i identifikatsionnye issledovaniya apparatnykh sredstv [Proceeding of computer forensic examination. P. I. Main part II. Diagnostic and identity hardware study]. Moscow, RFTsSE pri Minyuste RF Publ., 2009 (in Russ.).
[15] Rossinskaya E.R., ed. Sudebnaya ekspertiza v tsivilisticheskikh protsessakh [Forensic enquiry in civilized process]. Moscow, Prospekt Publ., 2018 (in Russ.).
[16] Zubakha V.S., Usov A.I., Saenko G.V., et al. Obshchie polozheniya po naznacheniyu i proizvodstvu komp'yuterno-tekhnicheskoy ekspertizy [General conditions of assignment and production of computer forensics]. Moscow, GU EKTs MVD Rossii Publ., 2001 (in Russ.).
[17] Usov A.I. Metody i sredstva resheniya zadach komp'yuterno-tekhnicheskoy ekspertizy [Methods and tools for solving tasks of computer forensics]. Moscow, GU EKTs MVD Rossii Publ., 2002 (in Russ.).
[18] Khatuntsev N.A. Current trends in forensic information technology. *Teoriya i praktika sudebnoy ekspertizy* [Theory and Practice of Forensic Science], 2018, vol. 13, no. 1, pp. 121–124. DOI: 10.30764/1819-2785-2018-13-1-121-124 URL: https://www.tipse.ru/jour/article/view/398 (in Russ.).

Bayush A.A. — Student, Department of Law, Intellectual Property and Forensic Examination, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Khairetdinov D.A., Senior Lecturer, Department of Law, Intellectual Property and Forensic Examination, Bauman Moscow State Technical University, Moscow, Russian Federation.