Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 7, Is. 1, pp. 20-29, 2016

DOI: 10.13187/vesp.2016.7.20
www.ejournal21.com

UDC 004.02

Basics of Computer Forensics

[1] Igor S. Pantiukhin
[2] Diana N. Shidakova

[1] National research university of information technologies, mechanics and optics, Russian Federation
Kronverkskiy prospekt, 49, Saint Petersburg 197101
Lecturer
E-mail: zevall@ya.ru
[2] National research university of information technologies, mechanics and optics, Russian Federation
Kronverkskiy prospekt, 49, Saint Petersburg 197101
E-mail: dianabingoyo@gmail.com

Abstract

In this article we will take a look at computer forensic expertise. We will try to answer some of the questions that arise during the investigation and hindering the work process. We will consider the basic tasks and those whose solution is better not to put on this kind of expertise and talk about a variety of methods and instruments of working with HDD, Internet resources and data. We will point at some of the most common mistakes made when generating reports on the results of the expertise to help young specialists avoid such oversights. And we will denote the issues facing the modern computer forensics expertise.

Keywords: forensics, computer expertise, methods of computer forensics, mistakes of generating reports.

Введение

В наше время стремительно развиваются компьютерные технологии и Интернет, именно поэтому перед криминалистами все чаще становится задача анализа уже не только физических объектов, но и компьютерной информации, которая занимает особое положение в современном мире. Ее исследование может принести большую пользу при проведении оперативно-розыскных мероприятий, однако возникает целый ряд проблем, связанных с различными аспектами как самой информации, так и методов ее хранения, обработки, передачи и удаления. Исследованием данных проблем и поиском их решений занимается наука форензика.

Современная форензика очень молода, а при сравнении уровня развития данной науки в России с другими странами мы видим, что в нашей стране еще многое предстоит сделать для налаживания механизмов и оптимизации работы в этой сфере. Поэтому зачастую возникают вопросы, которые, казалось бы, давно следует всем знать. Проблемы, встающие перед экспертами, сопряжены с самыми различными аспектами КТЭ: этапы, из которых

должна состоять экспертиза, методы и средства проведения анализа, в какой роли выступает информация в каждом конкретном случае и многими другими. Обзору и поиску решения этих вопросов посвящена данная статья.

Материалы и методы

Основным источником для написания данной статьи стали официальные документы, регламентирующие действия правоохранительных органов при проведении оперативно-розыскных мероприятий, связанных с различными аспектами, как самой информации, так и методов ее хранения, обработки, передачи и удаления, а также результаты последних исследований в области форензики.

Методологическую основу данного исследования составили логические приемы, определения, описания, анализа и синтеза. Также использован общенаучный метод анализа.

Обсуждение

В первую, очередь хотелось бы обозначить моменты компьютерно-технической экспертизы (КТЭ), которые являются очень важными, но иногда упускаются из виду.

1) Экспертами или экспертным учреждением могут быть назначены любой человек или учреждение, которых сочли достаточно компетентными следователь или суд. Специально «экспертное» образование или лицензия не требуются.

2) Существует определенный перечень допустимых для решения КТЭ вопросов, однако настоятельно рекомендуется при формулировке запросов к экспертам пользоваться помощью специалистов в этой сфере.

3) Большинство экспертов настоятельно рекомендуют проводить исследования над копией НЖМД, а если изъятие также проводилось посредством копирования, то совершить его вновь, чтобы имелась нетронутая мастер-копия.

4) Нарушает ли эксперт УПК, используя нелицензионное ПО? Нет, поскольку кодекс не содержит каких-либо требований к инструментам эксперта (специалист по сути даже не обязан указывать примененные инструменты, только методики). При этом нет нарушения авторского права, ибо закон гласит «Свободное воспроизведение произведения [в нашем случае ПО] для целей право применения допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение произведения для осуществления производства по делу об административном правонарушении, для производства дознания, предварительного следствия или осуществления судопроизводства в объеме, оправданном этой целью» (ГК, четвертая часть, ст. 1278)

5) Термин "компьютер" используется, когда концепции применяются к любому устройству, способному хранить цифровую информацию.

Компьютеры могут представлять собой "места преступления" или они могут содержать доказательства в виде писем, интернет-истории, документов и других файлов, относящихся к преступлениям, как убийство, похищение, мошенничество или незаконный оборот наркотиков.

Это не только содержание писем, документов и других файлов, которые могут представлять интерес для исследователей, но и "метаданных" (данные о данных), связанных с этими файлами. Компьютерная экспертиза может выявить, когда документ впервые появился на компьютере, когда был последний раз, когда в прошлом последний раз пользователь сохранял или печатал документ.

С недавних пор коммерческие организации стали использовать КТЭ для расследования таких событий, как:

- интеллектуальная кража собственности;
- промышленный шпионаж;
- мошенничество;
- подделки;
- банкротство;
- несоответствующее рабочему процессу пользование интернетом и прочими ресурсами на рабочем месте;
- несоответствие нормативным требованиям.

Хорошо зарекомендовал себя и широко используется набор руководящих принципов, которые могут направлять следователя в этой области, который называется Association of Chief Police Officers Good Practice Guidefor Digital Evidence (Практический гид для цифровой экспертизы Ассоциации руководства офицеров полиции). Хотя гид направлен на правоохранительные органы Соединенного Королевства, его центральные положения применимы к компьютерной экспертизе в целом.

Четыре основных принципа:

1) Никакие действия не должны изменять данные, хранящиеся на компьютере или носителях, которые впоследствии могут быть использованы в суде.

2) В случаях, когда человек считает необходимым добраться до оригинальных данных, хранящихся на компьютере или носителе информации, он должен быть достаточно компетентен для этого и быть способным дать обоснованное объяснение своих действий и их последовательности.

3) Весь аудит и совершенные действия должны быть зафиксированы, независимый эксперт должен быть в состоянии исследовать эти записи и добиться того же результата.

4) Лицо, ответственное за расследования несет общую ответственность за соблюдение закона и принципов КТЭ [1].

Результаты

Информация в различных аспектах

Поиск аппаратного обеспечения, которое могло служить средством совершения преступления, не является концептуально сложной задачей – то же самое, что и искать оружие – элементы осязаемы и занимают физическое пространство. Все становится сложнее, когда речь заходит о поиске программного обеспечения. Для ясности данный вид поиска следует разделять на две группы:

1) поиск, при котором запрашиваемая информация находится на компьютере в пределах поисковой зоны;

2) поиск, при котором искомая информация хранится на стороннем ресурсе и компьютер поисковой зоны использовался для доступа к ней.

В некоторых случаях, это различие незначительно, и многие типовые задачи могут относиться в равной степени к обеим группам. С другой стороны, есть определенные проблемы, возникающие только тогда, когда компьютер является частью сети. Например, есть законы (Federal Rules of Criminal Procedure 41(a)), требующие, чтобы постановление на обыск выдавалось судом округа, в котором находится имущество, и следователям, возможно, придется получать второе постановление в другом районе, если исследуемый компьютер отправлял данные на удаленный компьютер. И хотя в этом же законе к «имуществу» относят «документы, книги, бумаги и прочие материальные объекты», судами было постановлено, что нематериальное имущество, например, информация, также может быть изъято. Некоторые суды отмечают в сертификатах, что постановление распространяется и на данные (то есть и они могут подлежать изъятию), полученные путем слежки, подслушанные телефонные разговоры, данные, полученные с видеокамер и телескопов, номера телефонов, вызываемых по данной телефонной линии, местоположения. Однако есть суды, не приемлющие поддержки подобных сертификатов.

Информация как контрабанда

Иногда программное обеспечение может стать контрабандой, поскольку люди получают копии, вопреки законам об авторском праве, в этом случае, возможно, целесообразным является изъять ПО, как и любую другую документацию (например, фотокопии мануалов к ПО), поскольку они, вероятно, получены незаконным путем. Иногда производители ПО могут позволить сделать резервную копию купленного продукта, но ее нельзя распространять в силу законов об авторских правах. Списки кодов доступа телефонных карт, пароли правительственных компьютеров также можно считать контрабандой, потому что владение ими запрещено законом [2].

Информация как инструмент преступления

Есть законы, в широком смысле определяющие, что может быть изъято в качестве содействующего средства: «любое имущество, которое было спроектировано и предназначено для использования или было использовано для совершения уголовного преступления», причем подразумевается как материальное, так и нематериальное имущество. Таким образом, некоторые информационные и финансовые документы или инструменты, использованные при совершении преступления, могут быть изъяты. Например, документы, используемые в связи с незаконным статусом чужестранца являются инструментом преступления: фальшивые свидетельства о рождении, банковские документы, записи вакцинации и прочее. Изъятию подлежат также программные средства, созданные для использования в качестве орудий. Иногда предназначение очевидно вытекает из описания (как у программ, предназначенных для кражи паролей или номеров банковских карт), но иногда все не так просто. Однако если должность следователя (агента) компьютерной экспертизы занимает рассудительный (опытный или заработавший доверительную репутацию) человек, суд обычно прислушивается к его суждениям в этом вопросе. Таким образом, очень важны конкретные обстоятельства каждого дела. Например, если агент расследует дело, и знает, что данная программа работает только на одном компьютере, он, очевидно, поймет, что исследование второго компьютера, находящегося в зоне поиска, не имеет смысла. Однако если от надежного источника агент узнал, что подозреваемый хвастался расширением возможностей программы или работал в этом направлении, агент возьмет на проработку и вторую машину [2].

Информация как улика

Некоторые суды пришли к выводу, что когда дело доходит до документов, очень сложно разделить две категории: улики (свидетельства о преступлении, то, что поможет проанализировать преступника или его действия и так далее) и средства преступления. Некоторые эксперты утверждают, что простые доказательства в одном деле, могут оказаться средствами преступления в другом. Сейчас полезно признать, что в большинстве случаев документы и иная информация, соединяющие преступника и его преступления, следует рассматривать в качестве улики, а не средства. Например, рецепт с незаконной выпиской морфина пациенту, выписанный врачом, был классифицирован в качестве доказательства, а не орудия. Это иллюстрирует, какого типа документы могут быть изъяты в качестве доказательств: записи, которые раскрывают работу преступной деятельности в течение долгого времени. Другие примеры включают в себя списки клиентов наркоторговцев, телефонные счета хакеров, мошенничающих в интернете, планы на хищение или совершение иного рода преступлений. Эти улики могут быть в бумажном виде, в форме книг, в самом компьютере или на съемном электронном носителе. Как и доказательства другого рода, документы могут быть изъяты, если они помогают раскрыть намерения подозреваемого, или подтверждают обоснованность подозрений, даже если не относятся непосредственно к совершению преступления [5].

Результаты

Этапы экспертизы

Условно можно разделить КТЭ на 6 этапов:

1) Готовность к происшествиям

Со стороны потерпевшего это означает, что системы аудита начнут работу прежде, чем будет совершено преступление, со стороны экспертов – это проверка работоспособности оборудования, его актуальности, ознакомление с законами, повышение квалификации.

2) Оценка

Получение инструкций, разъяснение их, анализ рисков, распределение ролей и ресурсов.

3) Сбор

Если сбор элементов с места преступления будет осуществляться на месте, а не в компьютерной лаборатории судебной экспертизы, то этот этап будет включать в себя идентифицирование и сбор устройств, которые могут хранить доказательства. Интервью с персоналом, который может хранить информацию, важную для рассмотрения (ею могут

обладать конечные пользователи компьютера, менеджеры, лица, ответственные за предоставление компьютерных услуг, системные администраторы) также входит в эту часть экспертизы.

Этап сбора также включает в себя маркировку и расфасовку доказательных элементов в пронумерованные, защищенные от несанкционированного вскрытия мешки. Все это должно быть безопасно транспортировано в лабораторию эксперта.

4) Анализ

Непосредственно экспертиза, проверка оборудования, программного обеспечения, поддержка диалога с пострадавшим(-и).

5) Презентация

Эксперт представляет структурированный отчет о своих выводах, использованных средствах и методах, отчет должен быть написан с расчетом на то, что его поймет читатель, не сведущий в технической терминологии.

6) Обзор

Как и первую стадию, этот этап иногда упускают из виду. Подобное пренебрежение, возможно, вытекает из нежелания лишних затрат на неоплачиваемую работу или из необходимости скорее приступить к следующей экспертизе. Однако включение данного этапа в каждый проект поможет повысить качество экспертизы, сэкономить деньги и сделать более эффективными последующие работы. Эта стадия есть краткий обзор того, что пошло не так, а что сыграло на руку потерпевшему; любые уроки, полученные экспертом в ходе данного исследования, могут найти отражение на этом этапе [3].

Решаемые задачи, средства и методы КТЭ

КТЭ решает задачи типа:

1) Общей характеристики ПО, представленного на экспертизу

2) Системные или прикладные программные средства данного ПО, а также их различные свойства (тип, версия, явные или удаленные)

3) Есть ли признаки контрафактности

4) Разработчики (авторы) тех или иных программных средств или данных

5) Параметры данных

6) Наличие определенных средств для реализаций конкретных задач

7) Наличие недокументированных функций у программных средств

8) Определение методов реализации защиты данных на компьютере

9) Определение алгоритмов ПП (программных продуктов)

10) Модифицировались ли данные и, если да, то какой вид имели до модификации

11) Какова хронология изменений

12) Каким способом произведены изменения (умышленно, вредоносная программа, сбой ПО или аппаратуры)

13) Нахождение враждебных функций в программе, восстановление хронологии ее использования и результатов ее работы

14) Поиск информации в том числе в неявном (удаленном, скрытом, зашифрованном виде)

15) Поиск следов различного рода деятельности

16) Восстановление хронологии событий

17) Оценка квалификации и личных особенностей пользователя, его психологическая оценка (настройки, переписки, оформление, закладки музыка, фотографии и прочее), однако стоит учитывать, что эта оценка носит вероятностный характер.

КТЭ не решает задачи типа:

1) Контрафактность или лицензионность – косвенные признаки, которые могут быть обнаружены в ходе экспертизы не является прямым доказательством, поэтому однозначного ответа на этот вопрос специалист дать не может.

2) Стоимость – технический специалист не может определить ни стоимость, ни ущерб потерпевшему, данные вопросы носят экономический характер, специалист может лишь указать на особенности ценообразования на рынке программных продуктов.

3) Правомерность доступа – эксперт не может определить этот факт, поскольку это является юридическим вопросом, однако эксперт способен определить ряд признаков

указывающих на неправомерность (являются ли данные, к которым производился доступ, секретными, была ли информация защищена обладателем определенными средствами, производился ли «обход» этих средств со стороны подозреваемого).

4) Оценка содержания – специалист по КТЭ может найти сообщения и документы требуемой тематики, но не имеет права оценивать их содержимое.

Методы КТЭ.

К методам можно отнести: исследование файловых систем, копирование носителей, хэш-функции для установления тождественности, исследование файлов и другие.

Опишем несколько подробней указанные методы.

Исследование файловых систем. Скрытую информацию можно обнаружить в: *свободных блоках* (при стирании файлов стандартными средствами кластеры, содержащие тело файла, отмечаются как свободные, но запись производится не сразу, и какое-то время эти в этих блоках частично хранится информация об удаленных или модифицированных файлах), *хвосты файлов* (тело хранится в целом числе блоков, и если файл не заполняет полностью последний блок, то, вероятно, в нем (блоке) будут находиться прежде записанные данные), *свободные специальные разделы* (неиспользуемые сегменты диска, которые также хранят записанные раньше данные), иногда есть непредназначенные для пользователей области, например, *HostProtectedArea (HPA)* (при использовании определенного вида ПО в них могут записывать скрытую информацию).

Копирование носителей. Экспертиза любых носителей должна проводится не на оригинале, а на копии. При копировании, чтобы перенеслись даже скрытые данные, советуется использовать не стандартные средства операционной системы, а специализированные, разработанные для подобных целей программы, поскольку копирование должно быть произведено на уровне контроллеров (bit stream copiyng). Для исследования жесткого диска можно также использовать считывание внешними средствами, что позволит снять остаточную намагниченность или намагниченность на границах магнитных дорожек. Это очень действенный метод исследование, поскольку восстановлению подлежат даже многократно перезаписанные файлы, однако такое исследование подразумевает больших денежных вложений.

Хэш-функции для удостоверения тождественности. Часто для удостоверения целостности и неизменности данных на носителе используются однонаправленные хэш-функции, их можно даже заносить в протокол (если например перед копированием или изъятием НЖМД, есть желание убедиться что он доедет до места экспертизы, не утратив целостность). Обычно в качестве хэш-функций используются алгоритмы MD5 и SHA-1, они имеют достаточную стойкость, хотя есть и гораздо более стойкие хэш-функции (SHA-256, SHA-512, WHIRPOOL). Однако в России указанные алгоритмы не являются стандартными. У нас имеется собственный стандарт для алгоритма хэш-функций – ГОСТ Р-34.11. Проблема в том, что реализация хеширования – криптографическая техника, следовательно, ее реализация – регламентируется нормативными актами и подлежит обязательной сертификации, аттестации и лицензированию. При снятии копии диска в полевых условиях нет возможности провести аттестацию системы, поэтому нельзя ссылаться на совпадение значений хэша в качестве доказательств неизменности данных.

Исследование файлов. Файлы несут много служебной и сопровождающей информации, которая не видна для пользователя, что может послужить очередным доказательством, обнаруженным при экспертизе.

Современные методы КТЭ также можно структурировать, разделив по объектам исследований: методы исследования аппаратных средств (методы алгебры логики, методы синтеза цифровых узлов, архитектурные методы микропроцессоров, методы построения БИС и БИС памяти, методы обработки аудио- и видеосигналов), методы исследования программных средств (методы исследования исходных текстов, методы изучения алгоритмов программ, методы исследования загрузочных модулей (исполняемых программ) и методы исследования информации (данных) (методы поиска и доступа к данным (контекстный поиск, конвертирование данных), топологические методы, методы коммутации и маршрутизации) и другие.

В последнее время весьма распространенным методом сохранения своих данных стало их шифрование. Нынешние методы криптографии считаются довольно сильными. В некоторых устройствах функции шифрования являются встроенными. Вот перечень основных факторов, помогающих экспертам добраться до информации (иными словами, основные ошибки зашифровывающих):

1) примитивные методы шифрования;

2) недостаточная длина ключей и паролей;

3) выбор осмысленных слов или фраз в качестве ключей сокращает время перебора; удаление исходных файлов, после их зашифровки, стандартными средствами ОС; записывание пароля;

4) сохранение имен файлов, содержащихся в шифрованных папках, в оригинальном виде (в шифрованных архивах имена файлов часто не шифруются, отсюда можно выявить соответствие имя-размер и, например, найти где-нибудь оригинал);

5) в оперативной памяти может храниться исходная информация или ключи, даже если не будет возможность сделать дамп, можно найти способы для извлечения данных; кейлоггеры (средства, помогающие программно или аппаратно отследить пароль).

Поиск информации при КТЭ. На носителе, помимо файла, хранится различного рода информация о нем, и даже после его удаления, можно доказать его наличие в прошлом.

Такого рода непрямыми уликами могут служить:

1) копии тела файла и их фрагменты в секторах диска, которые считаются свободными; заголовок файла в каталоге, а также во всех копиях этого каталога в свободных секторах диска;

2) упоминания имени и других атрибутов в логах тех или иных прикладных программ; временные копии файла, которые создаются программами-редакторами; промежуточные копии файла и его атрибутов, образующиеся при его пересылке при помощи эл. почты;

3) архивные копии диска, его копии его отдельных каталогов, реестра, электронной почты и других объектов;

4) иконки, используемые в операционной системе и некоторых вьюверах для ознакомления с перечнем файлов.

При работе с интернет-ресурсами к методам можно причислить изучение архивов электронной почты, реконструкция просмотра веб-страниц, использование кэша, cookies (средства реконструкции веб-серфинга по данным браузера реализуют программы EnCase, FTK, Pasco, так же ее можно провести вручную).

При оценке найденного эксперту необходимо учесть и зафиксировать в отчете вероятности попадания той или иной информации на компьютер: вирусы, оставляющие «черные ходы» для недоброжелателей, использование компьютера иными пользователями, незащищенные порты при изъятии и прочее.

Исследование программ. Исследование кода, обнаружение в коде тех или иных алгоритмов, сравнение программ, причисление их к вредоносным и прочее. Советуется организовывать комплексный подход: использовать услуги не только специалиста по КТЭ, но и программиста.

К методам к КТЭ можно также отнести исследование мобильных устройств (анализ резервных копий смартфона, расшифровка баз таких приложений как WhatsApp, восстановление данных на девайсах, исследование R-UIM и USIM карт), исследование видеорегистраторов (восстановление и экспертиза данных), фото- и видеокамер и многое другое [1].

Ошибки в отчетах

Стоит указать одни из часто допускаемых ошибок в формировании отчетов по КТЭ:

1) неверно (некорректно) составленные вопросы к КТЭ

2) содержащиеся в формулировке вопросов неявные утверждения («Правда, что эта программа вредоносна?»)

3) проведение техническим экспертом оценочной деятельности (экономическая оценка, явная настроенческая оценка, высказывание допущений нетехнического характера)

4) проведение техническим специалистом экспертизы по установлению автора (правообладателя)

5) использование экспертом сравнительных образцов, полученных из неуказанного источника, вопреки установленному УПК порядку (все объекты экспертизы должны поставляться, специалист не может находить «образцы» самостоятельно)

6) путаница вредоносных программ и программ обхода ТСЗАП (это можно отнести к некомпетентности специалиста и его неразборчивости в терминах) [1].

Вопросы, стоящие перед компьютерной экспертизой

Их можно разделить на три основные группы: правовые, административные и технические.

1) Правовые

Юридические тонкости могут запутать или отвлечь от результатов экспертизы.

2) Административные

Используемые стандарты – есть множество стандартов и принципов КТЭ, некоторые из которых являются общепринятыми, причины этого: нормативные органы привязаны к определенному законодательству; стандарты направлены либо на форензику для правоохранительных органов, либо на коммерческую форензику, но не оба этих пункта; большая цена присоединения к профессиональным органам отговаривает практикантов от присоединения.

Практика – во многих странах нет квалификационных органов, проверяющих компетентность и добросовестность экспертов.

3) Технические

Шифрование – проблема: найти ключ.

Увеличение дискового пространства – проблема: необходима достаточная вычислительная мощность для обработки больших объемов данных.

Новые технологии – проблема: ни один эксперт не может быть экспертом во всех областях, технологии экспертизы развиваются медленнее, чем пользовательские инструменты.

Анти-форензика – действия, направленные на срыв экспертизы, проблема: маскировка информации, уничтожение, засорение лишними данными [3].

Заключение

Таким образом, можно сделать вывод, что в форензике существует много важных нюансов, которые в силу слабой подготовки или неопытности специалисты часто опускаются при проведении экспертизы. Это связано с тем, что данная область еще недостаточно изучена, и нет четких документов, следуя которым любой специалист хорошо знал, что ему делать и в каком направлении двигаться. Однако все больше публикуется работ по исследованию методов и средств КТЭ, поиску оптимальных путей решения ее задач. В частности и данная статья описывает наиболее значимые для специалистов моменты проведения экспертизы.

Основное, что надо помнить – информация может выступать в качестве контрабанды, инструмента преступления или улики. Всю экспертизу условно можно разделить на 6 этапов, каждому из которых следует уделить достаточное внимание. Провести экспертизу не единственная задача специалиста, качественно составленный отчет также важен для результатов следствия. Основные вопросы, стоящие перед КТЭ, можно разделить на административные, правовые и технические.

Примечания:

1. Н.Н. Федотов «Форензика. Компьютерная криминалистика», издательство «Юридический мир», Москва, 2007

2. http://www.computerforensicsworld.com/modules.php?name=Content&pa=showpage&pid=3

3. https://forensiccontrol.com/resources/beginners-guide-computer-forensics/

4. http://www.kroll.com/en-us/cyber-security/cyber-crime-investigations/computer-forensics

5. http://www.computerforensics.com/choose-forensics.html

6. http://computer-forensics-lab.org/lib/Библиотека

7. Брайан Кэрриэ. Криминалистический анализ файловых систем. СПб., Издательство «Питер»: 2007

8. The Artof Memory Forensics M. Ligh, A. Case, J. Levy, A. Walters

9. Харлэн Карви. Криминалистическое исследование Windows

10. Крис Поуг, Кори Алтеид, Тодд Хаверкос. Криминалистическое исследование Unix и Linux.

11. Федор Коржов. Совместное использование программно-аппаратного комплекса PC3000 и Encase v6.10/v4.20 при проведении СКТЭ. ГУ Омская лаборатория судебной экспертизы Минюста России, 2012.

12. Ростовцев А.В. Правовые, организационные и методические вопросы использования ЭВМ при производстве судебных физических и химических экспертиз. М.: Московский университет МВД России, 2012.

13. Поляков В.В. Судебная компьютерно-техническая экспертиза средств мобильной радиосвязи. //Журнал «Известия Алтайского государственного университета. Выпуск № 2 (82), 2000.

14. Усов А.И. Концептуальные основы судебной компьютерно-технической экспертизы. Диссертация на соискание ученой степени д-ра юрид. наук: специальность 12.00.09: Москва, 2002.

15. Яковлев А.Н. Теоретические и методические основы экспертного исследования документов на машинных магнитных носителях информации. Диссертация на соискание ученой степени кандидата юридических наук, специальность 12.00.09. Саратовский юридический институт МВД, 2000.

References:

1. N.N. Fedotov "Forensic. Computer Forensics ", publishing house " Yuridicheskiy mir ", Moscow, 2007

2. http://www.computerforensicsworld.com/modules.php?nam..

3. https://forensiccontrol.com/resources/beginners-guide..

4. http://www.kroll.com/en-us/cyber-security/cyber-crime..

5. http://www.computerforensics.com/choose-forensics.html

6. http://computer-forensics-lab.org/lib/Библиотека

7. Brian Carrier “ File System Forensic Analysis”, publishing house “Piter”, St. Petersburg, 2007

8. M. Ligh, A. Case, J. Levy, A. Walters , “The Art of Memory Forensics”

9. Harlan Carvey, “Windows Forensic Analysis”

10. Hris Pogue, Cory Altheide, Todd Haverkos, “UNIX and Linux Forensic Analysis”

11. Fedor Korzhov, “Joint use hardware and software PC 3000 and Encase v6.10 / v4.20 during computer-technical expertise”, SU Forensic Laboratory Russian Ministry of Justice in Omsk, 2012.

12. A.V. Rostovtsev, “The legal, organizational and methodological issues of using computers in the production of court physical and chemical examinations.”, M.: Moscow University of the Ministry of Interior of Russia, 2012.

13. V.V. Polyakov, “Forensic computer-technical expertise of mobile radio communications” // Journal "News of the Altai State University, №2 (82), 2000.

14. A.I. Usov, ”Conceptual bases of computer forensic and technical expertise. The thesis for the degree of Dr. jurid. Sciences: specialty 12.00.09 ”, Moscow, 2002.

15. A.N. Yakovlev, “Theoretical and methodical bases of expert research of papers on machine magnetic media. The thesis for the degree of candidate of legal sciences, specialty 12.00.09”, Saratov legal institute of the Ministry of Interior, in 2000.

УДК 004.02

Основы компьютерно-технической экспертизы

[1] Игорь Сергеевич Пантюхин
[2] Диана Нурчуковна Шидакова

[1] Национальный исследовательский университет информационных технологий, механики и оптики, Российская Федерация
197101 Санкт-Петербург, Кронверкский проспект, 49
Преподаватель
E-mail: zevall@ya.ru
[2] Национальный исследовательский университет информационных технологий, механики и оптики, Российская Федерация
197101 Санкт-Петербург, Кронверкский проспект, 49
E-mail: dianabingoyo@gmail.com

Аннотация. В данной статье мы рассмотрим такой раздел форензики, как компьютерно-техническая экспертиза. Мы попробуем ответить на некоторые вопросы, возникающие в ходе следствия и тормозящие процесс работы. Рассмотрим основные задачи КТЭ и те, решение которых лучше не возлагать на данный вид экспертизы. Поговорим о разнообразных методах и средствах работы с носителями, Интернет-ресурсами и данными. Обозначим некоторые из самых распространенных ошибок, допускаемых при формировании отчетов по результатам компьютерно-технической экспертизы, что нацелено помочь начинающим специалистам избежать подобных упущений. Озвучим вопросы, стоящие перед современной компьютерно-технической экспертизой.

Ключевые слова: форензика, компьютерно-техническая экспертиза, методы КТЭ, ошибки формирования отчетов.