УДК 004.083.72 DOI: 10.18698/2541-8009-2018-02-242

РАБОТА ЭКСПЕРТА ПРИ ИССЛЕДОВАНИИ HDD-ДИСКОВ

Р.Р. Джандарова RukishaDzhandarova@yandex.ru
SPIN-код: 3003-8260

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

Аннотация

Рассмотрены понятие и история появления HDD-дисков, этапы развития HDD-технологий, описан принцип их работы. Проиллюстрировано логическое строение жесткого диска и строение его сектора. Представлено экспертное исследование с помощью программных комплексов Encase Forensic и PC-3000 UDMA, а также этапы работы эксперта с жестким диском и способы удаления информации с него. Проведено диагностическое исследование жесткого диска с помощью программы SMART Vision HDD. Обозначены перспективы дальнейшего развития и использования таких дисков.

Ключевые слова

HDD-диск, компьютерно-техническая экспертиза, программный комплекс Encase Forensic, программный комплекс PC-3000 UDMA, диагностическое исследование HDD-диска, SMART-технология

Поступила в редакцию 27.11.2017

Введение. Рынок услуг, связанных с вопросами хранения данных, за последние несколько лет значительно изменился. Известно, что производство и поставки жестких дисков зависят от числа продаж компьютеров: если продажи низкие, то это отрицательно сказывается на реализации этого вида устройств [1]. Внешний HDD (жесткий диск) по-прежнему остается наиболее популярным средством хранения данных. Как правило, внешние жесткие диски очень удобны в качестве переносных устройств, поскольку легки, компактны и позволяют хранить всю необходимую информацию.

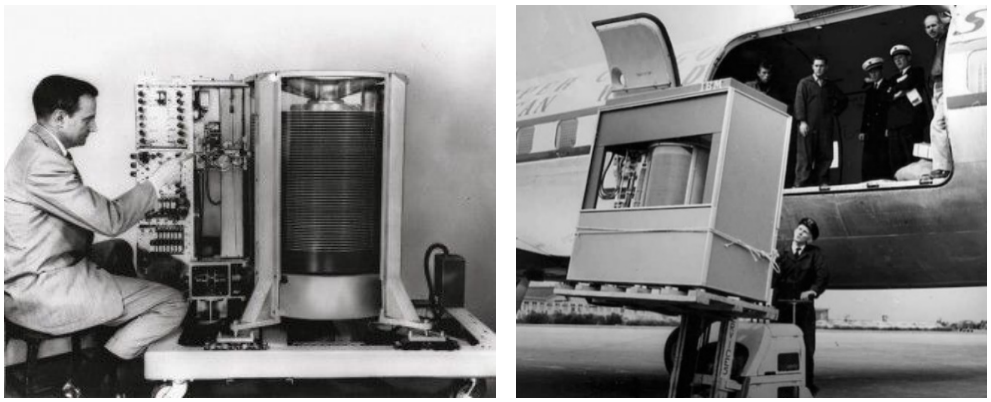
Описание исследуемого устройства. HDD-диск, или жесткий диск, или накопитель на жестких магнитных дисках — это постоянное запоминающее устройство компьютера и основное место хранения данных (операционной системы, программного обеспечения и др.) [2]. Необходимая информация в нужное время считывается с жесткого диска процессором и обрабатывается. Результат обработки может быть записан на жесткий диск. HDD, в отличие от оперативной памяти, не считается энергозависимой памятью, то есть после отключения от компьютера информация, ранее сохраненная на этом накопителе, не будет утрачена. Внешний вид устройства изображен на рис. 1.

Первый жесткий диск IBM 350 DiskStorageUnit (рис. 2) был представлен миру в сентябре 1956 года компанией IBM. Он мог хранить всего 5 Мб информации (приблизительно размер одного mp3-файла), представлял собой шкаф шириной 1,5 м, высотой 1,7 м и толщиной 0,74 м, весил почти тонну и стоил по современным меркам 300 000 долл. [3, 4].

а *б*

Рис. 1. Общий вид (*а*) и вид HDD с поднятой крышкой (*б*)

Для персонального компьютера IBM PC XT был разработан жесткий диск объемом 10 Мб, который имел 30 дорожек по 30 секторов в каждой дорожке. По аналогии с маркировкой многозарядного карабина 30/30 фирмы Winchester, жесткие диски стали именовать винчестерами [5].



а *б*

Рис. 2. Первый жесткий диск IBM 350 DiskStorageUnit (*а*) и его транспортировка (*б*)

В 1979 году в Дублине Аланом Шугартом и Финисом Коннером была основана компания Shugart Technology, ставшая крупнейшим производителем жестких дисков. Во избежание путаницы с другой компанией вскоре она была переименована в Seagate Technology. В этом же году компания выпустила свой первый продукт — жесткий диск ST-506 объемом 5 Мб, в 1980 году — новую модель ST-412 объемом 10 Мб.

На пути к успеху компания Seagate Technology поглотила многие известные бренды. Так, например в 1985 году Финис Коннер, участвовавший в разработке первого жесткого диска, основал собственную компанию Conner Peripherals, а уже в 1996 году она вошла в состав Seagate Technology. В 1989 году был выкуплен бизнес по производству жестких дисков Control Data Corporation/Imprimis, в 2006 году — Maxtor, в 2011 — объединены Samsung и Seagate [6].

В развитии технологии производства HDD можно условно выделить пять этапов [7]:

1) 1956–1979 годы — применение традиционных головок для записи и воспроизведения данных;

2) 1979–1991 годы связывают, прежде всего, с использованием тонкопленочных головок;

3) 1991–1995 годы — с использование магниторезистивных (Magneto-Resistive, MR) головок;

4) 1995–2000 годы — с применением супермагниторезистивных головок (GiantMagneto-Resistive, GMR). Уменьшен магнитный зазор в записывающей головке и повышена чувствительность головки чтения благодаря использованию материалов с повышенным коэффициентом магниточувствительности;

5) с 2000 года по настоящее время преимущественно используют модели с антиферромагнитной связью (AntiferromagneticCoupling, AFC).

Принцип работы HDD. При включении жесткого диска сначала происходит считывание с накопителя служебной информации (ее также называют нулевой дорожкой), которая содержит сведения о диске и его состоянии. Если сектора со служебной информацией повреждены, то жесткий диск не будет работать. Затем начинается непосредственно работа с данными, расположенными на диске. Частицы ферромагнитного материала, которым покрыта поверхность диска, под воздействием магнитной головки условно формируют биты — единицы хранения цифровой информации [8].

Данные на жестком диске распределены по дорожкам, представляющим собой кольцевую область на поверхности одного магнитного диска. Дорожка, в свою очередь, поделена на кластеры. Один кластер образуют несколько секторов. Сектор — это минимальная логическая единица на жестком диске. Обычно, говорят, что размер сектора равен 512 байт. На самом же деле размер сектора составляет 571 байт, 59 из которых занимает служебная часть, а 512 используют для записи информации. Дорожки, расположенные друг под другом на жестком диске, образуют логический элемент — цилиндр (рис. 3). Нумерация дорожек и цилиндров начинается с нуля, а нумерация секторов на дорожке — с единицы.

Вначале сектора записывается его заголовок, который включает в себя адрес сектора CHS, первую циклическую контрольную сумму CRC и первую зарезервированную область (рис. 4). Адрес сектора содержит информацию о номере цилиндра (cylinder), номере дорожки (head) и номере сектора (sector). Зарезервированная область после CRC нужна для того, чтобы создать резерв времени для расчета CRC и для того, чтобы контроллер определил целостность инфор-

мации. За зарезервированной областью следует 512 байт данных, за данными сектора — вторая циклическая контрольная сумма ECC, которая нужна для контроля целостности данных, записанных в область данных. После ECC располагается вторая зарезервированная область, необходимая для создания резерва времени, который позволит контроллеру закончить запись в области данных сектора и застраховать от перезаписи начало следующего сектора.

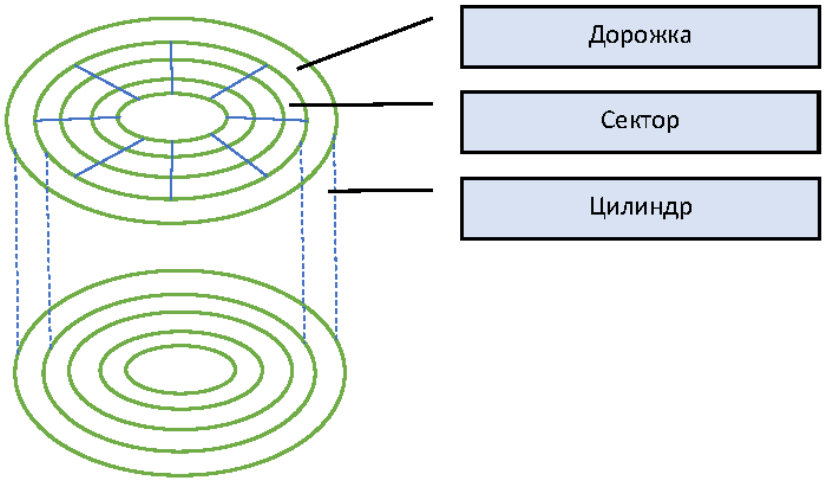


Рис. 3. Логическое строение HDD

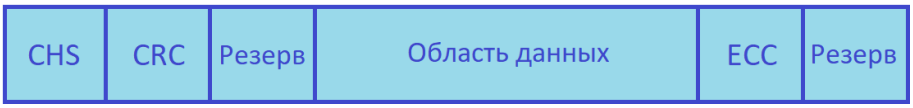


Рис. 4. Строение сектора HDD

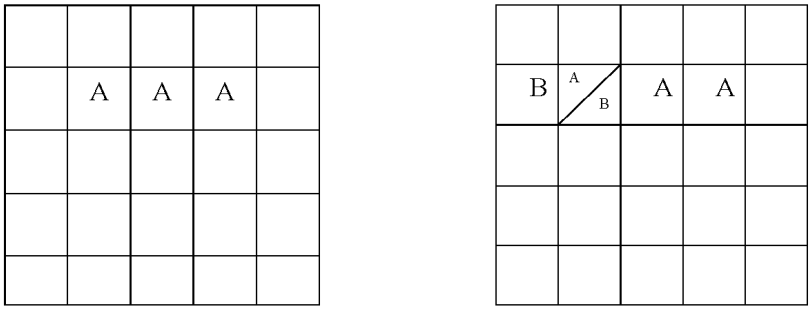
Вся эта информация записывается на этапе изготовления диска при низкоуровневом форматировании, предназначенном для геометрической разметки магнитной пластины.

Применение HDD в экспертной деятельности. Нередко в качестве объектов компьютерно-технической экспертизы к эксперту поступают периферийные устройства, в том числе жесткие диски.

Первым шагом в исследовании такого объекта является снятие образа («побитовой копии») с носителя, поскольку содержимое исследуемого носителя [9] должно быть «нетронутым». Для создания образа можно использовать программу FTKImager компании AccessData. Далее эксперту необходимо проверить хэш-значение. Если хэш-значение образа совпадает со значением оригинала, то эксперт может быть уверен, что исследуемая копия «побитово» соответствует оригиналу.

Существуют специализированные комплексы для работы с жесткими дисками, поступившими на экспертизу, например PC-3000 UDMA, Encase Forensic Software и др.

Многие пользователи считают, что информацию из устройства можно полностью удалить путем нажатия клавиши «Delete» и удаления ее из «Корзины», но это не так. Как уже было описано выше, на дисковых запоминающих устройствах информация хранится в секторах. Для того чтобы определить какой именно сектор занимает файл, нужна таблица размещения файлов (рис. 5, *а*). В нее записывается вся информация о файле: имя, размер и т. д. Когда пользователь помещает файл А в корзину, ничего не происходит, а когда помещает файл А в корзину и удаляет его, в секторе он физически остается, а в журнале ставится метка о том, что файл А удален, и дается информация, что сектор, где был файл А, свободен.



а *б*

Рис. 5. Таблица размещения файлов (*а*) и то же после перезаписи (*б*)

В случае когда файл В при записи на носитель частично перекрыл удаленный файл А, то файл А считают перезаписанным и данные восстановлению не подлежат (рис. 5, *б*). Файл А в секторе, куда не попал файл В, считают удаленным, но его можно восстановить.

Encase Forensic — это программный комплекс для проведения компьютерно-технической экспертизы, который позволяет осуществлять поиск и анализ данных имеющихся на устройстве, в том числе и удаленных. На базе Encase эксперт может создавать собственные инструменты для работы с программой с помощью скриптов. Данный программный комплекс имеет удобный графический интерфейс, состоящий из четырех подвижных окон (рис. 6). В первом окне *1* расположена древовидная структура каталогов. При выборе папки, она открывается во втором окне *2*, которое имеет несколько колонок. К примеру, в колонке Name отображаются наименования файлов. В колонке Filter можно увидеть выбранные пользователем условия, Signature — соотносит файл с определенной категорией. Если тип файла был изменен, например, с txt на jpeg, то в колонке FileExt (расширение файла) можно увидеть txt, а в Signature будет записано jpeg, поэтому всегда следует проверять значение сигнатуры.

В третьем окне *3* представлена структура файла в нечитаемом виде (на мониторе отображаются различные знаки вместо текста). В колонке doc файл можно открыть в виде документа. В четвертом окне *4* пользователь может задать одно или несколько условий (Condition) для поиска информации. В разделе Queries — менять условия.

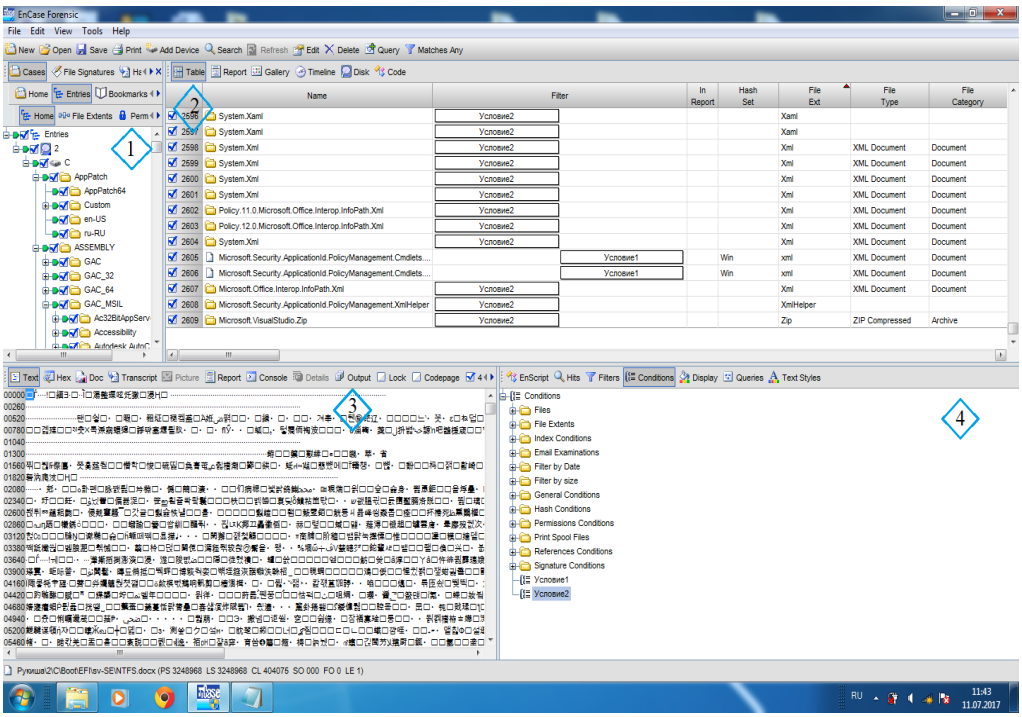


Рис. 6. Графический интерфейс программного комплекса Encase (скриншот)

Также в Encase можно осуществлять поиск на основе неограниченного числа ключевых слов по всем заданным носителям. Для этого имеется встроенный поиск Keywords. Возможен углубленный поиск слов при помощи GREP-запроса, то есть поиск разных вариантов написания определенного слова. Например, словосочетание «Сервис Экспресс» может быть написано с пробелом, без пробела, через дефис, с точкой и т. д. Используя KeySensetive, можно указать чувствительность к регистру.

PC-3000 UDMA — это комплекс для работы с поврежденными жесткими магнитными дисками (далее — ЖМД), который позволяет получить доступ к информации в случаях, когда накопитель поврежден и доступ к данным ограничен или не возможен.

В случае, если можно установить [10], что при запуске диска ситуация не ухудшится, ЖМД подключают к компьютеру эксперта и с помощью данного комплекса восстанавливают информацию.

При физическом повреждении ЖМД вскрывают (например, при повреждении блока магнитных голов или секторов) (рис. 7). Разбирать ЖМД следует крайне осторожно и в лабораторных условиях, поскольку попадание пыли на магнитные диски может стать критичным для дальнейшего восстановления данных. Также ЖМД чувствительны к ударам и вибрациям. Информация с магнитных дисков считывается с помощью блока магнитных голов. В процессе работы магнитные головки не касаются дисков, они расположены в несколь-

ких миллиметрах над ними. Если блок магнитных голов находится не в парковочной зоне, то диски не раскручиваются. На рисунке видно, что головки не запаркованы. Это может быть связано с их «залипанием». Если выявлена проблема, связанная с блоком магнитных голов, он может быть заменен блоком из донорского жесткого магнитного диска.

Рис. 7. Основные элементы HDD

Диагностическое исследование HDD. Для проверки исправности жестких дисков осуществляется его диагностирование стандартными способами или с помощью специальных программ [11].

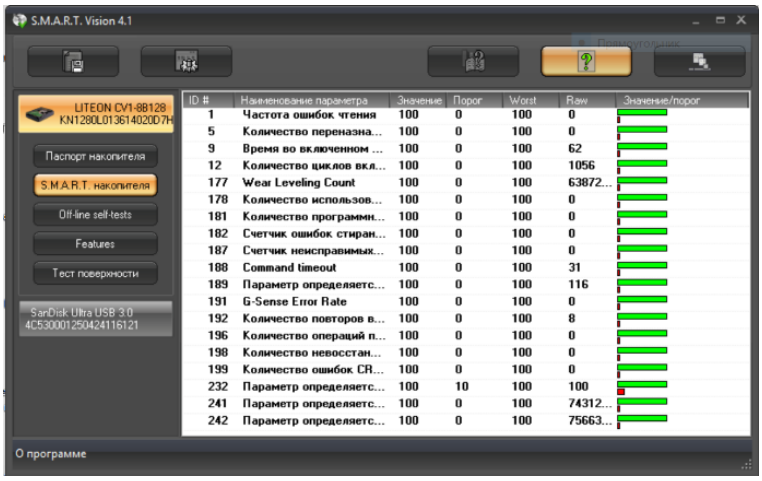
Диагностирование HDD-дисков стандартным путем на ОС Windows можно осуществить, задав «chkdsk» в командной строке. Это позволяет выполнить поиск и исправить ошибки на диске, используя определенный синтаксис.

В качестве одной из специальных программ диагностики HDD-дисков используют SMART Vision HDD. С ее помощью можно осуществить SMART-тестирование, то есть просмотр основных характеристик накопителя и оценку его состояния.

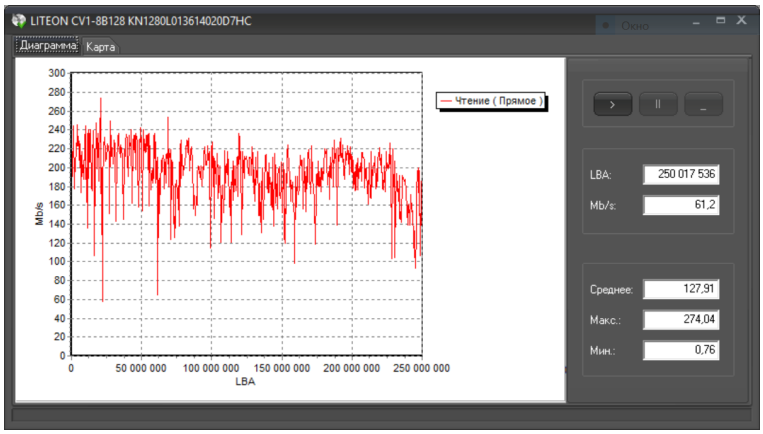
Программа SMART Vision HDD позволяет просматривать подробную информацию о носителе или следить только за интересующими параметрами (температурой, ошибками, счетчиками). Все сведения о накопителе содержатся в «паспорте» накопителя (рис. 8, *а*).

Запустим SMART-тестирование в данной программе. Полученный результат представлен на рис. 8, *б*. Также с помощью данной программы можно запустить тест, направленный на исследование поверхности диска. Результаты тестирования представлены на рис. 8, *в*. На основании полученных данных можно сделать вывод, что все параметры диагностируемого устройства находятся в рабочем состоянии.

а



б



в

Рис. 8. Фрагменты программы SMART Vision HDD (скриншоты):

а — «паспорт» накопителя; *б* — SMART накопителя; *в* — тестирование поверхности

Перспективы развития HDD. За последние несколько лет продажи жестких дисков значительно снизились. Связано это с ростом популярности твердотельных накопителей SSD, облачных сервисов хранения данных и др.

HDD во многом уступают SDD. В работе компьютеров, где важную роль играет быстродействие, намного целесообразнее использовать SDD, к тому же они практически бесшумны при использовании.

Однако у SSD-дисков есть и недостатки, основной из которых — это очень высокая стоимость. И если имеет смысл устанавливать в персональный компьютер SSD небольшого размера для того, чтобы ускорить работу программ, то для хранения большого объема данных такие диски использовать экономически нецелесообразно.

Для организации центра обработки данных большого объема (ЦОД) с помощью SSD понадобятся миллиарды рублей только на покупку самих дисков. Кроме того, максимальный объем информации SSD-накопителей меньше, чем HDD: 2 Тб и 10 Тб соответственно. Это значит, что понадобится больше SSD, поэтому и площадь, занимаемая ЦОД, будет больше.

По нашему мнению, у HDD все же есть будущее, хотя существующие методы записи информации близки к пику своих возможностей, в отношении плотности записи. Однако исследователи фирм-производителей продолжают разрабатывать новые технологии, которые позволят жестким дискам просуществовать еще несколько десятков лет. Старший вице-президент по финансам компании Seagate Technology Дэйв Мортон на 33-й конференции Nasdaq Investor Program заявил: «Я считаю, что жесткие диски останутся надолго, по крайней мере, на 15–20 лет» [12].

В заключение отметим, что жесткие диски будут актуальны в ближайшие годы, поскольку имеют невысокую стоимость, большую мощность, а также благодаря внедрению новых технологий, например HAMR (Heat-assisted magnetic recording — магнитная запись с тепловой поддержкой) и TDMR (Two-dimensional magnetic recording — двухмерная магнитная запись) сохранят свою популярность в ближайшем будущем.

Литература

[1] Добрынин В.В. Рынок услуг по восстановлению данных с поврежденных носителей: обзор формирования и развития. *Вестник ассоциации ВУЗов туризма и сервиса*, 2009, № 1, с. 87–95.

[2] Что такое HDD, жесткий диск и винчестер. URL: http://procomputer.su/sostav-kompyutera/33-chto-takoe-hdd-zhjostkij-disk-i-vinchester (дата обращения 15.10.2017).

[3] Computer hard drives. Failure rates, prices, backup and more. URL: https://www.backblaze.com/hard-drive.html (дата обращения 18.11.2017).

[4] RAMAC 350 restoration web site. URL: http://www.ed-thelen.org/RAMAC/ (дата обращения 15.10.2017).

[5] История HDD или кто и как изобрел первый жесткий диск (винчестер). URL: https://hddiq.ru/zhestkie-diski-hdd/istoriya-poyavleniya-zhestkih-diskov (дата обращения 15.10.2017).

[6] Топорков С.С. *Самоучитель продвинутого пользователя персонального компьютера или как перестать быть «чайником».* Москва, ДМК Пресс, 2004, 336 с.
[7] История жестких дисков. URL: http://www.storelab-rc.ru/history.htm (дата обращения 15.10.2017).
[8] Как работает жесткий диск. URL: http://www.it.ros-kit.ru/help/computers/kak-rabotaet-zhestkiy-disk/ (дата обращения 21.10.2017).
[9] Яковлев А.Н. Противодействие обороту контрафактного программного обеспечения: проблемы и решения. *Криминалистъ,* 2008, № 1, с. 19–23.
[10] Амелина К.Е., Коробец Б.Н., Кравченко А.А. *Охрана IT-решений: интернет-сайты.* Москва, Изд-во МГТУ им. Н.Э. Баумана, 2017, 155 с.
[11] Смолина А.Р., Шелупанов А.А. Методика проведения подготовительной стадии исследования при производстве компьютерно-технической экспертизы. *Доклады ТУСУР*, 2016, т. 19, № 1, с. 31–34.
[12] Seagate CFO claims HDDs to remain relevant for 15-20 more years. URL: https://www.eteknix.com/seagate-cfo-claims-hdds-remain-relevant-15-20-years/ (дата обращения 21.10.2017).

Джандарова Рукижат Расуловна — студентка кафедры «Юриспруденция, интеллектуальная собственность и судебная экспертиза», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

EXPERT WORK IN HDD DISKS RESEARCH

R.R. Dzhandarova RukishaDzhandarova@yandex.ru
SPIN-code: 3003-8260

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The study deals with the concept and history of appearance of HDD-disks, the stages of HDD-technology development. It examines the principle of their operation and illustrates the logical structure of the hard disk and the structure of the sector. Moreover, the paper describes an expert study done by means of the EncaseForensic and PC-3000 UDMA software packages, as well as the steps of the expert work with the hard disk and ways to delete information from it. Within the research we carried out a diagnostic test of the hard disk using the SMART VisionHDD program and indicated some prospects for the further development and use of such disks.

Keywords

HDD-disk, computer forensics, EncaseForensic software package, PC-3000 UDMA software package, diagnostic HDD-disk test, SMART-technology

References

[1] Dobrynin V.V. Services market for data recovery: development overview. *Vestnik assotsiatsii VUZov turizma i servisa* [Universities for Tourism and Service Association Bulletin], 2009, no. 1, pp. 87–95.

[2] Chto takoe HDD, zhestkiy disk i vinchester [What is HDD, hard drive and winchester disk]. Available at: http://procomputer.su/sostav-kompyutera/33-chto-takoe-hdd-zhjostkij-disk-i-vinchester (accessed 15 October 2017).

[3] Computer hard drives. Failure rates, prices, backup and more. Available at: https://www.backblaze.com/hard-drive.html (accessed 18 November 2017).

[4] RAMAC 350 restoration web site. Available at: http://www.ed-thelen.org/RAMAC/ (accessed 15 October 2017).

[5] Istoriya HDD ili kto i kak izobrel pervyy zhestkiy disk (vinchester) [History of HDD development or who and how invented the first hard drive (winchester disk)]. Available at: https://hddiq.ru/zhestkie-diski-hdd/istoriya-poyavleniya-zhestkih-diskov (accessed 15 October 2017).

[6] Toporkov S.S. Samouchitel' prodvinutogo pol'zovatelya personal'nogo komp'yutera ili kak perestat' byt' "chaynikom" [Teach-yourself guide for PC advanced user or how to avoid being dummy]. Moscow, DMK Press publ., 2004, 336 p.

[7] Istoriya zhestkikh diskov [Hard drive history]. Available at: http://www.storelab-rc.ru/history.htm (accessed 15 October 2017).

[8] Kak rabotaet zhestkiy disk [Hard drive working principles]. Available at: http://www.it.roskit.ru/help/computers/kak-rabotaet-zhestkiy-disk/ (accessed 21 October 2017).

[9] Yakovlev A.N. Counteraction against trafficking in counterfeit software: problems and solution. *Kriminalist*, 2008, no. 1, pp. 19–23.

[10] Amelina K.E., Korobets B.N., Kravchenko A.A. Okhrana IT-resheniy: internet-sayty [IT-solutions protection: websites]. Moscow, Bauman Press, 2017, 155 p.

[11] Smolina A.R., Shelupanov A.A. The methodology of preparatory stage of computer forensics. *Doklady TUSUR* [Proceedings of TUSUR University], 2016, vol. 19, no. 1, c. 31–34.
[12] Seagate CFO claims HDDs to remain relevant for 15-20 more years. Available at: https://www.eteknix.com/seagate-cfo-claims-hdds-remain-relevant-15-20-years/ (accessed 21 October 2017).

Dzhandarova R.R. — student, Department of Law, Intellectual Property and Forensic Examination, Bauman Moscow State Technical University, Moscow, Russian Federation.