Вестник Сибирского юридического института МВД России

УДК 340.692

Сергей Юрьевич ДЕМЕНЕВ,
заместитель начальника отдела – начальник отделения компьютерных экспертиз 6 отдела ЭКЦ ГУ МВД России по Красноярскому краю
demenevssb@mail.ru

Евгений Борисович МЕЛЬНИКОВ,
начальник кафедры криминалистики Сибирского юридического института МВД России (г. Красноярск), кандидат химических наук, доцент
ewgen0807@mail.ru

КЛАССИФИКАЦИЯ И УСТРАНИЕ НЕИСПРАВНОСТЕЙ НАКОПИТЕЛЕЙ ИНФОРМАЦИИ НА ЖЕСТКИХ МАГНИТНЫХ ДИСКАХ ПРИ ПРОИЗВОДСТВЕ КОМПЬЮТЕРНЫХ ЭКСПЕРТИЗ

CLASSIFICATION AND ELIMINATION OF MALFUNCTIONS OF DATA STORAGE DE-VICES ON HARD MAGNETIC DISKS IN THE PRODUCTION OF COMPUTER FORENSICS

В статье рассмотрены вопросы выявления и устранения неисправностей жестких магнитных дисков в процессе производства компьютерных экспертиз. Приведена классификация наиболее часто встречающихся неисправностей поврежденных носителей информации, предложены способы устранения аппаратных и программных неисправностей. На практических примерах показаны основные возможности и эффективность их использования с программно-аппаратным комплексом PC-3000, что позволяет в ходе производства компьютерных экспертиз извлекать информацию из неисправных накопителей на жестких магнитных дисках, в том числе поврежденных умышленно.

The article considers the issues of identifying and eliminating malfunctions of hard magnetic disks in the process of producing computer forensics. The classification of the most common malfunctions of damaged data storage is presented; methods of eliminating hardware and software malfunctions are proposed. The main capabilities and effectiveness of their use with the PC-3000 software and hardware complex are shown by practical examples; it allows, during the production of computer forensic examinations, to retrieve information from damaged storage devices, including those ones damaged intentionally.

Ключевые слова: компьютерная экспертиза, жесткие магнитные диски, устранение неисправностей.

Keywords: *computer forensics, magnetic hard disc, elimination of malfunctions.*

Несмотря на широкое распространение твердотельных накопителей (англ. Solid-State Drive, SSD), накопители информации на жестких магнитных дисках (далее – НЖМД) не утратили актуальности, удерживают лидерство в такой категории, как стоимость хранения 1 Гб информации, и продолжают активно использоваться.

С каждым годом количество исследуемых НЖМД увеличивается, вместе с тем неуклонно растет и количество предоставляемых на исследование неисправных накопителей.

Учитывая, что неисправные накопители могут содержать важную информацию, способную в дальнейшем эффективно использоваться в качестве доказательств по уголов-

ным делам различных категорий, выявление неисправностей НЖМД и их устранение представляется актуальным при производстве компьютерных экспертиз.

В общем случае неисправности НЖМД можно разделить на две категории аппаратные и программные. К аппаратным неисправностям обычно относят нечитаемые сектора, повреждения блоков магнитных головок (далее – БМГ), повреждения магнитных пластин, неисправности платы электроники, неисправность шпиндельного двигателя.

Нечитаемые сектора (bad блоки) – наиболее часто встречаемая неисправность, которая проявляется в виде ошибок чтения или записи при обращении к файлам или их копировании. Наличие нечитаемых секторов может не влиять на работу установленной на НЖМД операционной системы, но при этом могут возникнуть сложности с созданием копии или исследованием накопителя при подключении к стендовой ЭВМ с использованием устройств блокирования записи. При обращении к нечитаемому сектору накопитель делает паузу, пытаясь прочитать содержимое сектора. В микропрограммах контроллеров НЖМД установлено определенное количество попыток чтения сектора, после исчерпания которых происходит процедура замены сектора из резерва (переназначение) и добавлением его в пользовательский дефект-лист (G-list). Если нечитаемых секторов несколько, то время на их замену увеличивается, при этом диск и компьютер, к которому подключен НЖМД, перестает отвечать на запросы со стороны пользователя.

Повреждение БМГ, как правило, возникает при воздействии на НЖМД ударных нагрузок, превышающих предусмотренные производителем значения. Контакт БМГ с поверхностью магнитных пластин в процессе работы НЖМД приводит к деформации слайдера или к отрыву головок от него. Также повреждения могут быть получены в результате возникновения ударной нагрузки вдоль оси перемещения БМГ у выключенного НЖМД. Это связано с отсутствием у современных НЖМД механизма жесткой фиксации БМГ в зоне парковки. В некоторых случаях БМГ прилипает к поверхности, но остается при этом неповрежденным и после осмотра его состояния под микроскопом может быть использован для считывания данных.

Повреждение магнитных пластин, так же как и в вышеуказанном случае, происходит в результате их контакта с БМГ в процессе работы НЖМД. В результате деформируется слайдер, головка изменяет положение и происходит повреждение пластины, на поверхности образуются глубокие царапины. Это приводит к образованию внутри гермоблока НЖМД пыли, состоящей из защитного покрытия и магнитного слоя, которая попадая между головками и поверхностями других пластин, вызывает образование повреждений на остальных поверхностях за счет абразивного действия.

Неисправность платы электроники возникает, как правило, при проблемах с питанием и последующим выгоранием защитных диодов. Несмотря на предусмотренную производителем защиту цепей питания, нередки случаи выгорания микросхемы управления двигателем, процессора или иных деталей платы. Гораздо реже встречаются механические повреждения разъемов подключения питания и передачи данных. Для НЖМД, у которых элементы на плате управления расположены на наружной поверхности, характерны повреждения в виде отсутствующих элементов.

Неисправности шпиндельного двигателя по причине заклинивания вала или обрыва обмоток приводит к невозможности раскручивания двигателя.

К программным неисправностям относятся повреждения микропрограммы. Вследствие того, что микропрограмма управления НЖМД имеет модульную конструкцию, в процессе работы повреждаются модули, наиболее часто используемые накопителем, например модули SMART, таблицы дефектов, модули транслятора. Помимо этого зачастую повреждаются модули, необходимые для запуска НЖМД и его функционирования. Данного рода неисправность может быть вызвана ошибками, допущенными при создании микропрограммы производителем, изменени-

ем контрольных сумм, дефектов содержимого модулей.

Наиболее часто встречающиеся неисправности НЖМД будут приведены ниже на примере двух случаев из практики производства компьютерных экспертиз 6 отдела ЭКЦ ГУ МВД России по Красноярскому краю, которые в полной мере иллюстрируют способы их устранения.

В первом случае на исследование был предоставлен видеорегистратор NOVICAMPRO TR1016A, изъятый с места пожара. Внешний вид приведен на рис. 1 и 2.

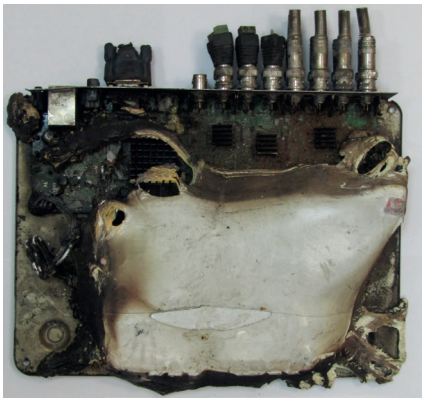

Рис. 1. Повреждения видеорегистратора (вид сверху)

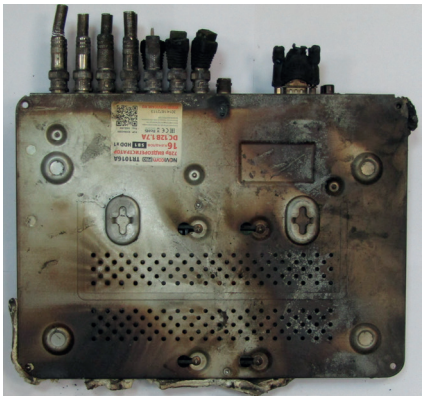

Рис. 2. Повреждения видеорегистратора (вид снизу)

Под оплавленной частью корпуса находился НЖМД (рис. 3), который был извлечен, очищен от сажи и осмотрен. НЖМД не имел повреждений, модель ST4000DM004, емкость 4 Тб (рис. 4). Плата электроники была снята, осмотрена и очищена в ультразвуковой ванне с использованием этилового спирта. На шине питания и шине передачи данных коротких замыканий не выявлено.

Рис. 3. Внешний вид НЖМД (вид снизу)

Рис. 4. Внешний вид НЖМД после очистки (вид сверху)

Далее плата электроники отдельно от НЖМД была подключена к PC-3000 Portable III и с использованием утилиты «Seagate F3 Architecture» через терминал было считано ПЗУ. У семейства накопителей «V11», к которому относится данный НЖМД, доступ к технологическому режиму работы заблокирован и поэтому считать и проверить целостность служебной микропрограммы без разблокировки невозможно. Для разблокирования доступа к считанному ПЗУ был применен патч разблокировки «Unlock Tech Mode», после чего модифицированное ПЗУ было записано в плату.

Далее плата была присоединена к НЖМД, затем подано питание и выполнено действие в меню утилиты «Unlock

tech mode, HDD подготовлен утилитой». В результате был получен доступ к технологическому режиму работы. Запуск накопителя происходил нетипично долго (более 1 минуты) и сопровождался сообщениями об ошибках в терминале. В процессе проверки и резервирования модулей микропрограммы было установлено, что модуль «MCMT» из копии N 0 не читается, при этом его копия N 1 читается нормально.

Особенностью данного накопителя является то, что он относится к поколению НЖМД, выполненных с применением технологии «SMR», также называемой «черепичной записью». Одним из аспектов реализации данной технологии в НЖМД производства «Seagate» является наличие особой буферной области на поверхности магнитных пластин (Media Cache), куда в первую очередь помещаются данные, записываемые пользователем, которые затем во время простоя накопителя в фоновом режиме перемещаются из Media Cache в область непосредственного хранения данных. Данный процесс сопровождается большим количеством операций записи данных и изменения служебных модулей, хранящих таблицы размещения данных, в частности «MCMT». В случае с неисправным накопителем в процессе записи может происходить повреждение как служебной информации, так и данных пользователя. В конкретном случае для предотвращения повреждения данных в утилите были выполнены действия по блокированию у НЖМД функции записи.

Затем с использованием «Data Extractor» был запущен процесс создания посекторной копии информации, имеющейся в памяти НЖМД, по предварительно сформированной карте голов. В ходе копирования было установлено, что головки N 1 и N 3 читают информацию медленно и с ошибками. Далее было принято решение о создании в первую очередь копии данных по головкам N 0 и N 2. После завершения вычитывания данных по головкам N 0 и N 2 было запущено чтение данных по головкам N 1 и N 3 с параметрами, приведенными на рис. 5, 6, 7 и 8.

В итоге создания копии данных из 3726 Гб информации, содержащейся на НЖМД, не было прочитано всего 1,43 Гб. Продолжительность процесса составила 93 часа непрерывной работы.

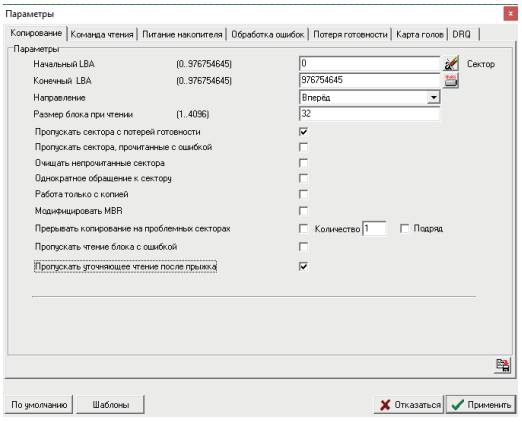

Рис. 5. Параметры копирования

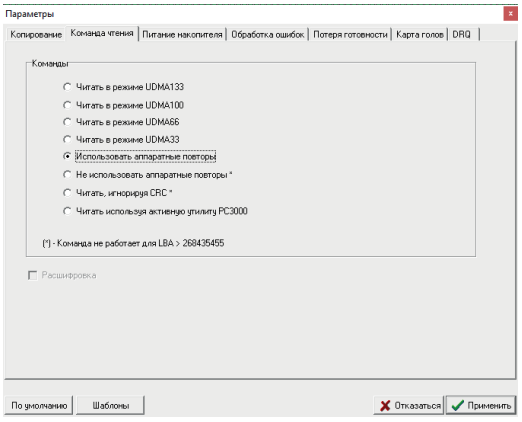

Рис. 6. Команда чтения

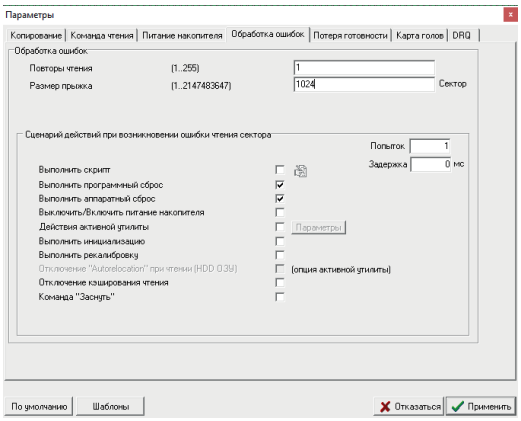

Рис. 7. Обработка ошибок

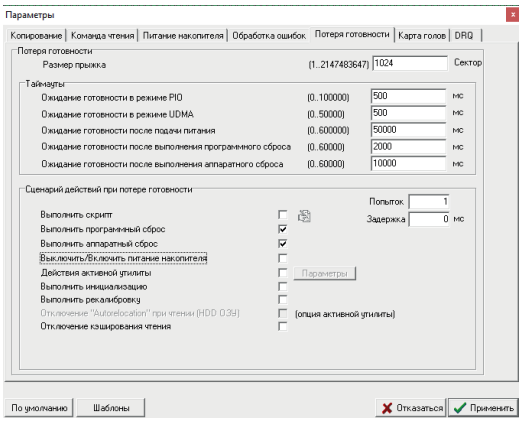

Рис. 8. Потеря готовности

Далее НЖМД был отключен от PC-3000 Portable III, а копия полученных данных средствами «Data Extractor» была смонтирована в операционную систему как виртуальный диск для дальнейшего исследования с использованием специализированного программного обеспечения просмотра видеозаписей.

Во втором случае на экспертизу был предоставлен НЖМД с интерфейсом подключения USB 3.0 (рис. 9, 10). Внешние повреждения корпуса в этом случае отсутствовали.

Рис. 9. НЖМД (вид сверху)

Рис. 10. НЖМД (вид снизу)

При подключении НЖМД не определялся операционной системой, шпиндельный двигатель не раскручивался, накопитель периодически издавал короткий звук высокой частоты (писк), что характерно для прилипших к поверхности магнитных пластин головок. Внутри корпуса находится накопитель Toshiba модели MQ01UBD100, отличительной особенностью которого является наличие разъема USB, установленного непосредственно на плате электроники (рис. 11).

После вскрытия корпуса в результате осмотра было установлено, что БМГ находится вне парковочной зоны и располагается на поверхности магнитных пластин (рис. 12).

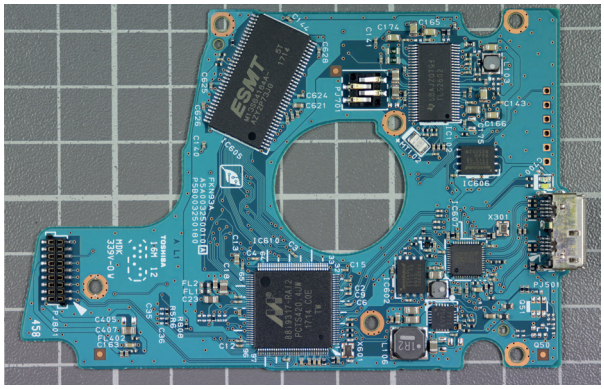

Рис. 11. Плата электроники НЖМД

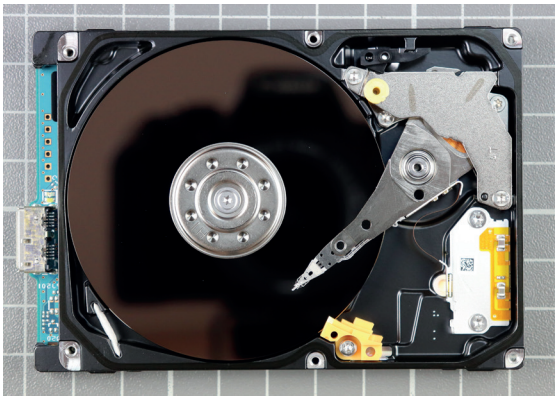

Рис. 12. БМГ за пределами зоны парковки

Для вывода БМГ с поверхности магнитных пластин в зону парковки необходимо осуществлять поворот вала шпиндельного двигателя против часовой стрелки одновременно с этим поворачивая БМГ по часовой стрелке на место парковки (рис. 13). Для того чтобы стронуть БМГ с места, можно аккуратно постукивать по коромыслу в области подшипника.

Следует помнить, что вращать вал двигателя по часовой стрелке категорически запрещается, так как это вызовет деформацию слайдеров и приведет в негодность БМГ.

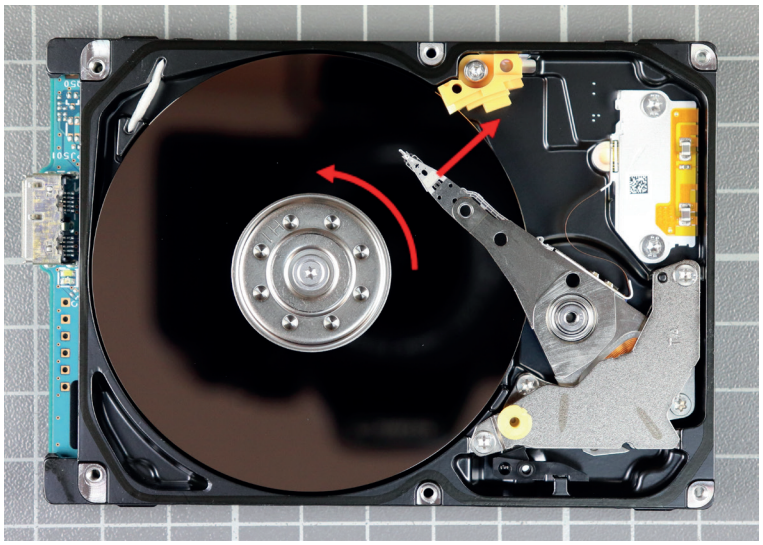

Рис. 13. Направление вращения вала двигателя и перемещения БМГ

Для определения наличия повреждений БМГ был демонтирован и в дальнейшем осмотрен под микроскопом. Важным условием выполнения операции демонтажа является необходимость предварительно ограничить подвижность слайдеров для предотвращения слипания головок, что достигается использованием специализированных съемников либо подручных средств. В данном случае были использованы нарезанные поперек полоски пластиковых закладок шириной 3-4 мм, согнутые в форме буквы «U» (рис. 14).

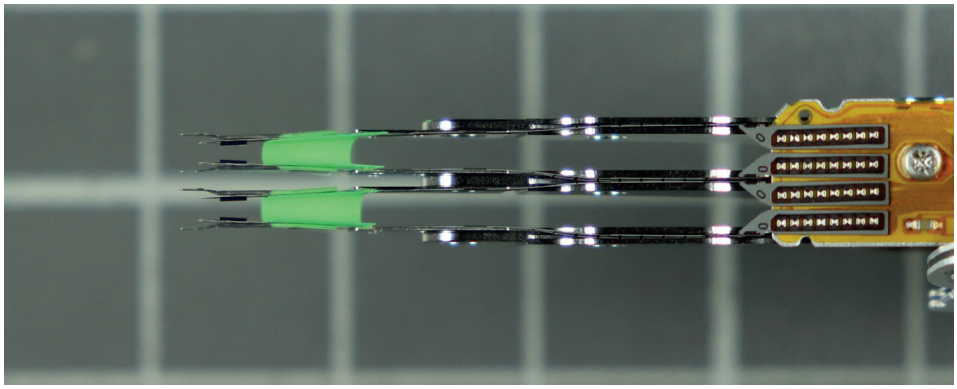

Рис. 14. БМГ с установленными разделителями слайдеров головокголовок

Осмотр под микроскопом повреждений не выявил, и БМГ был установлен обратно. Перед установкой крышки гермоблока необходимо удалить попавшие в гермозону частички пыли, для этого использовался баллончик со сжатым газом, предназначенный для очистки электроники.

В связи с тем, что в данном случае интерфейс USB не обеспечивал необходимый контроль работы неисправного накопителя, плата электроники была заменена на совместимую модель с разъемом SATA и перепайкой микросхемы ПЗУ (рис. 15).

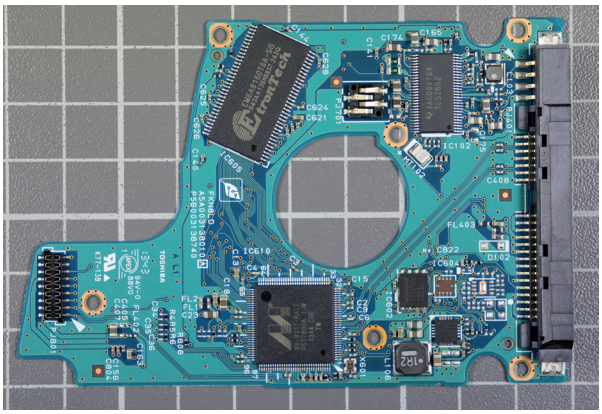

Рис. 15. Совместимая плата электроники с разъемом SATA

Далее НЖМД был подключен к PC-3000 Portable III и после подачи питания вышел в режим готовности. Затем была запущена специализированная утилита для работы с накопителями Toshiba (рис. 16). Проверка чтения модулей микропрограммы НЖМД в процессе их резервирования прошла успешно.

Для предотвращения зависания накопителя чтение данных осуществлялось в технологическом режиме, в котором с использованием соответствующей утилиты, можно отключить механизм переназначения секторов и обновление таблиц SMART. Особенностью технологического режима работы НЖМД Toshiba является то, что чтение по умолчанию происходит без коррекции ошибок ECC. Для того чтобы чтение осуществлялось с использованием ECC, в опциях утилиты необходимо отметить необходимые опции (рис. 17).

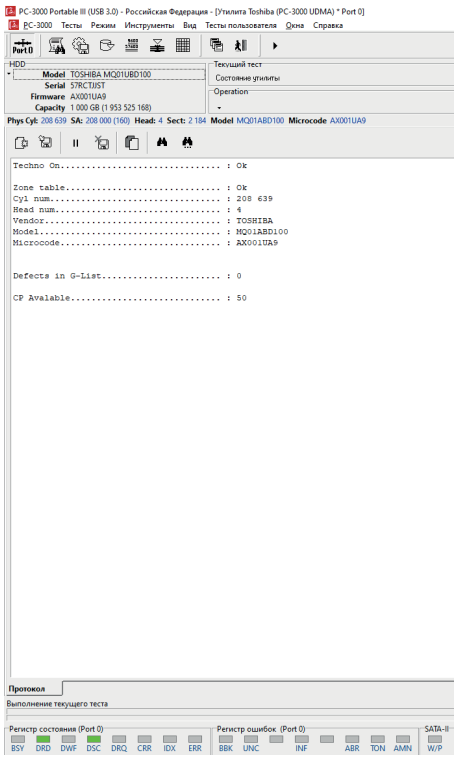

Рис. 16. Окно инициализации утилиты Toshiba

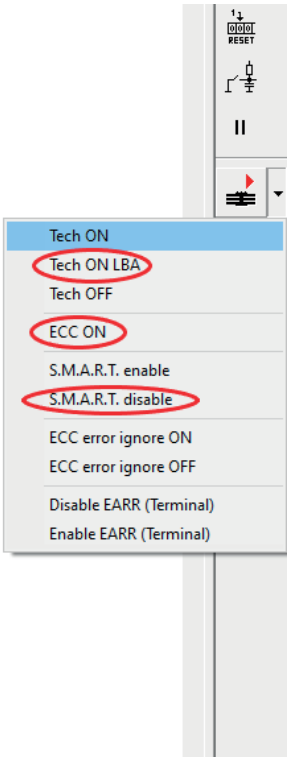

Рис. 17. Меню утилиты Toshiba

В дальнейшем с использованием «Data Extractor» был запущен процесс создания посекторного копирования информации, имеющейся в памяти НЖМД, по предварительно сформированной карте голов. В ходе копирования было установлено, что головка N 0 не читает, в связи с этим далее были осуществлены действия, аналогичные описанным выше при копировании данных с НЖМД ST4000DM004.

В дальнейшем с использованием «Data Extractor» был запущен процесс создания посекторного копирования информации, имеющейся в памяти НЖМД, по предварительно сформированной карте голов. В ходе копирования было установлено, что головка N 0 не читает, в связи с этим далее были осуществлены действия, аналогичные описанным выше при копировании данных с НЖМД ST4000DM004.

После окончания копирования информации по головкам N 1, 2 и 3 БМГ был заменен на исправный от аналогичного НЖМД донора и считана информация по головке N 0.

В итоге создания копии данных из 931,5 Гб информации, содержащейся на НЖМД, не было прочитано только 28 Кб. На создание копии данных в этом случае было затрачено 22 часа непрерывной работы.

Подводя итог, следует отметить, что рассмотренная классификация неисправностей накопителей информации на жестких магнитных дисках и способы их устранения в ходе производстве компьютерных экспертиз имеет важное практическое значение. Рассмотренные конкретные случаи из практики наглядно показывают эффективность использования предложенных методов выявления и устранения неисправностей. В совокупности с использованием программно-аппаратного комплекса PC-3000 они позволяют извлекать информацию с неисправных НЖМД, в том числе поврежденных умышленно, и могут применяться в случаях, когда это невозможно сделать стандартными способами.

Библиографический список

1. Руководство пользователя DATA Extractor. – URL: https://ts.acelab.ru/files.
2. Руководство пользователя PC-3000 Portable III. – URL: https://ts.acelab.ru/files.
3. Руководство пользователя Seagate Архитектура F3. – URL: https://ts.acelab.ru/files.
4. Руководство пользователя Toshiba. – URL: https://ts.acelab.ru/files.
5. Саенко, Г.В. Типовая методика исследования компьютерной информации / Г.В. Саенко, О.В. Тушканова. – М., 2010.