УДК 681.3.06(075)

С.Д. Прокопенко,
С.Р. Коженевский

ИССЛЕДОВАНИЕ ПРОТОКОЛОВ ВЗАИМОДЕЙСТВИЯ СОВРЕМЕННЫХ ПК С НАКОПИТЕЛЯМИ НА ЖЕСТКИХ МАГНИТНЫХ ДИСКАХ

Статтю присвячено дослідженню протоколів, у відповідності з якими здійснюється обмін командами і даними між ПК та НЖМД. Дослідження проведено на різних програмних та апаратних платформах, при цьому особливу увагу приділено командам, що модифікують дані на жорстких дисках. Також у статті наведено теоретичні дані щодо принципів взаємодії ПК з накопичувачами на жорстких магнітних дисках, подано загальний опис стандарту інтерфейсу ATA та системи команд, що використовується в ньому.

Ключові слова: *блокіратор запису, аналізатор протоколів, інтерфейс, стандарт ATA, Serial ATA, операційна система, команди запису, функціональний набір команд, жорсткий диск.*

Статья посвящена исследованию протоколов, в соответствии с которыми осуществляется обмен командами и данными между ПК и НЖМД. Исследования проведены на различных программных и аппаратных платформах, при этом особое внимание было уделено командам, модифицирующим данные на жестких дисках. Также в статье приведены теоретические сведения о принципах взаимодействия ПК с накопителями на жестких магнитных дисках, дано общее описание стандарта интерфейса ATA и применяемой в нем системе команд.

Ключевые слова: *блокиратор записи, анализатор протоколов, интерфейс, стандарт ATA, Serial ATA, операционная система, команды записи, функциональный набор команд, жесткий диск.*

The paper is devoted to the examination of actual commands that PC exchanges with HDD. Experiments are conducted on various software and hardware platforms, with special attention to commands modifying data on hard drives. Also paper describes theoretical principles of interaction between PCs and HDDs, gives common description of ATA standard and command set, used in it.

Keywords: *write blocker, protocol analyzer, interface, ATA standard, Serial ATA, operating system, write instructions, command function set, hard disk drive.*

При выполнении работ по восстановлению данных и расследованию компьютерных инцидентов важнейшее значение приобретает обеспечение целостности данных на носителе информации. Для исключения возможности случайного или преднамеренного внесения изменений в данные в процессе их съема и анализа необходимо использовать программные и аппаратные средства блокирования записи.

Настоящая статья является первой в цикле планируемых статей, посвященных особенностям построения и функционирования аппаратных блокираторов записи. В ней приведена информация о принципах взаимодействия ПК с жесткими дисками, дано общее описание стандарта интерфейса ATA и применяемой в нем системе команд.

В статье приведены результаты исследования наборов команд, которыми обмениваются компьютер и накопитель при выполнении типовых операций. Исследования проведены на различных программных и аппаратных платформах, при этом особое внимание было уделено командам, которые модифицируют данные на жестких дисках.

Общие сведения о взаимодействии компьютера и НЖМД

Накопители на жестких магнитных дисках (НЖМД) относятся к устройствам внешней памяти с прямым доступом. Они характеризуются возможностью обращения к блокам данных по их адресам в произвольном порядке, при этом допускается произвольное чередование операций записи и чтения блоков. Инициатором обмена данными всегда выступает *хост* – компьютер, обязательными элементами которого являются процессор и оперативное запоминающее устройство (ОЗУ).

Подключение НЖМД к компьютеру осуществляется через один из интерфейсов. Наибольшее распространение получили параллельный Parallel ATA (IDE) и последовательный Serial ATA (SATA) интерфейсы. Взаимодействие компьютера с НЖМД основано на подаче ему команд и передаче блоков данных из накопителя в системную память хоста и из этой памяти в накопитель. Как правило, выполнение каждой из таких команд состоит из четырех этапов:

1. Передача команды в накопитель. Указывается тип операции (чтение, запись или другая операция), адрес начального блока данных, который участвует в операции, количество передаваемых блоков данных;

2. Поиск запрашиваемых данных в накопителе. Эта операция является внутрен-ней для накопителя, ее выполнение возлагается непосредственно на контроллер накопителя. Время, требуемое для выполнения данной операции, является важной характеристикой накопителя и описывается как “время доступа”;

3. Передача данных между накопителем и системной памятью хоста. Скорость передачи определяется несколькими факторами – объемом запрошенных командой данных, внутренней скоростью передачи данных накопителя, пропускной способностью интерфейса и т. д.;

4. Завершение выполнения команды. На этом этапе хост проверяет регистры ошибок накопителя и определяет успешно или неуспешно (с указанием причины неуспеха) завершена запрошенная операция, кроме того, хост получает информацию о реальном количестве считанных или записанных блоков данных.

В общем случае команды выполняются последовательно, т.е. до передачи следующей команды накопитель должен завершить исполнение предыдущей. Однако такой подход не отличается высокой производительностью, особенно в многозадачных системах, зачастую требующих возможности параллельного выполнения запросов хоста к накопителю.

Такого недостатка лишены современные накопители, поддерживающие очереди команд. Они позволяют принимать новые команды до завершения выполнения предыдущих. Порядок исполнения команд определяется в таком случае самим накопителем (его контроллером) с учетом оптимизации времени на исполнение каждой команды в очереди с целью повышения общей пропускной способности. Например, для сокращения временных затрат на поиск и пози-

ционирование НЖМД может в первую очередь выполнять команды, данные для которых расположены ближе к текущему положению головок на поверхности пластин.

Система команд ATA/ATAPI и SATA

В настоящее время наборы команд и протоколы передачи данных унифицированы и описаны в спецификациях соответствующих интерфейсов подключения накопителя к хосту. В наиболее распространенных жестких дисках с интерфейсами PATA и SATA применяется система команд, основанная на спецификациях стандарта ATA.

Стандарт интерфейса ATA (AT Attachment) широко используется в компьютерной индустрии вот уже почти 20 лет, непрерывно совершенствуясь. С 1994 года Технический комитет T13 (http://www.t13.org), отвечающий за развитие стандарта, выпустил уже восьмую его версию.

В настоящее время стандарты семейства ATA (параллельные ATA/ATAPI и последовательные SATA) описывают систему команд, передаваемых по параллельному или последовательному интерфейсу. Первые версии спецификации были ориентированы только на НЖМД, впоследствии были добавлены поддержки других типов накопителей: на основе твердотельной Flash памяти, со съемными носителями (оптические приводы, ленточные накопители).

В Таблице 1 приведены основные сведения о принятых ревизиях стандарта ATA. С 2002 г. первые три ревизии ATA1-ATA3 определены как устаревшие.

Таблица 1

Принятые ревизии стандарта ATA

Ревизия стандарта	Год принятия	Количество определенных команд (команд записи)	Новые команды записи	Основные новые свойства
ATA-1	1994	76 (9)		
ATA-2	1996	78 (9)		28-битная LBA адресация
ATA-3	1997	54 (9)		S.M.A.R.T, парольная защита
ATA/ATAPI-4	1998	53 (7)	WRITE DMA QUEUED	Очереди команд, защищенная область HPA (Host Protected Area), пакетный интерфейс ATAPI
ATA/ATAPI-5	2000	48 (5)	–	
ATA/ATAPI-6	2002	63 (9)	WRITE DMA EXT WRITE DMA QUEUED EXT WRITE MULTIPLE EXT WRITE SECTORS EXT	48-битная LBA адресация, поддержка конфигурирования Device Configuration Overlay (DCO)
ATA/ATAPI-7	2005	70 (14)	WRITE DMA FUA EXT WRITE DMA QUEUED FUA EXT WRITE MULTIPLE FUA EXT WRITE STREAM DMA EXT WRITE STREAM EXT	SATA 1.0, потоковые операции, длинный логический/ физический сектор
ATA/ATAPI-8	2008	77 (15)	WRITE FPDMA QUEUED	Поддержка гибридных накопителей с энергонезависимым кэшем

В соответствии со спецификациями стандарта ATA хост передает команды по одному из девяти протоколов передачи данных, определенному для данной команды в стандарте:

- PI – ввод данных из накопителя в режиме PIO;
- PO – вывод данных в накопитель в режиме PIO;
- DM – обмен данными по каналу DMA (независимо от направления передачи);
- DMQ – обмен данными по каналу DMA с очередями;
- P – протокол передачи командного пакета SCSI (для ATAPI устройств);
- ND – без передачи данных;
- DD – протокол диагностики накопителя;
- DR – протокол сброса;
- VS – протокол вендор команд (команд производителя).

Не все команды требуют передачи информации, ряд команд (например, команда READ VERIFY SECTORS) выполняются без пересылки данных по интерфейсу.

В спецификациях стандарта ATA определено всего 256 возможных кодов команд. С точки зрения их описания в стандарте они подразделяются на:

Определенные (defined) команды. Это действующие команды (например, WRITE DMA EXT – 35h), для которых в стандарте описаны все параметры – действия накопителя в ответ на команду, тип командного протокола, содержимое регистров, подтверждение выполнения, ошибки и т.п.

Зарезервированные (reserved) команды. Коды и поля команд, не описанные в стандарте, которые оставлены для будущей стандартизации. В случае передачи хостом зарезервированной команды накопитель должен обрабатывать такую команду как ошибочную и прерывать ее выполнение. В стандарте ATA-8 статус reserved имеют 93 кода команд. Большая часть из них зарезервированы для общих целей, около четверти зарезервированы для поддержки SATA, Compact Flash и др.

Устаревшие (obsolete) команды. Коды и поля команд, не определенные в текущей ревизии стандарта, но которые могли быть описаны в предыдущих ревизиях. Устаревшие значения не могут быть переопределены для других применений в последующих ревизиях стандарта. Например, в ATA1 – ATA6 как обязательная для всех не ATAPI устройств была определена команда SEEK (7Dh). Начиная со стандарта ATA-7, она является устаревшей, но она может поддерживаться новыми накопителями для обратной совместимости.

Выбывшие (retired) команды. Коды и поля команд, не определенные в текущей ревизии стандарта, но которые могли быть описаны в предыдущих ревизиях. В отличие от устаревших команд, они могут быть переопределены в будущих версиях стандарта. При этом до их переопределения они должны выполняться так же, как были описаны в предыдущих версиях. Всего в стандарте ATA-8 статус retired имеют 40 команд, но есть только один пример переопределения – команда с кодом E9h, определенная как WRITE SAME в ATA-1 и ATA-2, будет переопределена как READ BUFFER DMA в следующей ревизии стандарта.

Вендор команды (vendor specific). Коды и поля команд, зарезервированы для реализации специфических для производителя накопителя (вендора) задач и функций, например, для получения доступа к служебной области данных ("нулевой дорожке"). Вендор команды не описываются в стандарте, а порядок их выполнения может отличаться у разных производителей и даже в различных моделях одного производителя. В стандартах ATA под нужды производителей выделено 27 команд.

В зависимости от назначения команд последняя версия стандарта ATA-8 определяет 25 функциональных наборов команд (feature sets). Из них только 2

являются обязательными для всех ATA устройств (наборы команд общего назначения и управления питанием), остальные являются опциональными. Даже такие "стандартные" для современных НЖМД характеристики, как поддержка емкости более 128 ГБ. SMART или парольная защита данных не являются обязательными, а реализуются в опциональных функциональных наборах команд 48-Bit Address feature set, SMART feature set и Security feature set.

Описанные принципы построения стандарта дают производителям возможность гибко настраивать функциональность конечных продуктов и быстрее выводить новые модели на рынок. В то же время это создает проблемы для специалистов в области расследования компьютерных инцидентов. Одна из важнейших задач для них – обеспечение неизменности данных. Но таблица 1 показывает, что практически каждая версия стандарта вносит новые команды записи. Всего первые восемь ревизий ATA описывают 21 различную команду записи. При этом только четыре команды записи определены во всех семи стандартах: WRITE BUFFER (E8h), WRITE SECTORS with retries (30h), WRITE MULTIPLE (C5h) и WRITE DMA (CAh).

При выполнении работ по восстановлению данных и расследованию компьютерных инцидентов необходимо также учитывать, что в различных операционных системах (и даже различных версиях одной и той же ОС) для доступа к диску могут использоваться разные наборы команд. Это связано с тем, что практически все современные ОС блокируют прямой низкоуровневый доступ к накопителю, предлагая для доступа к дисковым устройствам унифицированный программный интерфейс высокого уровня (драйвер). Таким образом, весь обмен данными, а значит, и набор передаваемых команд, контролируется операционной системой и зависит от набора используемых драйверов.

Исследование взаимодействия хост-НЖМД

Авторами были проведены исследования для определения фактических команд, которыми обмениваются хост и НЖМД в различных режимах работы ПК.

Регистрация команд, передаваемых хостом в НЖМД, осуществлялась с помощью анализатора протоколов EPOS ATA Analyzer. EPOS ATA Analyzer является универсальным инструментальным средством анализа протоколов интерфейса ATA и обеспечивает регистрацию и отображение команд и данных, передаваемых между хостом и любыми устройствами с интерфейсами Parallel ATA или Serial ATA (рис. 1).

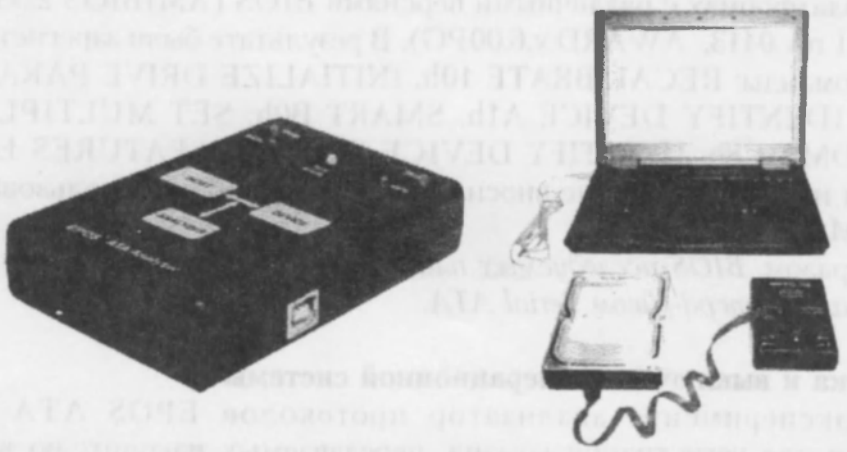

Рис. 1. Анализатор протоколов EPOS ATA Analyzer

Анализатор выполнен в виде адаптера, который включается в разрыв между исследуемой системой и накопителем. Он регистрирует все команды и данные, которыми они обмениваются, и через интерфейс USB передает их на отдельный инструментальный ПК. Программное обеспечение, исполняемое на инструментальном ПК, обеспечивает сохранение, обработку и отображение полученных данных.

Структурная схема стенда для проведения исследования приведена на рис. 2.

Рис. 2. Структурная схема стенда для проведения исследования

Целью исследования являлось определение команд (в первую очередь, команд записи), которыми обмениваются хост и НЖМД при выполнении типовых операций:

1. Определение НЖМД средствами BIOS;
2. Загрузка и выключение операционной системы;
3. "Горячее" подключение НЖМД;
4. Запись файлов на НЖМД.

1. Определение НЖМД средствами BIOS

Эксперименты по определению команд, которые передаются хостом при детектировании НЖМД средствами BIOS, были проведены на трех различных аппаратных платформах с различными версиями BIOS (AMIBIOS 2.53 rev.0207, AMIBIOS 2.61 rev.0413, AWARD v.6.00PG). В результате были зарегистрированы следующие команды: RECALIBRATE 10h, INITIALIZE DRIVE PARAMETERS 91H, ATAPI IDENTIFY DEVICE A1h, SMART B0h, SET MULTIPLE MODE C6h, READ DMA C8h, IDENTIFY DEVICE ECh, SET FEATURES EFh, IDLE E3h. Ни одна из этих команд не вносит изменений в область пользовательских данных НЖМД.

Таким образом, *BIOS исследуемых платформ не передает команд записи на жесткие диски с интерфейсом Serial ATA.*

2. Загрузка и выключение операционной системы

В этом эксперименте анализатор протоколов EPOS ATA Analyzer использовался для регистрации команд, передаваемых накопителю в процессе

загрузки и выключения операционной системы. В ходе исследования на тестовый стенд (материнская плата на чипсете Intel G41/ICH7, процессор Intel Core2 Duo E7600, ОЗУ 2ГБ) устанавливались распространенные операционные системы (Windows XP Pro SP2, Windows XP Pro SP3, Windows Server 2003 R2, Windows Vista Business x64, Windows 7 Professional x64, Windows Server 2008 R2, OpenSUSE 11.2, Fedora 11, FreeBSD 8.1). После установки к стенду подключались SATA НЖМД, содержащие один логический диск с файловой системой NTFS (для всех исследуемых ОС), ext3 (для OpenSUSE и Fedora), ext4 (для OpenSUSE), UFS2 (для FreeBSD), и выполнялась полная загрузка и последующее выключение операционной системы.

В результате исследования установлено, что принципы работы с дисковыми накопителями сходны у всех исследуемых операционных систем. На этапе загрузки НЖМД дважды детектируется операционной системой: первый раз на начальном этапе определения оборудования, второй раз на этане загрузки драйверов интерфейсного контроллера. На этапе монтирования логического диска выполняется считывание (и обновление) метаданных файловой системы. При выключении все исследуемые ОС сохраняют данные из энергозависимого кэша на пластины НЖМД (команды FLUSH CACHE и FLUSH CACHE EXT) и затем переводят накопитель в режим ожидания (команда STANDBY IMMEDIATE).

В то же время у различных операционных систем имеются свои особенности работы с НЖМД. Например, на этапе определения накопителя ОС Windows предыдущего поколения (XP SP2, XP SP3, Server 2003) передают команду 10h RECALIBRATE, которая начиная с ревизии ATA-4 определена как устаревшая; современные ОС Windows (Vista, Windows 7, Server 2008) сначала пытаются определить накопитель как ATAPI устройство (команда A1h ATAPI IDENTIFY DEVICE); Linux системы определяют полную емкость накопителя с помощью команды 27h READ NATIVE MAX ADDRESS (EXT).

Однако основные отличия заключаются в различном количестве дисковых операций, требуемых операционной системе для монтирования и размонтирования логического диска. Данные об общем количестве команд и количестве команд записи, выполняемых от запуска до выключения ОС при работе с разделом NTFS, приведены в Таблице 2.

Таблица 2

Загрузка и отключение ОС с подключенным НЖМД, содержащим логический раздел NTFS

Операционная система	Общее количество команд	Количество команд записи (WRITE DMA, WRITE DMA EXT)
Windows XP SP2	25079	69
Windows XP SP3	25028	35
Server 2003	25026	39
Vista x64	3912	835
Windows 7 x64	23091	838
Server 2008	385	111
OpenSUSE	308	0
Fedora	130	0
FreeBSD	2047	0

Таблица 2 показывает, что ОС Windows XP SP2, XP SP3, Server 2003, Windows 7x64 в процессе монтирования тома NTFS выполняют большое количество команд чтения, полностью считывая файловые таблицы MFT и другие метаданные файловой системы. Linux системы и Windows Server 2008 выполняют намного меньше дисковых операций, а Windows Vista x64 и FreeBSD занимают промежуточное положение.

Важно отметить, что все исследуемые операционные системы Windows выполняют операции записи при монтировании и размонтировании логического раздела NTFS. Другими словами, уже на этапе загрузки до выполнения каких-либо действий пользователем в пользовательскую область данных накопителя вносятся изменения. При этом объем записываемых данных для Windows Vista и Windows 7 составляет десятки мегабайт.

Linux и UNIX не выполняют запись на "неродную" для себя файловую систему NTFS. Тем не менее, в ходе исследования установлено, что при монтировании они выполняют операции записи на файловые системы Ext3 и UFS2 соответственно. ОС семейства Linux и UNIX поддерживают возможность монтирования логических дисков в режиме "только для чтения" (с ключом *–ro*). Тем не менее, в ходе исследования установлено, что при попытке монтирования поврежденной файловой системы даже в режиме "только для чтения" операционные системы Linux могут вносить изменения в данные на монтируемом диске.

Таким образом, все исследованные операционные системы в процессе загрузки и отключения вносят изменения в данные на подключенных (не загрузочных) НЖМД без выполнения в этот период каких-либо действий пользователем.

3. "Горячее" подключение НЖМД

Интерфейс SATA поддерживает возможность "горячего" (без перезагрузки) подключения накопителя к ПК, чем широко пользуются специалисты по расследованию ИТ инцидентов и восстановлению информации.

Для определения наборов команд, передаваемых хостом при горячем подключении SATA НЖМД, с помощью анализатора EPOS ATA Analyzer были сняты и проанализированы протоколы обмена данными. Полученные результаты приведены в табл. 3 (команды записи в ней выделены полужирным шрифтом).

Таблица 3

"Горячее" подключение НЖМД

Операционная система	Файловая система	Количество команд записи	Команды
Windows XP SP2	NTFS	20	A1h – ATAPI IDENTIFY DEVICE ECh – IDENTIFY DEVICE EFh – SET FEATURES 91h – INITIALIZE DRIVE PARAMETERS F5h – SECURITY FREEZE C6h – SET MULTIPLE MODE E1h – IDLE IMMEDIATE C4h(29h) – READ MULTIPLE (EXT) C8h(25h) – READ DMA (EXT) **CAh(35h) – WRITE DMA (EXT)**
Windows XP SP3	NTFS	6	
Server 2003	NTFS	12	
Vista x64	NTFS	7	A1h – ATAPI IDENTIFY DEVICE ECh – IDENTIFY DEVICE EFh – SET FEATURES B0h – SMART F5h – SECURITY FREEZE C6h – SET MULTIPLE MODE C8h(25h) – READ DMA (EXT) **CAh(35h) – WRITE DMA (EXT)**
Server 2008	NTFS	17	

Windows 7 x64	NTFS	22	A1h – ATAPI IDENTIFY DEVICE ECh – IDENTIFY DEVICE EFh – SET FEATURES B0h – SMART F5h – SECURITY FREEZE C6h – SET MULTIPLE MODE C8h(25h) – READ DMA (EXT) **CAh(35h) – WRITE DMA (EXT)** **30h – WRITE SECTOR(S)**
OpenSUSE	NTFS	0	ECh – IDENTIFY DEVICE EFh – SET FEATURES F8h (27h) – READ NATIVE MAX ADDRESS (EXT) E5h – CHECK POWER MODE B0h – SMART C8h(25h) – READ DMA (EXT) **CAh(35h) – WRITE DMA (EXT)**
Fedora	NTFS	0	
OpenSUSE	ext3	7	
OpenSUSE	Ext4	5	
Fedora	ext3	7	

Таблица 3 показывает, что аналогично "холодному" подключению с перезагрузкой ПК, при "горячем" подключении все ОС семейства Windows передают команды записи на НЖМД с файловой системой NTFS, а ОС Linux выполняют запись на логические диски с файловыми системами ext3 и ext4.

Таким образом, при "горячем" подключении НЖМД все исследованные операционные системы вносят изменения в данные без выполнения в этот период каких-либо действий пользователем.

4. Копирование данных на НЖМД

Для определения команд, которыми обмениваются ПК и НЖМД при выполнении копирования данных, на исследуемые накопители штатными средствами операционной системы выполнялось копирование двух наборов файлов: 1) 10 тысяч файлов размеров от 0,5 КБ до 10 КБ; 2) 12 файлов размером от 1 ГБ до 4,5 ГБ.

В ходе экспериментов установлено, что все исследуемые ОС используют для записи файлов на диск только команды WRITE DMA CAh и WRITE DMA EXT 35h. В то же время существуют отличия, связанные с размером блока записи, использованием при копировании команд чтения и команд переноса данных из кэша на пластины (FLUSH CACHE). Полученные результаты приведены в табл. 4.

Таблица 4

Копирование файлов на НЖМД

Операционная система (файловая система)	Большие файлы		Мелкие файлы	
	Размер блока записи (секторов)	Использование FLUSH CACHE (EXT)	Размер блока записи (секторов)	Использование FLUSH CACHE (EXT)
Windows XP SP2 (NTFS)	128	–	32 или 8	Однократно
Windows XP SP3 (NTFS)	128	–	32 или 8	Однократно
Server 2003 (NTFS)	128	Однократно	32 или 8	–
Vista x64 (NTFS)	256	–	до 128	–
Server 2008 (NTFS)	256	–	до 128	–
Windows 7 x64 (NTFS)	256	–	до 128	–
OpenSUSE (NTFS)	1024	–	до 64	–
OpenSUSE (ext3)	1024	Многократно	1024	Многократно
OpenSUSE (ext4)	1024	Многократно	1024	Многократно
Fedora (NTFS)	1024	–	до 128	–
Fedora (ext3)	1024	–	1024	–
FreeBSD (UFS2)	256	-	32	–

Таблица 4 показывает, что операционные системы семейства Windows и FreeBSD оперируют сравнительно небольшим размером блока при копировании файлов большого размера (128 и 256 секторов). Системы Linux выполняют копирование больших файлов с размером блока 1024 сектора независимо от типа файловой системы на НЖМД-приемнике. При копировании файлов маленького размера в ОС Windows и FreeBSD размер блока уменьшается (до 128 и 32 секторов), в ОС Linux он остается равным 1024 секторов при работе с файловыми системами ext3 и ext4.

Благодаря большему размеру блока при записи операции копирования выполняются эффективнее в Linux системах. Особенно заметным преимущество становится при копировании мелких файлов на разделы ext3 и ext4, когда ОС в оперативной памяти объединяет небольшие файлы в группы, значительно сокращая количество дисковых операций.

Интересной особенностью Linux и Unix систем при работе с НЖМД с поддержкой 48-битной адресации является применение 28-битных команд в области первых 128 ГБ накопителя и 48-битных команд за пределами 128 ГБ. При этом Windows системы используют только 48-битные команды.

1. Современные ОС вносят изменения в данные (модифицируют их) на подключенных к системе не загрузочных НЖМД до начала выполнения пользователем каких-либо действий на этапах загрузки и отключения системы, а также при "горячем" подключении НЖМД.

2. При выполнении работ по расследованию компьютерных инцидентов и восстановлению информации обязательным является применение средств блокирования записи, предотвращающих возможность случайного или преднамеренного внесения изменений в данные на исследуемом НЖМД.

3. Новые ревизии стандарта интерфейса ATA вносят поддержку новых команд, которые модифицируют данные на НЖМД, что необходимо учитывать при выборе средств блокирования записи.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Гук М.* Аппаратные интерфейсы ПК. Энциклопедия / М. Гук. – СПб. : Питер. –2002. – 528 с.

2. AT Attachment 8 – ATA/ATAPI Command Set (ATA8-ACS), Rev. 6a, 2008.

3. *Коженевский С.Р.* Безопасность хранения информации на жестких магнитных дисках. Часть I / С.Р. Коженевский. – К.: ООО "ЕПОС". – 2006. – 192 с.

4. Анализатор протоколов EPOS ATA Analyzer. Руководство по эксплуатации. – 2010.

5. *Коженевский С.Р.* Использование анализатора протоколов интерфейса ATA для установления доступа к данным / С.Р. Коженевский // Реєстрація, зберігання і обробка даних. – 2009. – № 4. – Т. 11.

6. www.epos.ua.

7. www.t13.org.

Отримано 31.03.2011