УДК 681.3.06(075)

С.Р. Коженевский,
С.Д. Прокопенко

РЕШЕНИЕ ПРОБЛЕМ СЪЕМА И АНАЛИЗА ДАННЫХ ПРИ РАССЛЕДОВАНИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Рассмотрены способы съема и методы анализа информации при расследовании компьютерных преступлений.

Ключевые слова: *блокиратор записи, информационная безопасность, защита данных, компьютерная криминалистика.*

Розглянуто способи зняття та методи аналізу інформації при розслідуванні комп'ютерних злочинів.

Ключові слова: *блокатор запису, інформаційна безпека, захист даних, комп'ютерна криміналістика.*

Takeoff ways and methods of the analysis of information at the computer crimes investigation are considered.

Keywords: *blockirator records, information safety, protection of the data, computer criminalistics.*

С каждым годом предприятия и государственные учреждения все чаще сталкиваются с инцидентами в области информационных технологий и информационной безопасности. Утечка информации, нарушения информационной безопасности, мошенничество с электронными платежными средствами, хищения конфиденциальной информации и уничтожение электронных документов приводят к значительным убыткам и представляют собой реальную угрозу деятельности организаций.

Проблемами расследования преступлений (инцидентов), совершаемых с помощью или направленных против цифровой техники, занимается относительно молодая прикладная наука – компьютерная криминалистика. В русскоязычной литературе иногда встречается также название "компьютерная форензика", являющееся калькой с широко используемого английского названия computer forensics. Основной задачей компьютерной криминалистики (computer forensics) является извлечение, сохранение, идентификация и документирование цифровых доказательств (улик), находящихся на компьютерах, системах хранения данных, в компьютерных сетях, на мобильных и других цифровых устройствах.

В настоящее время большая часть цифровой информации создается, обрабатывается и сохраняется в накопителях на жестких магнитных дисках (НЖМД). Поэтому этап съема данных и извлечения цифровых доказательств с НЖМД является ключевым в процессе проведения расследования практически любого ИТ инцидента. На этой стадии необходимо решить следующую важнейшую задачу: цифровые доказательства должны быть получены таким образом, чтобы исключить любую возможность внесения в них изменений.

Таким образом, на этапе съема данных (и последующем этапе анализа данных) обязательным требованием является применение так называемых блокираторов записи. Блокиратор записи (write blocker) – это специальное программное или аппаратное средство, которое блокирует передачу через интерфейс на исследуемый накопитель всех команд, которые могут привести к модификации данных, но обеспечивают прозрачный доступ к данным в режиме чтения.

Принципы взаимодействия ПК с жестким диском

Современные жесткие диски подключаются к компьютеру с помощью одного из доступных физических интерфейсов. В настоящее время в большинстве компьютеров применяются жесткие диски с интерфейсами Serial ATA (SATA) и Parallel ATA (ATA, IDE); внешние НЖМД обычно подключаются по интерфейсам USB и FireWire; в серверах распространены SAS (Serial Attached SCSI) и SCSI диски.

Чтобы получить доступ к жесткому диску и записать или сосчитать с него какие-либо данные, компьютерная система должна обменяться с ним неким набором команд через соответствующий интерфейсный контроллер. В настоящее время наборы команд и протоколы передачи данных унифицированы и описаны в спецификациях соответствующих интерфейсов подключения накопителя к ПК. В наиболее распространенных жестких дисках с интерфейсами SATA и PATA применяется система команд, основанная на спецификациях стандарта ATA.

Стандарт интерфейса ATA (AT Attachment) вот уже почти 20 лет широко используется в компьютерной индустрии. С 1994 года Технический комитет T13, отвечающий за развитие стандарта, выпустил уже восемь его версий, в настоящее время разрабатывается и уже доступен рабочий проект следующей его ревизии.

В таблице 1 привсдены 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 стандарга	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 логиический/ физический сектор
ATA/ATAPI-8	2008	77 (15)	WRITE FPDMA QUEUED	Поддержка гибридных накопителей с энергонезависимым кэшем

Спецификации протокола ATA всего определяют 256 возможных кодов команд. Не все из них являются действующими и поддерживаются накопителями. Так, в текущей ревизии ATA-8 из 256 возможных кодов только около 80 определено как команды общего назначения. Остальные команды описаны как зарезервированные (reserved), выбывшие (retired), устаревшие (obsolete) или вендор-команды (vendor specific). Например, ревизия ATA-8 содержит описания 59 кодов выбывших и устаревших команд. Такие команды были действующими и использовались в предыдущих версиях стандарта.

Из таблицы 1 видно, 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 восьми стандартах: WRITE BUFFER (E8h), WRITE SECTORS with retries (30h), WRITE MULTIPLE (C5h) и WRITE DMA (CAh). В четырех ревизиях в дополнение к существующим вводились новые команды записи; шесть команд записи были выведены из списка поддерживаемых. Таким образом, при работе с НЖМД необходимо понимать, что набор команд ATA изменяется со временем.

В то же время это создает проблемы для специалистов в области расследования компьютерных инцидентов. При принятии очередной ревизии стандарта необходимо обновлять программные и аппаратные средства (в первую очередь блокираторы записи) и проводить их тщательное исследование и тестирование. В обратном случае возможна ситуация, когда данные на жестком диске будут модифицированы с помощью новых команд записи.

Например, эксперту необходимо произвести съем данных на современном жестком диске с поддержкой ATA-8. Если для этого использовать блокиратор записи, разработанный в соответствии со спецификациями ATA-6, то данные на таком диске могут быть модифицированы шестью различными командами записи (WRITE DMA FUA EXT, WRITE DMA QUEUED FUA EXT, WRITE MULTIPLE FUA EXT, WRITE STREAM DMA EXT, WRITE STREAM EXT). Такие команды не описаны в стандарте ATA-6, поэтому для блокиратора они не будут являться запрещенными командами записи, следовательно, они могут быть переданы в накопитель.

Необходимо отметить, что в большинстве случаев пользователь ПК не может контролировать, какие именно команды будут использованы компьютером для доступа к жесткому диску. В различных операционных системах (и даже различных версиях одной и той же ОС) для чтения и записи данных на диск 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 используемого программного обеспечения и набора драйверов.

Исследование взаимодействия ПК – жесткий диск

Специалистами Центра восстановления информации ЕПОС были проведены исследования для определения фактических команд, которыми обмениваются компьютер и жесткий диск в различных режимах работы ПК.

Регистрация команд, передаваемых компьютером в накопитель, 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).

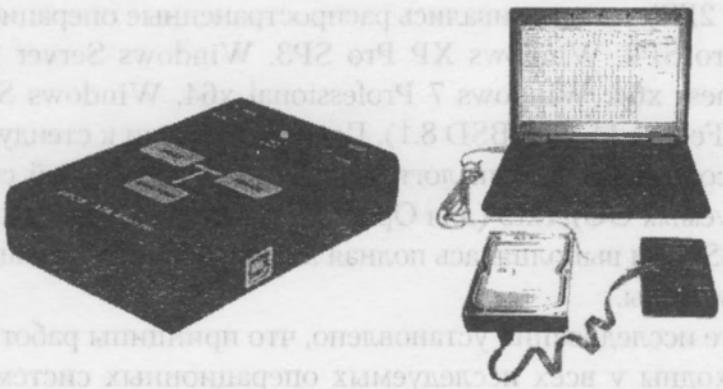

Рис. 1. Анализатор протоколов EPOS ATA Analyzer

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.

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 этапе 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).

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
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

Из таблицы 2 видно, что ОС Windows XP SP2, XP SP3, Server 2003, Windows 7 x64 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.

Следует 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.

По результатам исследования установлено, что Linux и UNIX не выполняют запись на "не родную" для себя файловую систему NTFS. Однако при настройках по умолчанию они выполняют операции записи при монтировании файловых систем Ext3 и UFS2 соответственно. ОС семейства Linux и UNIX поддерживают возможность монтирования логических дисков в режиме "только для чтения" (с ключом **-ro**). В то же время, 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.

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 таблице 3.

Таблица 3

"Горячее" подключение НЖМД

Операционная система	Файловая система	Количество команд записи
Windows XP SP2	NTFS	20
Windows XP SP3	NTFS	6
Server 2003	NTFS	12
Vista x64	NTFS	7
Server 2008	NTFS	17
Windows 7 x64	NTFS	22
OpenSUSE	NTFS	0
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).

Исследование показало, 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 сектор 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.

Современные блокираторы записи для расследования компьютерных преступлений

Использование аппаратных блокираторов записи является обязательным гребованием в процессе расследования компьютерных преступлений (инцидентов) на этапах съема и анализа данных. В то же время, по ряду объективных и субъективных причин в Украине сложилась ситуация, когда это требование выполняется далеко не всегда – в некоторых случаях исследования и экспертизы выполняются совсем без применения таких устройств, в других случаях применяется устаревшее оборудование. В качестве примера можно привести блокираторы FastBloc 2 производства Guidance Software. Они совместимы с жесткими дисками с поддержкой спецификаций ATA-5 и ATA-6, хотя большинство современных HDD разрабатываются в соответствии с требованиями ATA-7 и ATA-8.

Ниже приведен обзор доступных на украинском рынке аппаратных блокираторов записи, обеспечивающих возможность работы с современными накопителями.

Блокиратор записи EPOS WriteProtector

Аппаратный блокиратор записи EPOS WriteProtector предназначен для предотвращения случайного или преднамеренного внесения изменений в данные на HDD при выполнении работ по расследованию компьютерных инцидентов и преступлений (computer forensics). Благодаря этому достигается получение юридически значимых результатов при проведении исследования и анализе информации на HDD.

Рис. 2. Аппаратный блокиратор записи EPOS WriteProtector

Блокиратор записи EPOS WriteProtector работает абсолютно прозрачно для ПК и программного обеспечения. Таким образом, эксперт может использовать любую необходимую ему в процессе исследования платформу (DOS, Windows, Linux, MacOS, Unix...) и набор экспертного ПО (EnCase, X-Ways Forensics, FTK, The Sleuth Kit...).

EPOS WriteProtector – один из немногих доступных аппаратных блокираторов записи с поддержкой SATA и PATA HDD, который разработан в соответствии с требованиями последней версии стандарта протокола ATA-8. Это гарантирует защиту от записи на современные жесткие диски последних моделей, поддерживающие новые наборы команд записи.

EPOS WriteProtector обеспечивает возможность выбора режима работы с защищенной зоной жесткого диска Host Protected Area (HPA). В зависимости от ситуации эксперт может включать или отключать блокирование набора команд HPA Feature Set с индикацией выбранного режима.

Небольшие размеры и вес позволяют работать с блокиратором как в лаборатории, так и на выезде.

Мультиинтерфейсный блокиратор записи ICS Super DriveLock

Аппаратный блокиратор записи производства американской компании Intelligent Computer Solutions ICS Super DriveLock гарантирует защиту от записи на жесткие диски с интерфейсами SATA, PATA, USB, SCSI.

Он разработан как портативное устройство, которое подключается к компьютеру или ноутбуку через интерфейс e-SATA. Конструкция ICS Super DriveLock позволяет использовать его как в качестве внешнего устройства, так и для установки в стандартный 5,25" отсек стационарного ПК.

Рис. 3. Мультиинтерфейсный блокиратор записи ICS Super DriveLock

К основным особенностям ICS Super DriveLock относятся возможность горячего подключения жестких дисков, SSD накопителей, Flash носителей с интерфейсами SATA, PATA, USB, SCSI; поддержка накопителей с напряжением питания 3,3 В; детектирование скрытых областей жестких дисков HPA и DCO; возможность апгрейда внутренней прошивки.

Устройство неразрушающего съема и анализа данных ICS ImageMASSter Solo-4 Forensic

Многофункциональный прибор ICS ImageMASSter Solo-4 Forensic значительно расширяет возможности традиционных блокираторов записи. Он

представляет собой портативное устройство для неразрушающего копирования информации с жестких дисков, внешних носителей, ноутбуков и ПК по интерфейсам SATA, SAS, e-SATA, USB, PATA и SCSI на другой носитель, персональный компьютер или локальную сеть. Кроме того, прибор обеспечивает возможность предварительного просмотра данных перед созданием копии.

Рис. 4. Устройство неразрушающего съема и анализа данных ICS ImageMASSter Solo-4 Forensic

Прибор построен на операционной системе Windows XP и имеет встроенный жесткий диск достаточно большой емкости. Это позволяет устанавливать на него необходимый набор экспертного ПО для анализа данных. При этом ICS ImageMASSter Solo-4 Forensic фактически превращается в портативную лабораторию для расследования компьютерных происшествий, не требующую использования дополнительного ПК.

ICS ImageMASSter Solo-4 Forensic обеспечивает широкие возможности по съему данных: копирование с одного носителя на один носитель (режим одиночной копии), копирование с одного носителя одновременно на два носителя (режим тиражирования), копирование с двух накопителей на два накопителя (режим параллельного копирования). Для защиты данных на копии поддерживается режим шифрования копируемых данных "на лету" по стандарту AES 192/256, также предусмотрена поддержка хэш верификации (MD5, SHA-1, SHA-2) без потери скорости копирования.

Важной особенностью прибора является возможность съема данных на ноутбуках и компьютерах без вскрытия их корпуса.

В таблице 4 приведены основные сравнительные характеристики рассмотренных приборов.

Таблица 4

Сравнительные характеристики

	EPOS WriteProtector	**Super DriveLock**	**ImageMASSter Solo-4 Forensic**
Производитель	ООО "ЕПОС", www.epos.ua	Intelligent Computer Solutions, www.ics-iq.com	Intelligent Computer Solutions, www.ics-iq.com
Поддерживаемые интерфейсы	SATA, PATA	SATA, PATA, USB, SCSI	2 x SAS/SATA, 2 x USB eSATA, PATA, SCSI
Поддержка стандарта ATA	ATA-8	ATA-7	ATA-8

Поддерживаемые ОС	Любые	Windows XP, Vista, Linux	–
Размеры, мм	110 x 75 x 25	146 x 83 x 29	270 x 98 x 194
Вес, г	100	455	2,5
Дополнительные возможности	Управление режимом блокирования команд для работы со скрытой областью HPA	Поддержка накопителей с напряжением питания 3,3В. Детектирование скрытых областей жестких дисков HPA и DCO	Съем данных без вскрытия корпуса ПК/ ноутбука Хэширование и шифрование данных на лету. Съем данных в скрытых областях HPA и DCO
Ориентировочная стоимость (базовая комплектация), грн	2,150	9,800	30,600

Выводы. 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.

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.

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

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

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

4. [Электронный ресурс]. – Режим доступа : www.epos.ua.

5. [Электронный ресурс]. – Режим доступа : www.t13.org.

Отримано 05.06.2011