УДК 681.3.06(075) **Коженевский С.Р., Прокопенко С.Д.**

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ АНАЛИЗАТОРА ПРОТОКОЛОВ ИНТЕРФЕЙСА ATA ДЛЯ ВОССТАНОВЛЕНИЯ ДАННЫХ НА НЖМД

Введение

Стандарт интерфейса ATA (AT Attachment) широко используется для подключения устройств хранения данных, таких как НЖМД, оптических приводов, твердотельных накопителей SSD на основе Flash памяти и т.п., уже более 20 лет. В настоящее время индустрия заканчивает переход от параллельного интерфейса Parallel ATA к последовательному интерфейсу Serial ATA, который сохраняет полную программную совместимость с Parallel ATA на логическом уровне, хотя и отличается на физическом и транспортном уровнях.

Разработчики аппаратных и программных средств, работающих с носителями информации, часто сталкиваются с необходимостью регистрации и анализа данных, передаваемых по интерфейсу ATA. Для решения этих задач применяются анализаторы протоколов интерфейса ATA.

В частности, компания LeCroy предлагает линейку анализаторов протоколов для интерфейса SATA. Такие анализаторы работают на физическом и транспортном уровне, имея ограниченные возможности по регистрации команд и данных, передаваемых по интерфейсу. К относительным недостаткам подобных систем можно отнести ограниченный объем регистрируемых данных и сравнительно высокую стоимость.

Анализатор протоколов интерфейса ATA EPOS ATA Analyzer

В компании ЕПОС разработан анализатор протоколов интерфейса ATA - EPOS ATA Analyzer, который работает на логическом уровне и предназначен для регистрации и отображения данных и команд протокола. Анализатор состоит из двух частей:

1) аппаратного регистратора, который прослушивает анализируемую шину, по которой производится обмен данными;

2) программного обеспечения, которое обеспечивает просмотр и анализ собранных данных.

Типовая схема подключения анализатора протоколов EPOS ATA Analyzer приведена на рис. 1.

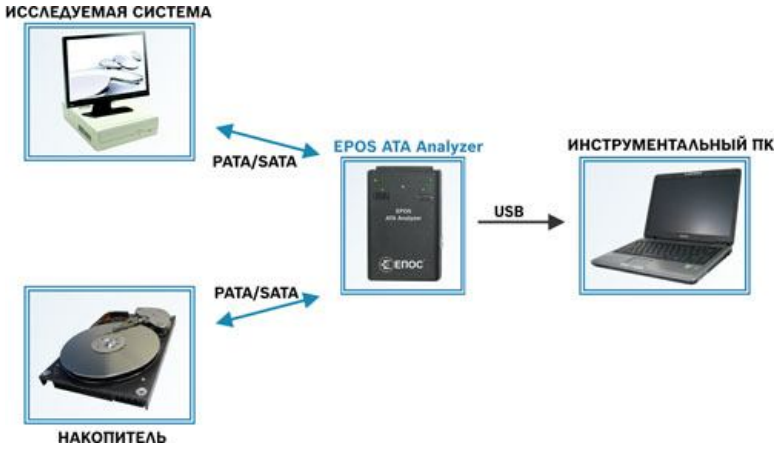


Рис. 1. Типовая схема подключения анализатора протокола EPOS ATA Analyzer

Анализатор EPOS ATA Analyzer представляет собой универсальное инструментальное средство анализа протоколов интерфейса ATA, предназначенное для регистрации и

отображения команд и данных, передаваемых между любыми устройствами с интерфейсами Parallel ATA или Serial ATA. Анализатор разработан с учетом требований инженеров и разработчиков, которым необходим простой в использовании, но функциональный инструмент, обеспечивающий возможность работы как в стационарных условиях, так и на выезде. Он подключается к ноутбуку (или другому инструментальному ПК) по высокоскоростному интерфейсу USB 2.0 и обеспечивает регистрацию, сохранение и обработку протоколов взаимодействия устройств с интерфейсами ATA.

Внешний вид анализатора EPOS ATA Analyzer приведен на рис. 2.

Рис. 2. Анализатор протокола EPOS ATA Analyzer

Структурная схема анализатора протоколов интерфейса ATA EPOS ATA Analyzer приведена на рис. 3.

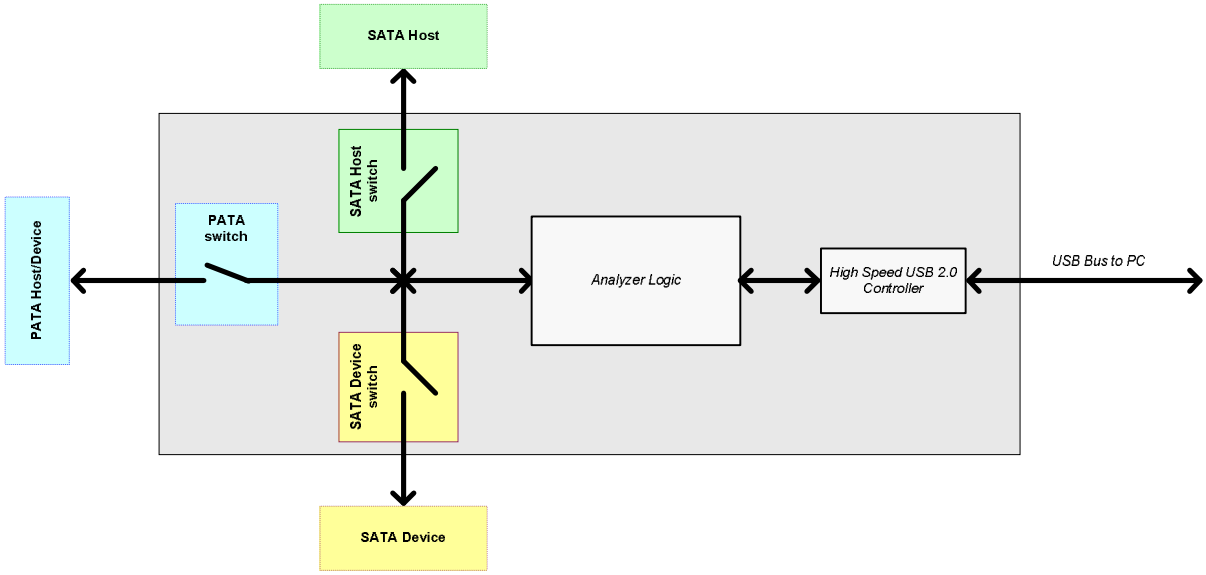
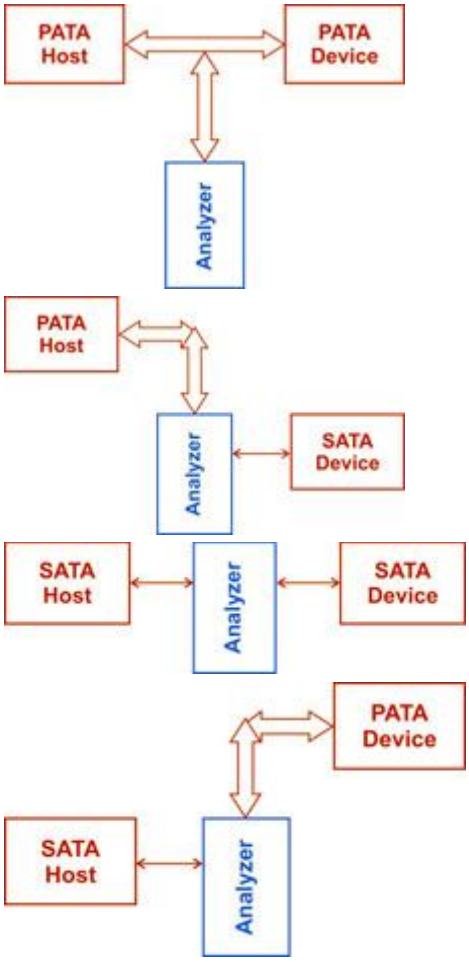


Рис. 3. Структурная схема анализатора протокола EPOS ATA Analyzer

Анализатор разработан с учетом требований самой последней версии спецификации интерфейса ATA-8. Он обеспечивает работу с хостами и устройствами с интерфейсами Parallel ATA и Serial ATA в любых комбинациях. Другими словами, к SATA хосту может быть подключено как SATA устройство, так и PATA устройство, и наоборот, к PATA хосту можно подключать PATA и SATA устройства. Схемы подключения анализатора EPOS ATA Analyzer приведены на рис. 4.



а) PATA хост --> PATA устройство

б) PATA хост --> SATA устройство

в) SATA хост --> SATA устройство

г) SATA хост --> PATA устройство

Рис. 4. Схемы подключения анализатора EPOS ATA Analyzer

EPOS ATA Analyzer представляет собой специальный адаптер, 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.

Возможности анализатора EPOS ATA Analyzer обеспечивают ему широкий спектр применений. В частности, он может использоваться:

- в качестве инструмента для разработки и отладки устройств и программного обеспечения, работающих с накопителями по интерфейсам PATA и SATA;
- в исследовательских и учебных целях для изучения работы дисковой подсистемы ПК;
- для оценки работы специального ПО, например, при поиске в нем программных закладок;
- для выявления специальных команд (т.н. вендор команд), используемых в технологических режимах работы накопителей в процессе ремонта и восстановления данных;
- для исследования взаимодействия программных и аппаратных криптографических средств с дисковой подсистемой ПК с целью поиска в них уязвимостей;
- для определения и снятия паролей, установленных на жестких дисках;
- для выявления алгоритмов взаимодействия специального оборудования (промышленных устройств, медицинской техники, автомобильных бортовых ПК и т.п.) с установленными в нем жесткими дисками при ремонте и восстановлении работоспособности такого оборудования;

- в любых других приложениях, где необходимы регистрация и анализ данных и команд, передаваемых по интерфейсу ATA при взаимодействии хоста с накопителями.

Основные характеристики анализатора EPOS ATA Analyzer приведены в табл. 1.

Таблица 1. Основные технические характеристики анализатора EPOS ATA Analyzer

Характеристика	Значение
Поддержка интерфейса ATA	Спецификация ATA-8
Физический тип анализируемого интерфейса	- Parallel ATA - Serial ATA (SATA 1, SATA 2)
Состав регистрируемых данных	- Адреса и содержание ATA регистров - Данные, передаваемые в режимах PIO и DMA - Тип выполняемой операции (запись / чтение)
Скорость передачи данных между анализатором и инструментальным ПК	До 33 Мбайт/сек
Объем регистрируемых данных	Не ограничен
Интерфейс с инструментальным ПК	HighSpeed USB 2.0
Габаритные размеры	111 x 75 x 25 мм
Электропитание	По шине USB

Методика восстановления данных на НЖМД, закрытых паролем

Рассмотрим пример использования анализатора EPOS ATA Analyzer в задачах восстановления данных на жестких дисках, закрытых с помощью парольной защиты, описываемой стандартом ATA.

Начиная со спецификации ATA-3, в стандарт ATA введена группа команд защиты – Security. С точки зрения защиты накопитель может находиться в одном из трех состояний:

1) **Unlocked** (открыто) – накопитель выполняет все свойственные ему команды.

2) **Locked** (закрыто) – накопитель отвергает все команды, связанные с передачей данных. Допустимы только команды общего управления, мониторинга состояния, управления энергопотребления и команда защиты ***SECURITY UNLOCK***.

3) **Frozen** (заморожено) – накопитель отвергает все команды управления защитой, но выполняет все остальные. Из этого состояния накопитель может выйти только по аппаратному сбросу или при следующем включении питания.

В соответствии со стандартом ATA система безопасности стандартного жесткого диска поддерживает установку двух видов паролей: главного (Master password) и пользовательского (User password); и двух уровней защиты – высокого (High level) и максимального (Maximum level). При высоком уровне защиты накопитель можно открыть любым из двух паролей. При максимальном уровне устройство открывается только пользовательским (User) паролем, а по главному паролю доступна только команда стирания, при это все данные на накопителе будут стерты.

Специалисты Центра восстановления информации ЕПОС регулярно сталкиваются с проблемой получения доступа к данным на НЖМД, закрытом паролем. Для ряда моделей жестких дисков разработаны специальные аппаратно-программные средства, обеспечивающие сброс пароля. Однако перечень поддерживаемых накопителей ограничен, как правило, в него не входят устаревшие и непопулярные на локальном рынке модели, а также новейшие модели накопителей. Существует ряд способов, позволяющих «обмануть» накопитель и установить собственный пароль, а затем с его помощью получить доступ к данным.

Недостатком таких подходов является то, что они являются деструктивными по отношению к паролю. Другими словами, они обеспечивают доступ к данным, но приводят к потере самого пароля. В то же время, во многих случаях пароль является неотъемлемой составляющей нормального функционирования сложных программно-аппаратных комплексов и автоматизированных рабочих мест, на которых необходимо выполнить работы по восстановлению данных. Сброс пароля приводит к невозможности восстановить работоспособность такой системы.

Такая ситуация характерна, например, для промышленного оборудования и медицинской техники зарубежного производства. В этих системах для защиты хранящихся данных и программного обеспечения используется парольная защита НЖМД, причем пароль устанавливается на этапе производства и не сообщается владельцу оборудования. Загрузка операционной системы при этом происходит прозрачно для оператора, поскольку пароль на жесткий диск вводится автоматически на этапе загрузки BIOS. В то же время при подключении накопителя к другому ПК доступ к данным блокируется, а оборудование не будет работать, если сбросить пароль на НЖМД.

Таким образом, существующие методы восстановления данных на закрытых паролем НЖМД не всегда обеспечивают возможность сохранения и/или восстановления работоспособности оборудования, в котором установлены такие накопители. Решить подобную проблему можно путем применения в процессе восстановления данных анализатора протокола ATA, поскольку пароль передается по интерфейсу в явном виде и его можно перехватить.

Методика восстановления данных с помощью анализатора протокола EPOS ATA Analyzer на закрытом паролем НЖМД, который установлен в специализированном оборудовании, состоит из следующих этапов:

1. ***Восстановление работоспособности НЖМД***.

При необходимости, в случае неисправности жесткого диска, выполняется комплекс технологических операций по диагностике и восстановлению его работоспособности, достаточный для выхода накопителя в состояние готовности.

2. ***Съем протокола*** обмена данными между исследуемой системой (хостом) и накопителем с помощью анализатора EPOS ATA Analyzer.

Анализатор EPOS ATA Analyzer включается в разрыв между системой и НЖМД. Сохранение протокола производится на отдельный инструментальный ПК. В табл. 2 приведены фрагменты протокола, снятого с помощью EPOS ATA Analyzer на этапе загрузки аппарата УЗИ (ультразвукового исследования).

3. ***Анализ протокола для определения пароля***.

После сохранения протокола производится его анализ с целью определения пароля (паролей), установленного на исследуемом НЖМД.

Из табл. 2 видно, что в записи №8 исследуемое устройство (хост) передало в накопитель команду ***IDENTIFY DEVICE***, в ответ на которую в записи №18 накопитель вернул паспорт. Следующей командой ***SECURITY UNLOCK*** (запись №26) хост подготовил накопитель к приему пароля. В блоке данных размером 512 байт в накопитель в явном виде был передан пароль (запись №36).

Таблица 2. Фрагмент протокола, снятого на этапе загрузки аппарата УЗИ

№ записи	**Направ-ление**	**Регистр ATA**	**Код регистров/ длина блока данных**	**Примечание**
0001	Rd	Alternate status	50	Device ready
0002	Wr	Features	00	
0003	Wr	LowLBA	01	
0004	Wr	Middle LBA	00	
0005	Wr	High LBA	00	
0006	Wr	Device/Head	A0	
0007	Wr	Sector count	01	
0008	***Wr***	***Command***	***EC***	***IDENTIFY DEVICE***
0009	Rd	Alternate status	D0	Not ready
0010	Rd	Alternate status	58	Data ready
0011	Rd	Status	58	Data ready
0012	Rd	Error	00	ICRC=0, UNC=0, MC=0, IDNF=0, MCR=0, ABRT=0, NM=0, MED=0
0013	Rd	LowLBA	01	
0014	Rd	Middle LBA	00	
0015	Rd	High LBA	00	
0016	Rd	Device/Head	A0	
0017	Rd	Sector count	00	
0018	**Rd**	**Data**	**512**	
0019	Rd	Alternate status	50	Device ready
0020	Wr	Features	00	
0021	Wr	LowLBA	01	
0022	Wr	Middle LBA	00	
0023	Wr	High LBA	00	
0024	Wr	Device/Head	A0	
0025	Wr	Sector count	00	
0026	***Wr***	***Command***	***F2***	***SECURITY UNLOCK***
0027	Rd	Alternate status	D0	Not ready
0028	Rd	Alternate status	58	Data ready
0029	Rd	Status	58	Data ready
0030	Rd	Error	00	ICRC=0, UNC=0, MC=0, IDNF=0, MCR=0, ABRT=0, NM=0, MED=0
0031	Rd	Low LBA	01	
0032	Rd	Middle LBA	00	
0033	Rd	High LBA	00	
0034	Rd	Device/Head	A0	
0035	Rd	Sector count	00	
0036	**Wr**	**Data**	**512**	
0037	Rd	Alternate status	D0	Not ready
0038	Rd	Alternate status	50	Device ready
0039	Rd	Status	50	Device ready
0040	Rd	Error	00	ICRC=0, UNC=0, MC=0, IDNF=0, MCR=0, ABRT=0, NM=0, MED=0
0041	Rd	Low LBA	01	
0042	Rd	Middle LBA	00	
0043	Rd	High LBA	00	
0044	Rd	Device/Head	A0	
0045	Rd	Sector count	FF	
0046	Rd	Alternate status	50	Device ready
…	…	…	…	…

Изображение сектора с паролем в шестнадцатеричной форме приведено на рис. 5.

```
00 00 14 12 1F 14 19 1E  1F 1F 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Рис. 5. Пароль, установленный на НЖМД

Из рис. 5 видно, что на накопителе установлен User пароль, уровня High level (об этом говорят байты 0000h в начале сектора). Следующие 8 символов в шестнадцатеричной форме (14h, 12h, 1Fh, 14h, 19h, 1Eh, 1Fh, 1Fh) соответствуют паролю.

4. ***Копирование данных*** на исправный накопитель и восстановление информации.

После ввода определенного на предыдущем этапе пароля НЖМД предоставляет доступ к сохраненным на нем данным. Это дает возможность скопировать их на исправный накопитель и при необходимости устранить логические разрушения информации.

5. ***Перенос восстановленных данных*** на целевой накопитель.

После восстановления данных они переносятся на новый или отремонтированный исходный НЖМД, после чего на него устанавливается оригинальный пароль. Благодаря этому удается сохранить работоспособность оборудования, в котором использовался накопитель.

Выводы

Существующие методы восстановления данных на закрытых паролем НЖМД не всегда обеспечивают возможность сохранения и/или восстановления работоспособности оборудования, в котором установлены такие накопители.

Анализатор протоколов EPOS ATA Analyzer обеспечивает возможность регистрации и определения паролей, передаваемых через интерфейс в явном виде. Это обеспечивает возможность восстановления данных на НЖМД, закрытых паролем, с сохранением работоспособности оборудования, в котором применяются такие накопители.

Список литературы

1. INCITS 452-2008 (D1699): AT Attachment 8 - ATA/ATAPI Command Set.

2. Гук М. Интерфейсы устройств хранения: ATA, SCSI и другие. Энциклопедия. – СПб.: Питер, 2007. – 447с.

Поступила 1.12.09