Аппаратный блокиратор записи

EPOS WriteProtector

Руководство пользователя

ООО «ЕПОС»
ул. Верхний Вал, 44, г. Киев, 04071, Украина
www.epos.ua

Декабрь 2011
Вер. 1.2

Продажа и поддержка

Центр восстановления информации ЕПОС
ул. Верхний Вал, 34, г. Киев, 04071, Украина
www.epos.ua/recovery

Тел. +380 (44) 467-7540
Факс: +380 (44) 467-7547
e-mail: recovery@epos.ua

Содержание

1. Введение

1.1. Общее описание прибора

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.

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, The Sleuth Kit…).

EPOS WriteProtector 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 условиях лаборатории, так и на выезде.

Внешний вид прибора EPOS WriteProtector

1.2. Особенности и характеристики прибора

- Работает прозрачно для программного обеспечения
- Возможность ручного включения/отключения выполнения команд для работы с защищенной областью HPA
- Возможность «горячего» подключения
- Высокая скорость передачи данных
- Поддержка НЖМД любой емкости
- Не требует установки дополнительных драйверов
- Небольшие размеры и вес

Характеристика	**Значение**
Интерфейс	SATA (вход и выход)
Поддерживаемые НЖМД	2,5”/3,5” SATA HDD 1,8”/2,5”/3,5” PATA HDD (с адаптером) 1,8” ZIF PATA HDD (с адаптером)
Пропускная способность	До 8 ГБ/мин
Совместимость со стандартом ATA	ATA-8
Поддержка HPA команд	Ручной переключатель для включения/отключения HPA команд
Совместимость с ОС	Любые (в том числе DOS, Windows XP, Vista, 7, Linux, MacOS, Unix)
Габаритные размеры	111 x 75 x 25 мм
Вес	100 г.
Электропитание	+5В 2А, +12В 2А

1.3. Комплект поставки прибора

№ п/п	**Наименование**	**Кол-во**	**Комплект поставки**	
			WP-01	WP-02
2.1	Блокиратор EPOS ATA WriteProtector	1 шт.	+	+
2.2	Интерфейсный SATA шлейф	2 шт.	+	+
2.3	Кабель питания 4pin P4-4pin Molex	1 шт.	+	+
2.4	Кабель питания 4pin P4-SATA power	1 шт.	+	+
2.5	Y-кабель питания 4pin P4-4pin Molex/SATA	1 шт.		+
2.6	Руководство пользователя	1 шт.	+	+
2.7	Технический паспорт	1 шт.	+	+
2.8	Адаптер SATA-PATA	1 шт.		+
2.9	Адаптер для подключения 2,5" PATA HDD, 1,8" ZIF PATA HDD/SSD, 1,8" PATA HDD/SSD	1 кт.		+
2.10	Интерфейсный шлейф eSATA –SATA	1 шт.		+
2.11	Блок питания 5В, 12В 2А	1 шт.		+
2.12	Сумка для переноса	1 шт.		+

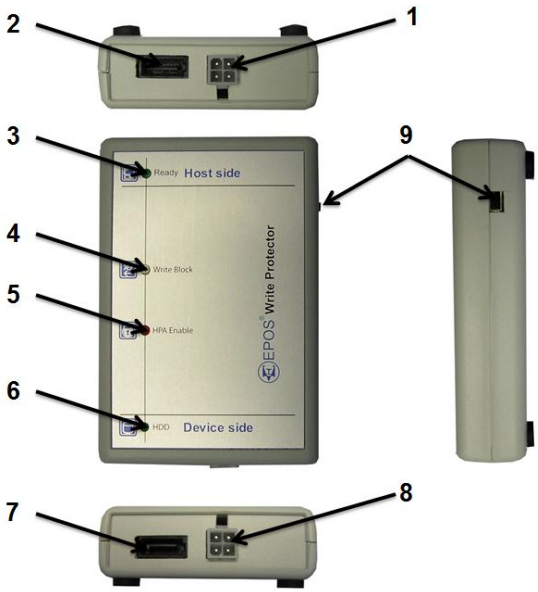
1.4. О данном Руководстве

Благодарим за приобретение прибора EPOS WriteProtector. Перед началом работы с прибором внимательно прочитайте данное Руководство и сохраните его в качестве справочника.

Компания ЕПОС непрерывно совершенствует свои изделия. Как технические характеристики, так и данное Руководство могут изменяться без предварительного уведомления.

2. Установка прибора

2.1. Органы управления и индикации прибора



Органы управления и индикации прибора

1. Разъем Host SATA Power. Подключение питания прибора.
2. Разъем Host SATA. Интерфейс для подключения прибора к хосту (ПК).
3. Светодиод Ready. Светится при готовности прибора.
4. Светодиод WriteBlock. Индикация блокирования команды записи.
5. Светодиод HPA Enable. Индикация режима поддержки HPA команд; светится при разрешенной передаче команд HPA.
6. Светодиод HDD. Индикация активности НЖМД.
7. Разъем Host SATA Power. Подключение питания НЖМД.
8. Разъем HDD SATA. Интерфейс для подключения НЖМД к прибору.
9. Переключатель HPA Enable. Переключение режима поддержки HPA команд.

2.2. Начало работы с прибором

1. Подключите интерфейсный шлейф SATA и кабель питания к прибору и исследуемому НЖМД (особенности работы с PATA НЖМД описаны в п. 3.1 данного Руководства).
2. Подключите интерфейсный шлейф SATA к прибору и ПК (особенности работы по интерфейсу eSATA описаны в п. 3.1 данного Руководства).
3. Подключите кабель питания прибора к блоку питания ПК или входящему в комплект поставки БП. Включите блок питания.
4. После включения питания на приборе загорится светодиод Ready. Если SATA контроллер и установленные в текущей ОС драйверы контроллера ПК поддерживают возможность горячего подключения дисковых устройств, то после автоматического определения исследуемого НЖМД загорится светодиод HDD. В противном случае необходимо вручную запустить процесс определения НЖМД. В операционной системе исследуемый НЖМД определится с приставкой «WP» в конце строки модели. Например, жесткий диск Samsung HD502HJ будет детектироваться как «Samsung HD502HJ WP».
5. После завершения работы с исследуемым НЖМД выключите блок питания, отключите прибор от ПК, отключите НЖМД от прибора.

3. Подключение и режимы работы прибора

3.1. Подключение прибора

В этом разделе описаны варианты подключения НЖМД с различными интерфейсами.

3.1.1. Горячее подключение

Для использования горячего подключения необходимо, чтобы:

- в БИОС ПК для SATA контроллера был установлен режим AHCI;
- SATA контроллер поддерживал горячее подключение;
- используемый в системе драйвер SATA контроллера поддерживал горячее подключение.

В противном случае возможно только холодное подключение с перезагрузкой ПК.

Основным признаком корректного подключения прибора и его готовности к работе является зеленый цвет светодиодов Ready и HDD.

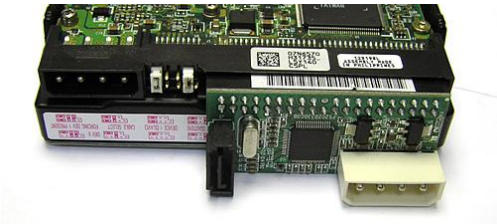
При первом подключении устройства дополнительно убедитесь, что операционная система корректно опознала исследуемый НЖМД. Для этого в панели **Управление компьютером** откройте **Диспетчер устройств** и проверьте наличие исследуемого НЖМД в ветке **Дисковые устройства**. В операционной системе исследуемый НЖМД определится с приставкой «WP» в конце строки модели. Например, жесткий диск Samsung HD502HJ будет детектироваться как «Samsung HD502HJ WP». В свойствах SATA контроллера, к которому подключено устройство, проверьте назначенный режим передачи данных – допустимым является любой режим **UDMA**.

При горячем подключении прибора обязательно сначала подключается НЖМД к прибору, затем прибор с подключенным НЖМД к компьютеру.

3.1.2. Подключение 3,5" PATA (IDE) НЖМД

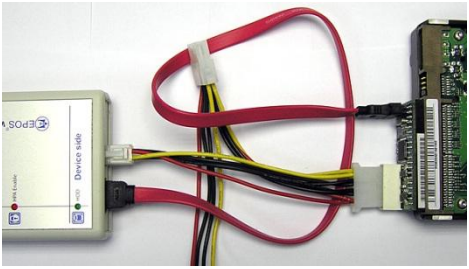
Для работы с IDE HDD необходим адаптер SATA-PATA. При подключении PATA НЖМД рекомендуется придерживаться следующей процедуры:

1. Перед началом работы с PATA НЖМД убедитесь, что накопитель установлен в режим Master/Single (обратитесь к документации на НЖМД для инструкций).
2. Подключите адаптер к интерфейсному разъему НЖМД. Разъем питания адаптера должен находиться с противоположной стороны от разъема питания НЖМД.



Подключение адаптера к НЖМД

3. С помощью входящего в комплект поставки Y-кабеля подключите питание адаптера и питание НЖМД.
4. Подключите НЖМД с адаптером к прибору с помощью кабеля питания и интерфейсного SATA шлейфа.



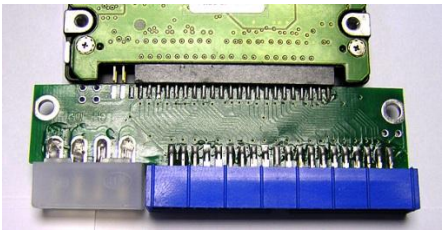
Подключение PATA НЖМД к прибору

Прибор работает с PATA HDD только в режиме UltraDMA (режим PIO не поддерживается). Поэтому для PATA HDD не поддерживается обработка дефектов.

3.1.3. Подключение 2,5" PATA (IDE) НЖМД

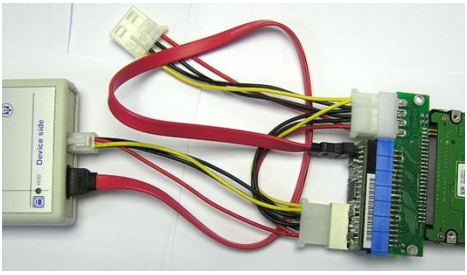
Подключение 2,5" PATA НЖМД осуществляется через адаптер SATA-PATA и дополнительный адаптер PATA 3,5" – PATA 2,5". При подключении 2,5" PATA НЖМД рекомендуется придерживаться следующей процедуры:

1. Перед началом работы с 2,5" PATA НЖМД убедитесь, что накопитель установлен в режим Master/Single (обратитесь к документации на НЖМД для инструкций).
2. Подключите адаптер PATA 3,5" – PATA 2,5"к интерфейсному разъему НЖМД. Разъем питания адаптера должен находиться с левой стороны, если смотреть на контроллер НЖМД сверху.



Подключение адаптера к НЖМД

3. С помощью входящего в комплект поставки Y-кабеля подключите питание адаптера и питание НЖМД.
4. Подключите НЖМД с адаптером к прибору с помощью кабеля питания и интерфейсного SATA шлейфа.



Подключение PATA НЖМД к прибору

3.1.4. Подключение 1,8" PATA (IDE) НЖМД

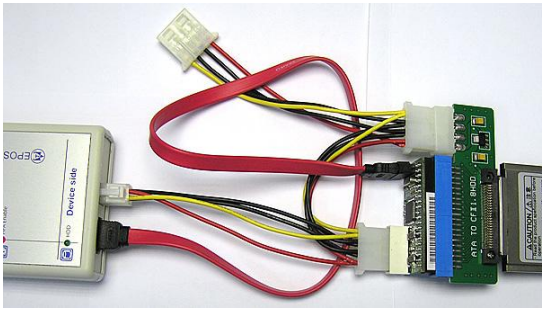
Подключение 1,8" PATA НЖМД осуществляется через адаптер SATA-PATA и дополнительный адаптер PATA 3,5" – PATA 1,8". При подключении 1,8" PATA НЖМД рекомендуется придерживаться следующей процедуры:

1. Подключите адаптер PATA 3,5" – PATA 2,5"к интерфейсному разъему НЖМД. Разъем питания адаптера должен находиться с левой стороны, если смотреть на контроллер НЖМД сверху.

Подключение адаптера к НЖМД

2. С помощью входящего в комплект поставки Y-кабеля подключите питание адаптера и питание НЖМД.

3. Подключите НЖМД с адаптером к прибору с помощью кабеля питания и интерфейсного SATA шлейфа.

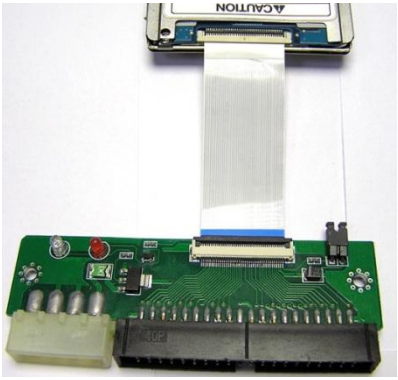


Подключение PATA НЖМД к прибору

3.1.5. Подключение 1,8" ZIF PATA (IDE) НЖМД

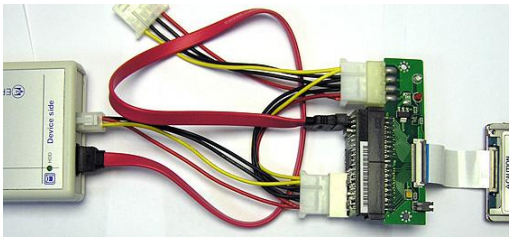
Подключение 1,8" ZIF PATA НЖМД осуществляется через адаптер SATA-PATA и дополнительный адаптер PATA 3,5" – ZIF PATA 1,8". При подключении 1,8" ZIF PATA НЖМД рекомендуется придерживаться следующей процедуры:

1. Подключите адаптер PATA 3,5" – PATA 2,5"к интерфейсному разъему НЖМД. Разъем питания адаптера должен находиться с левой стороны, если смотреть на контроллер НЖМД сверху.



Подключение адаптера к НЖМД

2. С помощью входящего в комплект поставки Y-кабеля подключите питание адаптера и питание НЖМД.
3. Подключите НЖМД с адаптером к прибору с помощью кабеля питания и интерфейсного SATA шлейфа.



Подключение PATA НЖМД к прибору

3.2. Работа со скрытой областью HPA

HPA (Host Protected Area) – это защищенная область накопителя, данные из которой не доступны для операционной системы ПК. Может быть выделена средствами BIOS некоторых материнских плат или специального программного обеспечения. В этой области может храниться информация о параметрах работы ПК, которая записывается туда при проверке системы средствами производителя ПК.

При создании или модификации области HPA данные на НЖМД не изменяются, однако доступная пользователю емкость НЖМД уменьшается на размер создаваемой области (уменьшается количество доступных секторов).

Решение о возможности работы с областью HPA оставлено на усмотрение эксперта. Прибор обеспечивает возможность ручного включения и отключения блокирования набора команд HPA Feature Set с помощью переключателя на правой боковой грани прибора. Текущий режим работы с набором команд HPA Feature Set отображается на светодиоде HPA Enable:

- Светодиод не светится. HPA команды блокируются.
- Светодиод светится. HPA команды разрешены.

4. Приложения

4.1. Перечень разрешенных команд

В перечень входят команды, выполнение которых разрешается прибором. Выполнением других команд, описанных в протоколе ATA, блокируется прибором.

Код команды (HEX)	**Наименование команды**
00	NOP
08	ATAPI SOFT RESET
10	RECALIBRATE
20	READ SECTOR(S)
21	READ SECTOR(S) (W/O RETRY)
22	READ LONG (W/RETRY)
23	READ LONG (W/O RETRY)
24	READ SECTOR(S) EXT
25	READ DMA EXT
26	READ DMA QUEUED EXT
27	READ NATIVE MAX ADDRESS EXT
29	READ MULTIPLE EXT
2A	READ STREAM DMA EXT
2B	READ STREAM EXT
2F	READ LONG EXT
40	READ VERIFY SECTOR(S)
41	READ VERIFY SECTOR(S) (W/O RETRY)
42	READ VERIFY SECTORS(S)
47	READ LONG DMA EXT
51	CONFIG STREAM
5B	TRUSTED NON DATA
5C	TRUSTED RECIV
5D	TRUSTED RECIVE DMA
60	READ FPDMA QUEUED
70	SEEK
90	EXECUTE DRIVE DIAGNOSTIC
91	INITIALIZE DRIVE PARAMETERS
A0	ATAPI PACKET
A1	ATAPI IDENTIFY DEVICE
A2	ATAPI SERVICE
B0	SMART
B6	NV CACHE
C4	READ MULTIPLE
C6	SET MULTIPLE MODE
C7	READ DMA QUEUED
C8	READ DMA
C9	READ DMA (W/O RETRY)
DA	GET MEDIA STATUS
DE	MEDIA LOCK
DF	MEDIA UNLOCK
E0	STANDBY MMEDIATE

E1	IDLE IMMEDIATE
E2	STANDBY
E3	IDLE
E4	READ BUFFER
E5	CHECK POWER MODE
E6	SLEEP
EC	IDENTIFY DEVICE
ED	MEDIA EJECT
EE	IDENTIFY DEVICE DMA
EF	SET FEATURES
F2	SECURITY UNLOCK
F5	SECURITY FREEZE
F6	SECURITY DISABLE PASSWORD
F8	READ NATIVE MAX ADDRESS

4.2. Поддерживаемые прибором команды стандарта ATA

Код команды	Наименование команды	Протокол команды
00h	NOP	ND
01h	Reserved	
02h	Reserved	
03h	CFA REQUEST EXTENDED ERROR	ND
04h	Reserved	
08h	DEVICE RESET	DR
12h	RECALIBRATE	
1Bh	RECALIBRATE	
1Eh	RECALIBRATE	
20h	READ SECTORS	PI
21h	READ SECTORS WITHOUT RETRY	PI
22h	READ LONG	PI
23h	READ LONG WITHOUT RETRY	PI
24h	READ SECTORS EXT	PI
25h	READ DMA EXT	DM
26h	READ DMA QUEUED EXT	DMQ
27h	READ NATIVE MAX ADDRESS EXT	ND
28h	Reserved	
29h	READ MULTIPLE EXT	PI
2Ah	READ STREAM DMA EXT	DM
2Bh	READ STREAM EXT	PI
2Eh	Reserved	
2Fh	READ LOG EXT	PI
30h	WRITE SECTORS	PO
31h	WRITE SECTORS WITHOUT RETRY	PO
32h	WRITE LONG	PO
33h	WRITE LONG WITHOUT RETRY	PO
34h	WRITE SECTORS EXT	PO

35h	WRITE DMA EXT	DM
36h	WRITE DMA QUEUED EXT	DMQ
37h	SET MAX ADDRESS EXT	ND
39h	WRITE MULTIPLE EXT	PO
3Bh	WRITE STREAM EXT	PO
3Ch	WRITE VERIFY	PO
3Dh	WRITE DMA FUA EXT	DM
3Eh	WRITE DMA QUEUED FUA EXT	DMQ
3Fh	WRITE LOG EXT	PO
40h	READ VERIFY SECTORS	ND
41h	READ VERIFY SECTORS WITHOUT RETRY	ND
42h	READ VERIFY SECTORS EXT	ND
43h	Reserved	
45h	WRITE UNCORRECTABLE EXT	ND
46h	Reserved	
47h	READ LOG DMA EXT	DM
4Ah	Reserved	
4Bh	Reserved	
4Eh	Reserved	
50h	FORMAT TRACK	VS
51h	CONFIGURE STREAM	ND
52h	Reserved	
53h	Reserved	
54h	Reserved	
55h	Reserved	
57h	WRITE LOG DMA EXT	DM
58h	Reserved	
5Ah	Reserved	
5Bh	TRUSTED NON-DATA	ND
5Ch	TRUSTED RECEIVE	PI
5Dh	TRUSTED RECEIVE DMA	DM
70h	SEEK	ND
90h	EXECUTE DEVICE DIAGNOSTIC	DD
91h	INITIALIZE DEVICE PARAMETERS	ND
92h	DOWNLOAD MICROCODE	PO
96h	STANDBY	
98h	CHECK POWER MODE	
A0h	PACKET	P
A1h	IDENTIFY PACKET DEVICE	PI
A2h	SERVICE	P/DMQ
A3h	Reserved	
A4h	Reserved	
A6h	Reserved	
A7h	Reserved	
A8h	Reserved	
AAh	Reserved	
ACh	Reserved	

ADh	Reserved	
B0h	SMART	ND/PI/PO
B1h	DEVICE CONFIGURATION	ND/PI/PO/DM
B6h	NV CACHE	DM/ND
B9h	Reserved for CFA	
BAh	Reserved for CFA	
BBh	Reserved for CFA	
BDh	Reserved	
BEh	Reserved	
BFh	Reserved	
C3h	Vendor specific	
C4h	READ MULTIPLE	PI
C5h	WRITE MULTIPLE	PO
C6h	SET MULTIPLE MODE	ND
C7h	READ DMA QUEUED	DMQ
C8h	READ DMA	DM
C9h	READ DMA WITHOUT RETRIES	DM
CAh	WRITE DMA	DM
CBh	WRITE DMA WITHOUT RETRIES	DM
CCh	WRITE DMA QUEUED	DMQ
CEh	WRITE MULTIPLE FUA EXT	PO
D0h	Reserved	
D1h	CHECK MEDIA CARD TYPE	ND
D5h	Reserved	
D6h	Reserved	
D7h	Reserved	
DEh	MEDIA LOCK	ND
DFh	MEDIA UNLOCK	ND
E0h	STANDBY IMMEDIATE	ND
E1h	IDLE IMMEDIATE	ND
E2h	STANDBY	ND
E3h	IDLE	ND
E4h	READ BUFFER	PI
E5h	CHECK POWER MODE	ND
E6h	SLEEP	ND
E7h	FLUSH CACHE	ND
E8h	WRITE BUFFER	PO
EAh	FLUSH CACHE EXT	ND
ECh	IDENTIFY DEVICE	PI
EDh	MEDIA EJECT	ND
EEh	IDENTIFY DEVICE DMA	DM
EFh	SET FEATURES	ND
F1h	SECURITY SET PASSWORD	PO
F2h	SECURITY UNLOCK	PO
F3h	SECURITY ERASE PREPARE	ND
F4h	SECURITY ERASE UNIT	PO
F5h	SECURITY FREEZE LOCK	ND
F6h	SECURITY DISABLE PASSWORD	PO

F8h	READ NATIVE MAX ADDRESS	ND
F9h	SET MAX	ND

4.3. Глоссарий

БП – Блок питания

ПК – Персональный компьютер

ПО – Программное обеспечение

НЖМД – накопитель на жестких магнитных дисках

ATA - AT Attachment, стандарт интерфейса подключения НЖМД к хосту

Device, устройство – исследуемый НЖМД

Host, хост – компьютер эксперта