EPOS® WriteProtector

Блокиратор записи

НАЗНАЧЕНИЕ ПРИБОРА

Съем данных с НЖМД и извлечение цифровых доказательств являются ключевыми этапами в процессе расследования всех компьютерных происшествий (преступлений) и инцидентов (computer forensics). Во всех этих случаях необходимо решать следующую важнейшую задачу: цифровые доказательства должны быть получены таким образом, чтобы исключить любую возможность внесения в них изменений. Поэтому при съеме данных с НЖМД и последующем их анализе обязательным требованием является применение специальных устройств – блокираторов записи.

Блокиратор записи (write blocker) – это специальное программное или аппаратное средство, которое блокирует передачу через интерфейс на исследуемый НЖМД всех тех команд, которые могут привести к изменению (модификации) данных, но обеспечивает прозрачный доступ к данным в режиме чтения.

Несмотря на доступность широкого спектра программных средств для защиты от записи, в настоящее время большинство специалистов в области computer forensics применяют в своей работе аппаратные блокираторы записи. Преимуществом аппаратных блокираторов записи является: возможность проведения исследования с использованием любой операционной системы, защищенность от вредоносного программного обеспечения и специализированных программ противодействия расследованиям и скрытия данных, снижение вероятности случайной модификации цифровых доказательств, вследствие программных сбоев и ошибок оператора.

Компанией ЕПОС разработан аппаратный блокиратор записи EPOS WriteProtector. Его достоинством является соответствие требованиям последней версии стандарта ATA-8. Это гарантирует защиту от записи при работе с современными жесткими дисками, поддерживающих новые наборы команд записи.

Аппаратный блокиратор записи EPOS WriteProtector предназначен для предотвращения случайного или преднамеренного внесения изменений в данные на НЖМД 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 НЖМД.

ЕПОС®

Центр восстановления информации ЕПОС
04071, г. Киев, ул. Верхний Вал 34, тел.: (044) 467-75-40
www.epos.ua

EPOS® WriteProtector

Блокиратор записи

Блокиратор записи EPOS WriteProtector работает абсолютно прозрачно для ПК и программного обеспечения. Таким образом, эксперт может использовать любую необходимую ему в процессе исследования операционную систему (DOS, Windows, Linux, MacOS, Unix…) и набор экспертного ПО (EnCase, X-WaysForensics, TheSleuthKit…).

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 блокиратора позволяют работать с ним как в лабораторных условиях, так и на выезде.

ОСОБЕННОСТИ ПРИБОРА

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

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Характеристика	Значение
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
Используемые интерфейсы	Serial ATA (вход и выход)
Совместимость со стандартом ATA	ATA-8
Поддержка HPA команд	Ручной переключатель для включения/отключения HPA команд
Совместимость с ОС	Все (в том числе DOS, Windows XP, Vista, 7, Linux, MacOS, Unix)
Режимы передачи данных	PIO, DMA, UltraDMA
Размеры	110 x 75 x 25 мм
Вес	100 г.
Электропитание	+5 В, +12 В (вход и выход)

ЕПОС®

Центр восстановления информации ЕПОС
04071, г. Киев, ул. Верхний Вал 34, тел.: (044) 467-75-40
www.epos.ua