УДК 681.3.06(075)

С. Р. Коженевский, С. Д. Прокопенко
ООО «ЕПОС»
ул. Верхний Вал, 34, 04071 Киев, Украина

Методика тестирования аппаратных блокираторов записи, применяемых в процессе расследования компьютерных происшествий

Рассмотрены принципы построения современных аппаратных блокираторов записи, применяемых в процессе расследования компьютерных происшествий. Выработаны требования, которым должны соответствовать такие устройства. Разработаны общие принципы проведения испытаний и предложена методика тестирования аппаратных блокираторов записи с интерфейсами PATA и SATA, которая может быть использована при проведении сертификационных испытаний.

Ключевые слова: *расследование компьютерных происшествий, съем данных, блокиратор записи, методика тестирования, сертификация, защита от записи, жесткий диск, НЖМД.*

Введение

При выполнении работ по расследованию компьютерных происшествий важнейшее значение приобретает вопрос обеспечения целостности данных на исследуемом носителе информации. Для исключения возможности случайного или преднамеренного внесения изменений в данные в процессе их съема и анализа широко используются аппаратные блокираторы записи (АБЗ).

В настоящее время на рынке доступно достаточно большое количество различных моделей блокираторов, которые отличаются способом своего построения, поддерживаемыми интерфейсами, наборами используемых команд, скоростью передачи и т.п. При этом производители зачастую не предоставляют подробного технического описания предлагаемых устройств, предлагая взамен только маркетинговые материалы. Однако для специалистов по расследованию компьютерных происшествий и преступлений очень важно иметь полное представление о возможностях и ограничениях используемых ими инструментов, чтобы быть уверенными в их надежности и целостности полученных результатов.

Для решения этой проблемы за рубежом принята практика проведения независимого тестирования и сертификации инструментов для расследования компьютерных происшествий. Так, в США сертификационные испытания такого обо-

рудования проводятся Национальным институтом юстиции (National Institute of Justice) [1, 2], методики и способы тестирования разрабатываются Национальным институтом стандартов и технологий (National Institute of Standards and Technology, NIST) [3]. В то же время в Украине практически отсутствует необходимая нормативная база и методология проведения испытаний оборудования для расследования компьютерных происшествий.

В предлагаемой статье описаны принципы построения современных АБЗ, а также определены требования, предъявляемые к ним. Авторами разработаны общие принципы проведения испытаний и предложена методика тестирования аппаратных блокираторов записи с интерфейсами PATA и SATA.

Принципы функционирования аппаратных блокираторов записи

Аппаратный блокиратор записи (hardware write blocker) — это специализированное устройство, которое блокирует передачу через интерфейс на исследуемый накопитель всех команд, которые могут привести к модификации данных, но обеспечивает прозрачный доступ к данным в режиме чтения. Следует отметить, что блокираторы обеспечивают защиту от модификации данных только в пользовательской области НЖМД, поскольку существуют области данных, которые могут модифицироваться самим накопителем независимо от действий хоста (например, данные подсистемы SMART).

Очевидным способом построения блокиратора может показаться подход, основанный на простом запрете передачи всех команд записи от хоста в накопитель. При таком сценарии блокиратор записи «прослушивает» интерфейсную шину, регистрируя поток команд и данных. Если обнаруживается, что хост передает «запрещенную» команду записи, ее выполнение прерывается. Тем самым на накопитель такая команда не поступает, хосту возвращается сообщение, что команда выполнена с ошибкой, или ее выполнение прервано накопителем (рис. 1).

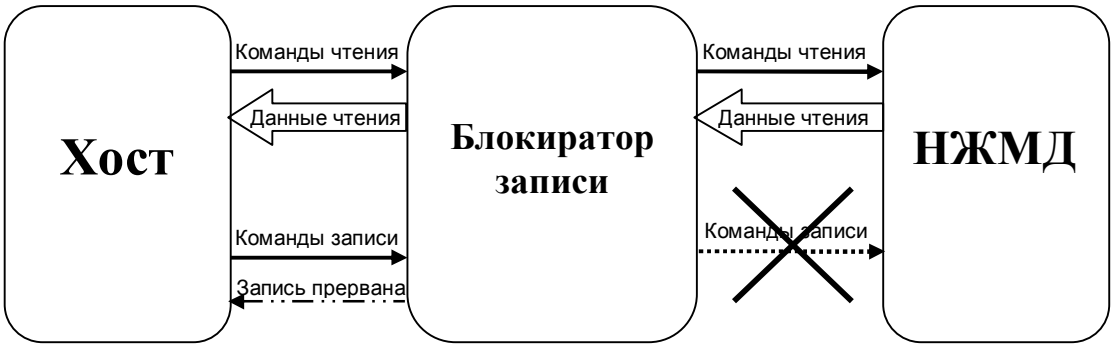

Рис. 1. Схема функционирования блокиратора записи с запретом выполнения команд записи

Однако на практике оказывается, что многие операционные системы не умеют корректно обрабатывать ситуацию, когда жесткий диск перестает выполнять запрашиваемые команды записи. Большинство ОС при этом просто зависают.

Поэтому широкое распространение получила другая схема построения блокираторов записи, основанная на разделении интерфейсной шины на сегменты.

Другими словами, шина между хостом и НЖМД делится на два сегмента: первый — между хостом и блокиратором, второй — между блокиратором и НЖМД. В такой схеме построения блокиратор перехватывает команды, анализирует их и затем выполняет одно из следующих действий:

— транслирует команду в жесткий диск без изменений;

— симулирует выполнение команды, не передавая ее в действительности на жесткий диск. Например, блокиратор может «знать» паспорт диска. Тогда в случае запроса хоста, он может не обращаться к диску, а просто вернуть соответствующий ответ непосредственно в хост;

— заменяет команду на другую и пересылает ее в жесткий диск. Такая схема характерна для блокираторов, имеющих различные интерфейсы для обмена с хостом и с НЖМД, а также для специализированных блокираторов записи для восстановления информации.

При такой схеме построения, запрещенные команды на НЖМД не поступают, но блокиратор возвращает в хост подтверждение их успешного выполнения (рис. 2).

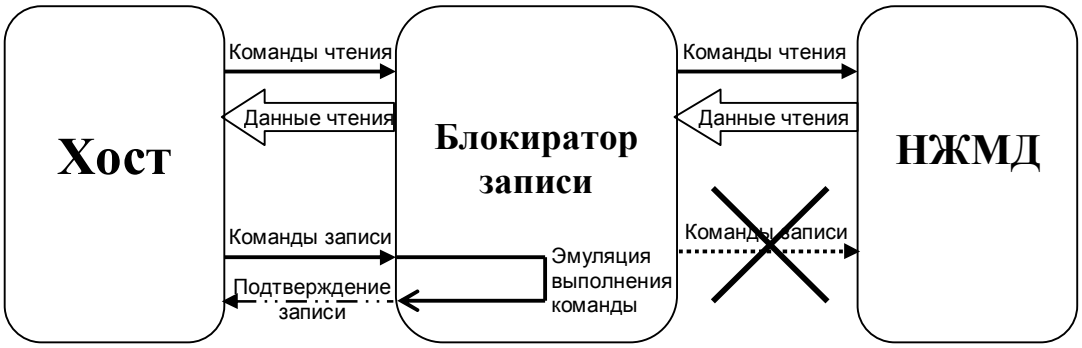

Рис. 2. Схема функционирования блокиратора записи с разделением интерфейсной шины на сегменты

Требования к аппаратным блокираторам записи

Очевидно, что основное требование можно описать как «блокиратор записи должен блокировать все команды записи, передаваемые в жесткий диск». Однако на практике такая формулировка оказывается недостаточно четкой. В первую очередь это связано с неопределенностью понятия «команды записи». Если предположить, что к командам записи относятся команды, содержащие слово «запись» («write») в определении стандарта ATA [4], то в перечень блокируемых команд не будут включены другие команды, которые модифицируют данные на диске, например, команда стирания данных SECURITY ERASE UNIT.

Таким образом, чтобы избежать неоднозначностей, необходимо выработать классификацию команд стандарта ATA, которая на основании формальных признаков разделила бы все команды на «разрешенные» и «блокируемые». В такой классификации каждая команда должна быть соотнесена только с одной выполняемой операцией и относиться только к одной классификационной категории.

Проанализировав набор команд стандарта ATA, можно выделить следующие категории операций [5].

1. ***Деструктивные операции***. В эту категорию входят все команды, которые:

1) непосредственно модифицируют данные. Например, команда WRITE DMA осуществляет запись в пользовательскую область жесткого диска;

2) потенциально могут модифицировать данные. К таким командам относятся вендор-команды и команды, не описанные в существующих ревизиях стандарта;

3) являются частью непрерывной командной последовательности, которая приводит к модификации данных. Например, после выполнения команды SECURITY ERASE PREPARE следует команда SECURITY ERASE UNIT, стирающая данные в пользовательской области;

4) изменяют идентификационные и конфигурационные параметры накопителя. Это команды, позволяющие изменить видимое количество секторов пользовательской области (команда SET MAX ADDRESS устанавливает защищенную область HPA — Host Protected Area) или любой из конфигурируемых параметров (команда DEVICE CONFIGURATION SET позволяет изменять ряд параметров НЖМД, в том числе доступную емкость, поддерживаемые режимы и т.п.).

2. ***Операции чтения***. В эту категорию входят все команды, которые запрашивают данные из пользовательской области жесткого диска и возвращают их хосту. Например, команда READ DMA EXT осуществляет чтение данных НЖМД с 48-битной адресацией.

3. ***Информационные операции***. В эту категорию входят команды, которые запрашивают данные, не хранящиеся в пользовательской области, а хранящиеся в области служебной информации НЖМД, и возвращают их хосту. В основном, это команды идентификации и конфигурации накопителя, такие как IDENTIFY DEVICE, DEVICE CONFIGURATION IDENTIFY.

4. ***Прочие недеструктивные операции***. К этой категории относятся другие команды, не модифицирующие данные в пользовательской области накопителя и не вошедшие в другие категории (например, команда READ VERIFY SECTOR(S) EXT).

Таким образом, с учетом изложенной классификации, к блокираторам записи, используемым в процессе расследования компьютерных происшествий, следует предъявлять следующие требования.

Требование 1. Блокиратор записи не должен передавать на защищаемый жесткий диск никаких команд, приводящих к выполнению деструктивных операций.

Требование 2. При получении любых команд, приводящих к выполнению операций чтения, блокиратор записи должен вернуть хосту запрашиваемые данные.

Требование 3. При получении любых команд, приводящих к выполнению информационных операций, блокиратор записи должен передать хосту запрашиваемые данные без каких-либо изменений, которые могут повлиять на доступ к диску.

Требование 4. При возникновении ошибок на жестком диске блокиратор записи должен транслировать их хосту.

Требование 5. Реакция блокиратора записи в случае поступления команды, не относящейся ни к одной из категорий, может определяться производителем блокиратора.

Отметим, что последнее требование является опциональным.

Рассмотренный набор требований к блокираторам записи для компьютерной криминалистики принят в Национальном институте стандартов и технологий США (NIST) и, фактически, является основой для сертификационных испытаний блокираторов записи в США.

Однако необходимо отметить, что среди специалистов широко обсуждается вопрос об обязательности блокирования команд, изменяющих идентификационные и конфигурационные параметры накопителя (категория **1г** классификации). Дело в том, что в эту категорию входят команды, позволяющие получить доступ к «скрытым» областям накопителя HPA (host protected area) и DCO (device configuration overlay), которые могут использоваться злоумышленниками и вредоносным ПО. В связи с необходимостью съема данных и извлечения доказательств из этих областей НЖМД, считается допустимым не блокировать эти команды при условии протоколирования таких операций в ПО для съема и анализа данных. В компании ЕПОС разработан блокиратор записи EPOS WriteBlocker [6], позволяющий переключать режимы работы, в одном из которых блокируется, в другом разрешается выполнение команд, изменяющих идентификационные и конфигурационные параметры накопителя.

Принципы тестирования аппаратных блокираторов записи

В предыдущем разделе были определены четыре обязательных требования к аппаратным блокираторам записи. Выполнение каждого из них можно проверять, используя различные подходы.

Например, **Требование 1** (АБЗ не должен передавать на жесткий диск деструктивных команд) можно проверить как минимум двумя способами. Для тестирования генерируется известная последовательность команд и передается на защищаемый накопитель через блокиратор. Первый способ заключается в мониторинге с помощью анализатора протокола команд, переданных блокиратором на жесткий диск, второй способ связан с исследованием возможных изменений на жестком диске после выполнения команд. Причем такое исследование можно проводить как непосредственно, сравнивая заданные сектора до и после теста, так и косвенно, путем вычисления и сравнения хеш-преобразований до и после теста. Оба способа могут определить, выполнил ли блокиратор свои функции при тестировании, но при использовании анализатора протокола имеется возможность зафиксировать *фактически переданные* команды, что иногда обеспечивает более высокую достоверность результатов проверки.

Проиллюстрировать это можно следующим примером. Допустим, для тестирования используются НЖМД с поддержкой набора команд ATA-5 и блокиратор записи, поддерживающий набор команд ATA-6. Если хост сгенерирует какие-либо деструктивные команды, определенные в стандартах ATA-7 или ATA-8 (но не определенные в ATA-6), блокиратор может ошибочно передать их на защищаемый НЖМД, в то же время никаких изменений на накопителе отмечено не будет. В этом случае анализатор протоколов позволит выявить такие ошибочно переданные команды.

Поэтому для проведения тестирования аппаратного блокиратора записи необходимы анализатор протоколов и генератор команд, который позволит создать

тестовый набор команд. В качестве генератора команд обычно применяется рабочая станция с предустановленными операционной системой и набором популярного экспертного ПО для расследования ИТ-инцидентов и/или специализированное тестовое ПО для генерации заданных наборов команд.

Общая методология тестирования аппаратного блокиратора записи основывается на последовательной проверке тестируемого АБЗ на соответствие требованиям, описанным в предыдущем разделе, и включает действия, описанные в таблице.

Общая методология тестирования аппаратных блокираторов записи

Требование	**Способ проверки требования**	**Условие несоответствия требованию**
1. Блокиратор записи не должен передавать на защищаемый жесткий диск никаких команд, приводящих к выполнению деструктивных операций.	1. В сегмент интерфейсной шины между блокиратором записи и НЖМД включается анализатор протоколов. Генератор команд передает предопределенный набор команд на блокиратор. Анализатор регистрирует команды, которые передаются между блокиратором записи и накопителем.	В протоколе анализатора присутствуют деструктивные команды
	2. Генератор команд передает предопределенный набор деструктивных команд с целью модифицировать данные в определенных секторах НЖМД. После выполнения теста данные в этих секторах проверяются на наличие изменений. Дополнительно выполняется сравнение хеш-преобразований до и после выполнения теста.	Выявление изменений данных в заданных секторах. Несоответствие хеш-преобразований до и после выполнения теста.
2. При получении любых команд, приводящих к выполнению операций чтения, блокиратор записи должен вернуть хосту запрашиваемые данные.	1. Генератор команд генерирует последовательность команд для создания полной посекторной копии данных в пользовательской области накопителя. В тесте используются два анализатора протоколов: один в сегменте между хостом и блокиратором, второй в сегменте между блокиратором и НЖМД. После завершения теста выполняется сравнение протоколов переданных команд обоих анализаторов. Выполняется сравнение хеш-преобразований данных защищаемого НЖМД и данных, скопированных через блокиратор записи.	Несоответствие хеш-преобразований данных защищаемого НЖМД и данных, скопированных через блокиратор записи.
	2. Генератор команд передает предопределенный набор команд чтения с целью чтения данных в определенных секторах накопителя. После выполнения теста считанные данные сравниваются с известными заранее данными на защищаемом НЖМД.	Несоответствие считанных данных с данными на защищаемом НЖМД.

3. При получении любых команд, приводящих к выполнению информационных операций, блокиратор записи должен передать хосту запрашиваемые данные без каких-либо изменений, которые могут повлиять на доступ к диску.	Генератор команд передает команды идентификации на защищаемый НЖМД с известной емкостью и конфигурацией. Результаты выполнения команд с подключенным блокиратором записи сравниваются с известными параметрами НЖМД.	Результаты выполнения команд не совпадают с известными параметрами НЖМД.
4. При возникновении ошибок на жестком диске блокиратор записи должен транслировать их хосту.	Генератор команд передает команду чтения данных из недействительного сектора (обычно из сектора за пределами емкости диска). Блокиратор записи должен вернуть хосту ошибку.	Блокиратор не возвращает ошибку хосту.

Методика тестирования аппаратных блокираторов записи

На основе описанных в предыдущем разделе принципов тестирования аппаратных блокираторов записи разработан набор тестов, позволяющий подтвердить, что исследуемый блокиратор удовлетворяет всем требованиям. Методика тестирования блокираторов записи с интерфейсами SATA и PATA включает в себя следующие операции и тесты.

1. Классификация команд.

На этом этапе все команды стандарта ATA на основании выполняемых ими операций относятся к одной из классификационных категорий: деструктивные операции, операции чтения, информационные операции, прочие недеструктивные операции. Каждая команда должна быть соотнесена только с одной выполняемой операцией и относиться только к одной классификационной категории.

2. Тест 1.

Наименование	Описание
Цель	Определение команд, блокируемых АБЗ.
Проверяемые требования	Требование 1 и Требование 5.
Состав тестового стенда	Тестовый ПК. Исследуемый НЖМД (без требований к записанным данным). Инструментальный ПК. Анализатор протоколов стандарта ATA. Генератор команд стандарта ATA.
Процедура тестирования	1. Подключить анализатор протоколов между АБЗ и исследуемым НЖМД. 2. Включить регистрацию протокола на инструментальном ПК. 3. Включить тестовый ПК и запустить генератор команд. 4. Выключить тестовый ПК. 5. Остановить регистрацию протокола и сохранить протокол.
Ожидаемые результаты	Требование 1. Протокол не содержит ни одной деструктивной команды. Требование 5. Фиксируется реакция АБЗ на каждую переданную команду.

3. Тест 2.

Наименование	Описание
Цель	Определение команд, блокируемых АБЗ, при попытке модифицировать данные с помощью экспертного ПО для расследования ИТ-инцидентов.
Проверяемые требования	Требование 1 и Требование 5.
Состав тестового стенда	Тестовый ПК. Набор исследуемых НЖМД. Инструментальный ПК. Анализатор протоколов стандарта ATA. Набор экспертного ПО для расследования ИТ-инцидентов.
Виды тестов	Тестирование включает в себя попытки модифицировать данные с помощью ОС, приложений, экспертного ПО. В процессе тестирования необходимо использовать различные версии ОС, набор исследуемых НЖМД должен включать жесткие диски с поддержкой 28-битной и 48-битной адресации. Должны быть выполнены следующие виды тестов: а) загрузка ОС с исследуемого НЖМД; б) изменение содержимого файловой системы на исследуемом НЖМД; в) запись (восстановление образа) на исследуемый НЖМД с помощью экспертного ПО.
Процедура тестирования	Для каждого из описанных видов тестов: 1) подключить анализатор протоколов между тестовым ПК и АБЗ; 2) включить регистрацию протокола на инструментальном ПК; 3) включить тестовый ПК и выполнить выбранный вид теста; 4) выключить тестовый ПК; 5) остановить регистрацию протокола, сохранить протокол и зафиксировать переданные деструктивные команды; 6) выключить инструментальный ПК; 7) включить инструментальный ПК; 8) подключить анализатор протоколов между АБЗ и исследуемым НЖМД; 9) включить регистрацию протокола на инструментальном ПК; 10) включить тестовый ПК и выполнить выбранный вид теста; 11) выключить тестовый ПК; 12) остановить регистрацию протокола, сохранить протокол и зафиксировать заблокированные деструктивные команды.
Ожидаемые результаты	Требование 1. Протокол передачи данных между АБЗ и исследуемым НЖМД не содержит ни одной деструктивной команды. Требование 5. Фиксируется реакция АБЗ на каждую переданную команду.

4. Тест 3.

Наименование	Описание
Цель	Определение разрешенных АБЗ команд операций чтения и информационных операций при работе с экспертным ПО для расследования ИТ-инцидентов.
Проверяемые требования	Требование 2, Требование 3, Требование 5.
Состав тестового стенда	Тестовый ПК. Исследуемый НЖМД (содержащий как минимум один логический раздел). Инструментальный ПК. Анализатор протоколов стандарта ATA. Набор экспертного ПО для расследования ИТ-инцидентов.
Виды тестов	Основной задачей этого теста является генерирование различных команд чтения и информационных команд при копировании данных с исследуемых НЖМД. В процессе тестирования необходимо использовать различные версии ОС, набор исследуемых НЖМД должен включать жесткие диски с поддержкой 28-битной и 48-битной адресации.
Процедура тестирования	1. Подключить анализатор протоколов между тестовым ПК и АБЗ. 2. Включить регистрацию протокола на инструментальном ПК. 3. Включить тестовый ПК и выполнить выбранный вид теста. 4. Выключить тестовый ПК. 5. Остановить регистрацию протокола, сохранить протокол и зафиксировать разрешенные команды чтения и информационные команды.
Ожидаемые результаты	Требование 2. Вычисленные до проведения теста и в процессе проведения теста хеш-функции скопированных данных совпадают. Требование 3. Копия содержит данные из всех адресуемых секторов пользовательской области данных исследуемого НЖМД. Требование 5. Фиксируется реакция АБЗ на каждую переданную команду.

5. Тест 4.

Наименование	Описание
Цель	Подтверждение того, что АБЗ не модифицирует основные конфигурационные параметры, включая информацию о емкости, исследуемого НЖМД.
Проверяемые требования	Требование 3.
Состав тестового стенда	Тестовый ПК. Набор исследуемых НЖМД с известной емкостью (количеством, размером секторов). Набор экспертного ПО для расследования ИТ-инцидентов.
Виды тестов	В процессе тестирования необходимо использовать различные версии ОС, набор исследуемых НЖМД должен включать жесткие диски с установленной скрытой областью HPA и DCO.
Процедура тестирования	Для каждого из описанных видов тестов: 1) включить тестовый ПК; 2) подключить исследуемый НЖМД к тестовому ПК через АБЗ;

	3) с помощью средств ОС и экспертного ПО установить количество секторов, размер сектора для исследуемого НЖМД; 4) зафиксировать результаты и выключить тестовый ПК.
Ожидаемые результаты	Требование 3. Тестовый ПК получает правильные конфигурационные параметры защищаемого НЖМД.

6. Тест 5.

Наименование	Описание
Цель	Подтверждение того, что АБЗ не блокирует передачу ошибок от исследуемого ПК в тестовый ПК.
Проверяемые требования	Требование 4.
Состав тестового стенда	Тестовый ПК. Исследуемый НЖМД. Генератор ошибок.
Процедура тестирования	1. Включить тестовый ПК. 2. Подключить исследуемый НЖМД к тестовому ПК через АБЗ. 3. С помощью генератора ошибок обратиться к сектору за пределами адресуемой области пользовательской области данных исследуемого НЖМД. 4. Зафиксировать результаты и выключить тестовый ПК.
Ожидаемые результаты	Требование 4. Ошибка транслируется в тестовый ПК от защищаемого НЖМД.

Выводы

Разработанная методика тестирования позволяет оценить соответствие аппаратных блокираторов записи с интерфейсами ATA предъявляемым к ним требованиям и может быть использована при проведении сертификационных испытаний.

1. *National* Institute of Justice. Special Report. Test Results for Hardware Write Block Device: FastBloc IDE (Firmware Version 16). — 2006.

2. *National* Institute of Justice. Special Report. Test Results for Hardware Write Block Device: ICS ImageMasster DriveLock IDE (Firmware Version 17). — 2006.

3. *National* Institute of Standards and Technology. Hardware Write Blocker (HWB). Assertions and Test Plan. — 2005.

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

5. *James R. Lyle.* A Strategy for Testing Hardware Write Block Devices. Digital Investigation / James R. Lyle. — 2006. — **3S**. — P. S3–S9.

6. *Аппаратный* блокиратор записи EPOS WriteProtector. Руководство пользователя. — ООО «ЕПОС», 2011.

Поступила в редакцию 17.08.2011