впроваджуються не тільки заради забезпечення безпеки охороняємих об'єктів або протидії злочинності.

Наприклад, ряд систем ідентифікації застосовуються в навчальних закладах. Деякі сучасні школи впроваджують сканування райдужної оболонки учнів з метою контролю відвідування і навіть для спрощення процедури оплати шкільних сніданків і обідів – учень приходить до їдальні, його сітківка сканується, з рахунку батьків списується конкретна сума за харчування дитини.

Використовуються і системи, що сканують відбитки пальців. На виробництві подібні системи дозволяють відмічати час проведений співробітником на робочому місці.

ВИСНОВОК

Вищевказані засоби ідентифікації користувачів надають змогу підвищити захищеність інформаційних ресурсів. Зокрема біометричні системи не виключають використання класичних засобів надання доступу а лише доповнюють їх при розумному впровадженні та налаштуванні, що в комплексі приведе до покращення ситуації з безпекою інформації.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Інформаційний ІТ-портал "Хабрахабр" [Електронний ресурс]: [Веб-сайт]. – Електронні дані. – Режим доступу: https://habrahabr.ru/ (дата звернення 15.11.2016) – Назва з екрана.

УДК 004.083.72+ 004.239

ОЦЕНКА ЗАЩИЩЕННОСТИ НАКОПИТЕЛЯ НА ЖЕСТКОМ МАГНИТНОМ ДИСКЕ ОТ УТЕЧКИ ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ КАНАЛАМИ

Автор: Цыбульников Артем Андреевич
Руководитель – соавтор: Кручинин Александр Владимирович
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua/, E-mail: artem111artem@gmail.com

Выполнен обзор современных накопителей на жестких магнитных дисках (НЖМД, HDD) и интерфейсов, которые они используют. Выполнен комплексный анализ информационных сигналов, возникающих при работе HDD. Сформулированы предложения по совершенствованию методов и средств специальных исследований HDD.

Ключевые слова - накопитель на жестких магнитных дисках, интерфейс, излучение, опасный сигнал, кодирование, тестовая программа, специальные исследования.

ВВЕДЕНИЕ

HDD – является неотъемлемой частью многих автоматизированных систем (АС). Поэтому актуальными является задачи обеспечение защиты информации и оценка уровня защищенности от утечки ее техническими каналами, за счет побочных электромагнитных излучений (ПЭМИ) от HDD и интерфейса, через который он подключен.

Для решения этих задач необходимо выполнить анализ структуры HDD и спецификаций интерфейсов, которые используются в настоящее время. На сегодняшний день, распространёнными являются интерфейсы SATA.

КЛАССИФИКАЦИЯ СИГНАЛОВ

Как известно, все сигналы, которые циркулируют в элементах вычислительной системы разделяются на: информативные, слабо информативные и не информативные. Опасность представляет перехват информативных и, в некоторых случаях, слабо информативных сигналов. Поэтому существует необходимость классификации основных электрических сигналов, которые циркулируют в самом HDD и его интерфейсе.

На основе анализа структурных, функциональных и принципиальных схем HDD можно сделать следующие выводы.

К информативным можно отнести сигналы, циркулирующие в:

- управляющем микроконтроллере (обеспечение взаимодействие всех блоков накопителя и связь с внешним интерфейсом);
- канале чтения-записи и цепи (выделение из сигнала, принятого от предусилителя, импульсы синхронизации и данных и формирующие сигналы записи);
- контроллере HDD (запись и считывание данных).

К мало-информативным можно отнести сигналы, циркулирующие в:

- блоке управления позиционированием (формирование импульсов управления соленоидом для перехода с цилиндра на цилиндр по команде микроконтроллера);
- внутренней ОЗУ (используется для считывания и записи секторов и локального кэширования);

К не информативным можно отнести сигналы, которые циркулируют в:

- детекторе сервометок (выделение сервометок из потока сигналов, принимаемых с головок считывания);
- блоке управления шпиндельным двигателем (обеспечивает запуск и остановку шпинделя по команде от микроконтроллера и поддерживающие заданную скорость вращения по сигналам от датчиков индекса, специальных датчиков вращения или/и сервометок);

• коммутаторе головок (улучшение отношения сигнал/шума при считывании).

Параметры этих сигналов зависят от многих факторов. В технической документации на HDD, как правило, приведены общие сведения о сигналах. Поэтому существует необходимость в более подробном их изучении.

Следует отметить, что интерфейсы, которые используются для подключения HDD, являются стандартизированными и параметры их сигналов достаточно подробно описаны в документации.

Рассмотрим, для примера, интерфейс SATA (Serial ATA), который является развитием интерфейса IDE. Его особенностью является не параллельная передача данных, а последовательная, что хотя и медленнее, но позволяет использовать более высокие частоты без необходимости синхронизации сигнала. Кабель интерфейса состоит из двух пар проводов (одной передачи и одной на прием) и несколько нулевых. Всего семь. Однако, этот факт является причиной того, что этот интерфейс является более уязвимым, с точки зрения перехвата информации каналом ПЭМИ.

Первый стандарт SATA 1.x мог работать на частоте 1.5 ГГц с пропускной способностью 1.2 Гбит/с (потери за счет передачи большого количества служебной информации). Стандарт 2.x работает на частоте 3 ГГц с пропускной способностью до 2.4 Гбит/сек и стандарт 3.0 на частоте 6.0 Гбит/с, с пропускной способностью 4.8 Гбит/с.

Тем не менее, авторы исследований утверждают, что частоты, на которых возможен съем информации находится в пределах от 1кГц до 3 ГГц. Однако Частота рассматриваемого сигнала составляет 1500 МГц, ширина сигнала порядка 5 МГц. Необходимо отметить, что уровни отличаются незначительно и частоты около 1500 МГц, на которых происходят излучения от SATA интерфейса, не оптимальны для передач данных – электромагнитная волна быстро затухает. Данный фактор играет против злоумышленника, но при грамотной настройке перехватывающей аппаратуры и последующей цифровой обработке сигнала возможен такой перехват со значительных расстояний [1].

СПЕЦИАЛЬНЫЕ ИССЛЕДОВАНИЯ

Для оценки уровня защищенности проводят, специальные исследования, основными этапами которых являются:

1) обнаружение излучения от объекта;

2) классификация излучений;

3) измерение параметров информативных излучений.

На практике наибольшую сложность представляют собой первые два этапа.

Для их реализации используются тестовые программы для формирования тестовых сигналов. Эти программы позволяют определять параметры тактовых сигналов элементов вычислительной системы, которые исследуются, и «подкрашивать» информативные сигналы.

Так, многие тестовые программы для определения тактовой частоты при исследовании HDD, производят запись-чтение файла достаточно большого размера. После определения времени, которое было затрачено, определяется тактовая частота. Однако данный способ не учитывает особенности логической структуры диска накопителя, равномерность его заполнения и другие факторы, которые оказывают влияние на время доступа к диску, а, следовательно, и на время чтения-записи файла. В результате этого, погрешность, при определении тактовой частоты, может составлять 100%. Кроме этого, не вполне понятно тактовая частота чего при этом определяется? Каким образом учитывается наличие блоков работающих с разными тактовыми частотами, использование буферов FIFO, пакетная передача данных?

При формировании тестовых последовательностей, оператор задает их типы. Наиболее распространенными являются «меандр» (101010….), «нули» (00000…) и «единицы» (11111…). Однако при этом не учитываются те преобразования данных, которые возникают в процессе обращения к HDD.

Так в интерфейсе SATA для кодирования передаваемой информации используется потенциальный код без возвращения к нулю (Non Return to Zero, NRZ). Он является одним из самых простых в реализации, благодаря двум резко различающимся потенциалам обладает хорошей распознаваемостью ошибок, но не обладает необходимым свойством самосинхронизации.

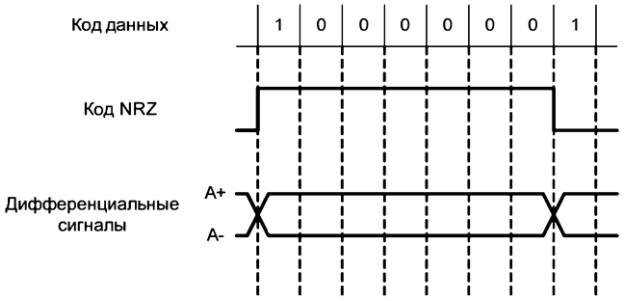

Рисунок1. Диаграмма формирования сигналов кода NRZ

Для обеспечения самосинхронизации применяется скремблирование. Перемешивая данные, подлежащие передаче определенным образом так, чтобы вероятность появления единиц и нулей на выходе была приблизительно одинаковой. Эта задача решается с помощью кодирования 8/10 (аналогия с кодами CD 8/14). При кодировании 8/10 байты заменяются 10-битными кодами, дающими 1024 возможные комбинации, из которых выбираются 256 двоичных кодов с ограниченным числом нулей. [4]

Кроме этого, на различных этапах передачи данных используются и другие способы модуляции и кодирования:

• частотная модуляция (FM);

• модифицированная частотная модуляция (MFM);

• кодирование с ограничением длины поля записи (RLL).

При выполнении специальных исследований, могут возникать сложности при идентификации

источника сигнала: интерфейс, контроллер HDD и др. Локализовать источник можно используя специальный набор антенн. Однако их использование в малом объеме может быть затрудненно. Частично решить эту проблему могло бы разделение во времени работы различных потенциальных источников сигналов.

ВЫВОДЫ

На основании проведенного анализа современных HDD и их интерфейсов, были определены их особенности, которые необходимо учитывать при проведении специальных исследований. Это обуславливает необходимость совершенствования существующих тестовых программ и методик проведения специальных исследований HDD для оценки уровня защищенности информации от утечки каналами ПЭМИ.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Гук Михаил Юрьевич “Аппаратные средства IBM PC” Санкт-Петербург, 2006. - 1034 с.[Електронный ресурс]. – Режим доступа: http://royallib.com/book/guk_mihail/apparatnie_interfeysi_pk_entsiklopediya.html, свободный;

2. Антясов И. С., Сафонов А. В., Соколов А. Н. «ПРОГРАММНО-ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ ТЕХНОЛОГИИ «МЯГКИЙ» ПЭМИН. 2015 — 4с. [Електронный ресурс]. Режим доступа: http://www.info-secur.ru/is_17/Antyasovsafonov.pdf, вільний;

3. Кенін А.М. Практичне керівництво системного адміністратора. – СПБХ. БХВ – Петербург, 2010. – 464 с.: ил. – (Системний адміністратор);

4. Вадим Авдеев «Периферийные устройства: интерфейсы, схемотехника, программирование» Москва, 2009 - 847 с.