УДК 681.3.06: 519.248.681

В. А. ГОРБАЧЕВ, канд. техн. наук, В. В. СТЕПАНЕНКО

СЕРТИФИКАЦИЯ ПЕРИФЕРИЙНЫХ УСТРОЙСТВ КОМПЬЮТЕРНЫХ СИСТЕМ

Рассматривается методика сертификации периферийных устройств современного компьютера с целью выявления неспецифицированных функций.

Анализ структуры современного ПК показывает, что наиболее уязвимыми, с точки зрения внедрения аппаратных закладок (АЗ), являются контроллеры ввода/вывода. Это связано с тем, что именно через них проходит большое количество информации, имеющей конфиденциальный характер. Кроме того, объёмы и скорость обмена информации в данных устройствах сравнительно невелики, а ущерб, наносимый при несанкционированном доступе к ней, может оказаться весьма ощутимым. Структура современного ПК такова, что практически все контроллеры ввода/вывода сосредоточены в одной интегральной схеме (ИС), имеющей название «SUPER I/O». Данная ИС включает в себя: контроллер клавиатуры, контроллер FDD, Secure Digital (SD) Memory card Interface, Extended Hardware Monitor, два контроллера UART с поддержкой IRDA и Smart Card Reader protocols, IEEE 1284 Parallel Port. Таким образом, данная ИС имеет доступ практически ко всей информации, вводимой и выводимой на ПК (исключение составляют контроллеры дисплея, LAN и USB) и, следовательно, необходимо уделять особое внимание её функционированию.

Таким образом, из приведённых выше рассуждений следует, что угроза безопасности информации со стороны АЗ – реальна. На современном уровне технологий возможно создание АЗ интегрированных в структуру штатных ИС, способных реализовать все виды угроз безопасности информации. Для эффективного противодействия аппаратным закладкам необходимо осуществлять сертификацию аппаратных средств, используемых в системах с высоким уровнем безопасности. Кроме того, поскольку уровень интеграции и технологий, используемых в современных вычислительных системах, очень высок, а технические возможности сертификационного оборудования на сегодняшний день не всегда соответствуют такому уровню технологии, то необходимо разрабатывать методики построения вычислительных систем, архитектура которых не позволит эффективно функционировать АЗ и сведёт к минимуму угрозу безопасности информации от данного класса устройств.

Рассмотрим методику сертификации клавиатуры персонального компьютера. Клавиатура выбрана не случайно, и связано это с тем, что через неё вводится большое количество информации, в том числе и различные пароли. Сертификация любого электронного устройства должна осуществляться путём прохождения следующих этапов сертификации:

- Построение поведенческой модели устройства.
- Синтез тестов для проверки специфицированных функций.
- Выполнение функционального тестирования для проверки специфицированных функций.
- Выбор модели АЗ.
- Синтез тестов для проверки наличия неспецифицированных функций.
- Выполнение функционального тестирования для проверки неспецифицированных функций.
- Выводы о соответствии устройства его спецификации.

Таким образом, на первом этапе нам необходимо построить поведенческую модель сертифицируемого устройства, а именно клавиатуры. Поведенческая модель в нашем случае представляет собой алгоритм функционирования двух интерфейсов клавиатуры:

1. Интерфейс опроса матрицы клавиш.
2. Интерфейс передачи данных.

Укрупнённый алгоритм функционирования клавиатуры показан на рис. 1.

Рис.1

Для осуществления сертификации нам необходим некоторый аппаратно-программный комплекс, который позволит осуществлять генерацию управляющих векторов для обоих интерфейсов клавиатуры с постоянным контролем текущих состояний. Обобщённая схема сертификационного комплекса показана на рис. 2.

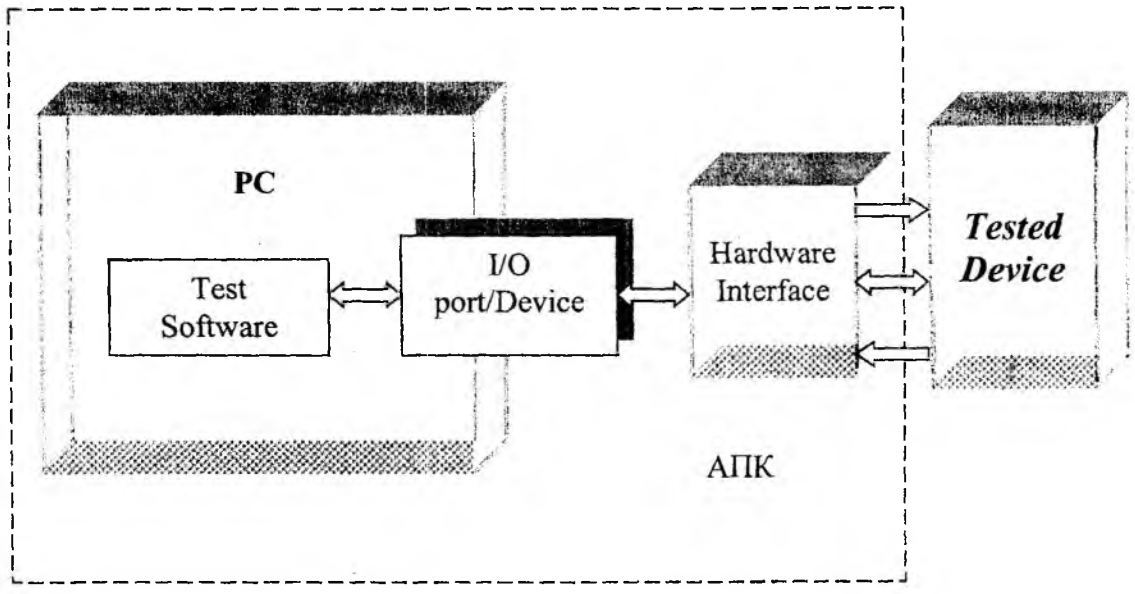

Рис. 2

Физически аппаратная часть сертификационного комплекса для данного случая выполнена в виде двух микроконтроллеров. Первый осуществляет эмуляцию интерфейса обмена данными с персональным компьютером, второй представляет собой управляемую матрицу клавиш.

Переходя ко второму этапу (генерация тестов для проверки специфицированных функций), следует отметить, что поскольку осуществляется сертификация двух интерфейсов, мы будем иметь две группы тестов (по числу интерфейсов). Первая группа тестов сканирует интерфейс обмена данными и проверяет на полном наборе специфицированных функций правильность работы устройства путём сравнения получаемых ответов с ответами, специфицированными в технической документации. Вторая группа тестов проверяет правильность генерации кодов нажатия и отжатия для всех клавиш клавиатуры по отдельности, а также для всех сочетаний в количестве до трёх. Верификация так же, как и в первом случае, осуществляется путём сравнения получаемых значений со значениями из таблицы истинности.

Далее необходимо выполнить функциональное тестирование клавиатуры. Данная операция выполняется при помощи управляющей программы, написанной с использованием знаний о функционировании клавиатуры и рассуждений, приведённых выше. Работа сертификационной программы в обоих режимах показан а на рис. 3.

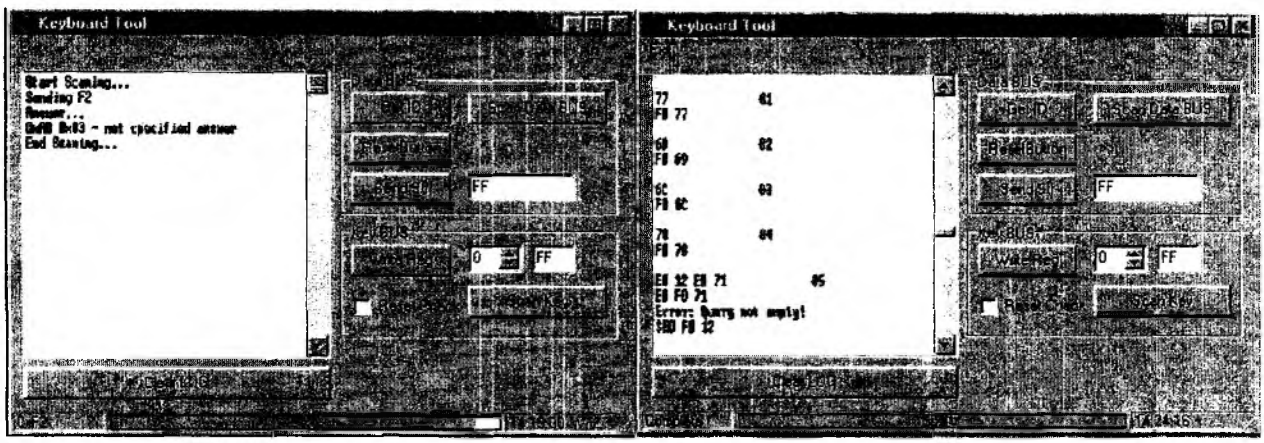

Рис. 3

Переходя к поиску неспецифицированных функций, прежде всего нам необходимо определить модель АЗ, поиск которой мы будем осуществлять. Прежде всего, это необходимо для определения реакции сертифицируемого устройства в нештатном режиме. В данном случае мы выбираем АЗ накопительного типа. Выбор связан с тем, что этот класс АЗ, располагаясь в данном устройстве, может нанести максимальный ущерб безопасности информации.

Генерация тестовых последовательностей для проверки наличия неспецифицированных функций осуществляется аналогично предыдущему случаю, за исключением двух моментов:

1. При сертификации интерфейса обмена данными используются неспецифицированные команды.
2. При сертификации интерфейса опроса матрицы клавиш рассматриваются различные сочетания нажатия и отжатия клавиш в количестве от 4-х до 10-ти.

Искомой реакцией в данном случае является несанкционированная передача данных через интерфейс обмена данными. Этап функционального тестирования в данном случае осуществляется при помощи тех же программных и аппаратных средств, что и в случае проверки специфицированных функций.

Оценка эффективности алгоритма и времени проведения сертификации на примере поиска АЗ накопительного типа [1] в контроллере клавиатуры показывает, что данный подход

является приемлемым. Предлагаемый подход позволяет выполнить сертификацию устройства, как на выполнение им специфицированных, так и неспецифицированных функций. При этом в обоих случаях сертификация проводится с использованием одинаковых алгоритмических, программных и аппаратных средств, что позволяет снизить стоимость сертификационного оборудования. Время поиска неспецифицированных функций зависит от быстродействия специфицируемого устройства и может быть уменьшено путём оптимизации алгоритма построения тестовых последовательностей.

Список литературы: 1. *Горбачев В.А., Степаненко В.В, Саранча С.Н.* Сертификация сложных электронных систем с использованием функциональной модели объекта на полном наборе входных слов // Наук.-техн. зб. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Київ: КНУ-КПІ, 2002. Вип. 5. С. 139 – 144.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 20.05.2003