Результаты, приведенные в табл. 4, позволяют отметить следующее.

1. По мере увеличения плотности случайного прерывания АКФ процесса обработки прерывания периодична с периодом $1/\alpha_п$, хотя значения локальных экстремумов оказываются значительно меньше, чем *K(0)*. По мере увеличения плотности числа периодических прерываний период АКФ уменьшается.

2. При постоянной плотности числа прерываний по мере увеличения времени обработки прерывания относительное время занятости МК выполнением основной программы $\phi(1)$, определяемое выражением (4), уменьшается. В случае $N_{ср}=1/(\alpha_п \alpha_с)$ МК не сможет выполнять основную программу.

VI Выводы

1. Предложен теоретико-числовой подход к моделированию процесса обработки аппаратных прерываний в микроконтроллерных системах, позволивший получить значения указанного процесса в каждый момент времени.

2. Результаты анализа показали, что процесс обработки аппаратных прерываний является стационарным и эргодичным. Вследствие этого он описывается дискретной функцией распределения, которая зависит от плотности появления прерываний и среднего времени обработки прерывания. Значения дискретной функции распределения $\phi(1)$ и $\phi(0)$ являются фактически описанием относительного времени выполнения МК основной программы и обработки прерывания.

3. АКФ процесса обработки прерываний при отсутствии периодических прерываний определяется исключительно средним временем обработки прерывания.

4. АКФ и дискретная функция распределения процесса обработки прерываний оказываются взаимно зависимыми.

5. При наличии периодических прерываний АКФ процесса также является периодической.

6. Совокупное воздействие случайных и периодических прерываний уменьшает время выполнения МК основной программы и может привести к полному прекращению обработки основной программы. При этом случайная составляющая в АКФ оказывается доминирующей.

7. Для того, чтобы МКС могла выполнять основную программу, необходимо выполнение соотношения

$$\phi(1) \le 0{,}5$$

Литература: 1. Каган Б. М. Электронные вычислительные машины и системы: Учеб. пособие для вузов./ 3-е изд., перераб. и доп. // М.: Энергоатомиздат. – 1991. – 592 с. 2. Фрир Дж. Построение вычислительных систем на базе перспективных микропроцессоров: Пер. с англ. // М.: Мир. – 1990. – 413 с. 3. Гивоне Д., Россер Р. Микропроцессоры и микрокомпьютеры. //М.: – Мир. – 1983. – 463 с. 4. Бродин В. Б., Шагурин И. И. Микроконтроллеры. Архитектура, программирование, интерфейс. //М.: Экон. – 1999. – 400 с. 5. Справочник по математике (для научных работников и инженеров) Г. Корн, Т. Корн – Изд. 4. – М.: Наука, 1978. – 831 с.

УДК 638.235.231

СЕРТИФИКАЦИЯ СЛОЖНЫХ ЭЛЕКТРОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ФУНКЦИОНАЛЬНОЙ МОДЕЛИ ОБЪЕКТА НА ПОЛНОМ НАБОРЕ ВХОДНЫХ СЛОВ

Валерий Горбачев, Владимир Степаненко, Сергей Саранча
Харьковский национальный университет радиоэлектроники

Анотація: **Розглядаються питання, пов'язані з розробкою методів та засобів сертифікації складних електронних систем на відповідність специфікованим функціям.**
Summary: **In the given work the questions connected with development of methods and means of certification of complex electronic systems for conformity to the specified functions are considered.**
Ключові слова: **Інформація, апаратні засоби, закладний пристрій, інформаційна безпека.**

В настоящее время во всем мире активно разрабатываются всевозможные программные средства защиты информации от несанкционированного доступа к ней и ее разрушения [1]. В то же время проблема поиска цифровых закладных устройств в вычислительной технике и любой цифровой технике вообще является практически не исследованной. Поскольку уровень аппаратных средств является самым низким уровнем доступа к информации, то контроль за доступом, осуществляемым при помощи аппаратных средств,

невозможно осуществлять на программном уровне. Таким образом, поиск аппаратных закладных устройств, а также контроль за функционированием аппаратных ресурсов вычислительной техники возможно осуществлять только с использованием специализированного диагностического оборудования, а также программного обеспечения, входящего в его состав. В работе *аппаратной закладкой (АЗ)* называется некоторое функционально-структурное изменение электронного устройства, приводящее к тому, что данное устройство становится активным источником угрозы безопасности информации.

Поскольку закладные устройства, введенные в структуру серийных устройств, могут иметь полный доступ ко всем аппаратным ресурсам, доступным данному устройству, то эффект от использования таких закладных устройств и вред наносимый с их помощью может быть значительно большим, нежели от программных закладок. Это связано с тем, что наряду с возможностью несанкционированного доступа к информации (копирование, модификация, разрушение), появляется возможность разрушения аппаратных средств, что ведет к выходу из строя всего вычислительного комплекса.

Целью данной работы является разработка метода сертификации сложных электронных систем на соответствие специфицированным функциям с использованием функциональной модели объекта и полного набора входных слов, а также его апробация на клавиатуре персонального компьютера.

Переходя к вопросу о сертификации электронных систем, прежде всего, необходимо определить значение понятия «сертификация».

Согласно определениям, имеющимся в отечественной литературе, сертификация определяется как действие, удостоверяющее посредством знака или сертификата соответствие изделия требованиям определенных стандартов или технических условий [2]. Это определение является очень обобщенным и в рамках рассматриваемых вопросов требуется более четкая формулировка, с учетом специфики темы.

В настоящей работе рассматривается проблема *сертификации* сложных электронных систем на соответствие специфицированным функциям, которая понимается как *совокупность действий, позволяющих произвести анализ структуры и тестирование электронных систем с целью определения степени соответствия ее специфицированным функциям с последующей выдачей сертификата соответствия*.

Обнаружение в ходе сертификации электронных устройств функций, не заявленных производителем, позволяет утверждать, что данное оборудование кроме действий, непосредственно необходимых для его функционирования, выполняет еще некоторые определенные действия, о функциях которых пользователю этого оборудования ничего не известно. В случае рассмотрения в качестве сертифицируемой системы оборудования, используемого для обработки, передачи либо накопления информации, наличие не специфицированных функций оказывается однозначно связанным с вопросом защиты информации. Таким образом, обнаружение не специфицированных функций позволяет утверждать, что данные технические средства не соответствуют заявленным функциям и следовательно не могут использоваться в системах, требующих высокого уровня безопасности и защиты информации.

Разработку методов сертификации предлагается осуществлять в рамках системного анализа, имитационного моделирования и технической диагностики, основной функцией которых, как научных направлений, является оценка качества изделия на этапах проектирования, производства и эксплуатации.

Анализ структуры современных КС показывает, что тип используемой АЗ связан с местом ее расположения и функциями, которые она выполняет.

Рассмотрим несколько возможных классов аппаратных закладок:

- закладные устройства разрушающего (блокирующего) типа;
- закладные устройства накапливающего типа;
- закладные устройства, изменяющие протокол передачи данных.

Таким образом, предлагается проводить анализ возможных мест размещения АЗ с учетом определенных выше классов, а также учитывая эффективность их функционирования.

Говоря о методах и средствах сертификации сложных электронных систем в общем и ПЭВМ в частности в первую очередь необходимо отметить, что невозможно предложить универсальный метод, позволяющий производить сертификацию любого оборудования. Это связано с тем, что каждый класс устройств выполняет свою определенную группу функций и в соответствии с этими функциями различны и классы возможных не специфицированных функций.

В данной работе сертификацию любого оборудования предлагается проводить путем построения определенной тестирующей последовательности и анализа реакции сертифицируемого оборудования на эту последовательность управляющих воздействий.

Из сказанного выше становится ясно, что наиболее сложным и трудоемким этапом при сертификации на наличие не специфицированных функций будет этап построения тестирующих последовательностей. В тоже время грамотность построения тестирующих последовательностей будет определять эффективность методов сертификации в целом.

Определяя общую схему сертификации сложных электронных систем можно выделить следующие основные этапы:

– анализ структуры сертифицируемого устройства с целью выявления возможных классов закладных устройств;

– генерация тестирующих последовательностей с учетом выполняемых функций, протоколов обмена, а также возможных классов АЗ;

– функциональное тестирование;

– анализ результатов функционального тестирования.

На этапе анализа структуры сертифицируемого устройства производится тщательный анализ структуры объекта. При этом в случае отсутствия полной технической документации (что является типичным) производится поиск и обработка информации о всех компонентах, размещенных на сертифицируемом устройстве, строятся поведенческие модели компонентов и всего устройства в целом. Также на этом этапе производится выявление наиболее вероятных классов АЗ и мест их размещения, с учетом требования максимальной эффективности их функционирования.

На этапе генерации тестирующих последовательностей производится генерация тест последовательностей с учетом всех выше описанных требований. При этом тест последовательности должны охватывать все возможные в рамках данной структуры не документированные комбинации управляющих сигналов и не документированных команд.

На этапе функционального тестирования производится тестирование сертифицируемого объекта. При этом возможно несколько вариантов оборудования, используемого для сертификации:

– сертификация производится при помощи стандартных средств, т. е. для передачи управляющих последовательностей и съема реакций используются стандартные средства персонального компьютера;

– сертификация производится при помощи аппаратно-программного комплекса, представляющего собой генератор и анализатор, работающие под управлением персональной ЭВМ.

На этапе анализа результатов функционального тестирования производится анализ результатов и в случае обнаружения не документированных реакций делается вывод о наличии не специфицированных функций.

Теперь рассмотрим конкретную задачу поиска АЗ в клавиатуре персонального компьютера. Клавиатура выбрана не случайно и связано это с тем, что через нее вводится большое количество информации, в том числе и пароли. Согласно подходу, изложенному выше, в первую очередь необходимо определить функциональную структуру и протоколы обмена данного устройства, а также с учетом его функций определить возможные классы АЗ. Рассматривая возможность применения различных классов АЗ в клавиатуре, впрочем как и в большинстве устройств ввода-вывода, можно отметить, что в данном случае наиболее вероятно размещение АЗ накапливающего либо разрушающего типа. В данной статье мы ограничимся АЗ накапливающего типа.

Итак, теперь необходимо рассмотреть структуру исследуемого устройства с целью определения возможных способов активации АЗ, а следовательно и возможных путей ее обнаружения.

Структура клавиатуры хорошо всем известна, а протоколы обмена стандартизированы, поэтому проблемы с определением модели ее поведения нет.

Со стороны персонального компьютера располагается контроллер Intel 8042.

В контроллере 8042 имеется внутренняя ROM, которая программируется с учетом кодов сканирования клавиатуры и рабочих команд. Контроллер 8042 взаимодействует с клавиатурой в двунаправленном последовательном формате с синхронизацией данных. Контроллер 8042 последовательно принимает данные, проверяет их паритет, преобразует коды сканирования в системные коды и прерывает МП для передачи данных системе.

На рис. 1 приведена блок-схема контроллера, располагающегося на материнской плате, а также схема контроллера клавиатуры.

Контроллер 8042 подключается к системе через шину периферийных устройств XD при помощи программно-доступных входного и выходного буферов, которые представляют собой два буфера шины данных: один для входа и один для выхода.

Контроллер 8042 и клавиатура связаны четырехпроводным экранированным кабелем, включающим линию питания (+5 В), линию заземления, линии сигнала данных и сигнала синхронизации.

Контроллер 8042 и клавиатура взаимодействуют с помощью механизма квитирования, используя линии данных и синхронизации для синхронного последовательного интерфейса.

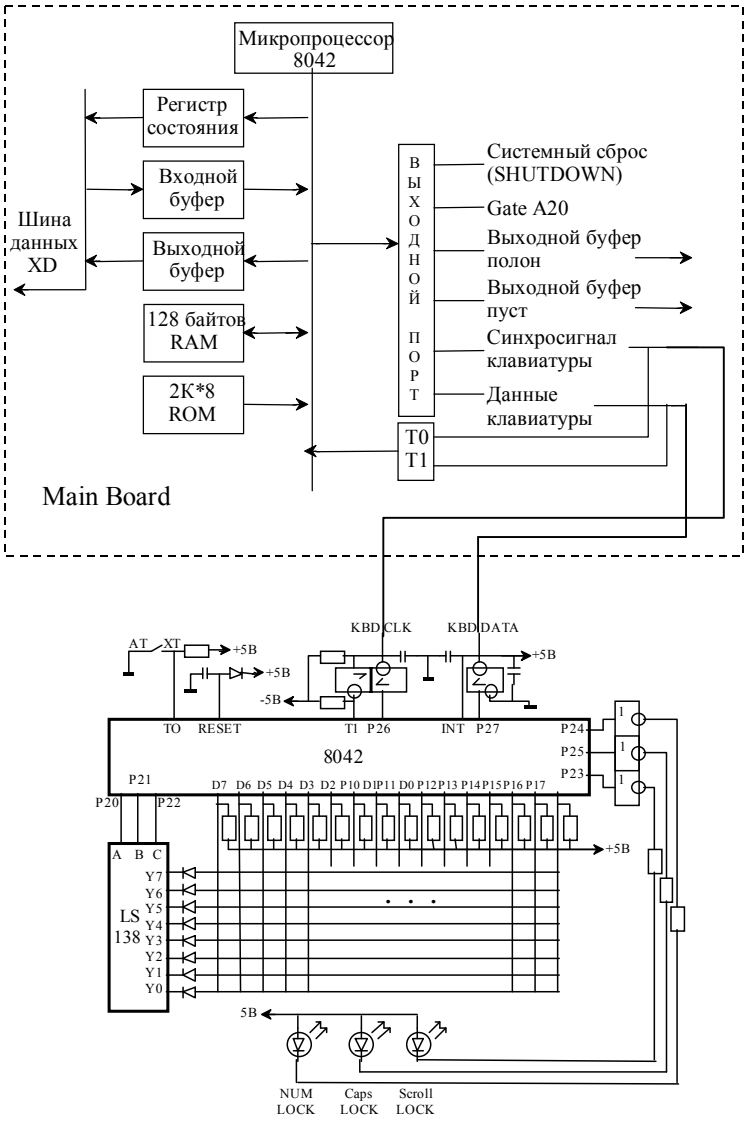

Рисунок 1 – Блок-схема контроллера клавиатуры

Формат передачи данных между клавиатурой и PC имеет вид, показанный на рис. 2.

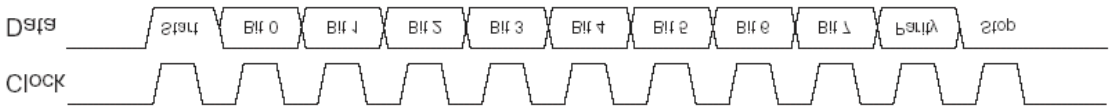

Рисунок 2 – Формат передачи данных клавиатуры

Передача данных на клавиатуру и с клавиатуры осуществляется потоком 11-разрядных данных, которые передаются последовательно по линии данных. При активном (высоком) уровне пересылается логическая единица.

Обмен данными осуществляется между системой и клавиатурой, при этом подразумевается обмен данными между двумя микропроцессорами 8042: одним в системе, другим в клавиатуре.

При каждой передаче команды или данных от системы на клавиатуру система требует подтверждения от клавиатуры. Если только система не запретит вывод данных с клавиатуры, последняя дает ответ в течении 20 мс.

Если ответ клавиатуры недействителен или содержит ошибку паритета, система повторно посылает ей команду или данные. Однако двухбайтовые команды требуют особой обработки. Если были переданы и подтверждены команды F3h (установить скорость/задержку повторения), F0h (выбрать альтернативные коды сканирования) или Edh (установить/сбросить индикаторы режима), а также передан байт данных, но ответ оказался недействительным или с ошибкой паритета, то система передаст повторно и команду и байт данных.

Как после нажатия, так и после отжатия клавиши контроллер клавиатуры генерирует аппаратное прерывание IRQ1. Обработчик прерывания INT 09h читает из порта 60 байт данных и начинает обработку нажатия/отжатия клавиши.

Управление клавиатурой возможно через порты 60, 61 64: прерывания INT 09h; прерывания INT 15h; функции DOS (INT 21h).

Доступ к клавиатуре через порты ввода-вывода является самым низкоуровневым методом доступа.

Команды контроллера клавиатуры приведены в табл. 1.

Таблица 1 – Команды контроллера клавиатуры

Код	Функция
Edh	Установить индикаторы состояния
Eeh	Эхо (средство диагностирования)
F0h	Выбрать альтернативный режим
Efh-F1h	Резерв – холостые команды (NOP)
F2h	Идентификатор расширенной клавиатуры
F3h	Установить частоту повторения клавиши
F4h	Разрешить клавиатуру
F5h	Запрет по умолчанию
F6h	Установить условия по умолчанию
F7h-Fah	Установить все клавиши
FBh-FDh	Установить отдельные клавиши
Feh	Послать повторно
FFh	Сброс

Коды ответов клавиатуры.

Клавиатура отвечает системе кодами, описанными ниже.

Подтверждение *(FAh)*. Клавиатура выдает подтверждение (ACK) в ответ на любую правильную команду, кроме команд “Эхо” RESEND. Если клавиатура прерывается во время передачи ACK, то ACK отменяется и клавиатура начинает обработку новой команды.

Код завершения включения питания *(AAh)*. После успешного завершения включения питания клавиатура передает системе код AAh. Передача любого другого кода после включения указывает на неисправность клавиатуры.

Эхо *(EEh)*. Клавиатура передает этот код в ответ на команду “Эхо”.

Идентификатор клавиатуры *(83Abh)*. Идентификатор клавиатуры состоит из двух байтов – 83ABh. Клавиатура отвечает на команду “Идентификатор расширенной клавиатуры” подтверждением, прерывает сканирование и передает два байта идентификатора. Первым передается младший байт. После вывода идентификатора клавиатура начинает сканирование.

Повторная посылка *(FEh)*. Клавиатура передает этот код после получения неправильных входных данных или данных с ошибкой паритета.

Таким образом, из приведенного выше описания видно, что активация АЗ, размещающейся в клавиатуре, может быть произведена двумя путями:

1) при помощи недокументированных команд, передаваемых из контроллера, располагающегося на материнской плате;
2) при помощи нажатия определенного сочетания клавиш на самой клавиатуре.

При размещении в клавиатуре АЗ накапливающего типа мы должны иметь возможность управлять ее функционированием. А именно: активизировать ее работу (накопление информации), останавливать ее работу, очищать память АЗ для повторного использования, активизировать передачу данных наружу. Накопленная информация может извлекаться из АЗ либо при помощи подключения клавиатуры к дополнительному устройству (не входящему в состав PC), либо же по стандартному каналу. Для этого злоумышленнику необходимо открыть любой текстовый редактор, имеющийся в составе ПО компьютера, и нажать определенную комбинацию клавиш, после чего вся информация, накопленная за время активности

АЗ, будет выведена в окно текстового редактора. Этот вариант на наш взгляд является наиболее интересным и поэтому остановимся на нем более подробно.

Функциональная модель АЗ в этом случае будет представлять некоторое дополнительное устройство, введенное в структуру контроллера клавиатуры. Функциональная модель АЗ приведена на рис. 3.

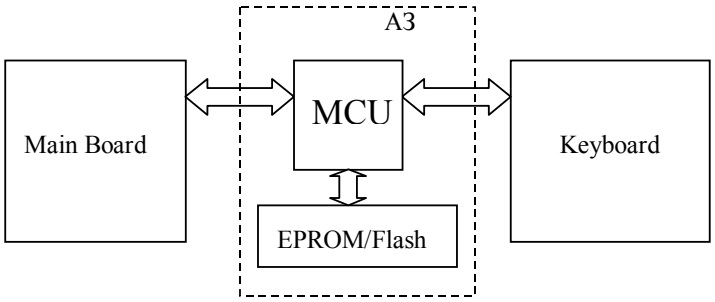

Рисунок 3 – Функциональная модель АЗ

Обобщенный алгоритм работы данной АЗ будет состоять из 2 шагов:

1) накопление информации, циркулирующей между клавиатурой и материнской платой персонального компьютера;
2) выдача накопленной информации при нажатии определенного сочетания клавиш.

Таким образом, для выполнения сертификации на соответствие специфицированным функциям необходимо проследить реакцию контроллера клавиатуры на нажатие клавиш.

Стандартный контроллер клавиатуры осуществляет сканирование матрицы клавиш с периодом 12,5 mS. Таким образом, максимальная производительность при опросе будет составлять 80 клавиш в секунду, реальная – не более 40. При этом контроллер понимает одновременное нажатие не более 3 клавиш (наиболее вероятный способ взвода АЗ – одновременное нажатие сочетания клавиш, иначе возможно ложное срабатывание).

Легко подсчитать, что для обнаружения подобной АЗ в стандартной клавиатуре из 102 клавиш перебором всех возможных вариантов потребуется:

при одновременном нажатии 3 клавиш $A_{102}^{3} = \frac{102!}{99!} = 1030200 \approx$ 7,1 часа

при одновременном нажатии 4 клавиш время составит

$$A_{102}^{4} = \frac{102!}{98!} = 101989800 \approx 708 \text{ часов} \approx 30 \text{ дней}$$

В заключение необходимо отметить, что сертификация сложных электронных систем с использованием функциональной модели и полного набора входных слов, как показано выше, действительно возможна. Несмотря на то, что полученное время сертификации достаточно велико, оно может быть существенно уменьшено при задании определенных правил составления комбинаций одновременно нажатых клавиш. Достаточно большое количество комбинаций можно исключить. Во-первых, одновременно нажиматься могут только клавиши из разных рядов матрицы, а во-вторых, некоторые сочетания клавиш человек не может выполнить без дополнительной помощи.

Для осуществления сертификации контроллеров клавиатур данным способом требуется несложное устройство, работающее под управлением персонального компьютера. При этом, поскольку в нем не требуется реализации сложных функций и высокой производительности, стоимость этого устройства будет очень невысокой.

Таким образом, данный способ сертификации является вполне приемлемым как с точки зрения затрат времени, так и с экономической точки зрения.

Литература: 1. Анин Борис. Защита компьютерной информации.– СПб.: BHV Санкт-Петербург, 2000. VIII. – 368 с.: ил. 2. Попов М. И. Основы сертификации электронной техники. – М.: издательство стандартов, 1988. – 277 с.