УДК 004.056.5

Эффективность применения средств тестирования программно-аппаратных СЗИ

Т. М. Каннер
Закрытое акционерное общество "ОКБ САПР", Москва, Россия

Описываются назначение, состав и принцип функционирования разработанного вспомогательного средства автоматизированного тестирования функций безопасности "мобильных" программно-аппаратных средств защиты информации (СЗИ), функционирующих в операционной системе средств вычислительной техники и имеющих USB-интерфейс подключения, — коммутатора USB-канала. Показана эффективность использования данного средства совместно с разработанным автором комплексом программ для тестирования функций безопасности программно-аппаратных СЗИ.

Ключевые слова: "мобильные" программно-аппаратные СЗИ, коммутатор USB-канала, комплекс программ тестирования функций безопасности.

Информационные системы создаются и развиваются очень быстро за счет использования эффективных инструментальных средств. В связи с этим необходимо максимально сократить время, затрачиваемое на разработку СЗИ, выделив этапы, которые можно полностью автоматизировать или автоматизировать при определенных условиях. К таким этапам относятся тестирование, верификация и исправление найденных ошибок. Эти этапы неоднократно повторяются в процессе разработки СЗИ. Сокращения временных затрат на разработку СЗИ можно достичь за счет автоматизации процесса тестирования его функций безопасности.

Для программных СЗИ существует большое количество разнообразных средств автоматизации тестирования [1], применение которых может быть затруднено для программно-аппаратных СЗИ из-за наличия аппаратного компонента и особенностей его функционирования, а также специфики реализации функций безопасности [2–4].

Аппаратный компонент может быть "мобильным" — отчуждаемым от средства вычислительной техники (СВТ) в течение эксплуатации программно-аппаратного СЗИ. В этом случае при проведении тестирования функций безопасности СЗИ его иногда необходимо переподключать к СВТ, т. е. физически отключать, а затем подключать к соответствующему интерфейсу.

Автоматизировать процесс тестирования функций безопасности таких СЗИ с использованием только комплекса программ тестирования затруднительно, необходимо применять вспомогательное средство, учитывающее особенности функционирования аппаратного компонента СЗИ [5, 6]. Такое средство должно эмулировать физическое отключение и подключение СЗИ к определенному интерфейсу СВТ автоматизированным способом.

Сэмулировать подключение и переподключение СЗИ к СВТ можно с помощью программных средств (с использованием BIOS, настройкой конкретной операционной системы (ОС)). Однако при этом такое подключение и переподключение может не полностью эмулировать физическое отключение (например, может не происходить отключение питания), что делает невозможным использование таких программных средств для тестирования функций безопасности "мобильных" программно-аппаратных СЗИ, функционирующих в среде ОС СВТ. Кроме того, такие программные средства могут быть неуниверсальными для различных версий ОС, BIOS и т. д. В связи с этим для подключения и переподключения к СВТ "мобильных" программно-аппаратных СЗИ, функционирующих в среде ОС, целесообразно применять именно программно-аппаратные, а не программные средства. Проведенный анализ открытых источников показал, что средств, реализующих возможность эмуляции физического подключения/отключения СЗИ к СВТ, на рынке не представлено, поэтому такое средство требуется разработать.

Вспомогательное средство тестирования — коммутатор USB-канала

При разработке средства, реализующего возможность эмуляции физического подключения/отключения СЗИ к СВТ, необходимо учитывать тип интерфейса подключения "мобильного" СЗИ к СВТ, при этом принцип работы для различ-

Каннер Татьяна Михайловна, начальник отдела сопровождения и верификации продуктов.
E-mail: tatianash@okbsapr.ru

Статья поступила в редакцию 22 февраля 2017 г.

© Каннер Т. М., 2017

ных интерфейсов должен быть единообразен. Также данное средство, реализованное для одного из типов интерфейса, должно быть применимо для различных СЗИ, использующих этот интерфейс для подключения к СВТ.

В соответствии с изложенными принципами в ОКБ САПР был разработан так называемый коммутатор USB-канала (внешний вид показан на рис. 1), предназначенный для автоматизации тестирования функций безопасности "мобильных" СЗИ, подключаемых к USB-интерфейсу СВТ.

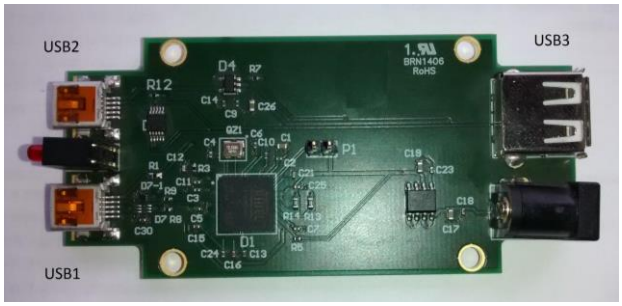

Рис. 1. Коммутатор USB-канала

Данный комплекс представляет собой:

- программно-аппаратное средство, устанавливаемое между USB-интерфейсом СВТ и СЗИ "в разрыв" USB-канала и осуществляющее его коммутацию в соответствии с командами, поступающими по каналу управления;
- программное обеспечение, позволяющее программно из ОС СВТ подать соответствующую команду по каналу управления (включить или отключить передачу данных и питание для коммутируемого USB-устройства).

Такое средство способно физически прерывать питание различных подключаемых к нему USB-устройств (например, ПСКЗИ ШИПКА и СН "Секрет" производства ОКБ САПР) без их физического отключения или переподключения. Коммутатор USB-канала с подключенным коммутируемым СЗИ — ПСКЗИ ШИПКА изображен на рис. 2.

Рис. 2. Коммутатор USB-канала с подключенным коммутируемым СЗИ – ПСКЗИ ШИПКА

Коммутатор USB-канала предназначен для выполнения следующих функций:

- управляемое переподключение USB-устройств в процессе автоматизированного тестирования функций безопасности СЗИ (т. е. коммутатор USB-канала используется как вспомогательное средство тестирования);
- управляемая блокировка доступа к USB-каналу (коммутатор USB-канала выступает как компонент СЗИ, реализующий блокировку запрещенных USB-устройств и позволяющий осуществлять доступ к разрешенным USB-устройствам).

Функционально коммутатор USB-канала состоит из следующих компонентов:

- аппаратный компонент с внутренним ПО (firmware), запускающимся при поступлении питания и выполняющим основной функционал программно-аппаратного комплекса;
- программный компонент (внешнее ПО), состоящий из:
  - библиотеки для встраивания и использования комплекса в стороннем ПО;
  - утилиты командной строки для выполнения коммутации USB-устройств (с использованием библиотеки).

Коммутация USB-канала обеспечивается синхронным включением и выключением мультиплексора линий данных и питания. Команды между внешним и внутренним ПО передаются путем обмена сообщениями специального формата по управляющему каналу данных.

С использованием библиотеки для встраивания комплекса в стороннее ПО или работающей на ее основе утилиты командной строки можно подать следующие команды аппаратному компоненту:

- включить передачу данных и питание;
- отключить передачу данных и питание;
- запросить состояние коммутации.

Программный интерфейс коммутатора USB-канала предоставляет следующий набор функций:

```
std::list<std::string> US_Enumerate();
std::string US_ON(std::string usbSwitcher);
std::string US_OFF(std::string usbSwitcher).
```

Здесь usbSwitcher — строка (из списка, возвращаемого US_Enumerate()), идентифицирующая коммутатор USB-канала, которому передается команда (вида "OKB SAPR USB Switcher X", где X — номер подключенного к СВТ коммутатора, начиная с "0");

US_Enumerate — функция, осуществляющая поиск и вывод списка найденных и доступных в данный момент коммутаторов USB-канала (либо

пустой список в случае отсутствия подключенных к СВТ коммутаторов);

US_ON — функция, передающая команду на включение передачи данных и питания устройств, подключенных к коммутатору USB-канала (в случае корректного завершения работы возвращает "SUCCESS", иначе – генерируется исключение типа std:string с подробным описанием ошибки);

US_OFF — функция, передающая команду на отключение передачи данных и питания устройств, подключенных к коммутатору USB-канала (в случае корректного завершения работы возвращает "SUCCESS", иначе — генерируется исключение типа std:string с подробным описанием ошибки).

При использовании коммутатора USB-канала с помощью утилиты командной строки (USBSwitcherConsole.exe) необходимо передавать на вход следующие параметры:

- list — для вывода списка доступных коммутаторов USB-канала (т. е. реализуется выполнение функции US_Enumerate из библиотеки встраивания и использования комплекса в стороннем ПО);
- on <switcherName> — для включения передачи данных и питания устройств, подключенных к соответствующему коммутатору (т. е. реализуется выполнение функции US_ON из библиотеки встраивания и использования комплекса в стороннем ПО). Без указания <switcherName> команда отправляется на первый доступный коммутатор;
- off <switcherName> — для отключения передачи данных и питания устройств, подключенных к соответствующему коммутатору (т. е. реализуется выполнение функции US_OFF из библиотеки встраивания и использования комплекса в стороннем ПО). Без указания <switcherName> команда отправляется на первый доступный коммутатор.

Комплекс программ тестирования функций безопасности программно-аппаратных СЗИ

С учетом требований к средствам тестирования различных видов функций безопасности программно-аппаратных СЗИ и среде их применения, представленных в [5] и [6], разработан программный комплекс "Тестирование функций безопасности программно-аппаратных средств защиты информации" (свидетельство о государственной регистрации программы для ЭВМ № 2016616332). Данный комплекс программ предназначен для тестирования функций безопасности следующих программно-аппаратных СЗИ при внедрении их в ИС: ПСКЗИ ШИПКА — персональное средство криптографической защиты; ПАК СЗИ НСД "Аккорд-X" — программно-аппаратное средство разграничения доступа пользователей в ОС. Также в комплекс входит программа верификации программно-аппаратных СЗИ по результатам тестирования.

Применение разработанного комплекса совместно с рассмотренным коммутатором USB-канала позволяет выполнять автоматическое тестирование различных видов функций безопасности программно-аппаратных СЗИ, обеспечивая при этом полноту тестирования и исключая неточности его проведения за счет "человеческого фактора", а также сократить временные затраты на данный процесс.

Оценка эффективности использования средств тестирования функций безопасности программно-аппаратных СЗИ

Для оценки эффективности использования разработанного комплекса программ тестирования, в том числе совместно с вспомогательным средством тестирования – коммутатором USB-канала, было проведено несколько экспериментов ручного тестирования функций безопасности различных версий следующих программно-аппаратных СЗИ: ПСКЗИ ШИПКА и ПАК СЗИ НСД "Аккорд-X". При этом тестирование поочередно проводилось на различных ОС, в которых, согласно документации на комплексы, может функционировать каждое из этих СЗИ, а также с различными исполнениями аппаратных компонент, реализующих функции безопасности рассматриваемых средств защиты. При проведении каждой проверки было измерено затраченное на нее время, а также время анализа полученных результатов. На основании среднего значения времени, затраченного на проведение ручного тестирования в каждой из поддерживаемых ОС со всеми вариантами исполнений аппаратной компоненты, а также времени анализа его результатов было рассчитано общее суммарное время ручного тестирования для каждого из рассматриваемых средств защиты. Также в каждом эксперименте на основании полученных при тестировании ошибок выполнена верификация СЗИ, измерено время ее ручного проведения (не включающее время, затраченное на тестирование) и получено его среднее значение.

Затем было проведено автоматическое тестирование функций безопасности выбранных программно-аппаратных СЗИ с использованием разработанных программ тестирования и необходимых вспомогательных средств тестирования (во всех ОС со всеми исполнениями аппаратной компоненты). После этого были рассчита-

ны общее суммарное время данного тестирования (рассчитывается с учетом параллельного выполнения программ тестирования и анализа результатов их работы) и время на проведение верификации с использованием соответствующей программы из разработанного комплекса.

При анализе экспериментов показано, что временные характеристики для ручного тестирования рассчитываются в человеко-часах, а для автоматического – в часах, кроме времени анализа результатов автоматических проверок. Помимо этого, при переводе затраченного на ручное тестирование времени из человеко-часов в человеко-дни необходимо учитывать, что рабочий день обычно составляет 8 ч. (т. е. 1 человеко-день соответствует 8 человеко-часам). Такого ограничения нет при расчете временных характеристик для автоматического тестирования: программы тестирования могут работать и без участия тестировщика, т. е. и в нерабочее время. Таким образом, общее затраченное время при переводе из часов в дни для ручного и автоматического тестирования рассчитывается по-разному. При этом необходимо учитывать, что анализ результатов автоматического тестирования может выполняться параллельно с функционированием программ тестирования.

Проведенные экспериментальные исследования показали, что временные затраты на ручное тестирование и верификацию одной версии любого из рассматриваемых средств защиты являются достаточно большими: для их проведения во всех возможных ОС со всеми возможными вариантами исполнения аппаратной компоненты в среднем необходимо более полугода работы одного тестировщика, из которых ручная верификация займет не менее двух рабочих дней. При этом важным является тот факт, что временные затраты на тестирование и верификацию включаются во время, затрачиваемое на внедрение СЗИ в ИС, а это значит, что в рассматриваемом случае внедрение будет также продолжаться не менее полугода. Кроме того, в процессе внедрения средства защиты в ИС может быть найден ряд ошибок, влияющих на пользовательские и функциональные характеристики данной системы. На основании этого будет необходимо вносить изменения в СЗИ с последующей сборкой его очередной версии, также требующей тестирования и верификации, а предыдущие их результаты окажутся неактуальными. Повторные тестирование и верификация увеличат срок внедрения еще на полгода. Таким образом, проведение ручных проверок с учетом достаточно быстрого изменения условий тестирования (выхода обновлений для ИС, ОС и т. п.) приводит к неадекватным срокам внедрения СЗИ в ИС [5, 6]. На автоматическое тестирование затрачивается не более одного-двух месяцев, а результаты автоматической верификации можно получить в течение нескольких минут, что уже представляет собой адекватные сроки.

В результате за время одного цикла полного ручного тестирования программно-аппаратного СЗИ со всеми возможными сочетаниями ОС и исполнений аппаратной компоненты при автоматическом тестировании с аналогичными условиями уже будут исправлены все выявленные ошибки, произведены повторное тестирование и верификация, а также завершено внедрение в ИС. Аналогичная ситуация будет складываться в случае, когда для внедрения в ИС нет необходимости тестировать все возможные сочетания ОС и исполнений аппаратной компоненты (временные характеристики будут другими, но их соотношение не изменится).

Данные временных затрат на ручное и автоматизированное тестирование функций безопасности нескольких программно-аппаратных СЗИ приведены на рис. 3.

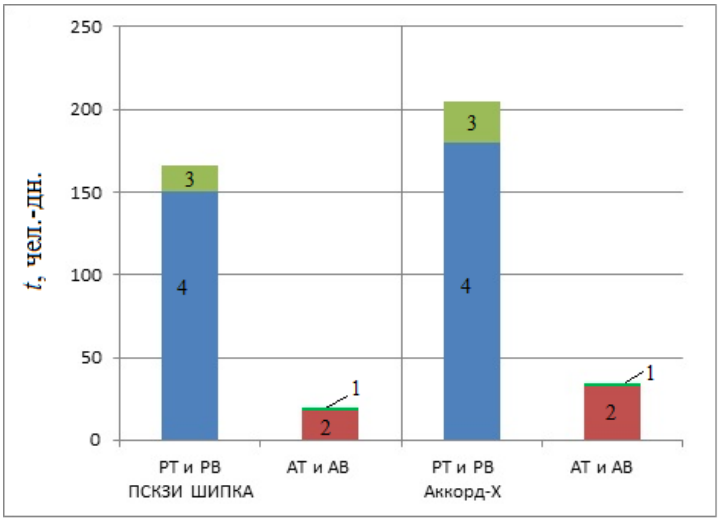

***Рис. 3. Гистограмма временных затрат на ручное (РТ/РВ) и автоматическое (АТ/АВ) тестирование/верификацию средств защиты, реализующих функции безопасности различных видов*:**
1 — время АВ; 2 — время АТ;
3 — время РВ; 4 — время РТ

Изложенные аспекты подтверждают положительный количественный эффект от применения разработанных программ тестирования, в том числе с использованием вспомогательного средства тестирования – коммутатора USB-канала, для тестирования функций безопасности программно-аппаратных СЗИ.

Заключение

Таким образом, разработанный программно-аппаратный комплекс при вызове команд по управляемой коммутации СЗИ полностью эмулирует его физическое отключение и подключение к СВТ как на уровне питания, так и на уровне канала передачи данных. Коммутатор USB-канала совместно с комплексом программ "Тестирование функций безопасности программно-аппаратных средств защиты информации" можно использовать для автоматизации тестирования функций безопасности "мобильных" программно-аппаратных СЗИ, функционирующих в среде ОС СВТ и имеющих USB-интерфейс подключения, достигая при этом существенного сокращения временных затрат.

Литература

1. *Каннер Т. М., Обломова А. И.* О выборе инструмента автоматизации тестирования для программно-аппаратных СЗИ // Вопросы защиты информации. 2014. № 4. С. 34—36.
2. *Каннер (Борисова) Т. М., Кузнецов А. В.* Проблемы тестирования СЗИ, функционирующих до старта ОС. Мат. XVIII Межд. конф. "Комплексная защита информации". 21—24 мая 2013 г. Электроника инфо. — Брест, 2013. С. 114—115.
3. *Каннер (Борисова) Т. М., Обломова А. И.* Способы автоматизации тестирования СЗИ, функционирующих в ОС, на примере ПСКЗИ ШИПКА. Мат. XVIII Межд. конф. "Комплексная защита информации". 21—24 мая 2013 г. Электроника инфо. — Брест, 2013.С. 117—118.
4. *Каннер Т. М., Куваева К. А.* Формирование подхода к автоматизации тестирования СЗИ, в конструктив которых входит флеш-память, функционирующих в ОС // Вопросы защиты информации. 2014. № 4. С. 52—54.
5. *Каннер Т. М.* Применимость методов тестирования ПО к программно-аппаратным СЗИ // Вопросы защиты информации. 2015. № 1. С. 30—39.
6. *Kanner T. M.* Applicability of Software Testing Methods to Software and Hardware Data Security Tools // Global Journal of Pure and Applied Mathematics. — 2016. — V. 12, № 1. P. 167—190.

The effectiveness of using supporting tools for testing software and hardware DST

T. M. Kanner
Closed Joint Stock Company "OKB SAPR", Moscow, Russia

The article describes the purpose, structure and operating principle of a developed tool for automated testing of the features of portable software and hardware data security tools (DST) that operate in an OS of a computer and have a USB connection interface – USB switcher. The efficiency of using this tool in conjunction with the program complex for testing the security features of software and hardware DST developed by the author is presented.

Keywords: portable software and hardware DST, USB switcher, program complex for testing the security features.

Bibliography — 6 references. *Received February 22, 2017*