УДК 004.056.5

РАЗРАБОТКА И ОЦЕНКА ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ СРЕДСТВ ТЕСТИРОВАНИЯ ФУНКЦИЙ БЕЗОПАСНОСТИ ПРОГРАММНО-АППАРАТНЫХ СЗИ

Т.М. Каннер

В статье рассматривается назначение, состав и принцип функционирования коммутатора USB-канала, применяемого для автоматизированного тестирования функций безопасности отчуждаемых программно-аппаратных средств защиты информации, функционирующих в операционной системе средств вычислительной техники и имеющих USB-интерфейс подключения. Обоснована необходимость эмуляции автоматизированного физического отключения и подключения средства защиты к определенному интерфейсу СВТ при использовании разработанного автором комплекса программ тестирования функций безопасности программно-аппаратных СЗИ.

Ключевые слова: автоматизированное тестирование функций безопасности, отчуждаемые программно-аппаратные СЗИ, коммутатор USB-канала.

Все чаще при создании информационных систем (ИС) применяются эффективные инструментальные средства, что приводит к достаточно быстрому развитию таких ИС, а, следовательно, и время, затрачиваемое на разработку применяемых в них СЗИ, должно быть максимально сокращено. Для уменьшения времени разработки СЗИ необходимо выделить этапы, которые можно полностью автоматизировать или хотя бы автоматизировать частично. К таким этапам можно отнести тестирование и верификацию средств защиты информации с последующим исправлением обнаруженных ошибок. Данные этапы многократно повторяются при разработке СЗИ, поэтому уменьшения затрачиваемого на данный процесс времени можно добиться путем автоматизации процесса тестирования функций безопасности средства защиты.

Для программных средств защиты информации существует большой спектр средств автоматизации тестирования [1]. Использование же таких средств для программно-аппаратных СЗИ может быть затруднено в силу наличия аппаратного компонента и особенностей его функционирования, а также специфики реализации функций безопасности [2].

Каннер Татьяна Михайловна – ЗАО «ОКБ САПР», руководитель обучающего центра,
e-mail: tatianash@okbsapr.ru

Аппаратный компонент ряда программно-аппаратных СЗИ необходимо отчуждать от средства вычислительной техники (СВТ) в процессе эксплуатации. Поэтому при проведении тестирования функций безопасности таких СЗИ также требуется отключать и подключать их аппаратный компонент к необходимому интерфейсу СВТ.

Автоматизация процесса тестирования функций безопасности таких средств защиты при помощи программ тестирования становится непростой задачей и требует применения вспомогательного средства, учитывающего особенности функционирования аппаратного компонента [3, 4]. Такое средство должно предоставлять возможность автоматизированного физического переподключения СЗИ к СВТ.

Эмуляцию подключения и отключения средства защиты можно реализовать, применяя программные средства: через BIOS, настройку операционной системы (ОС) СВТ. При этом необходимо учитывать, что эти способы не полностью эмулируют физическое отключение, например, может не происходить отключение питания, подаваемого на аппаратную компоненту СЗИ. Такие моменты показывают невозможность использования программных средств для тестирования функций безопасности отчуждаемых программно-аппаратных СЗИ, функционирующих в среде ОС СВТ. Помимо этого программные

средства могут быть неуниверсальными для различных версий ОС и BIOS. Поэтому для подключения/отключения к/от СВТ отчуждаемых программно-аппаратных СЗИ, функционирующих в среде ОС, целесообразным видится применение именно программно-аппаратных, а не программных средств. Исследования показали, что в настоящее время таких программно-аппаратных средств на рынке не представлено, поэтому такое средство необходимо разработать.

Предполагаемое средство должно учитывать тип интерфейса подключения отчуждаемого СЗИ к СВТ, а принцип работы для различных интерфейсов должен быть единообразен. Помимо этого такое средство должно быть применимо для различных средств защиты, использующих один и тот же интерфейс для подключения к средству вычислительной техники.

Перечисленные принципы были положены в основу разработанного в ОКБ САПР коммутатора USB-канала (см. рис. 1). Данный коммутатор предназначен для автоматизации тестирования функций безопасности отчуждаемых СЗИ, подключаемых к USB-интерфейсу СВТ.

Рис. 1. Коммутатор USB-канала с подключенным коммутируемым СЗИ – ПСКЗИ ШИПКА

В состав разработанного комплекса входит [5]:

– программно-аппаратное средство, устанавливаемое «в разрыв» USB-канала между СВТ и средством защиты, и осуществляющее его коммутацию при помощи команд, передаваемых по каналу управления;

– ПО, позволяющее программно из ОС СВТ подать соответствующую команду по каналу управления (включить или отключить передачу данных и питание для коммутируемого USB-устройства).

Коммутатор USB-канала физически прерывает питание подключаемых к нему USB-устройств, таких как ПСКЗИ ШИПКА, СН «Секрет Особого Назначения», СН «Личный Секрет» производства ОКБ САПР и других аналогичных, без их отключения от соответствующего интерфейса СВТ [5].

Помимо рассмотренного вспомогательного средства (коммутатора USB-канала) в целях автоматизации тестирования автором разработан комплекс программ «Тестирование функций безопасности программно-аппаратных средств защиты информации», в состав которого входят программы тестирования и верификации отчуждаемых СЗИ, функционирующих в ОС СВТ и подключаемых к его USB-интерфейсу.

Для демонстрации сокращения временных затрат на процесс тестирования при применении коммутатора USB-канала и программ тестирования проведен ряд экспериментов для различных версий выбранного программно-аппаратного СЗИ – ПСКЗИ ШИПКА. Ручное тестирование (РТ) проводилось поочередно на всех поддерживаемых данным средством защиты ОС и со всеми возможными вариантами исполнения аппаратной компоненты, с исполь-

зованием которой реализуются все функции безопасности. В ходе проверок измерялось затрачиваемое время на саму проверку, а также на анализ ее результатов.

Суммарное время РТ рассчитывается путем сложения среднего значения времен РТ в каждой из тестируемых ОС с каждым вариантом исполнений аппаратной компоненты со временем анализа результатов тестирования.

Помимо этого было рассчитано среднее значение времени ручной верификации (РВ) СЗИ, выполненной с использованием полученных при тестировании ошибок. В тех же условиях было проведено автоматическое тестирование (АТ) функций безопасности выбранного программно-аппаратного СЗИ с использованием разработанных коммутатора USB-канала и комплекса программ тестирования, вычислено суммарное время автоматического тестирования с учетом возможности параллельного выполнения программ тестирования и анализа результатов их работы (по готовности первых результатов).

Также было измерено время проведения автоматической верификации (АВ). Все измеренные и рассчитанные показатели занесены в таблицу.

Временные характеристики РТ/РВ и АТ/АВ для ПСКЗИ ШИПКА

	Характеристики, показатели экспериментальных исследований	**Значение хар-ки**
1	Количество ОС	10
2	Количество аппаратных компонент	6
3	Время РТ с анализом, чел.-ч. (1 ОС, 1 апп. компонента)	20
4	Общее время РТ, чел.-ч.	1200
5	Общее время РТ, чел.-д.	150
6	Время РВ, чел.-ч.	16
7	Время АТ (без анализа результатов), ч. (1 ОС, 1 апп. компонента)	2,5
8	Общее время АТ, ч.	150
9	Время анализа результатов АТ, чел.-ч. (1 ОС, 1 апп. компонента)	2,5
10	Общее время анализа результатов АТ, чел.-ч.	150
11	Общее время АТ, чел.-д.	18,75
12	Время АВ, ч.	0,04

Необходимо отметить, что временные характеристики для РТ представлены в таблице в человеко-часах (чел.-ч.), а для АТ – в часах (ч.).

Исключение составляет время анализа результатов автоматических проверок, которое представлено так же, как и для РТ в человеко-часах. При переходе от чел.-час в чел.-дни необходимо обратить внимание на продолжительность рабочего дня тестировщика (8 часов). Для АТ таких ограничений нет в связи с тем, что программы тестирования функционируют без участия человека, а значит, могут выполняться и в нерабочее время, и в то время, когда он анализирует результаты предыдущих этапов АТ. Описанные особенности показывают, что затрачиваемое на АТ время рассчитывается иначе, чем для РТ.

Из таблицы очевидно, что временные затраты на РТ и РВ даже одной версии средства защиты информации составляют около полугода работы одного тестировщика (при условии проведения тестирования и верификации во всех поддерживаемых ОС со всеми вариантами аппаратной компоненты).

Учитывая, что такое тестирование может выполняться при внедрении СЗИ в некоторую ИС, сроки окончания внедрения и, возможно, ввода ИС в эксплуатацию будут составлять не менее полугода. Также в ходе тестирования и верификации могут быть выявлены ошибки, наличие которых не позволяет использовать СЗИ в ИС. Это, в свою очередь, потребуют внесения

изменений в СЗИ с последующей необходимостью тестирования и верификации новой измененной версии (результаты предыдущей итерации тестирования и верификации при этом будут уже неактуальны). Такое повторное тестирование и верификация увеличат срок внедрения СЗИ в ИС и, возможно, ввод ИС в эксплуатацию еще, как минимум, на то время, которое было затрачено на первую итерацию. Таким образом, очевидно, что процесс РТ с учетом возможного достаточно быстрого изменение условий тестирования (изменение требований к ИС, выход обновлений для компонент ИС или ОС и так далее) приводит к неадекватным срокам внедрения в нее СЗИ.

В случае применения коммутатора USB-канала и комплекса программ тестирования на АТ затрачивается около одного месяца, а на АВ – всего несколько минут. Данные результаты даже при выявлении и исправлении серьезных ошибок в СЗИ представляют собой уже реальные сроки.

Таким образом, разработанные программно-аппаратное вспомогательное средство тестирования (коммутатор USB-канала) совместно с комплексом программ позволяют автоматизировать тестирование функций безопасности отчуждаемых программно-аппаратных СЗИ с USB-интерфейсом подключения на качественно новом уровне, добиться сокращения временных затрат на этот процесс, а также на процесс внедрения средств защиты в ИС и, возможно, ввод ИС в эксплуатацию.

Литература

1. Каннер Т.М., Обломова А.И. О выборе инструмента автоматизации тестирования для программно-аппаратных СЗИ // Вопросы защиты информации. Научно-практический журнал.— М., 2014.— № 4. — С. 34-36

2. Каннер (Борисова) Т.М., Обломова А.И. Способы автоматизации тестирования СЗИ, функционирующих в ОС, на примере ПСКЗИ ШИПКА // Комплексная защита информации. Электроника инфо. Материалы Электроника инфо. Материалы XVIII Международной конференции 21–24 мая 2013 года, Брест (Республика Беларусь). 2013. — С. 117-118

3. Каннер Т.М. Применимость методов тестирования ПО к программно-аппаратным СЗИ // Вопросы защиты информации. — М., 2015. — № 1. — С. 30-39

4. Kanner T. M. Applicability of Software Testing Methods to Software and Hardware Data Security Tools // Global Journal of Pure and Applied Mathematics. — 2016. — Vol. 12, no. 1. — Pp. 167–190

5. Каннер Т.М. Эффективность применения средств тестирования программно-аппаратных СЗИ // Вопросы защиты информации. Научно-практический журнал. — М., 2017. — № 2. — С. 9-13

Закрытое акционерное общество «ОКБ САПР»
Closed Joint Stock Company «OKB SAPR»

DEVELOPMENT OF SUPPORTING TOOLS FOR TESTING SECURITY FEATURES OF SOFTWARE AND HARDWARE DST

T.M. Kanner

The article considers the purpose, structure and operating principle of the USB switcher which can be used for automated testing of security features of removable software and hardware data security tools (DST) with USB-interface in operating system. Author justified the necessity of emulation for DST automated physical disconnection and connection to a specific interface with using security features' testing software complex developed by author.

Keywords: automated testing of security features, removable software and hardware DST, USB switcher.