

---

*V.S. Gorbatov, T.A. Kondratieva, A.A. Meshcheriakov*  
**Automated testing software and hardware protection of information**  
**in virtualized environments**

*Key words: testing, automation, virtualization*

The paper considers the problem of application virtualization technology for test automation software and hardware protection of information.

*В.С. Горбатов, Т.А. Кондратьева, А.А. Мецержаков*

**АВТОМАТИЗИРОВАННОЕ ТЕСТИРОВАНИЕ  
ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ  
В ВИРТУАЛИЗИРОВАННОЙ СРЕДЕ<sup>1</sup>**

В настоящее время в силу массового применения средств защиты информации (СЗИ) особую актуальность приобретают вопросы тестирования их работоспособности, решение которых позволяет повысить качество продукта, тем самым увеличивая его конкурентоспособность. Основная цель тестирования – выявление ошибок в программной реализации заданных свойств программного обеспечения (ПО), что в настоящее время практически невозможно без автоматизации, которая позволяет существенно увеличить производительность процесса тестирования и минимизировать «человеческий фактор», связанный с ошибками тестировщика. Такой подход задан современной методологией производства программных средств, при котором тестирование интегрировано в жизненный цикл ПО, что с учетом автоматизации этого процесса повышает скорость разработки.

Обычно для автоматизации тестирования программного обеспечения (ПО) используются скрипты, эмулирующие действия пользователя [1]. Но при перенесении данного подхода на программно-аппаратные комплексы (ПАК) СЗИ разработчики тестов сталкиваются с проблемами, описанными в статье [2]. Во-первых, скрипты могут функционировать только в операционной системе (ОС), поэтому их невозможно использовать для тестирования СЗИ, функционирующих до старта ОС. Во-вторых, при тестировании часто необходимо подключение/отключение аппаратной части СЗИ, что требует дополнительного вмешательства тестировщика.

Для устранения этих проблем в данной работе предлагается использовать подход, позволяющий применение технологий виртуализации. Он заключается в использовании виртуальных машин, эмулирующих работу ОС, как показано на рис. 1, где приведена схема стенда для тестирования ПАК СЗИ. Для контроля выполнения и эмуляции действий пользователя используется интерфейс программирования приложений (API), предоставляемый средством виртуализации. При этом аппаратная часть СЗИ «пробрасывается» в виртуальную машину.

---

<sup>1</sup> Данная работа выполнена в НИЯУ МИФИ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия», выполненного совместно с ООО «ОКБ САПР» по договору № 02.G25.31.0050

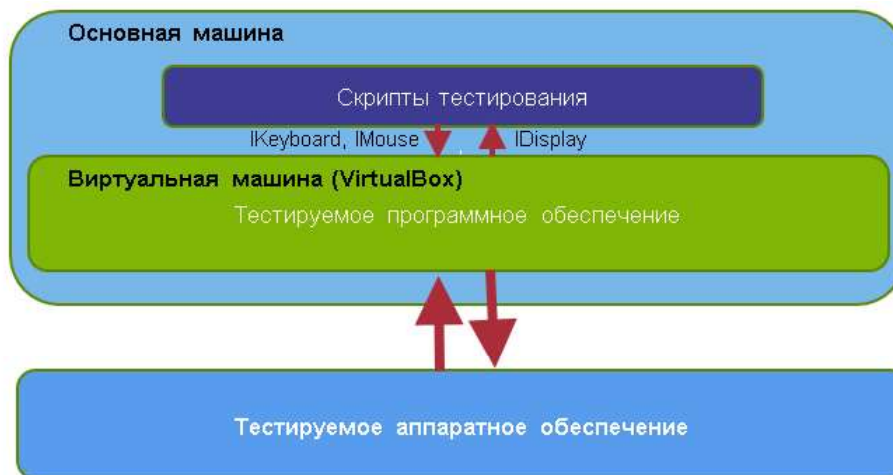


Рис. 1. Схема стенда для тестирования ПАК

Для практической реализации данного подхода предлагается использовать средство виртуализации VirtualBox, имеющее богатый набор API-функций для реализации скриптов тестирования. Эмуляция действий пользователя выполняется при помощи интерфейсов IKeyboard и IMouse, позволяющих имитировать клавиатурный и курсорный ввод через отправку скан-кодов клавиш и событий мыши. При этом необходимо учитывать то, что в ПАК СЗИ обработка событий клавиатурного и курсорного ввода требует определенного количества времени.

Обработку результатов выполнения теста можно осуществить двумя способами. Первый способ заключается в записи результата в файл с последующей отправкой в хост-систему (например, по сети либо через разделяемую файловую систему). Однако данный способ может быть не всегда реализуем из-за особенностей функционирования СЗИ. Второй способ опирается на выбор информации из интерфейса IDisplay, позволяющего получить скриншоты дисплея виртуальной машины. В таком случае о результате выполнения теста можно судить либо путем сравнения эталонного и полученного скриншота, либо с помощью распознавания текстовой информации, выводимой скриптом тестирования. При этом любая изменяющаяся информация, не относящаяся к процессу тестирования, например, значение системных часов, отбрасывается.

Использование данного подхода позволяет выполнять тестирование программно-аппаратных СЗИ как функционирующих в ОС, так и стартующих до запуска ОС. Другим преимуществом является то, что в данном случае выполняется полная имитация действий пользователя, что позволяет реализовать полное функциональное тестирование ПАК для оценки корректности и надежности его функционирования.

Основным ограничением данного подхода являются недоработки современных средств виртуализации, которые не позволяют «пробрасывать» некоторые аппаратные интерфейсы в виртуальную машину. К другим ограничениям описанного метода тестирования можно отнести невозможность контроля внутреннего состояния тестируемого ПАК СЗИ, а также выполнение тестовых сценариев в контексте пользователя, который может быть ограничен в правах. Помимо указанных ограничений данная технология автоматизации тестирования предъявляет повышенные требования к тестировщику, который должен обладать навыками программирования для написания и поддержки тестовых сценариев.

Для преодоления указанных выше ограничений в качестве дальнейшего развития описанной методики организации тестирования можно предложить такие варианты улучшений, как доступ к оперативной памяти СЗИ, и написание библиотеки для упрощения написания тестов.

VirtualBox API предоставляет интерфейс IMachineDebugger для доступа к оперативной памяти и регистрам процессора. Такой доступ может быть полезен для отслеживания состояния внутренних структур СЗИ. Написание библиотеки, реализующей повторяемые функции (отправка скан-кодов, сравнение скриншотов и т.д.), позволяет снизить сложность написания тестовых скриптов.

Технология виртуализации была использована при разработке тестовых сценариев для средства обеспечения доверенного сеанса (СОДС) «МАРШ!» [3], что позволило добиться полной автоматизации выполнения тестовых сценариев без внесения каких-либо изменений в ОС СОДС «МАРШ!».

### СПИСОК ЛИТЕРАТУРЫ:

1. Graham D., Fewster M. Experience of test automation / D. Graham, M. Fewster – Addison-Wesley, 2012. – 617 с.
2. Борисова Т.М. Особенности автоматизации тестирования программно-аппаратных СЗИ, 2013. URL: [http://www.okbsapr.ru/borisova\\_2013\\_1.html](http://www.okbsapr.ru/borisova_2013_1.html) (дата обращения 20.06.2015).
3. ПАК СОДС «МАРШ!», 2014. URL: <http://www.sodsmarsh.ru/> (дата обращения 20.06.2015).

### REFERENCES:

1. Graham D., Fewster M. Experience of test automation / D. Graham, M. Fewster – Addison-Wesley, 2012. – 617 с.
2. Borisova T.M. Features test automation software and hardware protection of information, 2013. URL: [http://www.okbsapr.ru/borisova\\_2013\\_1.html](http://www.okbsapr.ru/borisova_2013_1.html)
3. PAK SODS «MARSH!», 2014. URL: <http://www.sodsmarsh.ru>