УДК 004.054

# Особенности тестирования средств защиты информации от несанкционированного доступа в виртуальной инфраструктуре

*Н. В. Мозолина*
Московский физико-технический институт (государственный университет),
г. Долгопрудный, Московская область, Россия

*К. А. Луговцова*
Закрытое акционерное общество «ОКБ САПР», Москва, Россия

*Рассмотрены особенности и проблемы функционального тестирования средств защиты информации от несанкционированного доступа в виртуальной инфраструктуре. Предлагается способ их решения при помощи средств автоматизации тестирования и разделения процесса тестирования на два независимых этапа.*

*Ключевые слова*: функциональное тестирование, автоматизация процессов тестирования, виртуальная инфраструктура.

Неотъемлемым этапом разработки программного обеспечения, в том числе и средств защиты информации, является тестирование всех его компонентов на соответствие заданным требованиям. Существует множество видов тестирования. Ограничимся рассмотрением функционального тестирования, направленного на проверку того, какие функции программного обеспечения реализованы, и того, что они работают верным образом [1].

Процесс функционального тестирования состоит из четырех стадий: выбор действия, определение ожидаемого результата этого действия, определение фактического результата и сравнение результатов.

Одним из самых простых способов тестирования является выполнение всех этих операций человеком вручную. Такой подход хоть и не требует большого объема подготовительных действий от тестировщика, но вместе с тем имеет ряд существенных минусов: человек может случайно или осознанно пропустить часть тестов, неверно интерпретировать результаты испытания, сделать ложные выводы, а также такое тестирование может растянуться на недели и даже месяцы. Для решения таких проблем используют автоматизацию: IBM Rational Functional Tester (RFT), TestComplete и другие продукты позволяют воспроизводить действия пользователя программного обеспечения, обрабатывать результаты тестовых испытаний и сравнивать их с ожидаемыми. Это исключает ошибки, которые человек может сделать в силу усталости или невнимательности, а также значительно сокращает время выполнения тестов.

Чем сложнее устроен создаваемый продукт, тем более объемными и затратными становятся тестовые испытания не только с точки зрения времени, но и с точки зрения ресурсов, необходимых для работы тестируемого программного обеспечения. Особенно остро эта проблема стоит при испытании средств защиты информации для виртуальных инфраструктур.

Рассмотрим проблемы и особенности проведения тестовых испытаний при разработке программно-аппаратного комплекса Сегмент-В. и способ их решения.

Данный продукт предназначен для защиты инфраструктур виртуализации, построенных на базе платформы VMware vSphere. Сегмент-В. представляет собой совокупность технических и программных средств, предназначенных для обеспечения защиты от несанкционированного доступа [2].

Одна из основных функций программно-аппаратного комплекса — управление доступом субъектов к объектам в виртуальной инфраструктуре. Она осуществляется за счет перехвата всех команд управления прокси-сервером Segment-V. Module и их обработки на основе заранее созданных правил (метки и уровни доступа для объектов и субъектов, списки разрешенных действий пользователей, политики прокси-сервера). Эта функция осу-

**Мозолина Надежда Викторовна**, инженер группы разработки СЗИ для систем виртуализации.
E-mail: nmozolina@okbsapr.ru
**Луговцова Ксения Александровна**, тестировщик отдела тестирования.
E-mail: kuvaeva@okbsapr.ru

*Статья поступила в редакцию 26 июня 2016 г.*

ществляется модулем контроля доступа, входящим в прокси-сервер Segment-V. Module.

Для тестирования модуля контроля доступа необходимо провести тестовые испытания, охватывающие весь спектр возможных действий администратора виртуальной инфраструктуры. Результатом исполнения теста должны быть данные об исполняемой команде управления, субъекте и объектах, участвующих в данном действии.

Использование автоматизированных тестов, моделирующих операции пользователя, избавляет тестировщика от необходимости вручную исполнять каждое действие и следить за его результатами [3], но, как и прежде, требует наличия тестовой виртуальной инфраструктуры, предусматривающей всевозможные отношения между объектами и субъектами доступа.

Например, виртуальная машина может находиться на локальном хранилище хоста или на хранилище, подключенном по iSCSI, гипервизоры могут образовывать кластер или не быть объединенными в общий ресурс. Кроме того, Сегмент-В. позволяет назначать метки и уровни доступа субъектов и объектов, что рождает новые отношения между элементами инфраструктуры. Для полной проверки работы функции управления доступом Сегмента-В. тестовая инфраструктура должна предоставлять возможность работы с каждым типом объектов и всеми возможными отношениями между ними и субъектами. Виртуальная инфраструктура, удовлетворяющая этим условиям, требует значительных вычислительных ресурсов и места на хранилище.

Для решения этой проблемы был использован следующий подход. Четыре стадии процесса тестирования выполняются в два этапа:

1) выбор действия, определение ожидаемого результата этого действия с помощью записи команд в log-файл и создания файлов с эталонными результатами теста;

2) определение фактического результата проведения тестов модуля контроля доступа и сравнение его с эталонным.

Исполнение первого этапа (рис. 1) начинается с написания автоматизированных тестов (test_name.java), которые исполняются с помощью RFT на рабочем месте тестировщика и воспроизводят действия администратора виртуальной инфраструктуры в vClient. Команда управления, реализуемая в каждом отдельном тесте, перехватывается на прокси-сервере, который пишет в log-файл (message.log) все принятые HTTP-пакеты, содержащие данные об этом действии. Формат log-файла соответствует входным данным модуля контроля доступа. Файл message.log автоматически передается на рабочее место тестировщика, где переименовывается в test_name.log. В процессе исполнения теста в RFT также создается файл с ожидаемыми результатами выполнения тестового испытания test_name.etalon.

На втором этапе тестирования (рис. 2) test_name.log обрабатывается модулем контроля доступа, работающим на отдельной машине для тестовых испытаний. В результате работы модуля создается file.log, который с помощью скрипта проверки сравнивается с ожидаемым test_name.etalon.


***Рис. 1. Этап 1: схема получения ожидаемого результата выполнения теста (test_name.etalon) и log-файла (test_name.log)***

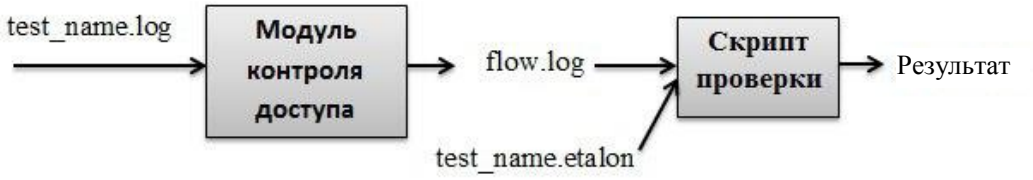


***Рис. 2. Этап 2: схема получения результата выполнения теста и его сравнение с ожидаемым результатом***

В результате такого разделения тестирования первый этап зависит только от виртуальной инфраструктуры, а второй — только от модуля контроля доступа.

Благодаря этому исполнение автоматизированных тестов на виртуальной инфраструктуре — наиболее объемная операция с точки зрения времени и ресурсов — становится редким действием, которое требуется проводить лишь при изменениях в платформе виртуализации. Это избавляет нас от постоянной необходимости содержать тестовую виртуальную инфраструктуру.

Непосредственное проведение тестов модуля контроля доступа на втором этапе требует незначительных вычислительных ресурсов и происходит значительно быстрее, чем при тестировании с использованием тестовой инфраструктуры, так как не зависит от времени получения данных об объектах: все необходимые сведения уже содержатся в test_name.log.

Таким образом, данный подход к функциональному тестированию решает проблемы, связанные с человеческим фактором, длительным временем проведения тестовых испытаний и большими вычислительными ресурсами, необходимыми для выполнения тестов. Автоматизация тестовых испытаний позволяет снять с человека ответственность за корректную интерпретацию результатов и выполнение всех тестов, а также сократить время тестирования, а разделение процесса тестирования на два независимых этапа позволяет сократить требуемые вычислительные ресурсы.

**Литература**

1. *Куликов С. С.* Тестирование программного обеспечения. Базовый курс: практ. пособие. — Минск: Четыре четверти, 2015. С. 63—110.

2. *Постоев Д. А.* Управление доступом в виртуальных системах на основе контроля информационных потоков // Безопасность информационных технологий. — М., 2014. № 4. С. 86—91.

3. *Каннер (Борисова) Т. М., Кузнецов А. В., Обломова А. И.* Тестирование средств защиты информации. Информационная безопасность. Материалы XIII Международной конференции. Таганрог, 2013. Ч. 1. С. 121—129.

## Features of testing data security tools from unauthorized access at the virtual infrastructure

*N. V. Mozolina*
Moscow institute of physics and technology (state university),
Dolgoprudny, Moscow region, Russia

*K. A. Lugovtsova*
Closed Joint Stock Company "OKB SAPR", Moscow, Russia

*The article discusses the features and problems of functional testing data security tools from unauthorized access at the virtual infrastructure, and offers the way to solve them with the help of automated functional testing tool and separation of the testing process in two independent stages.*

*Keywords:* functional testing, automation of testing processes, virtual infrastructure.

Bibliography — 3 references. *Received June 26, 2016*