A. A. Krasnopevtsev, A. V. Mamaev, Y. M. Tumanov

Functional and Load Testing Automatization Process Typical Solutions Development

Key words: testing automatization, load testing, functional testing, instrument of trusted session ensuring "MARSh 3.0", information security

The article describes functional and load testing automatization process for instrument of trusted session ensuring "MARSh 3.0", received during scientific work execution. Testing automatization is being realized for "MARSh 3.0" information security increase.

А. А. Краснопевцев, А. В. Мамаев, Ю. М. Туманов

РАЗРАБОТКА ТИПОВЫХ РЕШЕНИЙ ДЛЯ АВТОМАТИЗАЦИИ ФУНКЦИОНАЛЬНОГО И НАГРУЗОЧНОГО ТЕСТИРОВАНИЯ[1]

Работа рассматривает практическую часть процессов, связанных с автоматизацией функционального и нагрузочного регрессионного тестирования программно-аппаратных комплексов. Круг вопросов, возникающих при автоматизации процесса выполнения регрессионного тестирования, как функционального, так и нагрузочного, достаточно обширна [1]. При этом на момент написания данной работы не существует сторонней универсальной методики, которая позволила бы достаточно просто интегрировать процесс автоматизации тестирования в процесс разработки. Все происходит в рамках развития результатов, полученных на предыдущем этапе [2]. Более остро данная проблема стоит в случае с программно-аппаратными комплексами в связи с тем, что большая часть существующих подходов и методик автоматизации процесса тестирования в целом и выполнения регрессионного тестирования в частности направлена на контроль качества программного обеспечения [3].

Предмет проведения работ

Целью проведения работ по разработке типовых решений для автоматизации функционального и нагрузочного тестирования инновационных программно-аппаратных средств защиты информации программного обеспечения (ПО) средства обеспечения доверенного сеанса (СОДС) «МАРШ!-3.0» является определение типовых решений, которые должны использоваться для проверки ПО СОДС «МАРШ!-3.0» на соответствие функциональным и нефункциональным требованиям, с использованием инструментов функционального и нагрузочного тестирования. В состав ПО СОДС «МАРШ!-3.0» входят:

- Клиент доверенного сеанса связи (ДСС);
- Сервер ДСС;
- Сервис доверенного времени.

Для достижения указанной цели решаются следующие задачи:

- распределение функциональных и нефункциональных требований к ПО СОДС «МАРШ!-3.0» по структурным элементам ПО;
- определение основных технологических решений в разработке ПО СОДС «МАРШ!-3.0»;
- определение типовых решений для тестирования Клиента ДСС;
- определение типовых решений для тестирования Сервера ДСС;

[1] Данная работа выполнена в ходе НИР «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия» по теме "Разработка типовых решений для автоматизации функционального и нагрузочного тестирования». Шифр 2012-218-03-087.

- определение типовых решений для тестирования Сервиса доверенного времени;
- Разработка прикладных рекомендаций по управлению качеством ПО СОДС «МАРШ!-3.0».

Автоматизация процесса тестирования СОДС «МАРШ!-3.0»

В ходе работы были рассмотрены компоненты, входящие в ПО СОДС «МАРШ!-3.0», и для каждого из них было предложено решение по возможной автоматизации их тестирования. Необходимо отметить, что, в общем случае, полностью автоматизировать процессы функционального и нагрузочного тестирования не представляется возможным. Однако в ходе выполнения работы были получены следующие решения и предложения по автоматизации или возможной автоматизации тестирования компонентов, входящих в ПО СОДС «МАРШ!-3.0»:

— типовые решения для тестирования Клиента ДСС — в данной части проделанной работы были получены следующие результаты:

- типовое решение для тестирования операционной системы (ОС) — процесс тестирования подлежит автоматизации, возможно как тестирование отдельных элементов системы, так и проверка контрольных значений;
- типовое решение для тестирования функционального ПО (ФПО) — процесс тестирования подлежит автоматизации, возможно выделить три подхода к тестированию ФПО: проверка соответствия отдельных пакетов и/или контрольных сумм пакетов; проверка соответствия функций, реализованных в ФПО, заявленным требованиям; проверка работоспособности ФПО в целом;
- типовое решение для тестирования встроенных средств обеспечения VPN-соединения (VPN — Virtual Private Network) — процесс тестирования, в общем случае, с трудом подлежит автоматизации, однако было предложено проводить тестирование путем формальной проверки наличия решения среди установленных пакетов;
- типовое решение для тестирования ПО изоляции программных модулей ОС и разграничения доступа к ресурсам — процесс тестирования, в общем случае, с трудом подлежит автоматизации. В работе отдельно расписаны возможности по автоматизации требований, указаны причины невозможности автоматизации тестирования некоторых из них;
- типовое решение для тестирования серверного ПО (СПО) обеспечения аутентификации на основе криптографических алгоритмов — процесс тестирования подлежит автоматизации, требуется осуществить проверку отсутствия ошибок первого и второго рода в процессе аутентификации и возможность аутентификации в целом;
- типовое решение для тестирования ФПО обеспечения синхронизации доверенного времени — процесс тестирования подлежит автоматизации, необходимо осуществить тестирование собственно функции синхронизации доверенного времени;
- типовое решение для тестирования СПО обработки полученных доверенных обновлений ПО и изменений ключевой информации — процесс тестирования подлежит автоматизации, необходимо осуществить тестирование возможности самой системы в автоматизированном режиме как подгружать обновления и проверять корректность их установки, так и эмулировать действия пользователей, эмулируя их действия при установке обновлений;
- типовое решение для тестирования СПО встраивания криптопровайдера — возможно выполнить автоматизацию данного процесса тестирования. Автоматизация реализуется посредством формальной проверки процесса установки криптопровайдера в систему. При этом могут быть выполнены smoke-тесты функций для проверки корректности записи информации в файлы журналов и проверки работоспособности установленного в систему решения;

— типовые решения для тестирования Сервера ДСС — в данной части работы был рассмотрен анализ типовых решений, которые могут быть использованы для выполнения тестирования серверных частей ДСС, таких как:

- типовое решение для тестирования средства защиты информации от несанкционированного доступа (НСД), сертифицированного ФСТЭК России, — процесс тестирования подлежит автоматизации, необходимо осуществить автоматизированное тестирование путем формальной верификации, то есть сравнение hash-значений установленного и заявленного средства защиты информации от НСД, сертифицированного ФСТЭК России;
- типовое решение для тестирования ОС, сертифицированной ФСТЭК России, — процесс тестирования подлежит автоматизации, необходимо осуществить автоматизированное тестирование путем формальной верификации, то есть сравнение hash-значений установленной и заявленной операционной системы, сертифицированной ФСТЭК России;
- типовое решение для тестирования ФПО — аналогично клиентской части ДСС, процесс тестирования подлежит автоматизации, возможно выделить три подхода к тестированию ФПО: проверка соответствия отдельных пакетов и/или контрольных сумм пакетов; проверка соответствия функций, реализованных в ФПО, заявленным требованиям; проверка работоспособности ФПО в целом;
- типовое решение для тестирования средств криптографической защиты информации, сертифицированного ФСБ России — процесс тестирования, в общем случае, с трудом подлежит автоматизации. В работе отдельно расписаны возможности по автоматизации требований, указаны причины невозможности автоматизации тестирования некоторых из них;
- типовое решение для тестирования средства разграничения прав доступа пользователя к защищаемым информационным ресурсам — процесс тестирования подлежит автоматизации, необходимо осуществить автоматизированное тестирование путем формальной верификации средства разграничения прав доступа пользователя к защищаемым информационным ресурсам;
- типовое решение для тестирования службы синхронизации доверенного времени — процесс тестирования подлежит автоматизации, необходимо осуществить тестирование собственно функции синхронизации доверенного времени, как и в случае с клиентской частью ДСС;
- типовое решение для тестирования СПО, обеспечивающего централизованное распространение доверенных обновлений ПО, — процесс тестирования подлежит автоматизации, необходимо осуществить тестирование возможности самой системы в автоматизированном режиме как подгружать обновления и проверять корректность их установки, так и эмулировать действия пользователей, эмулируя их действия при установке обновлений, как и в случае клиентской части ДСС;
- типовое решение для тестирования СПО, обеспечивающего централизованное распространение изменений ключевой информации, — последовательная автоматизация тестирования функций аутентификации, авторизации, распределения, выработки ключей и иных, связанных с этим функций;

— типовые решения для тестирования сервиса доверенного времени:

- типовое решение для тестирования сервера доверенного времени — процесс тестирования подлежит автоматизации, необходимо осуществить генерацию задач, которые позволят описанным ранее образом выполнить тестирование заданной аппаратной части на соответствие требуемым характеристикам;
- типовое решение для тестирования web-сервиса доверенного времени — процесс тестирования подлежит автоматизации. Рассмотрено несколько принципиальных схем проведения такого тестирования. В целом, стоит отметить, что процесс тестирования выливается в композитный процесс, который реализуется за счет изменения настроек времени на клиентской системе и проверки корректности обновления данных от сервера. Отдельно можно рассматривать тот же самый тестовый сценарий, но при наличии арбитра, который будет являться точкой синхронизации и валидации того, что время на доверенном сервере было получено корректно.

Соответственно, из лаконичного описания предложенных типовых решений можно сделать вывод о том, что абсолютная автоматизация для такого неординарного решения, как СОДС

«МАРШ», в общем случае, не возможна, однако результатом проделанной НИР является описание типовых решений, которые позволят автоматизировать тестирование его компонентов, что значительно повысит надежность разрабатываемого программно-аппаратного комплекса.

Выводы

В результате проведенного анализа в НИР представлены типовые решения для обеспечения тестирования всех функций, изложенных в техническом задании к проекту. Часть функций может быть протестирована в полностью автоматическом режиме, часть функций подлежит процессу автоматизации (часть тестирования проводится с помощью организационных мер), часть функций не может быть протестирована в принципе.

СПИСОК ЛИТЕРАТУРЫ:

1. *Марков А. С., Ширлов В. Л., Барабанов А. В.* Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. – 192 с.
2. Разработка методов организации и проведения автоматического регрессионного функционального и нагрузочного тестирования инновационных программно-аппаратных средств защиты информации: отчет о НИР: Тема № 2012-218-03-087 / рук. работы Дураковский А. П.; исполн.: С. В. Запечников [и др.]. М.: МИФИ, 2013. – 213 с.
3. Анализ существующих решений в области автоматизации функционального тестирования программного, аппаратного и программно-аппаратного обеспечения. Разработка концепции проведения тестирования программно-аппаратных средств защиты информации: отчет о НИР: Тема № 2012-218-03-087 / рук. работы Дураковский А. П.; исполн.: С. В. Запечников [и др.]. М.: МИФИ. 2013. – 213 с.

REFERENCES:

1. *Markov A. S., Tsirlov V. L., Barabanov A. V.* Metody otsenki nesootvetstvija sredstv zashchity informatsii. M.: Radio i svjaz', 2012. – 192 p.
2. Razrabotka metodov organizatsii i provedenija avtomaticheskogo regressionnogo funktsional'nogo i nagruzochnogo testirovanija innovatsionnyh programmno-apparatnyh sredstv zashchity informatsii: otchet o NIR: Tema #2012-218-03-087 / ruk. raboty Durakovskij A. P.; ispoln.: S. V. Zapechnikov [i dr.]. M.: MEPhI, 2013. – 213 p.
3. Analiz sushchestvujushchih reshenij v oblasti avtomatizatsii funkcional'nogo testirovanija programmnogo, apparatnogo i programmno-apparatnogo obespechenija. Razrabotka kontseptsii provedenija testirovanija programmno-apparatnyh sredstv zashchity informatsii: otchet o NIR: Tema #2012-218-03-087 / ruk. raboty Durakovskij A. P.; ispoln.: S. V. Zapechnikov [i dr.]. M.: MEPhI, 2013. – 213 p.