ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

кандидата технических наук, доцента Магомедова Шамиля Гасангусейновича на диссертационную работу Каннер Татьяны Михайловны на тему «Моделирование состояний аппаратной компоненты для тестирования средств защиты информации», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Актуальность темы исследования

Достаточно много исследований, приведенных в настоящее время в научной литературе, посвящено проблемам тестирования. Как правило, в таких работах описываются рекомендуемые способы и средства тестирования именно программного обеспечения (ПО), и не рассматривается ограниченность их применения для функций безопасности программно-аппаратных средств защиты информации (СЗИ). В некоторых исследованиях описываются отличия в тестировании программного обеспечения и программно-аппаратных комплексов, и указываются сложности проведения некоторых проверок, но методические рекомендации по тестированию программно-аппаратных СЗИ не приводятся. Однако стоит учитывать, что для таких средств защиты информации существуют особенности, связанные с наличием аппаратной компоненты, которая может принимать различные состояния. Из-за таких особенностей применение существующих способов и средств тестирования для функций безопасности программно-аппаратных СЗИ зачастую становится принципиально невозможным. Таким образом, исследование Каннер Т.М., направленное на решение задачи тестирования программно-аппаратных СЗИ путем моделирования состояний аппаратной компоненты, является актуальным.

Научная новизна полученных результатов

В диссертационной работе получены следующие новые научно-обоснованные результаты:

1. Предложена модель программно-аппаратных СЗИ, в которой учитывается состояние аппаратной компоненты, что обеспечивает на основе обоснованных критериев применимости процедур тестирования проведение проверки заявленных производителем функций безопасности программно-аппаратного СЗИ, а также выявление функций безопасности, препятствующих проведению тестирования.

2. Предложен алгоритм тестирования функций безопасности СЗИ, обеспечивающий решение новой задачи – тестирование программно-аппаратных СЗИ.

3. Предложен алгоритм верификации функций безопасности программно-аппаратных СЗИ, отличающийся от подобных алгоритмов использованием процедур оценки критичности выявленных в ходе тестирования ошибок и их влияния на защищенность информационной системы.

Обоснованность и достоверность научных положений, сформулированных в диссертации

Обоснованность и достоверность научных результатов исследования достигнута благодаря корректной постановке цели и задач исследования, адекватному задачам исследования выбору математического аппарата и результатами экспериментальной апробации предложенного способа и основанного на нем средства тестирования функций безопасности программно-аппаратных СЗИ.

Результаты исследования опубликованы в 21 научной работе, 15 из которых – в рецензируемых журналах, рекомендованных ВАК РФ и Аттестационным советом УрФУ. Имеется 1 свидетельство о государственной регистрации программы для ЭВМ.

Практическая значимость результатов диссертации

Практическая значимость заключается в:

1. разработке рекомендаций по практической реализации средств тестирования функций безопасности программно-аппаратных СЗИ;

2. реализации на основе предложенных рекомендаций программно-аппаратного комплекса для тестирования функций безопасности СЗИ, заявляемых их производителем;

3. формулировке рекомендаций, обеспечивающих совместное использование средств тестирования функций безопасности программно-аппаратных СЗИ со сторонними вспомогательными для тестирования средствами и специализированными средствами тестирования СЗИ, что обеспечивает сокращение сроков внедрения средств защиты информации.

Оценка содержания диссертации и ее оформления

Диссертационная работа содержит 155 страниц основного текста (всего 176 с.), 40 рисунков и 3 таблицы. Состоит из введения, 4 глав, заключения, списка сокращений и условных обозначений, списка литературы, списка иллюстративного материала и 4 приложений.

Введение представляет собой обоснование актуальности, формулировку целей и задачи, научной новизны, теоретической значимости, практической ценности работы, и положений, выносимых на защиту.

В первой главе приведен анализ требований действующей нормативно-правовой базы в области защиты информации, а также – анализ подходов, способов и средств тестирования ПО. Проведено исследование возможности применения существующих способов и средств тестирования к различным видам функций безопасности программно-аппаратных СЗИ, определены особенности их тестирования. Приведено обоснование ограниченности существующих способов и средств тестирования программного обеспечения в задаче полной проверки функций безопасности программно-аппаратных СЗИ и необходимости их модификации.

Вторая глава посвящена разработке научно-обоснованного способа тестирования функций безопасности программно-аппаратных СЗИ. Приведены

описательная и формальная модели программно-аппаратных СЗИ, подробно рассмотрены общие и частные критерии возможности ручного, автоматизированного и автоматического тестирования. Описаны предложенные алгоритмы тестирования и верификации функций безопасности программно-аппаратных СЗИ, и на их основе сформулирован научно-обоснованный способ тестирования функций безопасности таких средств защиты.

В третьей главе диссертации сформулированы рекомендации по практической реализации средств тестирования функций безопасности программно-аппаратных средств защиты информации и описана их реализация.

В четвертой главе проведен анализ опыта применения разработанного способа и основанного на нем программно-аппаратного комплекса для тестирования СЗИ. Уделяется внимание внедрению результатов работы и их апробации.

В заключении приведен перечень основных выводов, полученных в результате выполнения диссертационной работы, а также указываются направления для дальнейших работ.

Диссертация имеет четкую структуру, грамотно оформлена, соответствует паспорту специальности 2.3.6. Методы и системы защиты информации, информационная безопасность. Автореферат достаточно полно и адекватно отражает содержание и суть работы.

Замечания и вопросы по работе

Вместе с этим следует отметить некоторые замечания по содержанию диссертации:

1. В тексте работы имеются погрешности в оформлении, например, рисунок 4.10 на странице 129 плохо читается, присутствует некоторое количество стилистических и орфографических ошибок.

2. В Главе 2 приводится несколько утверждений – общие и частные критерии возможности ручного, автоматизированного и автоматического тестирования функций безопасности программно-аппаратных СЗИ, при этом не

рассматриваются их доказательства со ссылкой на работы автора. Для ознакомления с доказательствами потребовалось изучение нескольких публикаций автора.

3. В Главе 3 приводится описание составляющих разработанного программно-аппаратного комплекса тестирования функций безопасности средств защиты информации, однако отсутствует его визуальное представление. Это не дает полного понимания состава предложенного решения, а также того, что сделано лично автором. Было бы более наглядно, если бы в конце главы была приведена схема разработанного комплекса тестирования и были четко выделены составляющие, которые разработаны лично автором, а которые – в соавторстве.

4. В приложении В приведены листинги исходных кодов разработанных программ тестирования, однако их объем представляется недостаточным для полного понимания реализации разработанного программно-аппаратного комплекса тестирования СЗИ. Расширение приведенных фрагментов листингов дало бы лучшее понимание содержания исходного кода.

Перечисленные недостатки не влияют на достоверность и не снижают как ценность предоставленных в работе результатов, так и положительную оценку диссертации в целом.

Заключение по работе

Диссертация Каннер Т.М. представляет собой законченную научно-квалификационную работу, выполненную на высоком научном уровне и удовлетворяющую всем необходимым критериям. Сформулированные по результатам исследования научные положения, выводы и рекомендации обоснованы теоретически, основаны на известных положениях теории моделирования, автоматов и графов, подтверждены проведенными экспериментами. Результаты достаточно полно изложены в тексте диссертации, опубликованы в ведущих научных изданиях по теме диссертации, а также апробированы на профильных научных конференция. Диссертационная работа

полностью соответствует п. 9 Положения о присуждении ученых степеней в УрФУ. Автор диссертации Каннер Татьяна Михайловна заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:

Кандидат технических наук, доцент,
заведующий кафедрой КБ-4 «Интеллектуальные системы информационной безопасности»

Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет» (РТУ МИРЭА)

Тел.: +7 (499) 681-33-56, доб. 6803
e-mail: magomedov_sh@mirea.ru
Адрес: 119454, г. Москва, Проспект Вернадского, д. 78

_____ Магомедов Шамиль Гасангусейнович

«04» 09 2023 г.

Подпись к.т.н., доцента Магомедова Ш.Г. заверяю:

Начальник
Управления кадров _____ М.М. Буханова

_____2023 г.