ОТЗЫВ

официального оппонента доктора технических наук, доцента
Духана Евгения Изовича
на диссертацию и автореферат диссертации Каннер Татьяны Михайловны
на тему «Моделирование состояний аппаратной компоненты для тестирования средств защиты информации», представленные на соискание ученой степени кандидата технических наук по специальности 2.3.6 — Методы и системы защиты информации, информационная безопасность

Актуальность темы исследования

Применение специализированных средств защиты информации (далее — СЗИ) является одним и важнейших методов обеспечения безопасности информации, обрабатываемой с помощью автоматизированных информационных систем (далее — АИС). Благодаря своей многофункциональности аппаратно-программные СЗИ (далее — АПСЗИ) наиболее распространены, активно совершенствуются и широко представлены на рынке систем безопасности, чем обусловливаются высокие требования к качеству выполнения средствами заявленных их производителем функций. Гарантирующее правильность выполнения функций тестирование СЗИ должно осуществляться масштабно в отношении возможных условий их работы: программной среды и аппаратного окружения. Полноценное тестирование СЗИ, охватывающее наиболее значимые и часто встречающиеся варианты их эксплуатации, не возможно без применения автоматизированных методов и средств.

Существующие в настоящее время способы и средства тестирования СЗИ весьма ограничены, не позволяют проводить тестирование изделий в автоматизированном режиме. Кроме того большинство способов охватывают только программную составляющую функционирования АПСЗИ, вообще не ориентированы на тестирование их аппаратной составляющей и не учитывают особенностей процесса их тестирования, возникающих, например, из-за нетривиального взаимодействия аппаратной компоненты СЗИ с программным обеспечением (далее — ПО) и аппаратного окружения защищаемой АИС.

Высокая потребность в разработке научно-обоснованных и пригодных для автоматизированного режима работы способов и реализующих эти способы средств тестирования АПСЗИ обусловливает актуальность диссертационного исследования Каннер Татьяны Михайловны.

Содержание диссертации и автореферата

Диссертация состоит из введения, четырех глав, заключения, списка литературы, содержащего 114 наименований, списков сокращений и наименова-

ний, иллюстративного материала, четырех приложений. Рукопись имеет общий объем 154 страницы и включает 40 рисунков, 3 таблицы. Порядок изложения материала в рукописи соответствует логике достижения поставленной научной цели.

Во введении обоснована актуальность тематики исследований, сформулированы цели, научная и частные задачи исследования, показаны научная новизна и практическая значимость полученных результатов, представлены основные положения, выносимые на защиту.

В первом разделе работы представлен анализ состояния предметной области, в том числе: требований нормативно-правовых актов в области защиты информации; подходов, способов и средств, используемых для тестирования ПО; аппаратно-программных средств защиты информации как объектов тестирования. В разделе показана ограниченность существующих подходов в задаче полной проверки функций безопасности АПСЗИ. Сформулирована цель исследования, заключающаяся в разработке научно-обоснованного способа тестирования функций безопасности АПСЗИ, обоснованы частные задачи исследования.

Второй раздел диссертации посвящен разработке модели аппаратно-программных СЗИ и основанного на этой модели способа тестирования функций безопасности АПСЗИ. В разделе рассмотрены условия и критерии применимости существующих способов тестирования программного обеспечения для тестирования функций безопасности аппаратно-программных средств защиты информации. Разработаны составляющие способ тестирования АПСЗИ алгоритм тестирования и алгоритм верификации их функций безопасности.

В третьем разделе рукописи «Разработка программно-аппаратного комплекса для тестирования функций безопасности СЗИ, реализующего предложенный способ тестирования программно-аппаратных СЗИ» приводится обоснование требований к средствам тестирования функций безопасности АПЗСИ; формулируются рекомендации по тестированию функций безопасности АПСЗИ на различных аппаратных платформах, применению средств виртуализации при тестировании их функций безопасности, практической реализации средств тестирования функций безопасности СЗИ; дается обоснование состава вспомогательных средств, используемых в программно-аппаратном комплексе для тестирования функций безопасности исследуемых изделий.

Четвертый раздел диссертации посвящен экспериментальному исследованию способа тестирования АПСЗИ и реализующего этот способ аппаратно-программного комплекса; приводится методика и анализируются результаты проведения экспериментальной их апробации. Отдельный подраздел посвящен анализу совместного использования разработанного аппаратно-программного

комплекса для тестирования СЗИ и сторонних вспомогательных для тестирования средств.

В заключении изложены итоги выполненного исследования, сформулированы основные выводы по диссертационной работе, обозначены направления дальнейших исследований.

В приложениях приводятся обоснованный перечень проверок для тестирования функций безопасности и нецелевых функций мобильных СЗИ, сведения о представлении аппаратной компоненты СЗИ в виртуальных машинах, фрагменты листингов разработанных программ тестирования, документы, подтверждающие внедрение результатов диссертации в практику.

Автореферат диссертации является самостоятельным авторским научным трудом Каннер Т.М., его содержание соответствует основным положениям выполненного диссертационного исследования.

Новизна научных результатов, выводов и рекомендаций, сформулированных в диссертации, заключается в следующем:

– разработана основанная на положениях теории автоматов модель АПСЗИ, которая учитывает состояния аппаратной компоненты, выработаны формальные критерии применимости процедур тестирования, что в совокупности позволяет обосновать возможность выполнения проверок для возможных видов функций безопасности, а также выявить функции безопасности и переходы СЗИ, препятствующие проведению тестирования.

– предложен базирующийся на авторской модели СЗИ алгоритм тестирования аппаратно-программных СЗИ, который позволяет обеспечивать полноту и оптимальность тестирования.

– предложен алгоритм верификации АПСЗИ, впервые предлагает процедуры оценки критичности выявленных в ходе тестирования ошибок и их влияния на защищенность информационной системы

Следует отметить, что в диссертации с использованием известных положений теорий графов, автоматов, оптимизации и принятия решений предложено решение новых задач по разработке алгоритмов тестирования и верификации аппаратно-программных СЗИ.

Теоретическая значимость диссертационной работы заключается в развитии научно-методического аппарата совершенствования процесса тестирования СЗИ путем моделирования состояний аппаратной компоненты, формулирования критериев применимости способов тестирования, разработки алгоритма тестирования и верификации различных видов функций безопасности аппаратно-программных средств защиты информации.

Практическая значимость заключается в разработке рекомендаций по практической реализации средств тестирования функций безопасности про-

граммно-аппаратных СЗИ при их совместном использовании со сторонними специализированными и вспомогательными средствами тестирования СЗИ, а также в разработке предложений по построению программно-аппаратного комплекса, позволяющего выполнять автоматическое тестирование различных видов функций безопасности и верификацию аппаратно-программных СЗИ, что способствует их своевременному появлению на рынке средств безопасности.

Выводы и рекомендации, сформулированные в диссертации, объективны, обоснованы полнотой анализа состояния вопроса в рассматриваемой предметной области, отражают существо полученных новых научных результатов. Основные научные результаты работы в достаточной мере и своевременно опубликованы.

Достоверность результатов исследований обусловлена: корректным использованием положений системного анализа и теории формальных систем, автоматов, графов, оптимизации и принятия решений, а также успешным применением в практических проектах предложенных модели, способа, алгоритмов, разработанных средств тестирования и верификации АПСЗИ.

Полученные соискателем научные результаты прошли апробацию на ряде научно-практических и научно-технических конференций. Основные положения, выносимые на защиту, своевременно и в достаточной степени опубликованы, в т.ч. в рецензируемых изданиях.

Диссертация Каннер Т.М. представлена в виде авторской рукописи. Личный вклад соискателя в достижение полученных результатов представлен достаточно полно.

Недостатки по содержанию и оформлению диссертации

1. В диссертации анализ нормативной базы выполнен (представлен) весьма поверхностно. Не описана модель угроз АИС, связанная с возможно некачественным функционированием СЗИ.
2. Не достаточно корректно сформулированы выносимые на защиту положения. Так, первое положение «Доказана ограниченность использования способов тестирования…» не выглядит как научное утверждение, подлежащее защите.

Представленный во втором разделе и выносимый на защиту « … способ тестирования функций безопасности … » описан на 2 страницах и по существу представляет собой простую последовательность алгоритмов тестирования и верификации АПСЗИ, которые, в свою очередь, в рукописи достаточно строго научно обоснованы. Необходимость «разработки» такого способа в диссертации описана слабо, его новизна вызывает сомнение.

Представленный в третьем разделе и выносимый на защиту « … программно-аппаратный комплекс для тестирования СЗИ … » имеет скорее прак-

тическую значимость, тогда как реализуемые им алгоритмы, как уже отмечалось, — научную ценность. Кроме того, в разделе не обоснованы в явном виде требования к комплексу, его структура, выбор аппаратной и программной платформ. На стр. 99 рукописи указано: «Разработанный программно-аппаратный комплекс (коммутатор USB-канала) можно использовать … ». Из чего следует, что заявляемый *комплекс* сводится к простому коммутатору. Названия ни одного из подразделов третьего раздела не соответствуют ожидаемому описанию процесса разработки программно-аппаратного комплекса; преамбула к разделу не соответствует его названию.

На взгляд оппонента в качестве защищаемых научных положений целесообразно было заявить впервые предложенную модель СЗИ, а также обладающие научной новизной алгоритмы тестирования и верификации, составляющие известную последовательность (способ) тестирования СЗИ.

3. В рукописи не дано строгого определения «потенциально вычислимые функции безопасности» АПСЗИ, при этом указанному понятию уделяется достаточно серьезное внимание.

4. В текстах диссертации и автореферата имеются неточности, стилистические и орфографические ошибки, снижающие качество рукописей.

Так, рисунок 1.3 более информативен и дублирует рисунок 1.1, при этом рисунок 1.2. вообще не информативен.

Рукопись изобилует повторами (недословными) информации, например, в первой главе несколько раз звучит утверждение о том, что аппаратно-программные СЗИ имеют особенности, которые необходимо учитывать в процессе их тестирования.

Не совсем понятно, чем отличаются ошибки, «приводящие к неработоспособности одной или нескольких функций безопасности СЗИ» и «ошибки, приводящие к неработоспособности или нарушению защищенности системы, в которой используется СЗИ» (стр. 72); почему внешнее воздействие — переподключение аппаратной компоненты — отнесено к множеству функций, которые могут выполняться СЗИ (стр. 52).

В ходе защиты соискателю предлагается ответить вопрос: если производителями средств вычислительной техники (АИС) не гарантируется соблюдение стандартов и полная совместимость интерфейсов подключения аппаратной компоненты СЗИ, то можно ли такую АИС использовать для обработки конфиденциальных данных даже при оснащении его протестированным средством защиты.

Выводы

Указанные выше замечания не снижают ценность основных научных результатов диссертационного исследования Каннер Т.М. и общего положительного впечатления о работе. Высокий уровень квалификации соискателя подтверждают разработанные автором, обладающие новизной и представленные в диссертации научно обоснованные модель СЗИ, алгоритмы их тестирования и верификации. Следует также отметить широкое внедрение результатов исследования, в том числе в ФАУ «ГНИИИ ПТЗИ ФСТЭК России и ЗАО «ОКБ САПР» — предприятии-производителе распространенных отечественных аппаратно-программных средств защиты информации.

Диссертационная работа Каннер Татьяны Михайловны содержит решение актуальной научной задачи, является самостоятельной завершенной научной квалификационной работой, выполненной на актуальную тему. Изложена достаточно грамотным научно-техническим языком, в полной мере отвечает требованиям по актуальности, научной новизне, практической значимости, а также полностью соответствует п. 9 Положения о присуждении ученых степеней в УрФУ. Автор работы, Каннер Татьяна Михайловна, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 — Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
доктор технических наук, доцент,
военнослужащий в/ч 69617
Тел.: +7-922-218-22-62
e-mail: ev.duhan@yandex.ru
Адрес: г. Екатеринбург, ул. Омская

Духан Евгений Изович

20.07.23

Подпись Духана Евгения Изовича заверяю:

Жаворонкова Татьяна Вячеславовна