Экз. № 1

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, профессора Язова Юрия Константиновича на диссертационную работу Каннер Татьяны Михайловны на тему «Моделирование состояний аппаратной компоненты для тестирования средств защиты информации», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность темы исследования

Тестирование программного обеспечения и программно-аппаратных средств защиты информации (СЗИ) является неотъемлемой частью процесса создания информационных систем (ИС) в защищенном исполнении. При этом сегодня оно направлено на проверку корректного использования функций безопасности и отсутствия негативного влияния СЗИ на функциональные и пользовательские характеристики ИС. Для тестирования программных СЗИ могут использоваться широко известные способы и средства тестирования ПО, однако их использование для программно-аппаратных СЗИ часто становится принципиально невозможным, так как реализованные в СЗИ функции безопасности нельзя проверить либо в некоторой их части, либо полностью. Это обусловлено тем, что аппаратная компонента СЗИ может как взаимодействовать с программной компонентой СЗИ в операционной системе средства вычислительной техники (СВТ), в результате чего возможно подключение или отключение СЗИ от СВТ в процессе работы, так и обладать собственной средой функционирования для автономной работы относительно СВТ и его программной среды. Кроме того, для своевременной фиксации нарушений функций безопасности и причин их возникновения, а также проведения тестирования в требуемые сроки необходимо автоматизировать данный процесс, однако средства автоматизации далеко не всегда применимы к программно-аппаратным СЗИ в неизменном виде. Все это обусловливает необходимость разработки новых средств тестирования и, прежде всего, на основе моделирования процессов функционирования СЗИ в операционных средах различных СВТ.

Известные сегодня результаты научных исследований по вопросам тестирования ориентированы преимущественно на программные СЗИ, а применительно к программно-аппаратным СЗИ – практически отсутствуют.

С учетом изложенного тема диссертации, посвященной моделированию состояний аппаратной компоненты средства защиты информации для его тестирования, является несомненно актуальной.

Научная новизна полученных результатов

В ходе диссертационных исследований автор поставил и решил **научную задачу**, имеющую существенное значение для разработки эффективных СЗИ в ИС, суть которой состояла в формировании научно-обоснованной модели и основанного на ней способа тестирования программно-аппаратных СЗИ, а также в разработке на этой основе рекомендаций по практической реализации средств тестирования программно-аппаратных СЗИ, устанавливаемых в ИС.

В интересах решения этой научной задачи автор в диссертации решал следующие частные задачи исследований:

1. Анализ известных подходов, используемых для тестирования программного обеспечения и обоснование их ограниченности в задаче полной проверки функций безопасности программно-аппаратных СЗИ.

2. Разработка научно-обоснованного способа тестирования функций безопасности программно-аппаратных СЗИ, основанного на использовании модели программно-аппаратных СЗИ и соответствующих алгоритмов тестирования и верификации их функций безопасности.

3. Разработка программно-аппаратного комплекса, реализующего предложенный способ тестирования функций безопасности программно-аппаратных СЗИ.

4. Апробация и анализ результатов применения разработанного способа тестирования и программно-аппаратного комплекса для тестирования функций безопасности программно-аппаратных СЗИ.

В результате в работе были получены **научные результаты, научная новизна** которых, на мой взгляд, состоит в следующем:

1. Модель программно-аппаратных СЗИ, основанная на положениях теории автоматов, отличающаяся тем, что в ней, во-первых, введены разработанные автором формальные критерии применимости процедур тестирования СЗИ, во-вторых, поставлена и решена формальная задача тестирования функций безопасности программно-аппаратного СЗИ, заключающаяся в выявлении последовательности переходов автомата по возможным состояниям с обеспечением полноты тестирования при разных наборах входных условий и оптимальности тестирования, при которой длина последовательности переходов оказывается минимальной, что позволяет обосновать возможность выполнения проверок для всевозможных видов

функций безопасности, а также выявить функции безопасности и переходы моделирующего автомата, препятствующие проведению тестирования.

2. Предложен алгоритм тестирования, в котором используется сформированная модель СЗИ и положения теории графов для решения новой задачи – тестирования программно-аппаратных СЗИ и отличается последовательным применением совокупности алгоритмов:

- Косараджу-Шарира – для поиска компонент связности и проверки связности графа, отражающего последовательность действий при тестировании;
- Флойда-Уоршелла – для вычисления длины кратчайших путей для вершин биграфа;
- Венгерского алгоритма – для выбора кратчайших путей на графе со сбалансированными вершинами и минимальной суммарной длиной;
- алгоритма Хиерхольцера – для построения Эйлерова цикла/пути в полученном мультиграфе,

что позволяет формальным путем определять порядок проведения тестирования СЗИ.

3. Предложен алгоритм верификации функций безопасности тестируемого СЗИ заявленным требованиям, в котором используются известные положения теории оптимизации и принятия решений для решения новой задачи – верификации программно-аппаратных СЗИ, и, в отличие от известных, предлагаются процедуры 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 обеспечена корректным использованием теорий формальных систем, автоматов, графов, оптимизации и принятия решений, строгого применения аппарата системного анализа, а также положительными итогами применения предложенной модели, способа, алгоритмов и разработанных средств тестирования для функций безопасности программно-аппаратных СЗИ в реализованных на практике проектах СЗИ, и совпадением ожидаемых результатов от их использования с полученными при экспериментальных исследованиях.

Теоретическая значимость результатов диссертации

Теоретическая значимость результатов диссертации заключается в доказательстве ограниченности использования способов тестирования программного обеспечения в задаче полной проверки функций безопасности программно-аппаратных СЗИ, обосновании условий и критериев их применимости, а также в разработке алгоритмов тестирования и верификации функций безопасности программно-аппаратных СЗИ.

Практическая значимость результатов диссертации

Практическая значимость заключается в том, что на базе полученных новых научных результатов:

1. Сформулированы рекомендации по реализации средств тестирования функций безопасности программно-аппаратных СЗИ, которые позволили реализовать программный комплекс «Тестирование функций безопасности программно-аппаратных СЗИ» и коммутатор USB-канала, используемый в программах тестирования для автоматического отключения/подключения средств защиты с USB-интерфейсом в СВТ и позволяющий автоматически выполнять необходимые переходы процесса тестирования из состояния в состояние при проверке функций безопасности СЗИ.
2. Сформулированы рекомендации, обеспечивающие совместное использование средств тестирования функций безопасности программно-аппаратных СЗИ со сторонними вспомогательными для тестирования средствами и специализированными средствами тестирования СЗИ.

Оценка содержания диссертации и ее оформления

Диссертационная работа содержит 155 страниц основного текста (всего 176 страниц), 40 рисунков (без приложений) и 3 таблицы (без приложений). Состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений, списка литературы из 114 наименований, 4 приложений.

В первой главе проводится анализ требований действующей нормативно-правовой базы в области защиты информации, рассматриваются программно-аппаратные СЗИ как объекты тестирования, выполняется анализ существующих способов и средств тестирования ПО. Приводится обоснование ограниченности этих способов и средств в задаче полной проверки функций безопасности программно-аппаратных СЗИ и необходимости их модификации.

Во второй главе описывается предложенная научно-обоснованная модель программно-аппаратных СЗИ и основанный на ней способ тестирования функций безопасности таких средств защиты.

В третьей главе диссертации приводится описание разработанного программно-аппаратного комплекса для тестирования функций безопасности СЗИ, реализующего предложенный способ тестирования.

В четвертой главе проводится анализ опыта применения разработанного способа и основанного на нем программно-аппаратного комплекса для тестирования СЗИ, описывается внедрение результатов работы. Дополнительно описывается анализ опыта и демонстрируется возможность совместного использования разработанного программно-аппаратного комплекса для тестирования СЗИ со сторонними вспомогательными для тестирования средствами и специализированными средствами тестирования СЗИ.

Результаты работы достаточно апробированы, обсуждались и получили одобрение на 9 международных научно-практических конференциях и опубликованы в 21 печатной работе, из которых 15 – в изданиях, рекомендованных ВАК при Минобрнауки России и Аттестационным советом УрФУ.

Автореферат полностью соответствует диссертации.

Замечания и вопросы по работе

Вместе с тем диссертация содержит ряд недостатков, к основным из которых, на мой взгляд, относятся следующие:

1. В работе не показано, каким образом повлияет класс защиты СЗИ на алгоритмы и время проведения тестирования, состав тестов, оптимальность и полноту тестирования функций безопасности СЗИ (например, в системах обнаружения вторжений, системах антивирусной защиты и т.д. устанавливаются 6 классов защиты и, по-видимому, это должно влиять на состав тестируемых функций безопасности, алгоритмы их тестирования и условия остановки процесса тестирования).
2. В работе практически не описано содержание тестов функций безопасности, а оно существенно меняется от функции к функции. При этом становится несколько неопределенным применяемое в работе понятие «полнота тестирования».
3. Автор лишь очень коротко упомянул о функциональном тестировании СЗИ, но ведь для этого потребуется разрабатывать модели атак на СЗИ, чтобы проверить их защищенность и возможность их компрометации. Это значительно усложнит алгоритмы тестирования, что в работе не нашло отражения.
4. При формулировании новизны и в соответствующем разделе 2.4 работы отмечается, что в работе разрабатывается алгоритм верификации программно-аппаратных СЗИ с применением теории оптимизации и принятия

решений. Однако по тексту работы отсутствует постановка оптимизационной задачи и не видно, каким образом используется автором теория принятия решений.

Однако, отмеченные недостатки не изменяют общего положительного впечатления от работы, не влияют на вывод о ее значимости и важности полученных автором научных и практических результатов.

Заключение по работе

Диссертационная работа представляет собой законченную научно-квалификационную работу, выполненную на актуальную тему, имеющая существенное значение для создания эффективных средств защиты информации и информационных систем в защищенном исполнении. Она обладает научной новизной и полностью соответствует п.9 Положения о присуждении ученых степеней в УрФУ, а ее автор – 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, профессор,
главный научный сотрудник научно-исследовательского управления
Федеральное автономное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»)

Тел.: +7 (473) 257-92-86
E-mail: gniii@fstec.ru
Адрес: 394020, г. Воронеж, ул. 9 января, д. 280а

_____Язов Юрий Константинович

«_7_» _августа_____2023_ г.

Подпись д.т.н. Язова Ю.К. заверяю

Ученый секретарь
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»,
к.т.н., старший научный сотрудник

_____Паринов Игорь Васильевич

«_7_» _августа_____2023_ г.