Федеральное государственное автономное образовательное учреждение
высшего образования «Уральский федеральный университет имени первого
Президента России Б.Н. Ельцина»

На правах рукописи

Каннер Татьяна Михайловна

Моделирование состояний аппаратной компоненты для тестирования средств защиты информации

2.3.6. Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Екатеринбург – 2023

Работа выполнена на кафедре №42 «Криптология и кибербезопасность» ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ».

Научный руководитель:	кандидат технических наук, доцент, **ЕПИШКИНА Анна Васильевна**
Официальные оппоненты:	**ЯЗОВ Юрий Константинович**, доктор технических наук, профессор, ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю», г. Воронеж, главный научный сотрудник научно-исследовательского управления;
	ДУХАН Евгений Изович, доктор технических наук, доцент, Войсковая часть 69617, г. Екатеринбург, военнослужащий;
	МАГОМЕДОВ Шамиль Гасангусейнович, кандидат технических наук, доцент, ФГБОУ ВО «МИРЭА – Российский технологический университет», г. Москва, заведующий кафедрой КБ-4 «Интеллектуальные системы информационной безопасности»

Защита диссертации состоится «19» сентября 2023 г. в 11:00 часов на заседании диссертационного совета УрФУ 2.3.12.13 по адресу: 620002, г. Екатеринбург, ул. Мира, 19, ауд. И-420 (зал Ученого Совета).

С диссертацией можно ознакомиться в библиотеке и на сайте ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»: https://dissovet2.urfu.ru/mod/data/view.php?d=12&rid=4968

Автореферат разослан «____» _____ 2023 года.

Ученый секретарь
диссертационного совета  Сафиуллин Николай Тахирович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Информационные системы (ИС) стали неотъемлемой частью жизни современного общества. При этом все больше конфиденциальной информации и персональных данных переносится в такие системы. Для обеспечения защиты данных в процессе их хранения и обработки в ИС по требованиям нормативных документов Российской Федерации необходимо использовать средства защиты информации (СЗИ): программные или программно-аппаратные. Программно-аппаратные СЗИ являются более надежными и рекомендуется применять именно их.

Достаточно часто ИС проектируются и разрабатываются без учета всех необходимых СЗИ. При этом на этапе аттестации возникает необходимость внедрения таких средств, как правило, уже разработанных, а для некоторых систем – сертифицированных. При создании же ИС с учетом средств защиты затрачиваемое время на разработку новых или адаптацию существующих СЗИ может значительно превышать время разработки самой системы. В обоих случаях для корректного использования функций безопасности и проверки отсутствия негативного влияния реализующего их СЗИ на функциональные и пользовательские характеристики системы необходимо проводить тестирование при установке таких средств в ИС. Для этого используются существующие широко известные способы и средства тестирования программного обеспечения (ПО). При этом использование существующих способов и средств тестирования ПО для функций безопасности программных СЗИ возможно без изменений, с дополнительными методическими рекомендациями по составу тестов, анализу ошибок и так далее. Это связано с тем, что среда функционирования таких средств защиты – операционная система (ОС) средства вычислительной техники (СВТ), в которой обрабатывается и хранится защищаемая информация.

Для программно-аппаратных СЗИ существуют особенности, связанные с использованием аппаратной компоненты для реализации некоторых функций безопасности. Эта компонента может, как взаимодействовать с программной компонентой СЗИ в ОС СВТ по некоторому интерфейсу и, возможно, подключаться/отключаться от СВТ в процессе работы СЗИ, так и обладать собственной средой функционирования для автономной работы относительно СВТ и его программной среды. В соответствии с этим использовать существующие спосо-

бы и средства тестирования для программно-аппаратных СЗИ часто становится принципиально невозможно: реализованные в СЗИ функции безопасности нельзя проверить либо в некоторой их части, либо полностью. При этом требуется учитывать, что такие СЗИ могут иметь множество состояний как программной, так и аппартной компоненты, а также различные их сочетания. Поэтому необходимо осуществлять моделирование состояний и переходов между ними для компонент программно-аппаратного СЗИ с целью обеспечения принципиальной возможности тестирования в части всех реализованных функций безопасности.

При внедрении СЗИ в ИС, особенно сертифицированных, могут нарушаться условия функционирования этого средства вследствие влияния информационной системы на реализуемые им функции безопасности. В большей части это касается СЗИ с аппаратной компонентой, так как программные СЗИ зависят только от ОС СВТ и не зависят, например, от аппаратной платформы и прочих подобных факторов. Из этого следует, что требуется выявлять нарушения, вносимые средой, в которой используется СЗИ, необходимых условий для выполнимости реализованных в нем функций безопасности. Такая проверка может зависеть от особенностей системы, и вследствие этого является достаточно сложной и продолжительной для каждой ИС. Кроме того, в ряде случаев время проведения всех проверок может превышать срок, по истечении которого изменятся условия тестирования функций безопасности, например, выход обновлений ОС, ИС и СЗИ. В связи с этим для своевременной фиксации нарушений функций безопасности и причин их возникновения, а также проведения тестирования в требуемые сроки необходимо автоматизировать данный процесс. Помимо этого средства автоматизации не всегда применимы к программно-аппаратным СЗИ в неизменном виде.

Таким образом, в настоящее время существует потребность в защите данных в информационных системах с применением программно-аппаратных средств защиты информации, но для проверки корректности их функций безопасности не применимы известные способы и средства тестирования программного обеспечения. В соответствии с этим требуется проведение моделирования состояний программно-аппаратных средств защиты информации и переходов между ними для разработки нового способа и средств тестирования, и тема диссертационной работы является актуальной.

Степень разработанности темы исследования. В научных трудах отечественных и зарубежных ученых и специалистов большое внимание уделяется проблемам качества и надежности ПО, а также способам и средствам его тестирования. Из таких работ необходимо прежде всего отметить труды В. В. Липаева, В. И. Грекула, И. В. Степанченко, С. В. Синицына, Н. Ю. Налютина, В. П. Котлярова, Г. Майерса (G. Myers), Р. Блэка (R. Black), Б. Бейзера (B. Beizer), Л. Тамре (L. Tamres), С. Канера (C. Kaner), Р. Калбертсона (R. Culbertson), К. Бэка (K. Beck) и Э. Дастина (E. Dusting), которые внесли наибольшее значение в развитие теории и практики тестирования.

В трудах перечисленных авторов рассматриваются способы и средства тестирования применительно к ПО. При этом вопрос применимости этих способов и средств к программно-аппаратным СЗИ в данных работах не изучается. Отличия в тестировании ПО и программно-аппаратных комплексов поверхностно рассмотрены в работах Р. Блэка, в которых обозначены сложности при проведении некоторых проверок. Однако каких-либо методических рекомендаций по тестированию программно-аппаратных средств не приводится. Таким образом, усилиями перечисленных ученых сформирована база для дальнейшего углубления и конкретизации теоретических и практических результатов для одного из актуальных на данный момент направлений исследования – тестирования функций безопасности программно-аппаратных СЗИ. Кроме того, вопросы тестирования функций безопасности программно-аппаратных СЗИ интересуют многих производителей, но описание применяемых ими на практике способов и средств тестирования обычно не публикуется в открытых источниках. Отсюда вытекает научная задача диссертации, которая состоит в формировании модели и основанного на ней способа тестирования, а также рекомендаций по практической реализации средств тестирования, устанавливаемых в информационные системы программно-аппаратных средств защиты информации. Это позволит в условиях наличия особенностей и директивных сроков тестирования их функций безопасности обеспечить возможность проведения, полноту и оптимальность тестовых испытаний.

Целью диссертационного исследования является разработка научно-обоснованного способа тестирования функций безопасности программно-аппаратных средств защиты информации.

Задачи работы. Для достижения поставленной цели в работе решались следующие задачи:

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.

Положения, выносимые на защиту. В диссертационном исследовании получены и выносятся на защиту следующие положения и научные результаты:

1. Доказана ограниченность использования способов тестирования программного обеспечения в задаче полной проверки функций безопасности программно-аппаратных СЗИ, а также определены условия и критерии их применимости для тестирования программно-аппаратных средств защиты информации.

2. Разработанный способ тестирования функций безопасности программно-аппаратных средств защиты информации, основанный на использовании модели программно-аппаратных средств защиты информации, алгоритмов тестирования и верификации программно-аппаратных СЗИ, обеспечивает учет состояний аппаратной компоненты программно-аппаратных СЗИ.

3. Созданный программно-аппаратный комплекс для тестирования СЗИ, в котором реализован предложенный способ тестирования программно-аппаратных СЗИ, обеспечивает тестирование и верификацию различных видов функций безопасности.

Научная новизна работы. Новизна полученных научных результатов состоит в следующем:

1. Предложена научно-обоснованная модель программно-аппаратных СЗИ, основанная на положениях теории автоматов, 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 (соответствует п.15 паспорта специальности «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности»).

2. Предложен алгоритм тестирования функций безопасности СЗИ, основанный на использовании разработанной модели программно-аппаратных СЗИ и положений теории графов, обеспечивающий решение новой задачи – тестирование программно-аппаратных СЗИ (соответствует п.11 паспорта специальности «Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты»).

3. Предложен алгоритм верификации функций безопасности программно-аппаратных СЗИ, основанный на использовании положений теории оптимизации и принятия решений, отличающийся от подобных алгоритмов использованием процедур оценки критичности выявленных в ходе тестирования ошибок и их влияния на защищенность информационной системы (соответствует п.11 и п.8 паспорта специальности «Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения»).

Теоретическая значимость исследования 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 разработке алгоритмов тестирования и верификации функций безопасности программно-аппаратных СЗИ.

Практическая значимость исследования заключается в разработке рекомендаций по практической реализации средств тестирования функций безопасности программно-аппаратных СЗИ, реализации на их основе программно-аппаратного комплекса для тестирования функций безопасности СЗИ, заявляемых их производителем, 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.

Методология и методы исследования. В диссертационной работе используются аппарат системного анализа и теории формальных систем, автоматов, графов, оптимизации и принятия решений.

Степень достоверности научных положений и выводов обеспечена корректным использованием теорий формальных систем, автоматов, графов, оптимизации и принятия решений, строгого 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, и совпадением ожидаемых результатов от их использования с полученными при экспериментальных исследованиях.

Внедрение результатов работы. Разработанный программно-аппаратный комплекс тестирования СЗИ внедрен в ЗАО «ОКБ САПР» и применяется для тестирования функций безопасности и верификации встраиваемых в ИС программно-аппаратных СЗИ. Результаты диссертационной работы также применяются при разработке перспективных средств тестирования программно-аппаратных СЗИ в ЗАО «ОКБ САПР», при разработке программ и методик сертификационных испытаний и верификации результатов тестирования сертифицируемых средств защиты информации в ФАУ «ГНИИИ ПТЗИ ФСТЭК России», а также при создании инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных СЗИ на базе перспективных высокоскоростных интерфейсов информационного взаимодействия в НИЯУ МИФИ в рамках исполнения работ по НИОКТР. Аналитические результаты используются в учебном процессе кафедры «Криптология и кибер-

безопасность» НИЯУ МИФИ в рамках дисциплины «Программно-аппаратные средства защиты информации». Соответствующие документы, подтверждающие практическое использование и внедрение результатов исследований, приведены в приложении к тексту диссертационной работы.

Апробация работы. Основные положения и результаты работы представлены и обсуждены на следующих научных конференциях: Международная конференция «Brain-Inspired Cognitive Architectures for Artificial Intelligence», г. Москва, 2020; Международная конференция «Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology», г. Екатеринбург, 2020; Международная конференция «Intelligent Technologies in Robotics», г. Москва, 2019; Международная конференция «Безопасность инфокоммуникационных технологий», г. Воронеж, 2016; XXI Международная конференция «Комплексная защита информации», г. Смоленск, 2016; Международная конференция «Обеспечение безопасности инфокоммуникационных и цифровых технологий», г. Воронеж, 2015; XIX Международная конференция «Комплексная защита информации», г. Псков, 2014; XVIII Международная конференция «Комплексная защита информации», г. Брест (РБ), 2013; XIII Международная конференция «Информационная безопасность», г. Таганрог, 2013.

Публикации. Основные результаты по теме диссертации изложены в 21 печатной работе общим объемом 9,84 п.л., в которых автору принадлежит 7,59 п.л. Из них 15 печатных работ изданы в рецензируемых научных изданиях, определенных Высшей аттестационной комиссией при Министерстве науки и высшего образования РФ и Аттестационным советом УрФУ, в том числе 5 – в журналах, индексируемых международной системой научного цитирования Scopus. Имеется 1 свидетельство о государственной регистрации программы для ЭВМ.

Личный вклад. Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в работу. Все основные представленные в диссертации результаты получены автором самостоятельно. В работах, опубликованных в соавторстве, лично автору принадлежат: исследование применимости существующих способов и средств тестирования ПО к программно-аппаратным СЗИ; обоснование необходимости использования вспомогательных программно-технических средств для автоматизации тестирования функций безопасности программно-аппаратных СЗИ; анализ осо-

бенностей верификации программно-аппаратных СЗИ, связанных с возможностью выявления ошибок разного уровня критичности, и предложенный алгоритм верификации; исследование возможности применения различных средств автоматизации для тестирования программно-аппаратных СЗИ; классификация программно-аппаратных СЗИ и выделение особенностей тестирования различных видов функций безопасности; алгоритм тестирования функций безопасности программно-аппаратных СЗИ с использованием средств виртуализации; модель программно-аппаратного СЗИ и его представление в виде графа.

Структура и объем работы. Диссертационная работа состоит из введения, 4 глав, заключения и 4 приложений. Объем основного текста диссертации составляет 155 страниц(ы) с 40 рисунками и 3 таблицами. Приложение также содержит документы, подтверждающие практическое использование и внедрение результатов диссертационного исследования. Количество наименований в списке литературы — 114.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертационного исследования, формулируются его цель и задачи, определяются научная новизна, теоретическая и практическая значимость полученных результатов. Рассматриваются положения, выносимые на защиту.

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

Проведен анализ действующей нормативно-правовой базы в области защиты информации и показана необходимость применения СЗИ. Получена классификационная схема функций безопасности программно-аппаратных СЗИ. Определены особенности их тестирования, не характерные для ПО и программных средств защиты, зависящие от вида реализующей аппаратной компоненты, вида взаимодействия с защищаемым СВТ и влияющие на возможность применения существующих подходов, способов и средств для тестирования функций без-

опасности программно-аппаратных СЗИ, а также на возможность его выполнения в требуемые сроки.

Показано, что проведение тестирования с последующей верификацией обнаруженных ошибок необходимо для подтверждения корректности реализованных функций безопасности, отсутствия негативного влияния на характеристики и защищенность ИС, проверки нарушения условий функционирования самого СЗИ. Перечисленное обосновывает ограниченность применения существующих подходов, способов и средств тестирования в задаче полной проверки функций безопасности программно-аппаратных СЗИ, а также необходимость моделирования состояний программно-аппаратных СЗИ, разработки нового научно-обоснованного способа тестирования их функций безопасности и автоматизации самого процесса тестирования для своевременной фиксации различных нарушений. Следовательно, также необходимо сформулировать рекомендации по практической реализации средств тестирования функций безопасности программно-аппаратных СЗИ и разработать такие средства.

Вторая глава посвящена разработке научно-обоснованного способа тестирования функций безопасности программно-аппаратных СЗИ, основанного на использовании модели программно-аппаратных средств защиты информации.

Предложены описательная и формальная модели программно-аппаратного СЗИ, в рамках которых введены следующие обозначения: M – множество всех программно-аппаратных СЗИ; m – произвольное СЗИ, $m \in M$. V – множество состояний, в которых может находиться m. I – множество функций m, которые могут выполняться в состояниях $v \in V$. $I_{фб}$, $I_{нц}$, $I_{вн}$ – множества функций безопасности m с формальными параметрами, нецелевых функций m и внешних воздействий на него соответственно. При этом $I = I_{фб} \cup I_{нц} \cup I_{вн}$.

Программно-аппаратное СЗИ m представляется в виде конечного детерминированного автомата $\widetilde{m} = (V, I, O, f, g)$, для которого: V – множество состояний автомата, где v_0 – начальное состояние; I – множество входов (стимулов) автомата – функций m, которые могут выполняться в состояниях автомата; $O = \{0, 1\}$ – множество выходов (реакций) – результатов выполнения стимулов в состояниях автомата (успешное или неуспешное выполнение); $f : I \times V \to V$ – функция переходов автомата: если $f((i,v)) = v'$, то по стимулу $i \in I$ из состояния $v \in V$ автомат переходит в состояние $v' \in V$; $g : I \times V \to O$ – функция

выходов автомата: если $g((i,v)) = o$, то по стимулу $i \in I$ из состояния $v \in V$ на выход автомата поступает $o \in O$.

Введены обозначения: M_p, M_a и M_{na} – множества программно-аппаратных СЗИ, для которых вне зависимости от человеческого фактора возможно выполнение ручного, автоматического и автоматизированного тестирования с применением способов ручного, автоматического тестирования и тестирование которых возможно автоматизировать частично, $M_a \subseteq M_{na} \subseteq M_p \subseteq M$. $V_{фб}$ – множество всех состояний СЗИ с потенциально вычислимыми функциями безопасности – состояний, в которых необходимо проверить функции безопасности m, $V_{фб} \subseteq V$. T – множество всевозможных переходов автомата: $T \subseteq V \times I \times O \times V$, при каждом переходе (v, i, o, v') выполняется $f((i,v)) = v'$ и $g((i,v)) = o$.

Определены последовательности переходов тестирования m, моделируемого с помощью автомата $\widetilde{m} = (V, I, O, f, g)$: пустая последовательность $\overline{s}_0$ длины $len(\overline{s}_0) = 0$ и последовательности $\overline{s}$ переходов $s_0, \ldots, s_{l-1} \in T$ длины $len(\overline{s}) = l \in \mathbb{N}$. Для $l > 0$ элементы последовательности $\overline{s}$ имеют вид: $s_j = (v'_j, i'_{j+1}, o'_{j+1}, v'_{j+1}) \in T$, где $j = 0, \ldots, l-1$, а для первого элемента последовательности $s_0 = (v'_0, i'_1, o'_1, v'_1) \in T$ выполняется $v'_0 = v_0$. Введено обозначение S – множество всевозможных последовательностей переходов тестирования различной длины.

Предполагается, что для моделируемого автоматом $\widetilde{m} = (V, I, O, f, g)$ СЗИ m решена задача тестирования с помощью последовательности переходов тестирования $\overline{s} \in S$, когда одновременно выполняются условия:

1. Условие возможности проведения тестирования: $m \in M_p$.
2. Условие полноты тестирования: $\forall s_j \in T$, для которого $v'_{j+1} \in V_{фб}$, является элементом последовательности $\overline{s}$.
3. Условие оптимальности тестирования:
   $len(\overline{s}) = \min\{len(\overline{s}') : \forall \overline{s}' \in S$ выполняется п.2$\}$.

Приведено доказательство ограниченности способов, используемых для тестирования программного обеспечения, в задаче полной проверки функций безопасности программно-аппаратных средств защиты информации. Сформулированы условия применимости существующих способов тестирования ПО к различным видам функций безопасности программно-аппаратных СЗИ. С уче-

том этих условий введены определения вычислимой/автоматически вычислимой функции безопасности $i \in I_{фб}$, вычислимого/автоматически вычислимого стимула $i \in I_{нц} \cup I_{вн}$. На основании этого формализованы критерии применимости – необходимые и достаточные условия тестирования для программно-аппаратного СЗИ m.

Общий критерий возможности автоматического тестирования функций безопасности программно-аппаратных СЗИ. Пусть автомат $\widetilde{m} = (V, I, O, f, g)$ находится в состоянии v_0. Тогда и только тогда для моделируемого этим автоматом СЗИ выполняется $m \in M_a$, когда существует последовательность переходов тестирования $\overline{s} \in S$ длины $len(\overline{s}) = l \in \mathbb{N}_0$ и для $\forall i \in I_{фб}$ выполняется одно из условий:

1. i является автоматически вычислимой функцией безопасности в состоянии v_0;

2. i является автоматически вычислимой функцией безопасности в состоянии $v'_j \in V_{фб}$, $1 \leqslant j \leqslant l$ и $\overline{s}$ содержит последовательные переходы $s_0, \ldots, s_{j-1} \in T$ с началом в $v'_0 = v_0$, такие, что $i'_1, \ldots, i'_j$ являются автоматически вычислимыми стимулами в состояниях $v'_0, \ldots, v'_{j-1}$ соответственно.

Смысл критерия состоит в том, что применение способа автоматического тестирования к функциям безопасности программно-аппаратных СЗИ возможно только тогда, когда: либо функции безопасности могут буть проверены автоматически в начальном состоянии, либо существует состояние, для которого есть последовательность переходов, в которой автоматически могут быть проверены стимулы и сама функция безопасности.

Предложен алгоритм решения задачи тестирования функций безопасности программно-аппаратных СЗИ с применением теории графов. Введено определение ориентированного графа без петель и кратных дуг, соответствующего программно-аппаратному СЗИ m, представленному в виде конечного детерминированного автомата $\widetilde{m} = (V, I, O, f, g)$: $G_m = (V, E)$, где V – множество вершин графа, соответствующих состояниям автомата, а $E \subseteq V \times I \times O \times V$ – множество ориентированных дуг графа, помеченных стимулами и реакциями – переходов $(v, i, o, v') \in T$ автомата.

Показано, что обход графа G_m должен осуществляться по вершинам из множества $V_{фб} \subseteq V$, а не по всему множеству вершин V. В соответствии с этим на основании определенных в работе условий удаления из графа G_m неиспользуемых при решении задачи тестирования некоторых вершин и дуг построен производный от него граф G'_m. Доказано, что решение задачи тестирования в части выполнения условий возможности, полноты и оптимальности тестирования для графа G'_m будет являться решением задачи тестирования для графа G_m.

Показано, что решение задачи тестирования существует тогда и только тогда, когда любая вершина $v \in V$ графа G'_m либо принадлежит орцепи, либо лежит в компоненте сильной связности. Доказано, что предложенный алгоритм решения задачи тестирования имеет полиномиальную сложность $O(|V|^3)$. Блок-схема алгоритма тестирования приведена на Рисунке 1.

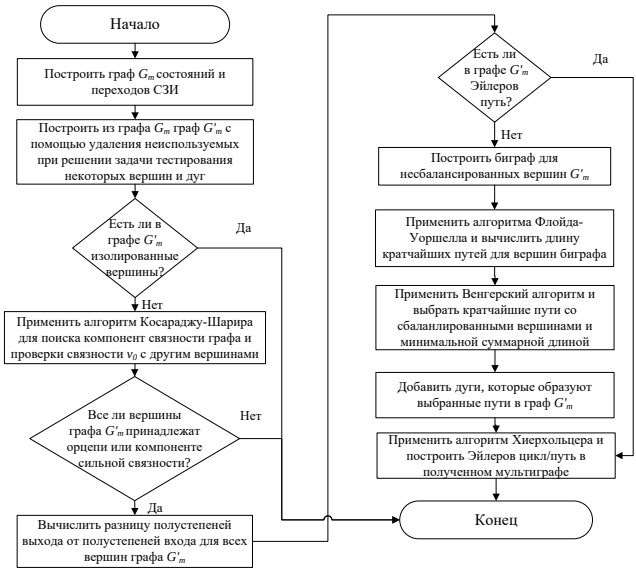

Рисунок 1 – Блок-схема алгоритма решения задачи тестирования функций безопасности программно-аппаратных СЗИ

Также предложен алгоритм верификации фунций безопасности программно-аппаратных СЗИ с применением теории оптимизации и принятия решений, основанный на классификации обнаруженных ошибок, анализе

степени их критичности и влияния на защищенность системы или данных. Данный алгоритм рассматривает критичность ошибок не в части нарушения работоспособности объекта тестирования, а с точки зрения возможности нарушения защищенности ИС или данных при некорректной работе функций безопасности. Блок-схема предложенного алгоритма верификации приведена на Рисунке 2.

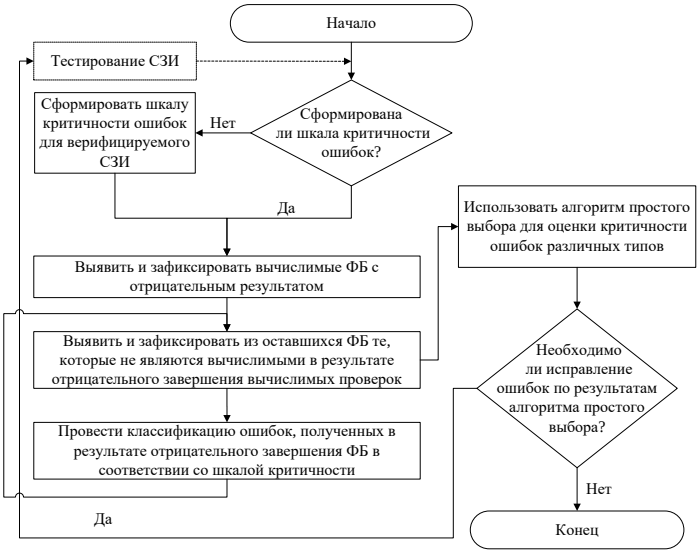

Рисунок 2 – Блок-схема алгоритма верификации функций безопасности программно-аппаратных СЗИ

На основании предложенных критериев, алгоритмов решения задачи тестирования и верификации сформулирован способ тестирования функций безопасности программно-аппаратных СЗИ, состоящий из приведенных на Рисунке 3 этапов. Предложенный способ тестирования учитывает состояния аппаратной компоненты, позволяет обеспечить полноту и оптимальность тестирования, а также оценить критичность выявленных в ходе тестирования ошибок программно-аппаратных СЗИ и их влияние на защищенность ИС.

Третья глава диссертации посвящена разработке программно-аппаратного комплекса для тестирования функций безопасности СЗИ, реализующего предло-

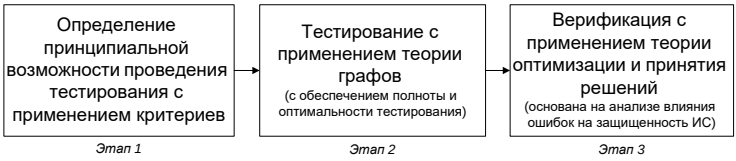

Рисунок 3 – Схема способа тестирования функций безопасности программно-аппаратных СЗИ

женный способ тестирования программно-аппаратных средств защиты информации.

Показано, что для корректной работы всех видов фунций безопасности программно-аппаратных СЗИ необходимо проверять совместимость их аппаратной и программной компоненты с аппаратной платформой. Для этого требуется проводить тестирование средств защиты на множестве СВТ с целью выявления возможных особенностей и несоответствия определенным стандартам последних, что может повлиять на возможность выполения функций безопасности.

Сформулированы рекомендации по использованию средств виртуализации в процессе тестирования функций безопасности программно-аппаратных СЗИ, на основании которых предложен содержащий правила проверки функций безопасности алгоритм тестирования с их использованием. Блок-схема предложенного алгоритма приведена на Рисунке 4.

Сформированы требования к средствам тестирования функций безопасности программно-аппаратных СЗИ различных видов. На основании данных требований сформирован принцип построения вспомогательных средств тестирования и программ тестирования, необходимых для обеспечения возможности проведения тестирования функций безопасности программно-аппаратных СЗИ.

Предложены рекомендации по практической реализации средств тестирования, а также программ тестирования и верификации функций безопасности программно-аппаратных СЗИ различных видов. На основании предложенных рекомендаций для средств тестирования выполнена разработка вспомогательного средства – коммутатора USB-канала, полностью эмулирующего физическое отключение и подключение СЗИ к СВТ как на уровне питания, так и на уровне канала передачи данных. Данный коммутатор может использоваться в програм-

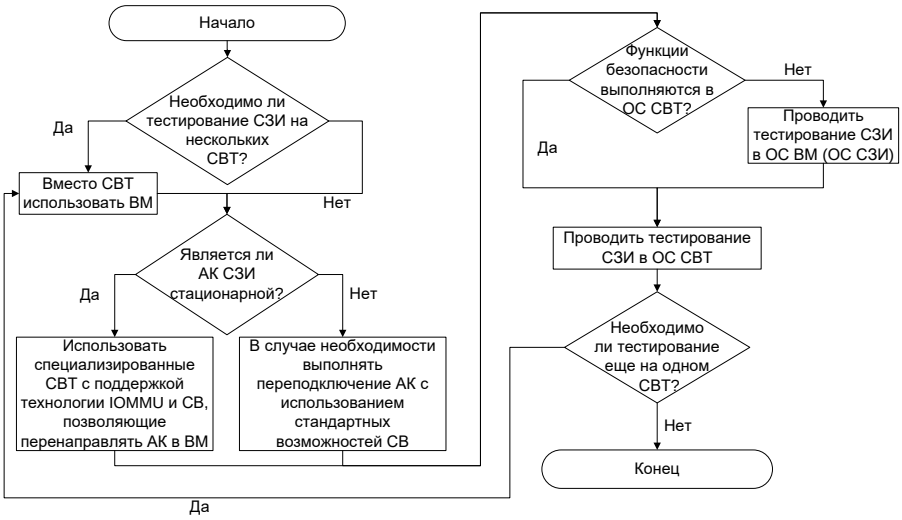

Рисунок 4 – Блок-схема алгоритма тестирования функций безопасности программно-аппаратных СЗИ с использованием средств виртуализации (АК – аппаратная компонента СЗИ, СВ – средство виртуализации)

мах тестирования для автоматического отключения/подключения к/от СВТ СЗИ с USB-интерфейсом, функционирующих в ОС данного СВТ. А на основании предложенных рекомендаций для программ тестирования и верификации на базе полученных научных результатов разработан программный комплекс «Тестирование функций безопасности программно-аппаратных (ТФБПА) средств защиты информации» (свидетельство о государственной регистрации программы для ЭВМ №2016616332). В данный комплекс входят программы тестирования и верификации для нескольких конкретных программно-аппаратных СЗИ, реализующих различные виды функций безопасности: на базе мобильной и стационарной аппаратной компоненты, взаимодействующие со средой ОС СВТ и не взаимодействующие с ней. Полученные результаты разработки для одного средства защиты могут быть с небольшими затратами адаптированы для применения в процессе тестирования другого СЗИ того же вида. Схема программно-аппаратного комплекса тестирования СЗИ представлена на Рисунке 5.

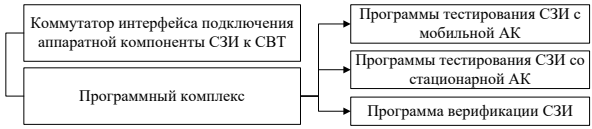

Рисунок 5 – Схема разработанного программно-аппаратного комплекса тестирования СЗИ

В четвертой главе проводится анализ опыта применения разработанного способа и основанного на нем программно-аппаратного комплекса для тестирования СЗИ, описывается внедрение результатов работы.

Приведена методика проведения экспериментальной апробации разработанного способа и основанного на нем программно-аппаратного комплекса для тестирования СЗИ. В результате применения данной методики показана возможность использования предложенного способа тестирования программно-аппаратных СЗИ для двух выбранных средств защиты, относящихся к различным видам: ПСКЗИ ШИПКА – функции безопасности которого реализованы на базе мобильной аппаратной компоненты и взаимодействуют со средой ОС СВТ и СЗИ НСД «Аккорд-АМДЗ» – функции безопасности которого реализованы на базе стационарной аппаратной компоненты и не взаимодействуют с ОС СВТ, выполняются независимо от ОС в составе СВТ.

Показано, что $m_{амдз} \in M_p$ и $m_{шипка} \in M_p$, а также $m_{амдз} \in M_a$ и $m_{шипка} \in M_a$ при наличии стредств автоматического подключения/отключения их аппаратных компонент к/от СВТ. Для данных СЗИ построены соответствующие графы, приведенные на Рисунках 6 и 7, применен алгоритм решения задачи тестирования и показано, что задача тестирования для данных СЗИ может быть решена, так как оба графа $G_{m_{амдз}}$ и $G_{m_{шипка}}$ являются сильно связными графами, а следовательно, по предложенному алгоритму для них можно построить оптимальный путь, проходящий по всем ребрам, то есть обеспечить полноту и оптимальность тестирования. Также для выбранных СЗИ продемонстрирована возможность применения алгоритма верификации программно-аппаратных СЗИ с применением теории оптимизации и принятия решений, реализованного в разработанной программе верификации.

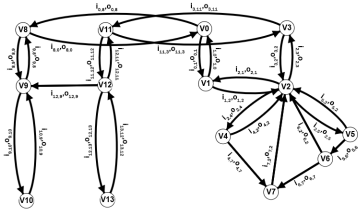

Рисунок 6 – Граф $G_{m_{амдз}}$ для СЗИ НСД «Аккорд-АМДЗ»

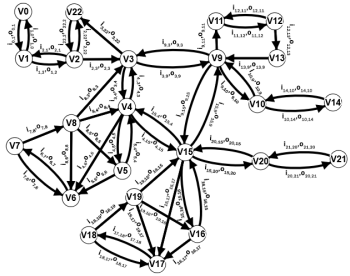

Рисунок 7 – Граф $G_{m_{шипка}}$ для ПСКЗИ ШИПКА

Проведена оценка количественных показателей применения результатов исследования для программно-аппаратных СЗИ различных видов. Экспериментально подтверждено, что для решения задачи принципиальной возможности тестирования функций безопасности в требуемые сроки внедрения СЗИ в ИС целесообразно использовать автоматическое тестирование и верификацию программно-аппаратных СЗИ. Также показано, что происходит уменьшение непроводимых ранее проверок функциц безопасности и увеличение общего числа проверок путем учета всех возможных переходов, как следствие обеспечения полноты тестирования.

Проведен анализ опыта и показана возможность совместного использования разработанного программно-аппаратного комплекса для тестирования СЗИ со сторонними вспомогательными для тестирования средствами и специализированными средствами тестирования СЗИ.

Основные положения и результаты работы представлены и обсуждены на 8 международных конференциях, имеются 4 акта об их внедрении.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

Основные результаты работы заключаются в следующем:

1. Проведен анализ существующих подходов, способов и средств тестирования программного обеспечения. Обоснована ограниченности известных подходов, используемых для тестирования ПО, в задаче полной проверки функций

безопасности программно-аппаратных СЗИ, и необходимость модификации данных подходов, а также соответствующих способов и средств тестирования.

2. Предложена модель программно-аппаратных средств защиты информации, учитывающая состояния аппаратной компоненты и на основе выработки формальных критериев применимости способов тестирования позволяющая выявить для конкретного средства защиты препятствующие проведению тестирования функции безопасности и переходы из одного состояния СЗИ в другое, и разработать новый способ и средства тестирования для обеспечения выполнимости всех проверок функций безопасности.

3. Разработан алгоритм тестирования функций безопасности программно-аппаратных СЗИ, основанный на известных положениях теории графов, позволяющий получить решение задачи тестирования, а также обеспечить его полноту и оптимальность.

4. Разработан алгоритм верификации функций безопасности программно-аппаратных СЗИ, основанный на известных положениях теории оптимизации и принятия решений и содержащий процедуры оценки критичности выявленных в ходе тестирования ошибок, позволяющий оценить степень влияния таких ошибок на защищенность ИС, на основании чего принять решение об успешном завершении тестирования или о возврате СЗИ на доработку.

5. Предложен способ тестирования функций безопасности программно-аппаратных СЗИ, учитывающий возможные состояния аппаратной компоненты, и устанавливающий порядок использования разработанных критериев применимости существующих способов тестирования ПО для таких средств защиты, алгоритмов тестирования и верификации их функций безопасности, позволяющий проводить тестирование различных видов функций безопасности программно-аппаратных СЗИ и обеспечить полноту и оптимальность данного тестирования.

6. Предложены рекомендации и на их основе разработан алгоритм тестирования функций безопасности программно-аппаратных СЗИ с применением средств виртуализации, позволяющий обеспечить возможность выполнения некоторых функций безопасности и стимулов в виртуальных машинах при невозможности их выполнения на реальных аппаратных платформах.

7. Предложены рекомендации по практической реализации средств и программ тестирования функций безопасности, на основе использования которых

создан программный комплекс «ТФБПА СЗИ» и коммутатор USB-канала, используемый во входящих в него программах тестирования для автоматического отключения и подключения СЗИ с USB-интерфейсом к/от СВТ.

8. Проведены апробация и анализ результатов применения разработанных способа тестирования функций безопасности и программно-аппаратного комплекса «ТФБПА СЗИ», а также проведена его апробация, результаты которой подтвердили их работоспособность и состоятельность результатов диссертационной работе как на качественном, так и на количественном уровне.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в рецензируемых научных изданиях, определенных ВАК РФ и Аттестационным советом УрФУ:

1. *Kanner, T. M.* Algorithm for Optimal and Complete Testing of Software and Hardware Data Security Tools / T. M. Kanner, A. M. Kanner, A.V. Epishkina // *Procedia Computer Science*. — 2021. — Vol. 190. — Pp. 408–413 (0.92 п.л. / 0.42 п.л.)(Scopus).
2. *Kanner, T. M.* Comprehensive Testing of Software and Hardware Data Security Tools Using Virtualization / T. M. Kanner, A. M. Kanner, A.V. Epishkina // *Advanced Technologies in Robotics and Intelligent Systems. Mechanisms and Machine Science*. — 2020. — Vol. 80. — Pp. 79–87 (0.52 п.л. / 0.23 п.л.)(Scopus).
3. *Kanner, T. M.* Testing Software and Hardware Data Security Tools Using the Automata Theory and the Graph Theory / T. M. Kanner, A. M. Kanner // *2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT 2020)*. — 2020. — Pp. 615–618 (0.4 п.л. / 0.2 п.л.)(Scopus).
4. *Kanner, T. M.* Applying a Mathematical Approach to Interpreting the Results of Testing Software and Hardware Data Security Tools during the Verification Process / T. M. Kanner, A. M. Kanner // *Journal of Engineering and Applied Sciences*. — 2019. — Vol. 14, no. 10. — Pp. 3482–3491 (1.02 п.л. / 0.5 п.л.)(Scopus).
5. *Каннер, Т. М.* Адаптация существующих способов верификации для программно-аппаратных СЗИ / Т. М. Каннер // *Вопросы защиты информации*. — 2018. — № 1. — С. 13–19 (0.55 п.л.).

6. *Каннер, Т. М.* Эффективность применения средств тестирования программно-аппаратных средств защиты информации / Т. М. Каннер // *Вопросы защиты информации*. — 2017. — № 2. — С. 9–13 (0.43 п.л.).
7. *Каннер, Т. М.* Разработка и оценка эффективности применения средств тестирования функций безопасности программно-аппаратных СЗИ / Т. М. Каннер // *Информация и безопасность*. — 2017. — № 3. — С. 330–333 (0.3 п.л.).
8. *Kanner, T. M.* Applicability of Software Testing Methods to Software and Hardware Data Security Tools / T. M. Kanner // *Global Journal of Pure and Applied Mathematics*. — 2016. — Vol. 12, no. 1. — Pp. 167–190 (1.23 п.л.)(Scopus).
9. *Каннер, Т. М.* Особенности применения средств виртуализации при тестировании программно-аппаратных СЗИ / Т. М. Каннер // *Информация и безопасность*. — 2015. — Т. 18, № 3. — С. 416–419 (0.25 п.л.).
10. *Каннер, Т. М.* Применимость методов тестирования ПО к программно-аппаратным СЗИ / Т. М. Каннер // *Вопросы защиты информации*. — 2015. — № 1. — С. 30–39 (0.81 п.л.).
11. *Каннер, Т. М.* Формирование подхода к автоматизации тестирования СЗИ, в конструктив которых входит флеш-память, функционирующих в ОС / Т. М. Каннер, К. А. Куваева // *Вопросы защиты информации*. — 2014. — № 4. — С. 52–54 (0.2 п.л. / 0.14 п.л.).
12. *Каннер, Т. М.* О выборе инструмента автоматизации тестирования для программно-аппаратных СЗИ / Т. М. Каннер, А. И. Обломова // *Вопросы защиты информации*. — 2014. — № 4. — С. 34–36 (0.24 п.л. / 0.17 п.л.).
13. *Каннер, Т. М.* Особенности верификации средств защиты информации / Т. М. Каннер, Х. С. Султанахмедов // *Вопросы защиты информации*. — 2014. — № 4. — С. 55–57 (0.25 п.л. / 0.18 п.л.).
14. *Борисова(Каннер), Т. М.* Особенности автоматизации тестирования программно-аппаратных СЗИ / Т. М. Борисова(Каннер) // *Безопасность информационных технологий*. — 2013. — № 2. — С. 27–31 (0.45 п.л.).
15. *Борисова(Каннер), Т. М.* Задача тестирования аппаратных средств защиты информации / Т. М. Борисова(Каннер), В. А. Гадасин // *Вопросы защиты информации*. — 2012. — № 3. — С. 10–16 (0.83 п.л. / 0.67 п.л.).

Свидетельство о регистрации программы:

16. Свидетельство о государственной регистрации программы для ЭВМ. Заявка 2016616332. Российская Федерация. Тестирование функций безопасности программно-аппаратных средств защиты информации / Авторы Каннер Т. М., Коробов В. В., правообладатель ЗАО «ОКБ САПР». — № 2016616332; заявл. 14.04.2016; опубл. 09.06.2016.

Другие публикации:

17. *Каннер, Т. М.* Коммутатор USB-канала как техническое средство для тестирования программно-аппаратных СЗИ / Т. М. Каннер // *Комплексная защита информации. Материалы XXI Международной конференции 17-19 мая 2016 года, Смоленск (Россия)*. — 2016. — Т. 1. — С. 200–204 (0.27 п.л.).
18. *Борисова(Каннер), Т. М.* Особенность тестирования СЗИ, в конструктив которых входит флеш-память / Т. М. Борисова(Каннер) // *Комплексная защита информации. Электроника инфо. Материалы XVIII Международной конференции 21-24 мая 2013 года, Брест (Республика Беларусь)*. — 2013. — № 6. — С. 119–120 (0.22 п.л.).
19. *Борисова(Каннер), Т. М.* Проблемы тестирования СЗИ, функционирующих до старта ОС / Т. М. Борисова(Каннер), А. В. Кузнецов // *Комплексная защита информации. Электроника инфо. Материалы XVIII Международной конференции 21-24 мая 2013 года, Брест (Республика Беларусь)*. — 2013. — № 6. — С. 114–115 (0.2 п.л. / 0.14 п.л.).
20. *Борисова(Каннер), Т. М.* Тестирование средств защиты информации / Т. М. Борисова(Каннер), А. В. Кузнецов, А. И. Обломова // *Информационная безопасность. Материалы XIII Международной конференции 9-12 июля 2013 года, Таганрог (Россия)*. — 2013. — Т. 1. — С. 121–129 (0.64 п.л. / 0.39 п.л.).
21. *Борисова(Каннер), Т. М.* Способы автоматизации тестирования СЗИ, функционирующих в ОС, на примере ПСКЗИ ШИПКА / Т. М. Борисова(Каннер), А. И. Обломова // *Комплексная защита информации. Электроника инфо. Материалы XVIII Международной конференции 21-24 мая 2013 года, Брест (Республика Беларусь)*. — 2013. — № 6. — С. 117–118 (0.24 п.л. / 0.17 п.л.).