Форма 501.КРАТКИЙ НАУЧНЫЙ ОТЧЕТ

1.1. Номер проекта
14-07-00417
1.2. Руководитель проекта
Десницкий Василий Алексеевич
1.3. Название Проекта
Разработка и исследование моделей и методик проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами на основе экспертных знаний
1.4. Код и название Конкурса
А - Конкурс инициативных научно-исследовательских проектов 2014 года
1.5. Год представления Отчета
2014
1.6. Вид Отчета (цифра 2- этап 2014 г.)
2
1.7. Аннотация
Проведен детальный анализ состояния исследований в предметной области проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами. В качестве источников знаний в предметной области проведен анализ трех существующих индустриальных информационно-телекоммуникационных систем со встроенными устройствами – системы удаленного автоматизированного контроля расхода электроэнергии потребителями, системы устройств оперативного реагирования и управления в чрезвычайных ситуациях и системы по предоставлению потребителю услуг цифровых потоковых мультимедиа-данных. Разработана обобщенная модель нарушителя встроенного устройства на основе анализа существующих классификаций нарушителя по уровню взаимодействия нарушителя со встроенным устройством и по возможностям нарушителя. На основе модели нарушителя разработана методика проведения верификации спецификаций информационно-телекоммуникационных систем. Методика позволяет осуществить анализ несанкционированных воздействий на встроенное устройство со стороны потенциального нарушителя с учетом его возможностей и ограничений. Разработана модель знаний о встроенном устройстве, которая включает иерархически организованную систему свойств защиты, их атрибутов и конфигураций защиты с учетом направленности процессов защиты на особенности конкретного проблемного домена в области защиты информационно-телекоммуникационных систем (доменно-ориентированный характер защиты). Разработана концептуальная комбинированная модель системы защиты встроенных устройств на основе применения экспертных знаний с использованием методов оптимизации и конфигурирования, методов верификации сложных систем и теории принятия решений.
1.8. Полное название организации, предоставляющей условия для выполнения работ по Проекту физическим лицам
Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Форма 503.РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1. Номер Проекта

14-07-00417

3.2. Название Проекта

Разработка и исследование моделей и методик проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами на основе экспертных знаний

3.3. Коды классификатора, соответствующие содержанию фактически проделанной работы

07-241, 07-235, 07-371, 01-217

3.4. Объявленные ранее цели Проекта на 2014 год

Основные цели проекта на 2014 год были связаны с разработкой и исследованием моделей и методик проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами с применением экспертных знаний и методов в области информационной безопасности встроенных устройств, в том числе анализом моделей нарушителя, моделированием и верификацией устройств и компонентов защиты информационно-телекоммуникационных систем. Ставились следующие задачи: 1) обзор и анализ существующих подходов, методов, моделей и методик проектирования и верификации комбинированных механизмов защиты систем со встроенными устройствами; 2) анализ индустриальных информационно-телекоммуникационных систем со встроенными устройствами в нескольких областях приложения (в том числе в электроэнергетике, в области реагирования и управления в чрезвычайных ситуациях, в телекоммуникации); 3) научное обоснование задачи проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами; 4) разработка обобщенной модели нарушителя встроенного устройства на основе анализа существующих классификаций нарушителя; 5) разработка методики верификации спецификаций информационно-телекоммуникационной системы на предмет анализа несанкционированных воздействий со стороны потенциального нарушителя; 6) разработка модели знаний о встроенном устройстве: построение деревьев свойств для функциональных свойств защиты, нефункциональных ресурсных свойств, свойств программно-аппаратной совместимости; формирование численных показателей для нефункциональных свойств защиты; определение доменно-специфичного представления систем со встроенными устройствами как средства для сопоставления требованиям к защите информационно-телекоммуникационной системы конкретных элементов формального представления; 7) разработка и уточнение концептуальной комбинированной модели системы защиты встроенных устройств на основе применения экспертных знаний, методов оптимизации и конфигурирования, методов верификации сложных систем и теории принятия решений.

3.5. Степень достижения поставленных в Проекте целей

Все задачи, запланированные в проекте на 2014 год, выполнены полностью. Дополнительно проведены исследования в области разработки программы для ЭВМ «Формирование модели нарушителя для анализа защищенности информационно-телекоммуникационных систем» по тематике проекта (государственная регистрация в реестре программ для ЭВМ Федеральной службы по интеллектуальной собственности от 22.10.2014, свидетельство № 2014661028).

3.6. Полученные в 2014 году важнейшие результаты

1. Проведен детальный анализ состояния исследований в области проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами. Работа по данному направлению, выполненная за 2014 год включает (1) анализ специфики встроенных устройств и современных тенденций в области разработки информационно-

телекоммуникационных систем со встроенными устройствами, (2) анализ ключевых проблем в области проектирования и верификации информационно-телекоммуникационных систем со встроенными устройствами, (3) научное обоснование направления исследований, (4) анализ существующих фундаментальных и прикладных научных работ в предметной области проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами. Использовано более 40 источников научно-технической и нормативной литературы.

2. Проведен анализ существующих информационно-телекоммуникационных систем со встроенными устройствами в нескольких областях приложения. Проведен анализ трех индустриальных информационно-телекоммуникационных систем в качестве источника экспертных знаний в области разработки защищенных систем со встроенных устройств: система удаленного автоматизированного контроля расхода электроэнергии потребителями (компания-разработчик Mixed-Mode, Германия), система устройств оперативного реагирования и управления в чрезвычайных ситуациях (компания-разработчик RUAG, Швейцария) и система по предоставлению цифровых мультимедиа сервисов массовому потребителю (компания-разработчик Technicolor, Франция). Выбор данных систем обусловлен необходимостью охвата нескольких областей приложения, различающихся структурой, назначением, функциональными характеристиками устройств и особенностями защиты. Достигнутая цель – обобщение знаний о конкретных системах и устройствах для их последующего применения в качестве паттернов проектирования и верификации в процессе разработки новых защищенных информационно-телекоммуникационных систем. К основным, полученным в рамках экспертного анализа, знаниям относятся требования к защите в виде функциональных свойств защиты и возможные альтернативы для выбора компонентов защиты с учетом возможных видов нарушителей; информация о функциональных особенностях устройства и связях между его компонентами, в том числе компонентами защиты; информация о типовых нефункциональных требованиях и их способ приоритезации на основе эвристики порядка учета требований защиты; информация о свойствах программно-аппаратной совместимости; характеристика ресурсопотребления устройств и их отдельных модулей; возможные виды конфликтов и аномалий компонентов защиты и информационных потоков системы и способы их разрешения. Полученные экспертные знания предназначены для построения на их основе моделей и методик проектирования и верификации информационно-телекоммуникационных систем со встроенными устройствами.

3. Разработана обобщенная модель нарушителя встроенного устройства на основе анализа классификаций нарушителя по уровню взаимодействия нарушителя со встроенным устройством и по возможностям нарушителя. Данная модель относится к классу аналитических моделей и описывает возможные виды нарушителей информационно-телекоммуникационных систем со встроенными устройствами и их наиболее существенные характеристики с использованием теоретико-множественного представления и средств языка UML. В соответствии существующими классификациями нарушителя (классификация, предложенная Pae и др., классификация Гранда, классификация Абрахама и др.) в рамках модели определены 15 возможных категорий нарушителя в соответствии с тремя уровнями возможностей и пятью типами доступа нарушителя ко встроенному устройству. При этом для каждой категории задается информация о возможностях нарушителя, возможных видах атак на устройство, а также особенностях защиты для противодействия таким атакам. Модель нарушителя представляется на основе следующего кортежа: <I, A, P, m>, где I – множество разновидностей нарушителей системы, A – множество возможных видов атак на систему, P – множество алгоритмов и средств защиты, которые могут быть имплементированы в систему защиты для противодействия атакам из A, m : I –> <A, P> – отображение, которое

для набора элементов из I сопоставляет соответствующие кортежи из элементов из множеств A и P. В свою очередь I = <T, S, R, Q, G, M>, где T – тип взаимодействия нарушителя с устройством, S – начальные возможности нарушителя, R – права доступа нарушителя к элементам системы, Q – квалификация нарушителя, G – цели нарушителя, M – мотивы нарушителя. Начальные возможности нарушителя S определяются наличием на устройствах системы уязвимостей, которые нарушитель может эксплуатировать в соответствии со своей квалификацией Q и видом взаимодействия с устройством T. Использование паролей по умолчанию в рамках технологических учетных записей устройств, восстановление пароля по хеш-значению из системных таблиц СУБД или конфигурационных файлов сетевого оборудования, использование недостаточно защищенных протоколов прикладного уровня, использование сетевых протоколов, позволяющих собирать информацию об устройствах системы и другие виды уязвимостей могут эксплуатироваться нарушителем для осуществления атак проникновения с целью установки на устройствах системы зловредного программного обеспечения и захвата управления устройствам. Подобные атаки часто осуществляются как процесс последовательного повышения привилегий, поэтому для анализа противодействия им ключевую роль играют начальные возможности нарушителя.

Тогда как теоретико-множественное представление предназначено для описания характеристик нарушителя в формализованном унифицированном виде, пригодным для использования в рамках формальных доказательств защищенности системы разработанное на основе UML представление модели нарушителя предназначено для описания взаимосвязей между моделируемыми сущностями, относящимися к нарушителю и к возможным атакам. К особенностям UML-представления можно отнести также возможность его непосредственного использования в процессе программной реализации компонентов защиты информационно-телекоммуникационной системы. Особенностями разработанной модели является однозначное и единообразное представление возможных нарушителей, причем модель может быть использована для сбора, накопления, хранения, разработки и отображения данных о конкретных видах нарушителей информационно-телекоммуникационных систем. Модель может применяться в качестве источника входных данных при проведении тестирования и верификации спецификаций таких систем на предмет наличия возможных уязвимостей. Модель нарушителя может применяться в процессах идентификации и формализации возможных атак на устройства системы, а также в процессе разработки тестов в рамках динамического тестирования готовых программно-аппаратных реализаций встроенных устройств.

4. Разработана методика проведения верификации спецификаций информационно-телекоммуникационных систем на предмет анализа несанкционированных воздействий со стороны потенциального нарушителя с использованием разработанной обобщенной модели нарушителя. Методика предназначена для выявления потенциальных угроз информационной безопасности, которым подвержено устройство, и относится к методам статического анализа. Для выполнения методики требуется информация об устройствах системы и ее функциональности, в том числе информация о коммуникационных интерфейсах, используемых криптографических алгоритмах, длине ключей и другая. Методика включает две стадии. Первая стадия представляет собой исследование спецификации встроенного устройства и выбор возможных типов нарушителей, имеющих цель его скомпрометировать в зависимости от функциональности устройства и ожидаемых сценариев использования. Полученные типы нарушителей анализируются в соответствии с разработанной обобщенной моделью нарушителя, после чего формируется список возможных атак на это устройство. На второй стадии проводится анализ спецификации устройства с целью реализации условий, необходимых для выполнения такой атаки, в том числе проверка наличия определенных аппаратных компонентов и коммуникационных интерфейсов, которые могут использоваться в качестве стартовой точки для проведения атаки. Если все эти условия выполняются, делается вывод о том,

что встроенное устройство потенциально уязвимо перед данной атакой. В противном случае делается вывод о невозможности такой атаки. Предложенная методика отличается итеративным характером выполнения и возможностью автоматизации процесса верификации. Разработанная в рамках проекта программа «Формирование модели нарушителя для анализа защищенности информационно-телекоммуникационных систем» (государственная регистрация в реестре программ для ЭВМ Федеральной службы по интеллектуальной собственности от 22.10.2014, свидетельство № 2014661028) представляет собой прототип программного средства для поддержки процесса верификации информационно-телекоммуникационных систем. В качестве входных данных программы задаются наиболее существенные функциональные и нефункциональные характеристики устройств системы и ограничения ее программно-аппаратного окружения. На выходе программа выдает список потенциальных атак, которым могут быть подвержены устройства системы. К преимуществам методики можно отнести возможность сужения множества всевозможных атак на устройства системы до некоторого их ограниченного подмножества в соответствии со спецификацией системы, ограничениями ее окружения и ожидаемыми видами нарушителей. Тем самым использование данной методики позволяет значительно сократить время, отводимое разработчиками информационно-телекоммуникационной системы на выполнение динамического тестирования физических реализаций устройств системы с использованием тестовых векторов атак.

5. Разработана модель знаний о встроенном устройстве. Модель включает иерархически организованные структуры свойств защиты («деревья свойств»), которые уточняются экспертом в области информационной безопасности и используются разработчиками систем со встроенными устройствами при построении и анализе требований к защите. Функциональные свойства защиты представляют собой бинарные величины, определяющие наличие или отсутствие некоторой защитного функционала устройства, например, контроля аутентичности данных с использованием удаленной аттестации, защищенного хранения криптографических ключей или механизма безопасного обновления программных модулей устройства. При этом функциональные свойства защиты подразделяются на базовые – определяемые реализацией некоторой функциональности, характерной широкому кругу встроенных устройств и сценариев их использования, и специфичные – свойства, которые задаются в рамках определенных проблемно-предметных доменов. К нефункциональным свойствам относятся численные характеристики программно-аппаратных компонентов защиты устройства, такие как энергопотребление, минимальная пропускной способности коммуникационного канала, требуемая для работы некоторого компонента защиты и другие. Конкретные правила использования знаний, являющиеся также частью предлагаемой модели, базируются на следующей цепочке: {функциональные и нефункциональные свойства защиты} → {требования к системе защиты} → {шаблоны защиты} → {компоненты защиты и их атрибуты} → {настройки системы защиты}. Доменно-специфичные представления для проектирования систем защиты встроенных устройств включают формальную спецификацию компонентов защиты и отношений между ними с учетом имеющихся угроз информационной безопасности и категорий нарушителей в терминах функциональных и не функциональных свойств защиты и их атрибутов. В практическом плане на основе подобных древовидных структур решается комплексная задача по разработке онтологий с использованием среды моделирования Protege, которые в свою очередь могут служить основой для разработки программных средств автоматизации проектирования систем и компонентов защиты встроенных устройств. Экспертные знания о встроенных устройствах, в том числе типовые требования, компоненты и настройки (конфигурации) защиты, угрозы информационной безопасности, а также типы и уровни возможного нарушителя, входящие в данную модель, предназначены для использования разработчиками на этапе проектирования информационно-телекоммуникационной

системы. В силу слабой структуризацией области знаний информационной безопасности встроенных устройств использование предложенной модели будет способствовать повышению защищенности конечных продуктов и сервисов информационно-телекоммуникационной системы за счет применения знаний, полученных на экспертном уровне. Введение модели знаний в процесс разработки систем со встроенными устройствами направлено также на делегирование части обязанностей экспертов по информационной безопасности непосредственно разработчикам в виде применения ими специализированных, в том числе автоматизированных методик проектирования, тестирования и оценки на базе имеющихся экспертных знаний в предметной области, знаний о конкретных индустриальных системах и программных инструментах, построенных на основе этих знаний. Использование модели знаний будет способствовать более эффективной организации процесса разработки систем защиты для семейств устройств, имеющих общую базовую функциональность, но отличающихся специфичными деталями и расширениями, определяющими особенности эксплуатации устройства и его стоимость. При этом использование модели знаний в рамках каждого проблемно-предметного домена позволит сократить количество итераций и продолжительность процесса разработки за счет адаптации уже имеющихся знаний с учетом специфики конкретных устройств.

6. Разработана концептуальная комбинированная модель системы защиты встроенных устройств. Концептуальная комбинированная модель системы защиты встроенных устройств определяет процесс комбинирования компонентов защиты, реализующих различные свойства безопасности путем выбора эффективных наборов компонентов (конфигураций защиты) с учетом их нефункциональных свойств и ограничений устройства. Модель описывает действия, которые должен выполнить разработчик встроенного устройства при интеграции и настройке (конфигурировании) его компонентов защиты. Применение существующих нормативов и стандартов позволяет среди имеющихся базовых компонентов защиты выбрать те из них, которые отвечают требованиям стойкости и надежности в соответствии с моделью нарушителя и актуальными видами угроз встроенного устройства. Нахождение оптимальной конфигурации защиты информационно-телекоммуникационной системы базируется на получении серии численных нефункциональных показателей защиты, и – путем постановки и решения оптимизационной экстремальной задачи при ограничениях на значения этих показателей и заданной целевой функции – позволяет получить наиболее эффективную конфигурацию защиты для обеспечения безопасности целевой системы. Выбор искомых конфигураций производится с использованием метода лексикографического упорядочения заданных критериев ресурсопотребления и согласуется с методологией моделирования MARTE. При этом упорядочивание осуществляется на основе эвристики, определяющей относительную важность аппаратных ресурсов для каждого вида устройств системы. Проведение многокритериального выбора включает определение показателей ресурсопотребления конфигураций защиты с использованием разработанного программного компонента оценки ресурсопотребления, уточнение эвристики многокритериального выбора, анализ конфликтов компонентов защиты и осуществление выбора наиболее эффективной конфигурации защиты с использованием программного модуля поддержки принятия решений для выбора конфигураций. Данный модуль предоставляет пользовательский интерфейс для задания информации об имеющихся компонентах защиты, их свойствах, требованиях со стороны устройства в терминах свойств и ограничений, критериях ресурсопотребления. Результатами работы модуля является информация о конфигурации, признанной в качестве эффективной в соответствии с заданными критериями. В качестве экспертных знаний, используемых в процессе комбинирования компонентов защиты были выявлены три типа скрытых конфликтов: (1) конфликты вследствие недостаточной согласованности компонента защиты и спецификации устройства, (2) конфликты между

функциями защиты нескольких компонентов, (3) конфликт между несколькими базовыми компонентами защиты в рамках комплексного компонента. Эти конфликты были выявлены эвристически – путем анализа существующих систем со встроенными устройствами и ряда работ в области безопасности встроенных устройств. В общем случае верификация спецификаций и моделей систем со встроенными устройствами на предмет выявления типовых конфликтов между компонентами защиты способствует ускорению процесса разработки целевой информационно-телекоммуникационной системы и позволяет повысить ее защищенность. К особенностям модели можно отнести выделение ролей эксперта по информационной безопасности и разработчика устройств системы с определением согласованных действий для каждой из них, осуществление автоматизированных процедур оценки ресурсопотребления и поддержку принятия решений выбора конфигураций из множества имеющихся альтернатив.

3.7. Степень новизны полученных результатов

Полученные научные результаты являются новыми и оригинальными, они основываются на разработках исполнителей проекта, выполненных ранее и выполняемых в настоящее время, а также базируются на современных достижениях в области информационной безопасности, программной инженерии, системного анализа, объектно-ориентированного проектирования и анализа и др.

3.8. Сопоставление полученных результатов с мировым уровнем

Все результаты, полученные в процессе выполнения проекта в 2014 году соответствуют мировому уровню. Авторы проекта опубликовали полученные результаты в нескольких журналах, сборниках и трудах конференций, а также апробировали результаты на множестве различных российских и международных конференций, в частности, на Шестнадцатой Международной конференция «РусКрипто 2014» по криптологии, криптографии, информационной безопасности и защите данных, Московская область, г. Солнечногорск, 25-28 марта 2014 г.; Международной научно-практической конференции «Теоретические и прикладные проблемы информационной безопасности», г. Минск, Беларусь, 19 июня 2014 г.; 23-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, 30 июня - 3 июля 2014 г.; Четвертом IFIP международном семинаре по безопасности и когнитивной информатике для национальной обороны (4rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense, SeCIHD 2014), г. Фрибург, Швейцария, 8 - 12 сентября, 2014 г.; конференции «Информационные технологии в управлении» (ИТУ-2014) в рамках 7-й Российской мультиконференции по проблемам управления (РМКПУ-2014), 7-9 октября 2014 г.; XIV Санкт-Петербургской Международной Конференции «Региональная информатика-2014» («РИ-2014»), г. Санкт-Петербург, 29-31 октября 2014 г.; XXIII Международной научно-практической конференции «Естественные и математические науки в современном мире», г. Новосибирск, 01 октября 2014 г.; XXXIX Международной научно-практической конференции «Технические науки - от теории к практике», г. Новосибирск, 22 октября 2014 г.; XXXVIII Международной научно-практической конференции «Инновации в науке», г. Новосибирск, 29 октября 2014 г.; Научно-технической конференции «Инновации Северо-Запада», г. Санкт-Петербург, 15-16 декабря 2014 г.

3.9. Методы и подходы, использованные в ходе выполнения Проекта

(1) Методы аналитического моделирования нарушителей в информационно-телекоммуникационных системах со встроенными устройствами с использованием существующих классификаций нарушителя встроенных устройств по уровню его взаимодействия с устройством и по возможностям нарушителя. (2) Подход к верификации и тестированию спецификаций и моделей информационно-телекоммуникационных систем на предмет определения возможных атак на встроенные устройства системы. Подход охватывает статическое и динамическое тестирование, причем статическое тестирование (верификация) позволяет разработчику на ранних стадиях процесса проектирования

выявить потенциальные угрозы информационной безопасности, которым подвержено устройство, тогда как динамическое тестирование ориентировано на применение на финальной стадии процесса разработки для проверки возможных векторов атак на физической реализации устройств. (3) Методы формирования знаний в области информационной безопасности встроенных устройств для построения моделей и методик проектирования и верификации информационно-телекоммуникационных систем со встроенными устройствами с использованием иерархически организованных структур функциональных и нефункциональных свойства защиты («деревьев свойств»), доменно-ориентированных представлений систем и компонентов защиты, знаний о скрытых несовместимостях и конфликтах компонентов защиты. (4) Основанный на эвристике подход к определению порядка учета нефункциональных требований к системе защиты в зависимости от функциональных и нефункциональных характеристик информационно-телекоммуникационной системы и входящих в нее устройств. Подход реализуется в использовании эвристики в качестве элемента комбинированной модели системы защиты с применением дискретной оптимизации на множестве компонентов защиты. (5) Подход к выявлению скрытых конфликтов между компонентами защиты, ориентированный на обнаружение в процессе проектирования информационно-телекоммуникационных систем конфликтов, которые, как правило, проявляться на стадии эксплуатации системы. Знания об известных видах конфликтов получаются путем экспертного анализа и моделирования систем со встроенными устройствами.

3.10.1.1 Количество научных работ по Проекту, опубликованных в 2014 году

16

3.10.1.2 Из них в изданиях, включенных в перечень ВАК

2

3.10.1.3. Из них в изданиях, включенных в системы цитирования (Web of Science, Scopus, Web of Knowledge, Astrophysics, PubMed, Mathematics, Chemical Abstracts, Springer, Agris, GeoRef)

1

3.10.2. Количество научных работ, подготовленных в ходе выполнения Проекта и принятых к печати в 2014 году (цифрами)

0

3.11. Участие в 2014 году в научных мероприятиях по тематике Проекта

- 16-я международная конференции «РусКрипто 2014» по криптологии, стеганографии, цифровой подписи и системам защиты информации, Московская область, г.Солнечногорск, 25-28 марта 2014 г. (В.А.Десницкий, А.А.Чечулин). - XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014), Санкт-Петербург, 23-25 октября 2014 г. (В.А.Десницкий, Е.В.Дойникова, А.А.Чечулин). - Четвертый IFIP международный семинар по безопасности и когнитивной информатике для национальной обороны (SeCIHD 2014), Фрибург, Швейцария, 8-12 сентября 2014 г. (В.А.Десницкий). - Конференция «Информационные технологии в управлении» (ИТУ-2014), Санкт-Петербург, 7-9 октября 2014 г. (В.А.Десницкий, Е.В.Дойникова, А.А.Чечулин). - Научно-техническая конференция «Инновации Северо-Запада», Санкт-Петербург, 15-16 декабря 2014 г. (В.А.Десницкий, А.А.Чечулин). - 23-я Общероссийская научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, 30 июня - 3 июля 2014 г. (В.А.Десницкий). - Международная научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности», 19 июня 2014 года, г. Минск, Беларусь, 2014 г. (В.А.Десницкий). - XXIII Международная научно-практическая конференция «Естественные и математические науки в современном мире», Новосибирск, 01 октября 2014 г. (В.А.Десницкий). - XXXIX Международная научно-практическая конференция «Технические науки - от теории к практике», Новосибирск, 22 октября 2014

г. (В.А.Десницкий). -XXXVIII Международная научно-практическая конференция «Инновации в науке», Новосибирск, 29 октября 2014 г. (В.А.Десницкий).

3.12. Участие в 2014 году в экспедициях по тематике Проекта, которые проводились при финансовой поддержке Фонда

3.13. Финансовые средства, полученные в 2014 году от РФФИ (в руб.)

500000,00

3.14. Адреса (полностью) ресурсов в Интернете, подготовленных авторами по данному проекту, например, http://www.somewhere.ru/mypub.html

http://www.comsec.spb.ru/ru/staff/desnitsky http://www.comsec.spb.ru/en/staff/desnitsky http://www.comsec.spb.ru/ru/projects http://www.comsec.spb.ru/en/projects

3.15. Библиографический список всех публикаций по Проекту, опубликованных в 2014 году, в порядке значимости: монографии, статьи в научных изданиях, тезисы докладов и материалы съездов, конференций и т.д.

1. Vasily Desnitsky, Igor Kotenko. Expert Knowledge based Design and Verification of Secure Systems with Embedded Devices // 4rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2014). September 8nd – 12th, 2014. Fribourg, Switzerland. Lecture Notes in Computer Science (LNCS), Vol.8708. Springer-Verlag. 2014. P.194-210.
2. Десницкий В.А., Котенко И.В. Использование экспертных знаний для разработки защищенных систем со встроенными устройствами // Информационные технологии и вычислительные системы, № 4, 2014, С.58-73.
3. Десницкий В.А., Котенко И.В. Проектирование и верификация защищенных систем со встроенными устройствами на основе экспертных знаний // Проблемы информационной безопасности. Компьютерные системы, № 3, 2014. С.16-22.
4. Десницкий В.А., Чечулин А.А. Обобщенная модель нарушителя и верификация информационно-телекоммуникационных систем со встроенными устройствами // Журнал «Технические науки — от теории к практике». Изд. НП «СибАК», №39, 2014, С.7-21. ISSN 2308-5991.
5. Десницкий В.А. Разработка модели знаний для проектирования защищенных встроенных устройств // Журнал «Естественные и математические науки в современном мире». Изд. НП «СибАК», №23, 2014, С.35-40. ISSN 2309-3560.
6. Десницкий В.А. Концептуальная комбинированная модель системы защиты встроенных устройств // Журнал «Инновации в науке». Изд. НП «СибАК», №38, 2014, С.55-59. ISSN 2308-6009.
7. Десницкий В.А. Анализ перспективных систем со встроенными устройствами для формирования экспертных знаний в области проектирования защищенных информационно-телекоммуникационных систем // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» («РИ-2014»), 29-31 октября 2014 г. Материалы конференции. СПб., 2014. С.130.
8. Котенко И.В., Чечулин А.А., Десницкий В.А. Особенности построения системы защиты информации в кибер-физических системах // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.67-69.
9. Десницкий В.А., Котенко И.В. Комбинированная модель защиты информационно-телекоммуникационных систем концепции «Интернет вещей» // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.65-66.
10. Десницкий В.А. Верификация сетевых информационных потоков систем со встроенными устройствами на основе экспертных знаний // Материалы конференции

«Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.596-600. ISBN 978-5-91995-042-4.
11. Десницкий В.А.Проектирование и верификация механизмов защиты систем со встроенными устройствами на основе экспертных знаний // Шестнадцатая Международная конференция «РусКрипто 2014». Московская область, г.Солнечногорск, 25-28 марта 2014 г. http://www.ruscrypto.ru/
12. Десницкий В.А., Дойникова Е.В. Разработка компонентов защиты встроенных устройств с учетом экспертных знаний // Международная научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности». 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.
13. Десницкий В.А., Котенко И.В. Концептуальная комбинированная модель системы защиты встроенных устройств и ее применение для конфигурирования компонентов многоуровневой интеллектуальной системы комплексной безопасности железнодорожного транспорта // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» («РИ-2014»), 29-31 октября 2014 г. Материалы конференции. СПб., 2014. С.131.
14. Десницкий В.А., Котенко И.В. Конфигурирование информационных систем со встроенными устройствами для обеспечения комплексной безопасности железнодорожного транспорта // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.89-90.
15. Десницкий В.А., Чечулин А.А. Верификация информационно-телекоммуникационных систем со встроенными устройствами на основе обобщенной модели нарушителя // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.66-67.
16. Бушуев С.Н., Копчак Я.М., Ногин С.Б., Десницкий В.А. Технология разработки и анализа компонентов защиты информационно-телекоммуникационных систем концепции Интернет вещей // Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014 г. СПб.: Изд-во СПбГЭТУ «ЛЭТИ». 2004. С.73-77.

3.16. Приоритетное направление развития науки, технологий и техники РФ, которому, по мнению исполнителей, соответствуют результаты данного проекта

Информационно-телекоммуникационные системы

3.17. Критическая технология РФ, которой, по мнению исполнителей, соответствуют результаты данного проекта

Технологии доступа к широкополосным мультимедийным услугам

3.18. Основное направление технологической модернизации экономики России, которому, по мнению исполнителей, соответствуют результаты данного проекта

Стратегические информационные технологии, включая вопросы создания суперкомпьютеров и разработки программного обеспечения.

Основные результаты проекта

В ходе первого этапа проекта был проведен детальный анализ состояния исследований в предметной области проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами на основе более 40 источников научно-технической литературы.

В качестве источников знаний в предметной области проведен анализ трех существующих индустриальных информационно-телекоммуникационных систем со встроенными устройствами – системы удаленного автоматизированного контроля расхода электроэнергии потребителями, системы устройств оперативного реагирования и управления в чрезвычайных ситуациях и системы по предоставлению потребителю услуг цифровых потоковых мультимедиа-данных.

Выбор данных систем обусловлен необходимостью охвата нескольких областей приложения, различающихся структурой, назначением, функциональными характеристиками устройств и особенностями защиты. Достигнутая цель – обобщение знаний о конкретных системах и устройствах для их последующего применения в качестве паттернов проектирования и верификации в процессе разработки новых защищенных информационно-телекоммуникационных систем.

Разработана обобщенная модель нарушителя встроенного устройства на основе анализа существующих классификаций нарушителя по уровню взаимодействия нарушителя со встроенным устройством и по возможностям нарушителя. Модель относится к классу аналитических моделей и описывает возможные виды нарушителей информационно-телекоммуникационных систем со встроенными устройствами и их наиболее существенные характеристики с использованием теоретико-множественного представления и средств языка UML. В соответствии существующими классификациями нарушителя (классификация, предложенная Рае и др., классификация Гранда, классификация Абрахама и др.) в рамках модели определены 15 возможных категорий нарушителя в соответствии с тремя уровнями возможностей и пятью типами доступа нарушителя ко встроенному устройству. При этом для каждой категории задается информация о возможностях нарушителя, возможных видах атак на устройство, а также особенностях защиты для противодействия таким атакам.

Особенностями разработанной модели является однозначное и единообразное представление возможных нарушителей, причем модель может быть использована для сбора, накопления, хранения, разработки и отображения данных о конкретных видах нарушителей информационно-телекоммуникационных систем. Модель может применяться в качестве источника входных данных при проведении тестирования и верификации спецификаций таких систем на предмет наличия возможных уязвимостей. Модель нарушителя может применяться в процессах идентификации и формализации возможных атак на устройства системы, а также в процессе разработки тестов в рамках динамического тестирования готовых программно-аппаратных реализаций встроенных устройств.

На основе модели нарушителя разработана методика проведения верификации спецификаций информационно-телекоммуникационных систем на предмет анализа несанкционированных воздействий со стороны потенциального нарушителя с использованием разработанной обобщенной модели нарушителя. Методика позволяет осуществить анализ несанкционированных воздействий на встроенное устройство со стороны потенциального нарушителя с учетом его возможностей и ограничений. Предложенная методика отличается итеративным характером выполнения и возможностью автоматизации процесса верификации. Использование данной методики позволяет значительно сократить время, отводимое разработчиками информационно-телекоммуникационной системы на выполнение динамического тестирования физических реализаций устройств системы с использованием тестовых векторов атак.

Разработана модель знаний о встроенном устройстве, которая включает иерархически организованную систему свойств защиты, их атрибутов и конфигураций защиты с учетом направленности процессов защиты на особенности конкретного проблемного домена в области защиты информационно-телекоммуникационных систем (доменно-ориентированный характер защиты).

Экспертные знания о встроенных устройствах, в том числе типовые требования, компоненты и настройки (конфигурации) защиты, угрозы информационной безопасности, а также типы и уровни возможного нарушителя, входящие в данную модель, предназначены для использования разработчиками на этапе проектирования информационно-телекоммуникационной системы. Конкретные правила использования знаний, являющиеся также частью предлагаемой модели, базируются на следующей цепочке: {функциональные и нефункциональные свойства защиты} → {требования к системе защиты} → {шаблоны защиты} → {компоненты защиты и их атрибуты} → {настройки системы защиты}. В силу слабой структуризацией области знаний информационной безопасности встроенных устройств использование предложенной модели будет способствовать повышению защищенности конечных продуктов и сервисов информационно-телекоммуникационной системы за счет применения знаний, полученных на экспертном уровне.

Введение модели знаний в процесс разработки систем со встроенными устройствами направлено также на делегирование части обязанностей экспертов по информационной безопасности непосредственно разработчикам в виде применения ими специализированных, в том числе автоматизированных методик проектирования, тестирования и оценки на базе имеющихся экспертных знаний в предметной области, знаний о конкретных индустриальных системах и программных инструментах, построенных на основе этих знаний.

Использование модели знаний будет способствовать более эффективной организации процесса разработки систем защиты для семейств устройств, имеющих общую базовую функциональность, но отличающихся специфичными деталями и расширениями, определяющими особенности эксплуатации устройства и его стоимость. При этом использование модели знаний в рамках каждого проблемно-предметного домена позволит сократить количество итераций и продолжительность процесса разработки за счет адаптации уже имеющихся знаний с учетом специфики конкретных устройств.

Разработана концептуальная комбинированная модель системы защиты встроенных устройств на основе применения экспертных знаний с использованием методов оптимизации и конфигурирования, методов верификации сложных систем и теории принятия решений.

Концептуальная комбинированная модель системы защиты встроенных устройств определяет процесс комбинирования компонентов защиты, реализующих различные свойства безопасности путем выбора эффективных наборов компонентов (конфигураций защиты) с учетом их нефункциональных свойств и ограничений устройства. Модель описывает действия, которые должен выполнить разработчик встроенного устройства при интеграции и настройке (конфигурировании) его компонентов защиты.

Нахождение оптимальной конфигурации защиты информационно-телекоммуникационной системы базируется на получении серии численных нефункциональных показателей защиты, и – путем постановки и решения оптимизационной экстремальной задачи при ограничениях на значения этих показателей и заданной целевой функции – позволяет получить наиболее эффективную конфигурацию защиты для обеспечения безопасности целевой системы. Выбор искомых конфигураций производится с использованием метода лексикографического упорядочения заданных критериев ресурсопотребления и согласуется с методологией моделирования MARTE. При этом упорядочивание осуществляется на основе эвристики, определяющей относительную важность аппаратных ресурсов для каждого вида устройств системы.

Аннотации публикаций

1. Vasily Desnitsky, Igor Kotenko. Expert Knowledge based Design and Verification of Secure Systems with Embedded Devices // 4rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2014). September 8nd – 12th, 2014. Fribourg, Switzerland. Lecture Notes in Computer Science (LNCS), Vol.8708. Springer-Verlag. 2014. P.194-210.

Повышенная сложность проектирования современных защищенных систем со встроенными устройствами обуславливается низкой структуризацией и формализацией области знаний информационной безопасности. В работе предлагается подход к выявлению экспертных знаний в данной области для последующего их использования в рамках автоматизированного проектирования и верификации информационно-телекоммуникационных систем со встроенными устройствами. Разработанная методика построена на основе предметно-ориентированного анализа нескольких индустриальных систем и характеризуется заложенной в нее специфичной экспертной информацией о системных ресурсах встроенных устройств, типовых конфликтах и аномалиях. В работе основное внимание уделяется методике проектирования и верификации информационно-телекоммуникационных систем со встроенными устройствами с использованием экспертных знаний об аппаратных ресурсах встроенных устройств, типовых конфликтах и аномалиях, возникающих в системе. К особенностям методики можно также отнести использование метода проверки на модели для верификации сетевых информационных потоков.

2. Десницкий В.А., Котенко И.В. Использование экспертных знаний для разработки защищенных систем со встроенными устройствами // Информационные технологии и вычислительные системы, № 4, 2014, С.58-73.

В статье предлагается подход к выявлению экспертных знаний в области информационной безопасности встроенных устройств для их дальнейшего использования разработчиками встроенных устройств, в том числе в качестве входных данных автоматизированных инструментов проектирования и верификации встроенных устройств. Разработанная методика построена на основе предметно-ориентированного анализа нескольких индустриальных систем и характеризуется заложенной в нее специфичной экспертной информацией о системных ресурсах встроенных устройств, типовых конфликтах и аномалиях. К особенностям методики можно отнести использование специализированных эвристических знаний в области безопасности встроенных устройств в качестве готовых паттернов проектирования и верификации с применением метода проверки на модели.

3. Десницкий В.А., Котенко И.В. Проектирование и верификация защищенных систем со встроенными устройствами на основе экспертных знаний // Проблемы информационной безопасности. Компьютерные системы, № 3, 2014. С.16-22.

В статье предложена методика проектирования и верификации информационных систем со встроенными устройствами, которая ориентирована на разработку и комплексный анализ защищенности комбинированных механизмов защиты встроенных устройств с учетом показателей ресурсопотребления, скрытых конфликтов и аномалий компонентов защиты и информационных потоков. К особенностям методики можно отнести использование специализированных эвристических знаний в области безопасности встроенных устройств в качестве готовых паттернов проектирования и верификации.

Основные результаты, представленные в статье, включают следующие стадии разработанной методики: конфигурирование компонентов защиты встроенного устройства, выявление скрытых конфликтов между компонентами защиты, верификация

сетевых информационных потоков. Разработанный программный прототип включает средство принятия решений о выборе оптимальных конфигураций на этапе проектирования устройств на основе свойств имеющихся компонентов защиты и ограничений и средство верификации сетевых информационных потоков на основе метода «проверка на модели».

4. Десницкий В.А., Чечулин А.А. Обобщенная модель нарушителя и верификация информационно-телекоммуникационных систем со встроенными устройствами // Журнал «Технические науки — от теории к практике». Изд. НП «СибАК», №39, 2014, С.7-21. ISSN 2308-5991.

Сложность разработки и реализации требований к защите информационно-телекоммуникационных систем и встроенных устройств обуславливает необходимость построения моделей и методов проектирования и верификации механизмов защиты с учетом угроз информационной безопасности, целей и ресурсов возможных нарушителей, а также функциональных особенностей устройств. Предложены обобщенная модель нарушителя на основе анализа существующих классификаций нарушителей и верификация спецификаций в качестве метода тестирования защищенности устройств в процессе проектирования. Тестирование позволяет разработчику выявить потенциальные угрозы и осуществить отбор возможных типов нарушителей в зависимости от функциональности устройств и ожидаемых сценариев использования, после чего формируется список возможных атак на это устройство. Верификация включает анализ спецификаций на предмет проверки условий, необходимых для выполнения выявленных видов атак, в том числе проверку наличия определенных аппаратных компонентов и коммуникационных интерфейсов, которые могут использоваться в качестве стартовой точки для проведения атаки.

5. Десницкий В.А. Разработка модели знаний для проектирования защищенных встроенных устройств // Журнал «Естественные и математические науки в современном мире». Изд. НП «СибАК», №23, 2014, С.35-40. ISSN 2309-3560.

Стремительное возрастание количества разновидностей и экземпляров встроенных устройств, их повсеместное распространение и организация в виде систем «Интернет вещей» ставят особенно остро вопросы разработки механизмов их защиты от широкого круга угроз информационной безопасности. Сложность проектирования защищенных встроенных устройств обуславливается во многом слабой структуризацией и формализацией области знаний информационной безопасности встроенных устройств. Модель знаний о безопасности встроенных устройств, включающая, требования, компоненты и настройки защиты, угрозы, а также типы и уровни возможного нарушителя в качестве системы экспертных знаний предназначена для ее использования разработчиками встроенных устройств на этапе проектирования. В силу слабой структуризацией области знаний информационной безопасности встроенных устройств использование предложенной модели разработчиками встроенных устройств будет способствовать повышению защищенности конечных продуктов и сервисов за счет применения знаний, полученных на экспертном уровне. Использование модели знаний будет способствовать более эффективной организации процесса разработки систем защиты семейств устройств, имеющих общую базовую функциональность, но отличающихся специфичными деталями и расширениями, определяющими особенности эксплуатации устройства и его стоимость. При этом использование модели знаний в рамках каждого проблемно-предметного домена позволит сократить количество итераций и продолжительность процесса разработки за счет адаптации уже имеющихся знаний с учетом специфики конкретных устройств.

6. Десницкий В.А. Концептуальная комбинированная модель системы защиты встроенных устройств // Журнал «Инновации в науке». Изд. НП «СибАК», №38, 2014, С.55-59. ISSN 2308-6009.

Проектирование защищенных систем со встроенными устройствами представляет собой важнейшую задачу в области информационной безопасности. Особенностями таких систем являются автономность устройств, входящих в систему, и ограничения, накладываемые на ресурсы устройств, и вытекающая из этого их слабая производительность. Предлагаемая в работе концептуальная комбинированная модель системы защиты встроенных устройств нацелена на нахождение наиболее эффективных комбинаций компонентов защиты на основе решения оптимизационной задачи с учетом нефункциональных свойств и ограничений устройства. На основе данных об ограничениях ресурсопотребления устройств системы и требованиях к защите принимается решение о выборе оптимальной конфигурации защиты. Верификация комбинированной системы защиты встроенных устройств проводится с использованием модели нарушителя встроенных устройств и позволяет выявить угрозы, которым подвержены устройства системы.

7. Десницкий В.А. Анализ перспективных систем со встроенными устройствами для формирования экспертных знаний в области проектирования защищенных информационно-телекоммуникационных систем // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» («РИ-2014»), 29-31 октября 2014 г. Материалы конференции. СПб., 2014. С.130.

В работе проводится анализ трех информационно-телекоммуникационных систем в качестве источника экспертных знаний в области проектирования защищенных систем со встроенных устройств: система удаленного автоматизированного контроля расхода электроэнергии потребителями, система устройств оперативного реагирования и управления в чрезвычайных ситуациях и система по предоставлению цифровых мультимедиа сервисов массовому потребителю. Выбор данных систем обуславливается необходимостью охвата нескольких областей приложения, различающихся структурой, назначением, функциональными устройств и особенностями защиты. Конечная цель проводимого анализа – обобщение знаний о конкретных системах и устройствах и их последующее применение в качестве паттернов проектирования и верификации в процессе разработки новых информационно-телекоммуникационных систем.

8. Котенко И.В., Чечулин А.А., Десницкий В.А. Особенности построения системы защиты информации в кибер-физических системах // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.67-69.

В настоящее время наблюдается стремительное развитие кибер-физических систем или т.н. Интернета вещей. Повышение сложности систем влечет за собой увеличение числа их возможных уязвимостей. Хотя, в настоящее время, многие разработчики проявляют большой интерес к механизмам защиты таких сетей, очень мало внимания уделяется устойчивости инфраструктуры к атакам, что представляет собой угрозу нормального функционирования таких систем. Современные механизмы защиты ориентированы в основном на предоставление защиты против определенных угроз и чаще всего не могут быть установлены на специализированные устройства. В работе предлагается использовать комплексный подход к моделированию инфраструктурных атак, процессов безопасности происходящих внутри сетей кибер-физических систем. Такой подход защиты отличается от существующих аналогов ориентированностью на особенности кибер-физических систем и включает в себя методы, методики и алгоритмы, предназначенные для: (1) анализа и построения архитектуры системы защиты для кибер-

физической системы, включающей в себя как центры управления безопасностью, так и сенсоры для сбора информации (2) сбора данных для построения моделей объектов и процессов характерных для конкретных кибер-физических систем; (3) выработки конкретных требований к защищенности кибер-физических систем; (4) построения аналитической модели системы, ее процессов функционирования, возможных атакующих и т.д.; (5) предварительной оценки защищенности; (6) построения модели событий безопасности влияющих как на процесс функционирования, так и на состояния отдельных объектов; (7) организации интеллектуального анализа событий безопасности в реальном времени для выявления возможных атакующих действий; (8) формирования отчета и элементов визуализации результатов работы системы безопасности.

9. Десницкий В.А., Котенко И.В. Комбинированная модель защиты информационно-телекоммуникационных систем концепции «Интернет вещей» // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.65-66.

Современные информационно-телекоммуникационные системы отличаются сложной распределенной структурой, разнообразием угроз информационной безопасности (ИБ) и возможных видов нарушителей ИБ, высокой динамикой внедрения новых телекоммуникационных технологий, изменением во времени сетевой топологии, одновременным использованием нескольких типов коммуникаций на основе широкополосных и беспроводных протоколов, мобильностью и автономностью входящих в нее устройств, тенденцией к увеличению объемов обрабатываемой информации и вытекающей отсюда нехваткой вычислительных и коммуникационных ресурсов устройств. В работе исследуются новые эффективные подходы к проектированию защищенных распределенных информационно-телекоммуникационных систем в рамках концепции «Интернет вещей» на основе комбинирования средств противодействия атакам со стороны широкого класса потенциальных нарушителей. Предлагаемая модель защиты ориентирована на достижение компромисса между функционалом системы и отдельных устройств и уровнем их защищенности.

10. Десницкий В.А. Верификация сетевых информационных потоков систем со встроенными устройствами на основе экспертных знаний // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.596-600. ISBN 978-5-91995-042-4.

Ограничения на системные ресурсы встроенных устройств определяют сложность применения существующих методов и алгоритмов, используемых традиционно для защиты персональных компьютеров и серверных станций. В результате разработка защищенных встроенных устройств требует специализированных подходов к проектированию механизмов защиты, которые могли бы обеспечить стойкость системы к атакам не только за счет дополнительных средств защиты, но и за счет особенностей архитектуры системы. Верификация информационной системы со встроенными устройствами на всех этапах проектирования, как один из путей достижения этой цели, позволяет избежать архитектурных ошибок, которые, в свою очередь, снижают уровень защищенности всей системы. В работе предложена методика верификации информационных потоков, которая построенная на основе экспертных знаний об известных видах аномалий сетевых информационных потоков. Методика нацелена на проведение оценки защищенности разрабатываемой информационной системы со встроенными устройствами, проверки корректности политики безопасности этой системы и определение уровня соответствия информационных потоков в реальной системе заданным политикам.

11. Десницкий В.А. Проектирование и верификация механизмов защиты систем со встроенными устройствами на основе экспертных знаний // Шестнадцатая Международная конференция «РусКрипто 2014». Московская область, г.Солнечногорск, 25-28 марта 2014 г. http://www.ruscrypto.ru/

Рассматриваются модели, методики и программные средства проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами, основанные на использовании экспертных знаний специалистов в области защиты информации.

12. Десницкий В.А., Дойникова Е.В. Разработка компонентов защиты встроенных устройств с учетом экспертных знаний // Международная научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности». 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.

В статье рассмотрены вопросы формирования, структуризации и уточнения экспертных знаний, характеризующих различные аспекты проектирования и верификации механизмов защиты встроенных устройств. Приведены результаты поиска и адаптации существующих и разработки новой методики и автоматизированного программного стенда в интересах их последующего использования разработчиками встроенных устройств.

13. Десницкий В.А., Котенко И.В. Концептуальная комбинированная модель системы защиты встроенных устройств и ее применение для конфигурирования компонентов многоуровневой интеллектуальной системы комплексной безопасности железнодорожного транспорта // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» («РИ-2014»), 29-31 октября 2014 г. Материалы конференции. СПб., 2014. С.131.

В работе предлагается концептуальная модель системы защиты встроенных устройств, определяющая процесс комбинирования отдельных компонентов защиты, реализующих различные свойства безопасности устройства путем выбора эффективных компонентов с учетом их нефункциональных свойств и ограничений устройства. Модель описывает действия, которые должен выполнить разработчик встроенного устройства при конфигурировании его компонентов защиты. Применение существующих нормативов и стандартов позволяет среди имеющихся базовых компонентов защиты выбрать те из них, которые отвечают требованиям стойкости и надежности в соответствии с моделью нарушителя и актуальными видами угроз встроенного устройства.

14. Десницкий В.А., Котенко И.В. Конфигурирование информационных систем со встроенными устройствами для обеспечения комплексной безопасности железнодорожного транспорта // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.89-90.

Существующие системы поддержки процессов на железнодорожном транспорте (ЖТ) представляют собой информационно-телекоммуникационные сетевые и распределенные архитектуры, которые включают взаимодействующие между собой, как стационарные, так и мобильные подсистемы и устройства. Предлагаемая в работе модель процесса конфигурирования представляет нахождение оптимальной конфигурации компонентов защиты и основывается на получении нефункциональных показателей защиты для решения оптимизационной экстремальной задачи при ограничениях на значения этих показателей и заданной целевой функции позволяет построить наиболее

эффективную конфигурацию. Конфигурирование отличается направленностью на возникающие изменения в требованиях, вносимые на различных этапах процесса проектирования и влекущие пересмотр ранее проведенных этапов. Проектирование встроенных систем защиты в рамках сервисов многоуровневой интеллектуальной системы комплексной безопасности ЖТ включает: (1) анализ моделей нарушителя, спецификацию функциональных свойств защиты и свойств программно-аппаратной совместимости; (2) задание ограничений ресурсопотребления платформы устройства; (3) поиск и формирование репозитория имеющихся компонентов защиты встроенных устройств, определение их свойств; (4) проведение анализа несовместимостей компонентов защиты с использованием экспертных знаний; (5) проведение оценки ресурсопотребления компонентов защиты при помощи автоматизированных модулей тестирования на основе эмуляции устройств; (6) выбор компонентов защиты на основе учета показателей ресурсопотребления с использованием эвристик по выбору порядка учета критериев ресурсопотребления.

15. Десницкий В.А., Чечулин А.А. Верификация информационно-телекоммуникационных систем со встроенными устройствами на основе обобщенной модели нарушителя // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.66-67.

В работе представлена обобщенная модель нарушителя встроенных устройств, которая используется при разработке моделей, методов и реализующих их средств обеспечения безопасности информационно-телекоммуникационных систем со встроенными устройствами. Для определения возможных атак на встроенное устройство применяется применять аналитический подход с использованием существующих классификаций нарушителя встроенного устройства по уровню взаимодействия нарушителя с устройством (классификация Рае и др.) и по возможностям нарушителя (классификация Гранда, классификация Абрахама). Обобщенная модель нарушителя используется для проведения верификации спецификации встроенного устройства на наличие потенциальных уязвимостей, формирования тестов физической проверки устройства, построения первоначального списка необходимых программных и программно-аппаратных компонентов защиты, которые интегрируются в устройство, а также для определения необходимого уровня защищенности от нарушителей различных типов и уровней. К недостаткам рассматриваемой модели нарушителя можно отнести отсутствие в ней классификации нарушителей по уровню доступа к администрированию устройств и системы в целом. Так, например, если пользователь имеет права администратора системы, то он может, как намеренно или так не умышленно нарушить политику безопасности системы.

16. Бушуев С.Н., Копчак Я.М., Ногин С.Б., Десницкий В.А. Технология разработки и анализа компонентов защиты информационно-телекоммуникационных систем концепции Интернет вещей // Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014 г. СПб.: Изд-во СПбГЭТУ «ЛЭТИ». 2004. С.73-77.

Технология разработки и анализа компонентов защиты информационно-телекоммуникационных систем концепции Интернет вещей включает совокупность решений проектирования, верификации и тестирования компонентов защиты информационно-телекоммуникационных систем, реализующих концепцию Интернет вещей. Разработаны основные принципы и методические подходы в области проектирования, верификации и тестирования компонентов защиты информационно-телекоммуникационных систем в рамках концепции Интернет вещей. Разработаны

математические модели информационно-телекоммуникационных систем и компонентов защиты в рамках концепции Интернет вещей, отражающие их основные характеристики, в том числе сетевую топологию, используемое программно-аппаратное обеспечение, конфигурацию системы защиты и учитывающих особенности устройств, специфичных для концепции Интернет вещей на основе сформированных принципов и методических подходов в области проектирования, верификации, тестирования. Разработана математическая модель нарушителя, отражающая основные его характеристики, в том числе тип, начальные возможности и права в системе, квалификацию, цели и мотивы на основе сформированных принципов и методических подходов в области проектирования, верификации, тестирования и анализа сценариев применения.