Форма 503 (итог). 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 (в порядке значимости) (поле заполняется автоматически, коды вносятся из заявки)

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

3.4 Объявленные ранее цели Проекта

Основные цели Проекта на 2014-2016 г. определялись как разработка и исследование моделей и методик проектирования и верификации механизмов защиты систем со встроенными устройствами на основе экспертных знаний в области безопасных встроенных устройств. При этом были выделены следующие научные направления: (1) разработка моделей и методик проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами; (2) разработка модели и методик конфигурирования компонентов защиты встроенных устройств; (3) разработка и анализ методик верификации информационных потоков в рамках систем со встроенными устройствами. Для достижения поставленных целей планировалось решение следующих задач:
- обзор и анализ существующих подходов, методов, моделей и методик проектирования и верификации комбинированных механизмов защиты систем со встроенными устройствами;
- 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);
- научное обоснование задачи проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами;
- разработка обобщенной модели нарушителя встроенного устройства на основе анализа существующих классификаций нарушителя;
- разработка методики верификации спецификаций информационно-телекоммуникационной системы на предмет анализа несанкционированных воздействий со стороны потенциального нарушителя;
- 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;
- 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;

- разработка методики выявления функциональных и нефункциональных несовместимостей между компонентами защиты встроенных устройств информационно-телекоммуникационных систем;
- разработка методики оценки ресурсопотребления компонентов защиты с использованием концепции моделирования и анализа систем реального времени и встроенных устройств MARTE;
- разработка модели процесса конфигурирования компонентов защиты встроенных устройств с использованием экспертных знаний, эвристик и правил для осуществления многокритериального выбора компонентов защиты;
- моделирование с использованием языка UML и программная реализация прототипа средства конфигурирования, а также экспериментальная оценка его эффективности;
- обзор и анализ существующих моделей и методик верификации сетевых, программных, программно-аппаратных информационных потоков и выявления аномальных данных информационно-телекоммуникационных систем со встроенными устройствами;
- разработка методики верификация информационных потоков на основе топологического анализа с использованием ориентированных графов для представления анализируемой информационно-телекоммуникационной системы;
- разработка методики верификации информационных потоков на основе анализа политик безопасности, обнаружения конфликтов сетевых информационных потоков;
- разработка методики выявления аномальных данных от сенсоров в информационно-телекоммуникационных системах со встроенными устройствами на основе ограничений и правил функционирования целевой системы;
- реализация программного прототипа средств верификации сетевых информационных потоков с использованием метода «проверка на модели» (model checking) и оценка эффективности предложенных методик.

3.5 Полученные в ходе выполнения Проекта 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 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 встроенными устройствами: 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).
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 ожидаемых видов нарушителей; информация о функциональных особенностях устройства и связях между его компонентами, в том числе компонентами защиты; информация о типовых нефункциональных требованиях и способ их 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 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.

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 уровнем 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 систем 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» 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. 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. 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 рамках некоторого проблемно-предметного домена информационной безопасности (например, домен защищенных коммуникаций между устройствами системы или домен защищенного хранения критически важных данных в постоянной памяти устройства).

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.
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 защиты (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 встроенных устройств. 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.
7. Разработана методика выявления функциональных и нефункциональных

несовместимостей компонентов защиты встроенных устройств информационно-телекоммуникационных систем. Целью методики является верификация механизмов защиты системы в части выявления в процессе ее проектирования скрытых несовместимостей, в которые вовлечены отдельные компоненты защиты, устанавливаемые на устройства системы. Несовместимость рассматривается, как отношение между двумя или более компонентами защиты и представляет собой противоречие между их защитными функционалами, между какими-либо их нефункциональными ограничениями и/или ограничениями программно-аппаратной платформой устройства. При этом несовместимости подразделяются на аномалии, которые свидетельствуют о потенциальной некорректной работе механизма защиты при достижении определенных условий, и конфликты, представляющие собой программно-аппаратные ошибки, напрямую влияющие на работу функций защиты устройства и предоставляемых им сервисов. Методика базируется на использовании знаний, полученных путем экспертного анализа существующих информационно-телекоммуникационных систем со встроенными устройствами, представляющих информацию о существующих системах, устройствах, компонентах защиты и сценариях их взаимодействия, некоторых видах типовых конфликтов и направлений их разрешения. В частности, выделяются три следующие типа несовместимостей: (1) несовместимости вследствие недостаточной согласованности компонента защиты и спецификации устройства, (2) несовместимости между функциями защиты нескольких компонентов, (3) несовместимости между несколькими базовыми компонентами защиты в рамках комплексного компонента защиты, а также построены примеры для каждой из таких несовместимостей. Разработанная методика ориентирована на применение в процессе комбинирования компонентов защиты встроенных устройств для устранения скрытых, как функциональных, так и нефункциональных противоречий между ними, что в конечном итоге позволяет повысить безопасность и надежность целевой системы и предоставляемых ей сервисов.
Отметим, что способ разрешения несовместимостей индивидуален и определяется в зависимости от специфики конкретной несовместимости и вовлеченных в нее компонентов защиты. В качестве вариантов разрешения возможен пересмотр одного или нескольких компонентов защиты, изменение способа их интеграции, корректировка требований к защите или спецификации устройства. Кроме того более раннее выявление несовместимостей, осуществляемое на стадии формирования требований к защите будет способствовать сокращению количества итераций процесса разработки целевой информационно-телекоммуникационной системы и снижению его сложности.
8. Разработана методика оценки ресурсопотребления компонентов защиты с использованием концепции моделирования и анализа встроенных устройств и систем реального времени и на основе методологии MARTE, являющейся де-факто международным стандартом в области встроенных устройств. Методика осуществляет оценку расхода компонентами защиты заданных аппаратных ресурсов встроенных устройств целевой системы с использованием, предложенных в рамках MARTE проблемно-ориентированных доменов знаний и моделирования на основе языка UML. В соответствии с MARTE выделены четыре основные стадии методике по оценке следующих аппаратных ресурсов: вычислительных ресурсов (установленные домены знаний HW_Computing и HW_ProcessingMemory), коммуникационных ресурсов (HW_Communication), ресурсов хранения (домен HW_StorageManager) и энергоресурсов (домены HP_Power, HW_PowerSupply и HW_Battery) с определением численных нефункциональных показателей, определяющих величину расхода каждого ресурса. Для определения значений этих показателей используется понятие, так называемого, «сценария наихудшего выполнения», введенное в рамках MARTE, и аппаратных характеристик, заданных производителем конкретного программно-аппаратного компонента. При этом показатель ресурсопотребления рассчитывается по формуле gnr

(component) = gnr(ВУо) - gnr(ВУz), где ВУо – незащищенное встроенное устройство, ВУz - встроенное устройство, защищенное при помощи компонента защиты component. При этом выборка и минимизация расхода ресурса осуществляется путем моделирования и программной реализации целевых функций компонента защиты на физических реализациях встроенных устройств и их эмуляторах. Так, например, для каждого из имеющихся альтернативных алгоритмов удаленной аттестации критических бизнес-данных встроенного устройства определяется величина необходимой оперативной памяти (Кб), которое устройство должно предоставить, и объем коммуникационного ресурса, расходуемого на передачу аттестующих подписей доверенному серверу в единицу времени (Mbit/sec). Реализация и эксперименты по оценке ресурсопотребления компонентов защиты проведены на одноплатных компьютерах Raspberry Pi 2 Model B и Arduino Uno Rev3. Разработанная методика предназначена для комплексной оценки ресурсопотребления программных и программно-аппаратных компонентов защиты с целью последующего учета полученных значений в процессе комбинирования таких компонентов и их интеграции на конкретное встроенное устройство целевой системы.

9. Разработана и уточнена модель процесса конфигурирования компонентов защиты встроенных устройств с использованием экспертных знаний, эвристик и правил для осуществления многокритериального выбора компонентов защиты. Предложенное конфигурирование представляет собой процесс формирования комбинированного механизма защиты встроенных устройств с учетом характеристик отдельных компонентов защиты. Процесс включает следующие этапы: (1) определение функциональных требований к защите; (2) определение нефункциональных ограничений, существенных для проектируемого данного устройства; (3) для каждого функционального требования защиты выявление множества альтернатив компонентов защиты, которые его реализуют; (4) определение правил выбора компонентов защиты, исходя из связей между ними; (5) вычисление значений нефункциональных показателей для заданных компонентов; (6) упорядочивание альтернатив компонентов по степени ухудшения значений установленных нефункциональных ограничений; (7) определение порядка учета рассматриваемых нефункциональных показателей; (8) исследование альтернатив компонентов защиты и вычисление суммарных значений нефункциональных показателей наборов компонентов защиты, а также выбор оптимальной конфигурации.

10. Осуществлены моделирование с использованием языка UML и программная реализация прототипа средства конфигурирования, а также экспериментальная оценка его эффективности. Разработана архитектура прототипа программного средства конфигурирования компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами с использованием диаграмм классов, последовательностей и активностей языка моделирования UML с учетом принципов объектно-ориентированного проектирования. Данное средство представляет собой инструмент поддержки принятия решений о выборе компонентов защиты, позволяющий автоматизировать процессы их перебора и вычисления. Средство конфигурирования целесообразно применять, в особенности, в случае большого числа рассматриваемых функциональных требований защиты и имеющихся в наличие альтернатив компонентов защиты. Произведена оценка эффективности разработанного средства путем сравнения результатов конфигурирования с альтернативными путями комбинирования компонентов защиты без использования средств поддержки принятия решений по выбору компонентов защиты. Установлено преимущество использования разработанного программного средства, во-первых, в снижении в среднем потребления аппаратных ресурсов комбинированным механизмом защиты в процессе эксплуатации устройства и, во-вторых, в обеспечении возможности развертывания на устройства системы компонентов защиты, изначально более требовательных к ресурсам, но вместе с тем характеризующихся повышенной

защищенностью.
11. Проведен анализ и составлен обзор существующих моделей и методик верификации сетевых, программных, программно-аппаратных информационных потоков и выявления аномальных данных информационно-телекоммуникационных систем со встроенными устройствами. Проанализировано более 30 научных статей в предметной области верификации указанных разновидностей информационных потоков и выявления аномальных данных в системах со встроенными устройствами с учетом существующих программно-аппаратных решений и действующих российских и международных стандартов.
12. Разработана методика верификация информационных потоков на основе топологического анализа с использованием ориентированных графов для представления анализируемой информационно-телекоммуникационной системы. Методика состоит из двух стадий.
На стадии 1 формируются модели системы на базе графовых представлений топологии целевой системы с определением разновидностей встроенных устройств, их коммуникационных интерфейсов, пропускной способности коммуникационных каналов и др. характеристик. На стадии 2 производится вычисление показателей защищенности каждого информационного маршрута и проверка выполнимости установленных требований информационной безопасности. В частности, в рамках методики верификации решается задача определения устройств системы и их элементов, через которые проходят анализируемые информационные потоки с определением уровня защищенности информации в процессе прохождения ее через заданный узел маршрута. При обнаружении узлов с низким уровнем защищенности возможна обратная связь на уровень модели системы с целью изменения множества регламентируемых маршрутов прохождения информации для устранения отрезков маршрутов, снижающих уровень защищенности проходящих через них информационных потоков.
Методика позволяет подтвердить корректность информационных потоков в системе при передаче информации по определенному маршруту или выявить некоторое ожидаемое нежелательное свойство системы в рамках определенного маршрута в системе, обусловленное наличием в системе некоторой уязвимости. Для систем с большим количеством устройств число анализируемых путей может быть значительным, причем возможно большое количество ошибок первого рода, что существенно усложняет процесс верификации. Для снижения ложных срабатываний вводится дополнительная статическая семантика в модель процесса верификации. В общем случае нахождение всех маршрутов в графе является задачей класса NP, поэтому для верификации информационно-телекоммуникационной системы с большим числом задействованных встроенных устройств, сенсоров и соединений между ними применяются различные алгоритмы перебора, такие как алгоритм Дейкстры и др.
13. Разработана методика верификации информационных потоков на основе анализа политик безопасности и обнаружения конфликтов сетевых информационных потоков.
Методика определяет последовательность действий, выполняемых в процессе статического анализа спецификаций информационно-телекоммуникационной системы и входящих в нее устройств для выявления конфликтов и несогласованностей правил разрешения и запрета информационных потоков между отдельными устройствами с учетом специфицированной модели системы. На первом этапе исходные данные преобразуются в единый внутренний формат данных, после чего на втором этапе строится общая модель системы для верификации правил, представленная в виде конечного автомата и инициализированная входными данными во внутреннем формате. В рамках модели для задания аномалий используются формальные утверждения, выполнение которых обуславливает переход анализируемой системы в некорректное состояние. Методика осуществляется с использованием программных средств верификации на основе метода «проверки на модели»,

реализующих проверку выполнимости правил разрешения и запрета информационных потоков. Верификация позволяет определить все некорректные состояния анализируемой системы согласно заданным правилам. В общем случае результатом методики является описание обнаруженных аномалий и информационных потоков, которые приводят к появлению данных аномалий.

14. Предложена методика выявления аномальных данных от сенсоров в информационно-телекоммуникационных системах со встроенными устройствами на основе ограничений и правил функционирования целевой системы. К анализируемым атакам относятся киберфизические атаки, включающие физические воздействия на сенсоры для искажения данных с последующими программно-информационными воздействиями на компоненты системы; атака подмены сенсора; воздействия на аппаратные порты устройств, в том числе беспроводные сетевые порты, такие как RFID-сканеры и датчики инфракрасного излучения. Методика определяет последовательность действий, которые необходимо выполнять в процессе мониторинга событий безопасности целевой системы для выявления физических, кибернетических и киберфизических атакующих воздействий с использованием сенсоров на устройствах системы. В частности, правила учитывают бизнес-правила системы, историю показаний сенсоров, значения текущего времени, даты, допустимых ограничений на значения данных от сенсоров, согласованность этих данных с внешними источниками данных, такими как базы данных, облачные хранилища и др. Методика реализована в рамках программно-аппаратного прототипа системы Умного дома с использованием Raspberry Pi. Промоделирована атака на сенсор температуры, направленная на завышение реальных показаний температуры. В результате этого в соответствии с бизнес-логикой системы производится включение энергозатратного устройства охлаждения – кондиционера, что приводит к бесцельному расходу энергоресурсов и соответственно неоправданным материальным расходам. Промоделированные действия атакующего представляет собой кибер-физическую атаку, которая включает замену подлинного сенсора на модифицированный, а также предварительное исследование атакующим объекта атаки и подготовку необходимых атакующих средств, включая задание соответствующих электротехнических параметров используемого микроконтроллера.

15. Реализован программный прототип средств верификации сетевых информационных потоков с использованием верификатора SPIN и получена оценка эффективности предложенных методик. Данный прототип производит итеративный перебор и анализ возможных состояний, в которое механизм управления информационными потоками может прийти в процессе его работы. Прототип ориентирован на обнаружение скрытых противоречий между заданными правилами системы. Процесс перебора правил производится в порядке уменьшения их приоритета и продолжается до момента первого срабатывания каждого из правил. Использование приоритезации обеспечивает возможность комплексного управления правилами контроля информационных потоков с заданием правил, применяемых по умолчанию. Верификация спецификаций систем с числом правил более 40 шт. с заданием различных конфигураций целевой системы на основе различных типов коммуникационных интерфейсов, разновидностей встроенных устройств и ролей пользователей с различными правами доступа подтвердила применимость предложенной методики на практике.

3.6 Сопоставление полученных результатов с мировым уровнем

Все результаты, полученные в процессе выполнения проекта соответствуют мировому уровню. Исполнители проекта опубликовали полученные результаты в ряде журналов, сборников и трудов конференций, индексируемых в базах Scopus и РИНЦ и входящих в список ВАК, 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.; Семнадцатой Международной конференции «РусКрипто'2015» по криптологии, криптографии, информационной безопасности и защите данных, Московская область, г. Солнечногорск, 17-20 марта 2015 г.; Международном конгрессе по интеллектуальным системам и информационным технологиям IS&IT, Краснодарский край, пос. Дивноморское, 2-9 сентября 2015 г.; 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, 29 июня - 2 июля 2015 г.; LI Международной научно-практической заочной конференции «Технические науки - от теории к практике», Новосибирск, 26 октября 2015 г.; IX Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России» (ИБРР-2015), 28-30 октября 2015 г.; LII Международной научно-практической заочной конференции «Технические науки - от теории к практике», Новосибирск, 18 ноября 2015 г.; XIX Международной конференции по мягким вычислениям и измерениям (SCM'2016); Восемнадцатой Международной конференции «РусКрипто'2016»; конференции «Информационные технологии в управлении» (ИТУ-2016); 25-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»; Конгрессе по интеллектуальным системам и информационным технологиям IS-IT'16; Конференции региональная информатика «РИ-2016»; XXIX Международной научной конференции «Математические методы в технике и технологиях – ММТТ-29» (2016).

3.7.1 Методы и подходы, использованные в ходе выполнения Проекта (описать, уделив особое внимание степени оригинальности и новизны)

(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 и незащищенных информационных потоков в системе. 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 свойств защиты («деревьев свойств»), доменно-ориентированных представлений систем и компонентов защиты, знаний о скрытых несовместимостях и конфликтах компонентов защиты, потоков данных в системе и правилах управления ими.
(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 и аномалий в системе, ориентированный на обнаружение в процессе проектирования информационно-телекоммуникационных систем конфликтов между компонентами защиты и аномальных данных от сенсоров устройств, которые, как правило, проявляться на стадии эксплуатации системы. Знания об известных видах конфликтов и аномалий получаются путем экспертного анализа и моделирования систем со встроенными устройствами.
(6) Подход к получению экспертных знаний в области информационной безопасности встроенных устройств для построения моделей и методик конфигурирования, оценки ресурсопотребления и выявления несовместимостей компонентов защиты с использованием иерархически организованных структур функциональных и нефункциональных характеристик («деревьев свойств»), доменно-ориентированных представлений и знаний о скрытых несовместимостях компонентов защиты.
(7) Методы аналитического моделирования компонентов защиты с определением их функциональных и нефункциональных характеристик, связей, конфликтов и аномалий между компонентами защиты в информационно-телекоммуникационных системах со встроенными устройствами с использованием языка UML.
(8) Методы программного моделирования компонентов защиты в части оценки их ресурсопотребления на основе концепции моделирования встроенных устройств MARTE с использованием проблемно-ориентированных доменов знаний, языка моделирования UML и программно-аппаратных средств платформ Raspberry Pi и Arduino.
(9) Оптимизационный подход к конфигурированию компонентов защиты с использованием существующих моделей нарушителя встроенных устройств, эвристик для определения порядка учета нефункциональных требований и правил для осуществления многокритериального выбора компонентов защиты.
(10) Подход к экспериментальной оценке эффективности средств конфигурирования путем сравнений найденного решения с результатами альтернативных путей комбинирования программно-аппаратных компонентов защиты встроенных устройств.
(11) Метод «проверки на модели» для осуществления формальной верификации спецификаций информационно-телекоммуникационных систем с применением моделирования, перебора и оценки корректных и некорректных состояний, в которые переходит система в зависимости от набора заданных тестовых данных и сформулированных правил выявления конфликтов и аномалий, заложенных в спецификации системы.
(12) Подход к верификации информационных потоков на основе

топологического анализа с применением аппарата построения и анализа ориентированных графов для моделирования топологии информационно-телекоммуникационной системы, анализа защищенности устройств и маршрутов в системе с учетом связей между отдельными устройствами и уровня защищенности каждого из них.
(13) Подход к анализу данных от встроенных устройств на основе ограничений и правил функционирования целевой системы с учетом специфики конкретных видов сенсоров, их допустимых диапазонов значений, способов подключения сенсоров к устройству, критичности получаемых от сенсоров данных, их точности и достоверности.

3.7.1 Вклад каждого члена коллектива в выполнение Проекта в 2016 году (указать работу, выполненную каждым членом коллектива по Проекту в 2016 году с новой строки)

Десницкий В.А. - руководство работой по Проекту, разработка и уточнение предложенных методик верификация информационных потоков, анализ полученных результатов.
Чечулин А.А. - реализация программного прототипа средств верификации сетевых информационных потоков с использованием метода «проверки на модели» и оценка эффективности предложенных методик.
Саенко И.Б. - разработана методики выявления аномальных данных от сенсоров в информационно-телекоммуникационных системах со встроенными устройствами на основе ограничений и правил функционирования целевой системы, составление обзора работ по тематике верификации информационных потоков и выявления аномальных данных в системах со встроенными устройствами.
Дойникова Е.В. - формирование стадий методики верификация информационных потоков на основе топологического анализа с использованием ориентированных графов для представления анализируемой информационно-телекоммуникационной системы.
Федорченко А.В. - подготовка исходных данных и анализ условий выполнимости методики верификация информационных потоков на основе топологического анализа с использованием ориентированных графов для представления анализируемой информационно-телекоммуникационной системы.
Браницкий А.А. - подготовка исходных данных для методики верификации информационных потоков на основе анализа политик безопасности и обнаружения конфликтов сетевых информационных потоков.
Комашинский Д.В. - поиск англоязычных источников научно-технической литературы по тематике верификации сетевых, программных, программно-аппаратных информационных потоков и выявления аномальных данных информационно-телекоммуникационных систем со встроенными устройствами.
Новикова Е.С. - поиск российских источников научно-технической литературы по тематике верификации сетевых, программных, программно-аппаратных информационных потоков и выявления аномальных данных информационно-телекоммуникационных систем со встроенными устройствами.

3.8.1 Количество научных работ по Проекту, опубликованных в 2016 году (цифрами) (пункт заполняется автоматически, выводится количество заполненных 509 форм)

18

3.8.1.1 Из них в изданиях, включенных в перечень ВАК

3

3.8.1.2 Из них в изданиях, включенных в библиографическую базу данных РИНЦ

10

Из них в изданиях, включенных в международные системы цитирования
3.8.1.3 (библиографические и реферативные базы научных публикаций)

1

Количество научных работ, подготовленных в ходе выполнения Проекта и принятых к печати в 2016 году(пункт заполняется автоматически, выводится
3.8.2 количество заполненных 509 форм)

0

Участие в 2016 году в научных мероприятиях по тематике Проекта (каждое
3.9 мероприятие с новой строки, указать названия мероприятий и тип доклада)

- XIX International Conference on Soft Computing and Measurements (SCM'2016), St. Petersburg, May 25-27, 2016 (один секционный доклад);
- 9-я конференция «Информационные технологии в управлении» (ИТУ-2016), 4-6 октября 2016 г., Санкт-Петербург (четыре секционных доклада);
- 25-я научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», 4 июля - 7 июля 2016 г., Санкт-Петербург (один секционный доклад);
- XV Санкт-Петербургская Международная Конференция «Региональная информатика-2016» («РИ-2016»). Санкт-Петербург, 26-28 октября, 2016 г. (два секционных доклада);
- XXIX Международная научная конференция «Математические методы в технике и технологиях – ММТТ-29», 31 мая - 3 июня 2016 года, Санкт-Петербургский государственный технологический институт, Санкт-Петербург, Россия (один секционный доклад).

Участие в 2016 году в экспедициях по тематике Проекта, которые проводились
3.10 при финансовой поддержке Фонда (указать номера проектов)

-

Адреса (полностью) ресурсов в Интернете, подготовленных авторами по
3.12 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

Библиографический список всех публикаций по проекту за весь период выполнения проекта, в порядке значимости: монографии, статьи в научных
3.13 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. (Scopus, РИНЦ).
2. Desnitsky V.A., Kotenko I.V. Design and Verification of Secure Systems with Embedded Devices on the basis of Expert Knowledge // Automatic Control and Computer Sciences, № 8, 2015, Springer, 2015. (Scopus, РИНЦ).
3. Vasily Desnitsky, Igor Kotenko. Event analysis for security incident management on a perimeter access control system // XIX International Conference on Soft Computing and Measurements (SCM'2016). IEEE Xplore, 2016. P.481-483. DOI: 10.1109/SCM.2016.7519819. (SCOPUS, WEB OF SCIENCE)

4. Десницкий В.А., Котенко И.В. Формирование экспертных знаний для разработки защищенных систем со встроенными устройствами // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015, С. 35-41. (ВАК, РИНЦ).
5. Саенко И.Б., Котенко И.В. Применение средств генетической оптимизации и визуального анализа для формирования схем доступа в виртуальных локальных вычислительных сетях // Информационные технологии и вычислительные системы, № 1, 2015, С.33-46. (ВАК, РИНЦ).
6. Котенко И.В., Чечулин А.А., Комашинский Д.В. Автоматизированное категорирование веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Проблемы информационной безопасности. Компьютерные системы, № 2, 2015. С.69-79. (ВАК, РИНЦ).
7. 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.
8. 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.
9. Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.С., Коломеец М.В. Комбинированная методика проектирования защищенных кибер-физических устройств // Труды СПИИРАН. 2016. Вып. 5(48). С.5-31. (ВАК, РИНЦ)
10. Александров В.А., Десницкий В.А. Чалый Д.Ю. Разработка и анализ защищенности фрагмента информационно-телекоммуникационной системы, реализующей концепцию Интернета вещей // Моделирование и анализ информационных систем. Т. 23. №6. 2016. С.767-776.
11. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. Вып. 2(45). С.207-244. DOI: http://dx.doi.org/10.15622/sp.45.13 (ВАК, РИНЦ)
12. Новикова Е.С., Котенко И.В. Выявление аномальной активности в сервисах мобильных денежных переводов с помощью RADViz-визуализации // Труды СПИИРАН. 2016. Вып. 5(48). С.32-13. (ВАК, РИНЦ).
13. 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.
14. 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.
15. 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.
16. Десницкий В.А. Конфигурирование компонентов защиты встроенных устройств на основе эвристического подхода // Журнал «Технические науки — от теории к практике». Изд. НП "СибАК", №10 (46), 2015, С.16-20. (РИНЦ).
17. Десницкий В.А. Методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами // Журнал "Технические науки - от теории к практике", №11 (47). Изд. НП "СибАК", 2015, С.14-18. (РИНЦ).
18. Десницкий В.А., Дойникова Е.В. Архитектура и оценка эффективности программного средства конфигурирования компонентов защиты систем со встроенными устройствами // Журнал "Технические науки - от теории к практике", №11 (47). Изд. НП "СибАК", №47, 2015, С.14-18. (РИНЦ).
19. Десницкий В.А. Выявление аномальных данных от сенсоров встроенных устройств на основе экспертных знаний // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.676-679.
20. Десницкий В.А. Реализация средства верификации сетевых

информационных потоков с использованием метода «проверки на модели» // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.680-683.
21. Дойникова Е.В., Федорченко А.В. Методики автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности в системах взаимодействующих сервисов // XXIX Международная научная конференция "Математические методы в технике и технологиях - ММТТ-29", 31 мая - 3 июня 2016 года, Санкт-Петербургский государственный технологический институт, Санкт-Петербург, Россия.
22. Чечулин А.А. Алгоритмы построения и модификации моделей атак для анализа защищенности компьютерных сетей // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.782-785.
23. Дойникова Е.В., Котенко И.В. Методика оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С. 694-699.
24. 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.
25. 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.
26. 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.
27. 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.
28. 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/
29. 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.
30. 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.
31. 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.
32. 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.
33. 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.
2015:
34. Десницкий В.А. Методика выявления функциональных и нефункциональных несовместимостей между компонентами защиты встроенных устройств информационно-телекоммуникационных систем // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.70-71.
35. Десницкий В.А. Модели процесса разработки комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'15, 2015, Том 2. С. 113-118.
36. Десницкий В.А. Модель процесса конфигурирования компонентов защиты встроенных устройств // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 65-66.
37. Десницкий В.А. Методика оценки ресурсопотребления компонентов защиты встроенных устройств // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 66-67.
38. Бушуев С.Н., Десницкий В.А. Формирование экспертных знаний для разработки защищенных систем "Интернета вещей" // Семнадцатая Международная конференция “РусКрипто’2015”. Московская область, г.Солнечногорск, 17-20 марта 2015 г. http://www.ruscrypto.ru/.
39. Десницкий В.А. Методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.69-70.
40. Левшун Д.С., Чечулин А.А., Коломеец М.В., Котенко И.В. Архитектура системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 76.
41. Чечулин А.А. Классификация и модели представления связей между объектами в компьютерных сетях // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'15, 2015, Том 2. С. 165-170.
42. Чечулин А.А. Математические модели и алгоритмы моделирования атак и выработки контрмер в режиме, близком к реальному времени // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность

регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 90.
43. Браницкий А.А. Методы вычислительного интеллекта для обнаружения и классификации аномалий в сетевом трафике // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 61-62.
44. Федорченко А.В. Правило-ориентированный метод корреляции событий безопасности в SIEM-системах // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 86-87.
45. Котенко И.В., Новикова Е.С., Архипов Ю.А. Визуализация метрик защищенности для мониторинга безопасности и управления инцидентами // Семнадцатая Международная конференция "РусКрипто'2015". Московская область, г.Солнечногорск, 17-20 марта 2015 г. http://www.ruscrypto.ru.
46. Десницкий В.А., Левшун Д.С. Выбор и комбинирование элементов для построения комплексной системы кибер-физической безопасности // Восемнадцатая Международная конференция "РусКрипто'2016". Московская область, г.Солнечногорск, 22-25 марта 2016 г. http://www.ruscrypto.ru.
47. Десницкий В.А. Подход к верификации информационных потоков систем Интернета вещей // Материалы 25-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 4 июля - 7 июля 2016 г. Санкт-Петербург. Издательство Политехнического университета. 2016. С.34-35.
48. Десницкий В.А. Выявление аномальных данных от сенсоров в информационно-телекоммуникационных системах со встроенными устройствами // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'16, 2016, Том 1. С.217-223.
49. Десницкий В.А., Чечулин А.А. Методики верификации информационных потоков в системах интернета вещей // XV Санкт-Петербургская Международная Конференция "Региональная информатика-2016" ("РИ-2016"). Материалы конференции. СПб., 2016. С 156 - 157.
50. Десницкий В.А., Александров В.А. Модель нарушителя информационно-телекоммуникационных систем Интернета вещей // XV Санкт-Петербургская Международная Конференция "Региональная информатика-2016" ("РИ-2016"). Материалы конференции. СПб., 2016. С 155 - 156.
51. Федорченко А.В., Котенко И.В. Методики корреляции событий безопасности для обнаружения целевых атак // Восемнадцатая Международная конференция "РусКрипто'2016". Московская область, г.Солнечногорск, 22-25 марта 2016 г. http://www.ruscrypto.ru.
52. Десницкий В.А., Котенко И.В. Компонент сбора данных о системе для проектирования, верификации и тестирования компонентов защиты информационно-телекоммуникационных систем, реализующих концепцию Интернет вещей. Свидетельство № 2015615411. Зарегистрировано в Реестре программ для ЭВМ 18.05.2015.
53. Десницкий В.А. Программное средство представления исходных данных для конфигурирования компонентов защиты встроенных устройств. Свидетельство № 2015662185. Зарегистрировано в Реестре программ для ЭВМ 18.11.2015.
54. Десницкий В.А. Генератор отчетных форм анализа защищенности систем Интернета вещей. Свидетельство № 2015662184. Зарегистрировано в Реестре программ для ЭВМ 18.11.2015.
55. Десницкий В.А., Котенко И.В. Программное средство оценки эффективности конфигурирования компонентов защиты систем Интернета вещей. Свидетельство № 2015662025. Зарегистрировано в Реестре программ для ЭВМ 16.11.2015.
56. Десницкий В.А. Компонент обнаружения аномальных данных от сенсоров для системы контроля температурного режима помещения. Свидетельство №

2016663374. Зарегистрировано в Реестре программ для ЭВМ 06.12.2016. 57. Десницкий В.А., Котенко И.В. Компонент оценки эффективности верификации информационных потоков на основе метода проверки на модели. Свидетельство № 2016663477, Зарегистрировано в Реестре программ для ЭВМ 08.12.2016.

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

Информационно-телекоммуникационные системы

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

Технологии и программное обеспечение распределенных и высокопроизводительных вычислительных систем

3.16 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 работы над проектом получены следующие важнейшие результаты. Разработана обобщенная модель нарушителя встроенного устройства на основе анализа классификаций нарушителя по уровню взаимодействия нарушителя со встроенным устройством и по возможностям нарушителя. 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.

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. 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.

Разработана модель знаний о встроенном устройстве. Введение модели знаний в процесс разработки систем со встроенными устройствами направлено, в частности, 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.

Разработана концептуальная комбинированная модель системы защиты встроенных устройств. 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. 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.

Разработана методика выявления функциональных и нефункциональных несовместимостей компонентов защиты встроенных устройств информационно-телекоммуникационных систем. Целью методики является верификация механизмов защиты системы в части выявления в процессе ее проектирования скрытых несовместимостей, в которые вовлечены отдельные компоненты защиты, устанавливаемые на устройства системы. Отметим, что способ разрешения несовместимостей индивидуален и определяется в зависимости от специфики конкретной несовместимости и вовлеченных в нее компонентов защиты. В качестве вариантов разрешения возможен пересмотр одного или нескольких компонентов защиты, изменение способа их интеграции, корректировка требований к защите или спецификации устройства. Кроме того более раннее выявление несовместимостей, осуществляемое на стадии формирования требований к защите будет способствовать сокращению количества итераций процесса разработки целевой информационно-телекоммуникационной системы и снижению его сложности.

Разработана методика оценки ресурсопотребления компонентов защиты с использованием концепции моделирования и анализа встроенных устройств и систем реального времени и на основе методологии MARTE, являющейся де-факто международным стандартом в области встроенных устройств. Реализация и эксперименты по оценке ресурсопотребления компонентов защиты проведены на одноплатных компьютерах Raspberry Pi 2 Model B и Arduino Uno Rev3. Разработанная методика предназначена для комплексной оценки ресурсопотребления программных и программно-аппаратных компонентов защиты с целью последующего учета полученных значений в процессе комбинирования таких компонентов и их интеграции на конкретное встроенное устройство целевой системы.

Разработана и уточнена модель процесса конфигурирования компонентов защиты встроенных устройств с использованием экспертных знаний, эвристик и правил для осуществления многокритериального выбора компонентов защиты. Предложенное конфигурирование представляет собой процесс формирования комбинированного механизма защиты встроенных устройств с учетом характеристик отдельных компонентов защиты.

Осуществлены моделирование с использованием языка UML и программная реализация прототипа средства конфигурирования, а также экспериментальная оценка его эффективности. Разработана архитектура прототипа программного средства конфигурирования компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами с использованием диаграмм классов, последовательностей и активностей языка моделирования UML с учетом принципов объектно-ориентированного проектирования. Данное средство представляет собой инструмент поддержки принятия решений о выборе компонентов защиты, позволяющий автоматизировать процессы их перебора и вычисления.

Разработана методика верификация информационных потоков на основе топологического анализа с использованием ориентированных графов для представления анализируемой информационно-телекоммуникационной системы. Методика состоит из двух стадий. Методика позволяет подтвердить корректность информационных потоков в системе при передаче информации по определенному маршруту или выявить некоторое ожидаемое нежелательное свойство системы в рамках определенного маршрута в системе, проявляемое, обусловленное наличием в системе некоторой уязвимости. Для систем с большим количеством устройств число анализируемых путей может быть значительным, причем возможно большое количество ошибок первого рода, что существенно усложняет процесс верификации. Для снижения ложных срабатываний вводится дополнительная статическая семантика в модель процесса верификации.

Разработана методика верификации информационных потоков на основе анализа политик безопасности и обнаружения конфликтов сетевых информационных потоков. Методика определяет последовательность действий, выполняемых в процессе статического анализа спецификаций информационно-телекоммуникационной системы и входящих в нее устройств для выявления конфликтов и несогласованностей правил разрешения и запрета информационных потоков между отдельными устройствами с учетом специфицированной модели системы.

Предложена методика выявления аномальных данных от сенсоров в информационно-телекоммуникационных системах со встроенными устройствами на основе ограничений и правил функционирования целевой системы. К анализируемым атакам относятся киберфизические атаки, включающие физические воздействия на сенсоры с последующими программно-информационными воздействиями на компоненты системы в результате искажения данных; атака подмены сенсора; воздействия на аппаратные порты устройств, в том числе беспроводные сетевые порты, такие как RFID-сканеры и датчики инфракрасного излучения. Методика определяет последовательность действий, которые необходимо выполнять в процессе мониторинга событий безопасности целевой системы для выявления инцидентов, классифицируемых как признаки физических, кибернетических и киберфизических атакующих воздействий с использованием сенсоров на устройствах системы. Методика реализована в рамках программно-аппаратного прототипа системы Умного дома с использованием Raspberry Pi. Промоделирована атака на сенсор температуры, направленная на завышение реальных показаний температуры.

Реализован программный прототип средств верификации сетевых информационных потоков с использованием верификатора SPIN и получена оценка эффективности предложенных методик. Прототип ориентирован на обнаружение скрытых противоречий между заданными правилами системы. Процесс перебора правил производится в порядке уменьшения их приоритета и осуществляется до момента первого срабатывания каждого из правил.

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. (Scopus, РИНЦ).

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. Desnitsky V.A., Kotenko I.V. Design and Verification of Secure Systems with Embedded Devices on the basis of Expert Knowledge // Automatic Control and Computer Sciences, № 8, 2015, Springer, 2015. (Scopus, РИНЦ).

Предложен 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. Цель работы – формирование, структуризация и уточнение экспертных знаний, характеризующие различные аспекты проектирования и верификации механизмов защиты встроенных устройств, а также поиск и адаптация существующих и разработка новых методик и автоматизированных программных инструментов для их последующего использования разработчиками устройств. Основной вклад настоящей статьи – предлагаемая методика проектирования и верификации на основе выявленных экспертных знаний в предметной области, нацеленная на разработку комбинированных механизмов защиты встроенных устройств с учетом показателей ресурсопотребления, а также возможных конфликтов и аномалий компонентов защиты и информационных потоков. Методика характеризуется заложенной в нее специфичной экспертной информацией о системных ресурсах встроенных устройств, типовых конфликтах и аномалиях. Методика включает следующие основные стадии: (1) конфигурирование компонентов защиты встроенного устройства; (2) верификация системы защиты на предмет выявления скрытых конфликтов; (3) верификации сетевых информационных потоков.

3. Vasily Desnitsky, Igor Kotenko. Event analysis for security incident management on a perimeter access control system // XIX International Conference on Soft Computing and Measurements (SCM'2016). IEEE Xplore, 2016. P.481-483. DOI: 10.1109/SCM.2016.7519819. (SCOPUS, WEB OF SCIENCE)

Работа посвящена вопросам анализа и управления инцидентами безопасности в информационно-телекоммуникационных системах Интернета вещей. Представлен общий подход к анализу событий безопасности на основе принципов проактивности, динамичности и многоаспектности. Предложены элементы программно-аппаратной реализации для системы управления инцидентами безопасности на примере кибер-физической системы контроля и управления доступом с использованием микроконтроллеров и RFID-сканеров.

4. Десницкий В.А., Котенко И.В. Формирование экспертных знаний для разработки защищенных систем со встроенными устройствами // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015, С. 35-41. (ВАК, РИНЦ).

Раскрывается подход к формированию экспертных знаний для разработки защищенных систем со встроенными устройствами. Комбинирование компонентов защиты, выявление аномальных данных в системе и структурных несовместимостей компонентов защиты производится на основе знаний о целевой системе, требованиях и компонентах защиты. Настоящая работа нацелена на формирование, структуризацию и уточнение экспертных знаний, характеризующих различные аспекты проектирования, верификации и тестирования механизмов защиты систем со встроенными устройствами, а также поиск и адаптацию существующих и разработку новых методик и автоматизированных программных инструментов для их последующего использования разработчиками устройств. Основной вклад настоящей статьи – методика проектирования, верификации и тестирования на основе выявленных экспертных знаний в предметной области в части комбинирования компонентов защиты с использованием эвристики, верификации системы для выявления известных видов несовместимостей компонентов защиты и тестирования системы на предмет выявления аномальных данных в них.

5. Саенко И.Б., Котенко И.В. Применение средств генетической оптимизации и визуального анализа для формирования схем доступа в виртуальных локальных вычислительных сетях // Информационные технологии и вычислительные системы, № 1, 2015, С.33-46. (ВАК, РИНЦ).

Рассматривается подход к проектированию виртуальной локальной вычислительной сети (ВЛВС), основанный на использовании программного средства генетической оптимизации и визуального анализа схемы доступа ВЛВС. Излагается формальная постановка задачи оптимизации схемы доступа ВЛВС, решение которой повышает надежность и безопасность функционирования корпоративной вычислительной сети. Показано, что рассматриваемая задача относится к одной из форм булевой матричной факторизации и является NP-полной. В разработанном генетическом алгоритме, предложенном для решения поставленной задачи, реализован ряд усовершенствований, касающихся формирования начальной популяции, вида функции пригодности, кодирования хромосом и выполнения операций скрещивания и мутации. Разработанное программное средство реализует генетический алгоритм, формирует визуальное отображение хода решения задачи и обеспечивает оценку решения задачи. Экспериментальные результаты показали высокую эффективность разработанного генетического алгоритма

6. Котенко И.В., Чечулин А.А., Комашинский Д.В. Автоматизированное категорирование веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Проблемы информационной безопасности. Компьютерные системы, № 2, 2015. С.69-79. (ВАК, РИНЦ).

В статье представлен подход к классификации веб-страниц с помощью методов интеллектуального анализа данных. Предложена архитектура и алгоритмы работы системы сбора, хранения и анализа данных, необходимой для классификации сайтов по определенным категориям. Разработана программная система для автоматизации классификации веб-страниц. Проведены эксперименты, выявившие основные проблемы, возникающие при построении систем классификации веб-страниц. Эксперименты, описанные в статье, показали высокую точность классификации веб-страниц, что подтверждает возможность использования разработанной технологии в системах блокирования веб-сайтов с неприемлемым содержимым.

7. 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.

8. 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".

9. Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.С., Коломеец М.В. Комбинированная методика проектирования защищенных кибер-физических устройств // Труды СПИИРАН. 2016. Вып. 5(48). С.5-31. (ВАК, РИНЦ)

С точки зрения информационной безопасности встроенные устройства представляют собой элементы сложных киберфизических систем, работающих в потенциально враждебном окружении. Поэтому разработка таких устройств является сложной задачей, часто требующей экспертных решений. Сложность задачи разработки защищенных встроенных устройств обуславливается различными типами угроз и атак, которым может быть подвержено устройство, а также тем, что на практике вопросы безопасности встроенных устройств обычно рассматриваются на финальной стадии процесса разработки в виде добавления дополнительных функций защиты. В статье предлагается методика проектирования, применение которой будет способствовать разработке безопасных и энергоэффективных киберфизических и встроенных устройств. Данная методика организует поиск наилучших комбинаций компонентов защиты на основе

решения оптимизационной задачи. Работоспособность предлагаемой методики демонстрируется на основе разработки прототипа защищенной системы охраны периметра помещения.

10. Александров В.А., Десницкий В.А. Чалый Д.Ю. Разработка и анализ защищенности фрагмента информационно-телекоммуникационной системы, реализующей концепцию Интернета вещей // Моделирование и анализ информационных систем. Т. 23. №6. 2016. С.767-776.

В работе исследуются вопросы разработки и реализации систем, использующих концепцию Интернета вещей. В условиях активного развития отраслей, использующих концепцию Интернета вещей, актуальна проблема информационной безопасности. Для того чтобы определить актуальные угрозы необходимо использовать детальный анализ рисков в соответствии с действующими стандартами ГОСТ. Выбирая защитные меры, необходимо учитывать все идентифицированные актуальных угроз информационной безопасности. В статье определяются актуальные угрозы и защитные меры, необходимые для разработки и внедрения защищенного фрагмента программно-аппаратной системы Умный дом в части контроля доступа в помещение. Решены следующие задачи: описание системы Умный дом, описание этапов оценки и обеспечения безопасности системы Умный дом; осуществление аппаратной сборки и написания программного кода для выбранного фрагмента системы; оценка безопасности выбранного фрагмента Умного дома и определение актуальных угроз; выработка рекомендаций по противодействию актуальным угрозам; программная реализация одной из актуальных угроз и программная реализация защитных мер для выбранной угрозы. Особенностью работы является комплексный подход к проектированию с использованием моделей нарушителя, анализа активов системы и оценки их защищенности.

11. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. Вып. 2(45). С.207-244. DOI: http://dx.doi.org/10.15622/sp.45.13 (ВАК, РИНЦ)

В работе рассматриваются различные методы обнаружения сетевых атак. Основное внимание уделяется построению обобщенной классификационной схемы методов обнаружения сетевых атак, представлению сущности каждого из рассмотренных методов и их сравнительному анализу в рамках предложенной классификационной схемы.

12. Новикова Е.С., Котенко И.В. Выявление аномальной активности в сервисах мобильных денежных переводов с помощью RADViz-визуализации // Труды СПИИРАН. 2016. Вып. 5(48). С.32-13. (ВАК, РИНЦ).

В настоящее время широкое распространение получили сервисы мобильных денежных переводов (СМДП), в которых ключевая роль принадлежит оператору мобильной связи. В работе авторы предлагают новый подход к анализу транзакций для выявления аномальной активности в СМДП, в основе которого лежит RadViz-визуализация ее пользователей. Особенностями данной методики визуализации являются возможность разбиения пользователей на группы, имеющих одинаковое поведение, и низкая вычислительная сложность. В работе представляются и обсуждаются результаты применения разработанной методики визуального анализа транзакций для выявления различных сценариев финансовых мошенничеств, характерных для сервисов мобильных денежных переводов.

13. 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.

14. 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.

15. 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.

16. Десницкий В.А. Конфигурирование компонентов защиты встроенных устройств на основе эвристического подхода // Журнал «Технические науки — от теории к практике». Изд. НП "СибАК", №10 (46), 2015, С.16-20. (РИНЦ).

Цель работы – разработка процесса конфигурирования компонентов защиты встроенных устройств в части комбинирования компонентов защиты. с использованием экспертных знаний в предметной области. В работе предложена эвристика для определения порядка учета нефункциональных характеристик в процессе комбинирования, а также используются правила для осуществления многокритериального выбора компонентов защиты.

17. Десницкий В.А. Методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами // Журнал "Технические науки - от теории к практике", №11 (47). Изд. НП "СибАК", 2015, С.14-18. (РИНЦ).

Цель работы – построение методики оценки ресурсопотребления компонентов защиты систем со встроенными устройствами. Методика используется в процессе конфигурирования встроенных устройств для нахождения наиболее эффективных конфигураций защиты. Методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем базируется на определениях и методологическом аппарате MARTE, разработанном в рамках международной рабочей группой OMG в области объектно-ориентированных технологий и стандартов. MARTE определяет в частности, следующие наиболее важные виды системных ресурсов: вычислительные ресурсы, коммуникационные ресурсы, ресурсы хранения и энергоресурсы с определенным численным нефункциональным показателем ресурсопотребления, который определяет величину расхода заданного ресурса в процессе работы встроенного устройства. В качестве примера можно привести следующие показатели «объем оперативной памяти устройства» и «объем передаваемых данных». Для определения значений этих показателей используется понятие так называемого «сценария наихудшего выполнения». При этом выборка и максимизация расхода ресурса осуществляется путем программного моделирования функций компонента защиты на физических реализациях встроенных устройств. Ограничения на ресурсные показатели встроенного устройства задают на основе данных, полученных из формальных спецификаций и значений, заданных производителем конкретного программно-аппаратного компонента.

18. Десницкий В.А., Дойникова Е.В. Архитектура и оценка эффективности программного средства конфигурирования компонентов защиты систем со встроенными устройствами // Журнал "Технические науки - от теории к практике", №11 (47). Изд. НП "СибАК", №47, 2015, С.14-18. (РИНЦ).

В работе исследуется программный прототип средства компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами на основе оптимизационного подхода к выбору комбинаций компонентов защиты (конфигурирование). Прототип реализует функцию конфигурирования, которая по установленным функциональным требованиям и нефункциональным ограничениям, а также перечню заданных альтернатив компонентов защиты определяет на выходе наиболее эффективную (оптимальную) конфигурацию защиты. Прототип содержит функцию проверки эффективности заданной конфигурации защиты в соответствии с заданным критерием. Целью работы является разработка архитектуры для программной реализации средства конфигурирования компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами. Предложенная архитектура базируется на использовании средств языка моделирования UML, принципах объектно-ориентированного программирования и теории принятия решений. Произведена оценка эффективности

разработанного средства путем сравнения результатов конфигурирования с альтернативными путями комбинирования компонентов защиты.

19. Десницкий В.А. Выявление аномальных данных от сенсоров встроенных устройств на основе экспертных знаний // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.676-679.

В работе исследуются экспертные знания в области информационно-телекоммуникационных систем для выявления аномальных данных от сенсоров встроенных устройств в результате атакующих воздействий на компоненты устройства. К таким атакам относятся физическое воздействие на сенсор, атака подмены сенсора, воздействия на коммуникационные интерфейсы устройства, подмена данных на устройстве с использованием злонамеренного программного обеспечения и др. Предложен подход к выявлению аномальных данных путем проверки ограничений на значения данных в соответствии с паттернами, задаваемыми для каждого из устройств системы. Реализован прототип системы «Умный дом» с использованием Raspberry Pi, реализующий предложенный подход и проведена его экспериментальная оценка. Проведены эксперименты и проанализированы их результаты. В качестве будущих исследований по данному направлению планируется построение комплексной среды тестирования готовых встроенных устройств на основе выявления конкретных знаний для разработки наборов тестов с учетом специфики систем Интернета вещей на некорректных, неполных и неожиданных входных данных, а также разработка системы правил для выявления таких атак в рамках компонента мониторинга.

20. Десницкий В.А. Реализация средства верификации сетевых информационных потоков с использованием метода «проверки на модели» // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.680-683.

В работе реализован подход к верификации информационных потоков в части проверки корректности политики контроля сетевых информационных потоков в информационно-телекоммуникационных системах со встроенными устройствами. Подход базируется на применении метода «проверки на модели» путем последовательного перебора правил разрешения и запрета информационных потоков в системе в порядке уменьшения их приоритета до факта первого срабатывания. Воспроизведение в динамике процесса контроля политики на модели некоторой системы позволяет выявлять аномальные правила политики, которые могу приводить к некорректной работе целевой системы. Программный прототип средств верификации реализован на языке Promela и использован для обоснования практической действенности и применимости предложенного подхода на практике.

21. Дойникова Е.В., Федорченко А.В. Методики автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности в системах взаимодействующих сервисов // XXIX Международная научная конференция "Математические методы в технике и технологиях - ММТТ-29", 31 мая - 3 июня 2016 года, Санкт-Петербургский государственный технологический институт, Санкт-Петербург, Россия.

Рассмотрены и классифицированы существующие подходы к автоматизированному реагированию на атаки. Выявлены недостатки существующих подходов. Предложен подход к автоматизированному реагированию на инциденты на основе графов атак и открытых стандартов по представлению информации по безопасности.

22. Чечулин А.А. Алгоритмы построения и модификации моделей атак для анализа защищенности компьютерных сетей // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.782-785.

В работе рассматриваются алгоритмы построения и модификации моделей атак для оценки защищенности компьютерных сетей. Для повышения скорости работы алгоритмов предлагается разбить общую последовательность действий, выполнение которых необходимо в зависимости от анализируемой компьютерной сети, изменений, происходящих в этой сети, и типов возможных нарушителей.

23. Дойникова Е.В., Котенко И.В. Методика оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С. 694-699.

В работе описывается методика оценки защищенности компьютерных сетей. Методика основана на комплексе показателей защищенности, вычисляемых на основе графов атак и графов зависимостей сервисов. Основным отличием методики является ее многоуровневая структура, объединяющая несколько уровней оценки и позволяющая оценить защищенность на каждом уровне в зависимости от имеющихся входных данных. Оценка защищенности основана на определении рисков компрометации компьютерной сети. В состав методики традиционно входит идентификация источников риска, анализ риска и сравнительная оценка риска. Для идентификации риска применяется модельно-методический аппарат, включающий представление входных данных в виде моделей сети (граф зависимости сервисов), атак (граф атак), атакующего, событий и контрмер, и ряд стандартов унифицированного представления данных по безопасности. На этапе анализа риска применяется комплекс показателей защищенности на основе графов атак и графов зависимостей сервисов и алгоритмы вычисления данных показателей. В том числе логический

вывод на основе графа зависимостей сервисов и матричные вычисления для определения критичности активов сети, Байесовский вывод для определения вероятности компрометации ресурсов сети и влияния событий на развитие атаки. Вычисляемые показатели определяются в зависимости от доступных входных данных. Сравнительная оценка результатов проводится путем сопоставления полученных количественных оценок риска качественной шкале. В докладе показано применение методики для оценки защищенности различных сетей и разных наборов входных данных.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. Десницкий В.А. Методика выявления функциональных и нефункциональных несовместимостей между компонентами защиты встроенных устройств информационно-телекоммуникационных систем // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.70-71.

В работе предложена методика выявления функциональных и нефункциональных несовместимостей между компонентами защиты встроенных устройств информационно-телекоммуникационных систем. В общем случае выявление несовместимостей является составной частью процесса выбора эффективных конфигураций защиты и проводится разработчиками информационно-телекоммуникационных систем в процессе проектирования. При этом несовместимость рассматривается, как отношение между двумя или более компонентами защиты и представляет собой противоречие между функционалами нескольких компонентов защиты, какими-либо их нефункциональными ограничениями и/или программно-аппаратной платформой устройства. Предложенная методика базируется на известных экспертных знаниях о существующих системах, устройствах, компонентах защиты и сценариях их взаимодействия. Выделяются три следующие типа несовместимостей: несовместимости вследствие недостаточной согласованности компонента защиты и спецификации устройства; несовместимости между функциями защиты нескольких компонентов; несовместимости между несколькими базовыми компонентами защиты в рамках комплексного компонента защиты. В работе приводятся примеры таких несовместимостей, полученные путем анализа существующих систем со встроенными устройствами. Отметим, что способ разрешения несовместимостей индивидуален и определяется в зависимости от специфики конкретной несовместимости и вовлеченных в нее компонентов защиты. В качестве вариантов разрешения рассматриваются пересмотр одного или нескольких компонентов защиты, изменение способа интеграции компонентов, корректировка требований к защите или спецификации устройства. Кроме того более раннее выявление несовместимостей,

осуществляемое на стадии формирования требований к защите будет способствовать сокращению количества итераций процесса разработки целевой информационно-телекоммуникационной системы и снижению его сложности.

35. Десницкий В.А. Модели процесса разработки комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'15, 2015, Том 2. С. 113-118.

В работе предложены модели для проектирования, верификации и тестирования комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами на основе знаний о существующих системах и компонентах защиты. Модели предназначены для разработки на их основе автоматизированных методик и программных средств, используемых в процессе проектирования, верификации и тестирования компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами. Под встроенным устройством понимается набор взаимосвязанных программно-аппаратных и программных модулей, процесс выполнения непосредственно связан с реакцией на различные процессы физического окружения. Примерами таких устройств являются устройства считывания текстовой, звуковой и другой информации с различных носителей, устройствами отображения, разнообразными коммуникационными устройствами, бытовыми и промышленными устройствами нагревания, вентиляции, устройствами мониторинга и диагностики, насосными станциями, системами поддержки навигации и другими. Цель работы – выявление экспертных знаний в области проектирования, верификации и тестирования систем со встроенными устройствами и разработка на их основе специализированных моделей, которые направлены на повышение защищенности целевых систем и автоматизацию процесса разработки таких систем.

36. Десницкий В.А. Модель процесса конфигурирования компонентов защиты встроенных устройств // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 65-66.

В работе предложена модель процесса конфигурирования компонентов защиты встроенных устройств, применение которой в процессе проектирования устройств будет способствовать разработке безопасных и энергоэффективных программно-аппаратных решений. Данная модель организует поиск наилучших комбинаций компонентов защиты на основе решения оптимизационной задачи с использованием экспертных знаний, эвристик и правил для осуществления многокритериального выбора компонентов защиты. Отличительной особенностью разработанной модели является учет функциональных и нефункциональных характеристик компонентов защиты, ограничений устройства и связей между компонентами с использованием оптимизационного подхода.

37. Десницкий В.А. Методика оценки ресурсопотребления компонентов защиты встроенных устройств // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 66-67.

Предлагаемая в работе методика оценки ресурсопотребления компонентов защиты используется в рамках процессов конфигурирования компонентов защиты встроенных устройств для определения эффективных наборов компонентов защиты, которые должны быть реализованы в рамках механизмов обеспечения информационной безопасности от широкого класса угроз. Методика включает действия по определению нефункциональных ограничений, существенных для проектируемого данного устройства. Источником возможных нефункциональных ограничений является методология MARTE (Modeling and Analysis of Real-Time Embedded Systems), являющаяся де-факто стандартом, разработанным в рамках международного консорциума OMG, где релевантные нефункциональные показатели, характерные для встроенных устройств, специфицированы с использованием языка моделирования UML. Фактически, MARTE определяет базовую систему понятий, программных и аппаратных характеристик устройств для поддержки процессов спецификации, синтеза, верификации, оценки производительности, количественного анализа и сертификации устройств с использованием специализированных UML-профилей. Вычисление численных значений показателей ресурсопотребления осуществляется с использованием методов программного моделирования, а также аналитически путем поиска и сопоставления фактических данных о характеристиках компонентов защиты, предоставленных организациями-производителями анализируемых программно- аппаратных компонентов. Предложенная методика апробирована в процессе проектирования защищенной системы охраны периметра помещения в части реализации функций контроля доступа с использованием одноплатных компьютеров Arduino и набора программных и программно-аппаратных компонентов для нее. На основе количественных данных, являющихся результатом методики выл выбран набор программных и программно-аппаратных компонентов из списков имеющихся альтернатив, применение которых позволило построить защищенную систему, с учетом улучшения ее целевых показателей, в том числе, цены и некоторых показателей ресурсопотребления.

38. Бушуев С.Н., Десницкий В.А. Формирование экспертных знаний для разработки защищенных систем "Интернета вещей" // Семнадцатая Международная конференция “РусКрипто’2015”. Московская область, г.Солнечногорск, 17-20 марта 2015 г. http://www.ruscrypto.ru/.

Доклад посвящен анализу знаний в области безопасности информационно-телекоммуникационных систем,

отличающихся разнородностью входящих в них устройств, структурно-функциональными особенностями и специфичным набором угроз информационной безопасности. Конкретные экспертные знания, выявленные при анализе систем концепции "Интернет вещей", используются в качестве основы для разработки специализированных методик и программных средств проектирования компонентов защиты для таких систем. Экспертные знания, используемые для тестирования информационно-телекоммуникационных систем Интернет вещей включают знания о конкретных видах атак на устройства системы, в том числе атаки на проводные и беспроводные коммуникационные интерфейсы, атаки на сенсоры, аналоговые или цифровые пины устройств, атаки типа отказ в обслуживании, атаки на истощение энергоресурсов устройств, работающих автономно и другие. Тестирование проводится на программном прототипе системы «Умный дом», который построен на базе устройств программно-аппаратных платформ Raspberry Pi и Arduino. При этом тестирование включает также процедуры выявления аномальных данных, поступающих от сенсоров в работающей системе, которые базируются на определенных правилах и ограничениях бизнес-логики системы, а также ожидаемых диапазонах значений целевых показателей системы. К примеру, аномальные данные от сенсора освещенности, сенсора температуры или показания приборов учета электропотребления Умного дома может рассматриваться в качестве признака какой-либо информационной или кибер-физической атаки на Умный дом путем подмены критически важных данных нарушителем.

39. Десницкий В.А. Методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.69-70.

В работе предложена методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами. Методика базируется на определениях и методологическом аппарате, предложенным в рамках методологии моделирования встроенных устройств и систем реального времени MARTE. MARTE задает следующие наиболее важные виды аппаратных ресурсов, которые учитываются в процессе комбинирования системы: вычислительные ресурсы, коммуникационные ресурсы, ресурсы хранения и энергоресурсы. Каждый ресурс характеризуется численным показателем ресурсопотребления – нефункциональным ресурсным свойством, определяющим величину его расхода в процессе функционирования устройства.

Методика оценки значения нефункциональных ресурсных свойств состоит из следующих стадий:

а) для циклически детерминированного устройства выделяются временные циклы, которыми можно ограничить анализ поведения физической реализации устройства или его программной модели. В противном случае должна рассматриваться вся «линия жизни» жизненного цикла устройства, что несколько затрудняет процесс получения значения свойства в техническом плане;

б) производится вычисление множества значений SampleRealizations. Как правило, эти значения представляют собой некоторые однотипные измерения, вычисляемые последовательно на различных фазах цикла. При этом процедура измерения представляет некоторую одномоментную «фиксацию» текущего состояния устройства и позволяет получить широкий спектр данных о процессе выполнения;

в) применение заданной вычисляющей функции на множестве полученных значений с целью вычисления искомого значения ресурсного свойства.

Для получения значений нефункционального ресурсного свойства компоненты защиты запускаются в рамках эмулятора устройства, или в качестве альтернативы процедура оценки свойства непосредственно встраивается в систему защиты. В последнем случае следует учитывать возможный побочный эффект данной процедуры и, возможно, корректировать получаемые значения.

40. Левшун Д.С., Чечулин А.А., Коломеец М.В., Котенко И.В. Архитектура системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 76.

Данная работа посвящена разработке архитектуры системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт. В статье рассматриваются основные функциональные требования к системам такого типа, на основе которых формируются альтернативные компонентные составы встроенных устройств. Также, на основе нефункциональных требований к системам такого типа был выбран оптимальный компонентный состав, который стал основой системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт.

41. Чечулин А.А. Классификация и модели представления связей между объектами в компьютерных сетях // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'15, 2015, Том 2. С. 165-170.

Современные информационные системы характеризуются большим объемом обрабатываемых данных, поэтому средства визуализации стали важным средством для решения задач анализа данных. Визуальный анализ данных позволяет значительно повысить эффективность работы аналитика благодаря использованию особенностей обработки зрительной информации человеком и возможностей вычислительных средств, предоставляя удобный инструмент по извлечению новых знаний из зашумленных данных большого объема. Одним из направлений в визуализации является визуализация компьютерных сетей. В данной работе предложена классификация и математические модели для представления связей между сетевыми объектами.

Разработанные модели позволят повысить эффективность процессов мониторинга и управления информационной безопасностью в информационно-телекоммуникационных системах.

42. Чечулин А.А. Математические модели и алгоритмы моделирования атак и выработки контрмер в режиме, близком к реальному времени // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 90.

Основной темой данной публикации является разработка новых математических моделей и алгоритмов моделирования атак и выработки контрмер, которые могли бы использоваться в условиях больших объемов исходных данных и производить анализ системы защиты в условиях проводящихся атак в режиме близком к реальному времени, и, как следствие, рекомендовать оператору способы изменения политики безопасности системы защиты за ограниченное время.

43. Браницкий А.А. Методы вычислительного интеллекта для обнаружения и классификации аномалий в сетевом трафике // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 61-62.

В работе рассматривается задача обнаружения и классификации сетевых атак с применением методов вычислительного интеллекта и различных способов их комбинирования.

44. Федорченко А.В. Правило-ориентированный метод корреляции событий безопасности в SIEM-системах // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 86-87.

Рассматриваются основы правило-ориентированного метода корреляции событий безопасности. Указаны особенности использования данного метода в SIEM-системах, а также описана возможные варианты применения на разных стадиях процесса корреляции

45. Котенко И.В., Новикова Е.С., Архипов Ю.А. Визуализация метрик защищенности для мониторинга безопасности и управления инцидентами // Семнадцатая Международная конференция “РусКрипто’2015”. Московская область, г.Солнечногорск, 17-20 марта 2015 г. http://www.ruscrypto.ru.

В статье представлен анализ существующих методов визуализации информации, относящейся к безопасности. Приведена архитектура визуальной модели для отображения набора метрик, которая позволяет проводить их сравнительный анализ. Разработанная визуальная модель может быть использована для представления разных типов метрик, в том числе и для традиционных параметров безопасности, таких как, например, сетевые потоки.

46. Десницкий В.А., Левшун Д.С. Выбор и комбинирование элементов для построения комплексной системы кибер-физической безопасности // Восемнадцатая Международная конференция “РусКрипто’2016”. Московская область, г.Солнечногорск, 22-25 марта 2016 г. http://www.ruscrypto.ru.

Доклад посвящен выбору и комбинированию различных элементов кибер-физической безопасности на примере построения комплексной системы безопасности с учетом функциональных и нефункциональных требований к защите, моделей нарушителя и оптимизационного подхода к выбору компонентов защиты с использованием программируемых микроконтроллеров в рамках платформы Arduino.

47. Десницкий В.А. Подход к верификации информационных потоков систем Интернета вещей // Материалы 25-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 4 июля - 7 июля 2016 г. Санкт-Петербург. Издательство Политехнического университета. 2016. С.34-35.

Предлагается подход к выявлению и использованию экспертных знаний в области информационной безопасности встроенных устройств, а также их дальнейшее применение в качестве шаблонов защиты в части проверки корректности информационных потоков в системе. Анализ информационных потоков систем Интернета вещей проводится, как на аппаратном уровне, когда проводится анализ физических связей между отдельными микросхемами, так и на программной уровне, когда анализируется исходный программ на некотором устройстве с построением графов потоков управления и потоков данных. В отличие от существующих программно-аппаратных средств, таких как SIFA, реализующих верификацию программных и/или аппаратных потоков, реализованная нами возможность отслеживания информационных потоков на сетевом уровне позволяет находить аномальное поведение системы и возможные ошибки составления политики контроля сетевых информационных потоков. Для верификации правил разрешения и запрета конкретных видов сетевых информационных потоков между устройствами системы применяется метод «проверки на модели». Разработанное программное средство, осуществляющее итеративный перебор возможных состояний, в которое может перейти система в процессе функционирования, нацелено на выявление скрытых противоречий между отдельными правилами системы.

48. Десницкий В.А. Выявление аномальных данных от сенсоров в информационно-телекоммуникационных системах со встроенными устройствами // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'16, 2016, Том 1. С.217-223.

Предложен подход к обнаружению аномальных данных от сенсоров систем со встроенными устройствами вследствие несанкционированных действий потенциального нарушителя. Подход

апробирован в рамках реализованного фрагмента защищенной системы Умного дома, проведен анализ полученных результатов. В дальнейшем планируется выявление разработки наборов тестов систем Интернета вещей с использованием методов fuzzy-тестирования на некорректных, неполных и неожиданных входных данных.

49. Десницкий В.А., Чечулин А.А. Методики верификации информационных потоков в системах интернета вещей // XV Санкт-Петербургская Международная Конференция "Региональная информатика-2016" ("РИ-2016"). Материалы конференции. СПб., 2016. С 156 - 157.

В работе предложены методики верификация информационных потоков в информационно-телекоммуникационных системах Интернета вещей на основе топологического анализа с использованием ориентированных графов для представления анализируемой информационно-телекоммуникационной системы и на основе анализа политик безопасности с использованием знаний о конфликтах сетевых информационных потоков. В рамках топологического анализа строится ориентированный граф, определяющий сетевые соединения между устройствами системы, и оцениваются различные пути в графе с точки зрения информационной безопасности. В рамках подхода, основанного на политиках безопасности, информационные потоки описываются с применение формальных средств спецификации и анализируются на предмет наличия противоречий между ними. В рамках методики верификации на основе топологического анализа производится выявление всех компонентов, которые лежат между двумя выбранными вершинами графа, как правило, между источником данных с высоким уровнем защищенности и вершиной с низким уровнем защищенности. Подобный анализ используется для определения периметра защиты или критически важного сегмента системы для того, чтобы оперативно устранить незащищенные компоненты системы или повысить их защищенность. В рамках методики верификации на основе политик безопасности производится оценка защищенности системы Интернета вещей путем проверки корректности политики безопасности этой системы и определения уровня соответствия информационных потоков в реальной системе заданной политике.

50. Десницкий В.А., Александров В.А. Модель нарушителя информационно-телекоммуникационных систем Интернета вещей // XV Санкт-Петербургская Международная Конференция "Региональная информатика-2016" ("РИ-2016"). Материалы конференции. СПб., 2016. С 155 - 156.

В работе предложен подход к разработке типовой модели нарушителя в системах Интернета вещей. Модель относится к классу аналитических моделей и специфицирует релевантные категории нарушителей информационной безопасности с указанием целей нарушителя, его возможностей и видов атакующих воздействий. Проведен анализ систем Интернета вещей на предмет их подверженности следующим классам атакующих воздействий: (1) атаки обратной разработки («реверсинг»), направленные на локализацию и последующую модификацию важнейших функций и данных внутри ПО устройств; (2) атаки на окружение выполняющегося программного обеспечения с использованием модифицированных виртуальных машин, эмулятор устройств, отладчиков и средств трассировки, которые позволяют отслеживать и перехватывать библиотечные вызовы процедур, динамически изменять содержимое регистров процессора и стека вызовов и без прямого воздействия на исполняемый программный код; (3) атаки «клонирования устройств», представляющие собой одновременное использование нарушителем двух физических экземпляров некоторого устройства системы – оригинального устройства и модифицированного.

51. Федорченко А.В., Котенко И.В. Методики корреляции событий безопасности для обнаружения целевых атак // Восемнадцатая Международная конференция "РусКрипто'2016". Московская область, г.Солнечногорск, 22-25 марта 2016 г. http://www.ruscrypto.ru.

Рассматриваются исследования целевых атак с целью разработки методов их обнаружения. Предлагается определение теоретических свойств и практических особенностей атак данного класса. Основу методик составляют различные способы корреляции получаемых событий безопасности. Описываются программный стенд испытаний разработанных методик и результаты оценки их результативности.

52. Десницкий В.А., Котенко И.В. Компонент сбора данных о системе для проектирования, верификации и тестирования компонентов защиты информационно-телекоммуникационных систем, реализующих концепцию Интернет вещей. Свидетельство № 2015615411. Зарегистрировано в Реестре программ для ЭВМ 18.05.2015.

Приводятся листинг и краткое описание работы программного средства компонент сбора данных о системе для проектирования, верификации и тестирования компонентов защиты информационно-телекоммуникационных систем, реализующих концепцию Интернет вещей.

53. Десницкий В.А. Программное средство представления исходных данных для конфигурирования компонентов защиты встроенных устройств. Свидетельство № 2015662185. Зарегистрировано в Реестре программ для ЭВМ 18.11.2015.

Приводятся листинг и краткое описание работы программного средства представления исходных данных для конфигурирования компонентов защиты встроенных устройств.

54. Десницкий В.А. Генератор отчетных форм анализа защищенности систем Интернета вещей. Свидетельство № 2015662184. Зарегистрировано в Реестре программ для ЭВМ 18.11.2015.

Приводятся листинг и краткое описание работы генератора отчетных форм анализа защищенности систем Интернета вещей.

55. Десницкий В.А., Котенко И.В. Программное средство оценки эффективности конфигурирования компонентов защиты систем Интернета вещей. Свидетельство № 2015662025. Зарегистрировано в Реестре программ для ЭВМ 16.11.2015.

Приводятся листинг и краткое описание работы программного средства программное средство оценки эффективности конфигурирования компонентов защиты систем Интернета вещей.

56. Десницкий В.А. Компонент обнаружения аномальных данных от сенсоров для системы контроля температурного режима помещения. Свидетельство № 2016663374. Зарегистрировано в Реестре программ для ЭВМ 06.12.2016.

Приводятся листинг и краткое описание работы программного средства обнаружения аномальных данных от сенсоров для системы контроля температурного режима помещения.

57. Десницкий В.А., Котенко И.В. Компонент оценки эффективности верификации информационных потоков на основе метода проверки на модели. Свидетельство № 2016663477, Зарегистрировано в Реестре программ для ЭВМ 08.12.2016.

Приводятся листинг и краткое описание работы компонента оценки эффективности верификации информационных потоков на основе метода проверки на модели.