Форма 503. РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1 Номер Проекта

14-07-00417

3.2 Название Проекта

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

3.3 Коды классификатора, соответствующие содержанию фактически проделанной работы (в порядке значимости) (поле заполняется автоматически, коды вносятся из заявки)

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

3.4 Объявленные ранее цели Проекта (заполняется автоматически из пункта 4.1. "Цель и задачи фундаментального исследования " формы 4 заявки. Внимание: в этом пункте были указаны цель и задачи на весь период выполнения Проекта)

Основными целями исследования на 2015 год является продолжение работ по разработке и экспериментальной оценке моделей и методик проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами с использованием экспертных знаний в предметной области, основывающихся на анализе моделей нарушителя и компонентов системы защиты, своевременном обнаружении аномалий и конфликтов информационной безопасности, возникающих в системе, оценке ресурсопотребления компонентов защиты.

3.5 Полученные в 2015 году важнейшие результаты

Получены следующие основные результаты:
1. 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.
2. 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(ВУo) - gnr(ВУz), где ВУo – 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.
3. 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.
Этап 1 процесса конфигурирования включает определение функциональных требований защиты на основе анализа спецификации встроенного устройства с использованием методов аналитического моделирования действий нарушителя и моделей нарушителя Рае и Абрахама. Этап 2 включает действия по определению нефункциональных ограничений, существенных для проектируемого устройства на основе проблемно-ориентированных доменов знаний MARTE. На этапе 3 процесса конфигурирования для каждого функционального требования защиты осуществляется определение множества альтернатив компонентов защиты, которые его реализуют с указанием конкретных криптографических примитивов. На этапе 4 осуществляется определение правил выбора компонентов защиты, исходя из связей между ними с учетом семантики компонентов защиты, установленных требований защиты и сценариев использования. Каждое такое правило представляется в виде формальной четверки, имеющей следующие элементы (req, Alts, reason, justif), где req - формулировка функционального требования защиты, Alts - набор альтернатив компонентов, каждый из которых реализует данное требование, reason - причинно-следственная связь в определении предпочтительности компонентов из Alts в зависимости рассматриваемых для данного требования нефункциональных показателей (т.е. формулировка критерия выбора) и justif - фактическое обоснование предлагаемого порядка предпочтительности компонентов из Alts для данного функционального требования защиты. На этапе 5 производится определение значений нефункциональных ограничений для заданных компонентов защиты следующими способами: путем сбора данных от конкретных производителей используемых программно-аппаратных модулей; эмпирически – на основе программного моделирования компонентов защиты (когда это возможно); экспертно – с учетом предыдущего опыта работы с данными или сходными компонентами. Этап 6 включает упорядочивание альтернатив компонентов защиты по степени ухудшения значений их нефункциональных ограничений.

Фактически, для каждого нефункционального показателя осуществляется упорядочивание компонентов защиты. Например, для учета энергопотребления имеющихся разновидностей некоторого программно-аппаратного компонента защиты возможные альтернативы упорядочиваются в соответствии с уменьшением величины потребляемого ими тока (измеряемого в mA).
На этапе 7 определяется порядок учета рассматриваемых нефункциональных ограничений в зависимости от критичности каждого из них с использованием предложенной эвристики. Данная эвристика задает общий алгоритм приоритезации нефункциональных ограничений встроенного устройства. По существу, для каждого нефункционального ограничения выделяется набор специфичных функциональных и нефункциональных признаков встроенного устройства, таких как "наличие постоянного источника питания", "возможность замены устройства или аккумулятора без ущерба для предоставляемых им сервисов", "высокая зависимость достижения бизнес-целей устройства от энергоресурсов" и др. Для каждого такого признака предопределено значение ранга (с заданием значений от 1 до 3, где 1 - низкая важность, 3 - высокая важность) в зависимости от критичности данного признака для выполнимости заданного нефункционального ограничения (например, ограничения на ресурс энергопотребления). В результате спецификация целевого встроенного устройства анализируется на предмет наличия у него обозначенных признаков. Для каждого нефункционального ограничения выбирается максимальное значение ранга по всем выявленным у разрабатываемого устройства признакам, в соответствии с которыми происходит упорядочивание уже, собственно, нефункциональных ограничений. При этом ограничения, получившие одинаковые результирующие значения ранга, упорядочиваются между собой согласно порядку, предопределенному экспертно.
На заключительном этапе 8 процесса конфигурирования осуществляются комбинаторный перебор альтернатив компонентов защиты и вычисление суммарных значений нефункциональных показателей наборов компонентов защиты (конфигураций). Этап включает также выбор оптимальной конфигурации на основе полученных значений.
4. 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.

3.6 Сопоставление полученных результатов с мировым уровнем

Все результаты, полученные в процессе выполнения проекта в 2015 году 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 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.

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

(1) 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.
(2) 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.
(3) 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.
(4) 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.
(5) Подход к экспериментальной оценке эффективности средств конфигурирования путем сравнений найденного решения с результатами

альтернативных путей комбинирования программно-аппаратных компонентов защиты встроенных устройств.

3.7.2 Вклад каждого члена коллектива в выполнение Проекта в 2015 году (указать работу, выполненную каждым членом коллектива по Проекту в 2015 году с новой строки)

Десницкий В.А. - руководство работой по Проекту, разработка методики оценки ресурсопотребления компонентов защиты, модели процесса конфигурирования компонентов защиты, прототипа средства конфигурирования.
Чечулин А.А. - разработка и уточнение модели процесса конфигурирования в части использования моделей нарушителя и разработка методики выявления функциональных и нефункциональных несовместимостей компонентов защиты.
Саенко И.Б. - разработка и уточнение модели процесса конфигурирования в части использования эвристик для осуществления выбора компонентов защиты, анализ путей оценки ресурсопотребления компонентов защиты.
Дойникова Е.В. - моделирование с использованием языка UML прототипа средства конфигурирования.
Федорченко А.В. - программная реализация прототипа средства конфигурирования.
Браницкий А.А. - экспериментальная оценка эффективности прототипа средства конфигурирования.
Комашинский Д.В. - поиск иностранных источников научно-технической литературы по тематике Проекта.
Новикова Е.С. - поиск российских источников научно-технической литературы по тематике Проекта.

3.8.1 Количество научных работ по Проекту, опубликованных в 2015 году (пункт заполняется автоматически, выводится количество заполненных 509 форм)

23

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

7

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

1

3.8.2 Количество научных работ, подготовленных в ходе выполнения Проекта и принятых к печати в 2015 году (цифрами)

1

3.9 Участие в 2015 году в научных мероприятиях по тематике Проекта (указать названия мероприятий и тип доклада)

- Семнадцатая Международная конференция «РусКрипто'2015» по криптологии, криптографии, информационной безопасности и защите данных, Московская область, г. Солнечногорск, 17-20 марта 2015 г., (два секционных доклада);
- Международный конгресс по интеллектуальным системам и информационным технологиям “IS&IT”, Краснодарский край, пос. Дивноморское, 2-9 сентября 2015 г. , доклад на секции (два секционных доклада);
- 24-я научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, 29 июня - 2 июля 2015 г., доклад на секции (два секционных доклада);
- LI Международная научно-практическая заочная конференция «Технические науки - от теории к практике», Новосибирск, 26 октября 2015 г., статья на конференцию (секционный доклад);
- IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015), 28-30 октября 2015 г., (шесть секционных докладов);
- LII Международная научно-практическая заочная конференция «Технические науки - от теории к практике», Новосибирск, 18 ноября 2015 г, статья на конференцию (два секционных доклада).

3.10 Участие в 2015 году в экспедициях по тематике Проекта, которые проводились при финансовой поддержке Фонда (указать номера проектов)

-

3.11 Финансовые средства, полученные в 2015 году от Фонда (указать общий объем, в руб.)

600000,00

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

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

3.13 Библиографический список всех публикаций по Проекту, опубликованных в 2015 году, в порядке значимости: монографии, статьи в научных изданиях, тезисы докладов и материалы съездов, конференций и т.д.

1. 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).
2. 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).
3. 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).

4. 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).
5. 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).
6. 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).
7. 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).
8. 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.
9. 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.
10. 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.
11. 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.
12. 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/.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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/.
20. 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.
21. 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.
22. Десницкий В.А. Генератор отчетных форм анализа защищенности систем Интернета вещей. Свидетельство № 2015662184. Зарегистрировано в Реестре программ для ЭВМ 18.11.2015.
23. 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.

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 доступа к широкополосным мультимедийным услугам

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 второго этапа проекта была 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.

Также 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. Для определения значений показателей ресурсопотребления 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(ВУo) - gnr(ВУz), где ВУo – незащищенное встроенное устройство, ВУz - встроенное устройство, защищенное при помощи компонента защиты component.

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. 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.

Также 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.

Аннотации публикаций

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

Приводится 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.

21. 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.

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

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

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

23. 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.

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