Форма 503 (итог). РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1 Номер Проекта

13-01-00843

3.2 Название Проекта

Математические модели и методы мониторинга и управления информационной безопасностью в компьютерных сетях и системах критических инфраструктур, основывающиеся на интеллектуальных сервисах защиты информации

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

01-217, 01-202, 01-216, 07-235, 07-241

3.4 Объявленные ранее цели Проекта (заполняется автоматически из пункта 10.4 "Цели на 2015 год, связь с основной задачей Проекта" формы 510 отчета за 2014 год)

Основные цели исследований на 2015 год связаны с дальнейшим продолжением работ по разработке и экспериментальной оценке моделей и методов мониторинга и управления информационной безопасностью в компьютерных сетях и системах критических инфраструктур, основывающихся на интеллектуальных сервисах защиты информации, в частности, сбора и корреляции событий и информации безопасности, анализа событий безопасности и прогнозирования атакующих действий нарушителя, выработки решений по реагированию на целевые компьютерные атаки и сетей, выявления основного смыслового содержимого веб-сайтов для определения нежелательной и вредоносной информации.

3.5 Полученные в ходе выполнения Проекта важнейшие результаты

1. Проведен детальный анализ состояния современных исследований в области построения интеллектуальных сервисов защиты информации в критически важных инфраструктурах.
В качестве основных тенденций создания интеллектуальных сервисов мониторинга и управления информационной безопасностью в критически важных инфраструктурах выделены: разработка надёжных и устойчивых средств обеспечения осведомлённости пользователей о безопасности; совершенствование механизмов распределённого управления безопасностью для адаптивного конфигурирования политик безопасности; достижение более высокой масштабируемости, обеспечивающей требуемый рост производительности при увеличении скорости поступления и количества обрабатываемых данных; использование инновационных моделей прогнозирования безопасности, позволяющих осуществлять проактивную обработку инцидентов и событий безопасности; децентрализация сбора и обработки событий безопасности и др. Определены интеллектуальных сервисов защиты информации, составляющие основу процессов мониторинга и управления информационной безопасностью, в том числе сервисы сбора и корреляции событий и информации безопасности, анализа событий безопасности и прогнозирования атакующих действий нарушителя, активного аудита и защиты информационных и программных ресурсов от вредоносного программного обеспечения, исследовательского моделирования компьютерных атак и процессов защиты от них, анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации визуального анализа событий и информации безопасности, верификации политики безопасности, выработки решений по реагированию на целевые компьютерные атаки и сетей.

2. Разработаны формальная постановка задачи исследования и основные требования к интеллектуальным сервисам мониторинга и управления информационной безопасностью.
К числу новых компонентов системы мониторинга и управления информационной безопасностью, предложенных в проекте, относятся: компонент гибридного хранения данных о событиях безопасности, компонент моделирования атак и анализа защищенности, компонент визуализации, универсальный транслятор событий, высоконадежная шина событий, прогностический анализатор безопасности, масштабируемый процессор событий, система поддержки принятия решений и реагирования.
Компонент моделирования атак и анализа защищенности способен генерировать графы атак, вычислять метрики защищенности от несанкционированного доступа и оценивать уровень защищенности посредством анализа графов (деревьев) атаки. Результатами работы этого компонента являются отчеты с рекомендациями по повышению защищенности и аналитические отчеты о событиях для обнаружения атакующих действий, что позволяет распознавать модели возможного поведения злоумышленника и его последующие шаги.
Компонент визуализации предназначен для реализации в системе интеллектуальных сервисов защиты информации нового поколения функций визуального анализа информации безопасности. Его архитектура состоит из слоя графических примитивов, слоя управляющих сервисов и интерфейсного слоя.
Универсальный транслятор событий обеспечивает управление неоднородными данными и их защиту на удаленных инфраструктурных элементах за счет реализации процедур межуровневого сбора данных, их первоначальной обработки, многоуровневой корреляции, агрегации, шифрования полей событий и анонимизации.
Высоконадежная шина событий о разграничении доступа реализует телекоммуникационную подсистему для распределенных приложений, которые должны осуществлять обмен данными с высокой устойчивостью и эффективностью. Этот компонент включает в себя ряд методов, использующих избыточную доступность в физической сети, которые позволяют доставлять пакеты данных в неоптимальных условиях.
Прогностический анализатор безопасности использует в качестве входных данных модели обработки, политики разграничения доступа, требования защищенности и события о разграничении доступа, поступающие в реальном масштабе времени. Целью его функционирования является оказание помощи в принятии решений, касающихся выработки контрмер по противодействию атакам и угрозам, которые воздействуют на информационно-телекоммуникационную систему в текущий момент времени.
Масштабируемый процессор событий обеспечивает адаптивную вычислительную поддержку всех задач обработки данных о разграничении доступа и функционирует в реальном масштабе времени. Вычислительная адаптивность этого компонента означает, что он может тщательно контролировать входную нагрузку. В случае ее резкого возрастания, автоматически инициируется выполнение задач на новых узлах, что позволяет устранить пиковые нагрузки и равномерно распределить задания.
Система поддержки принятия решений и реагирования позволяет осуществлять конфигурирование политик безопасности, вызываемых соответствующими средствами.

3. Разработаны формальные модели, методики функционирования и архитектуры компонентов исследовательского моделирования компьютерных атак и процессов защиты от них. Эти модели , методики и прототипы основаны на построении и анализе графов атак, позволяющих, с одной стороны, оценить защищенность компьютерной сети от атак, а с другой – участвовать в анализе событий безопасности для выявления наиболее вероятных трасс атак и, как следствие, наиболее вероятных нарушителей.

Основной особенностью, отличающей предложенные модели и методики от существующих, является способ использования графов атак и учета текущих событий безопасности для идентификации фрагмента графа атак.
На этапе подготовки к построению деревьев атак для каждого хоста строится трехмерная матрица по следующим данным: класс атак (сбор данных, подготовительные действия, повышение привилегий, выполнение цели атаки); необходимый тип доступа (удаленный источник без прав доступа, удаленный пользователь системы, локальный пользователь системы, администратор); уровень знаний нарушителя (типы уязвимостей, которые нарушитель может реализовывать).
В результате, для каждого хоста формируется список возможных атакующих действий, разбитых на группы по следующим параметрам: класс атаки, необходимый тип доступа и необходимый уровень знаний нарушителя, а для каждой группы, в свою очередь, формируется список конкретных атак и уязвимостей, которые эти атаки используют. Общий список уязвимостей формируется на основе описания программно-аппаратного обеспечения хоста на языке Common Platform Enumeration (CPE) и таких открытых баз уязвимостей, как National Vulnerability Database (NVD). Источниками данных об открытых уязвимостях также могут служить отчеты сканеров безопасности, таких как Nessus, MaxPatrol и др. Уязвимости в системе хранятся в формате Common Vulnerabilities and Exposures (CVE). Кроме отдельных уязвимостей при построении графа атак используются шаблоны атак в формате Common Attack Pattern Enumeration and Classification (CAPEC), которые могут выступать не только в качестве входной информации для построения графов атак, но и как результат анализа безопасности – они могут описывать наиболее часто встречающиеся последовательности эксплуатации уязвимостей и других действий атакующего.
После формирования матрицы потенциальных атак для каждого хоста, для анализируемой сети выбираются возможные типы нарушителей и точки доступа, в которых они могут получить доступ к сети.
Далее для каждой выбранной модели нарушителя составляется список возможных целей. Так, для внутреннего пользователя это может быть месть (то есть причинение максимального ущерба компании), для внешнего хакера это может быть доступ к некоторой конфиденциальной информации, расположенной на определенном сервере внутри сети, а для червя целью может быть распространение инфекции по сети.
Соответственно, моделью нарушителя для конкретной сети является множество пар (тип нарушителя, цель), которые определяют ограничения по использованию атакующих действий и возможные начальные точки доступа в сеть. После этого на основе собранной информации формируются графы атак для всех выбранных моделей нарушителя.
В режиме обработки событий безопасности основная функция системы защиты информации – выявление конкретных нарушителей и формирование направленной защиты.
Предлагаемый подход использования графов атак для обнаружения атак, проводимых в реальной сети, содержит три основных этапа: (1) на основе модели сети и вероятных нарушителей формируется граф атак; (2) в реальной сети формируется сеть связанных сенсоров, которые позволяют обнаруживать отдельные атакующие действия; система мониторинга позволяет построить общую картину событий, происходящих в сети, на основе собранной от сенсоров информации; (3) далее общая система управления ищет соответствия между графами атак и событиями в реальной сети. Таким образом, на основе анализа инцидентов с учетом деревьев атак становится возможным делать выводы о том, что существует большая вероятность того, что инциденту «производится сканирование хоста С хостом В» предшествовал необнаруженный инцидент «хост В был атакован хостом А» и что последующим действием нарушителя будет «хост С подвергается атаке со стороны хоста В».

4. Разработаны формальные модели, методики функционирования и архитектуры компонентов анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации.
Предлагаемый подход к анализу защищенности и определению рисков безопасности основывается на иерархической системе показателей защищенности, специфицирующей различные уровни представления компьютерной системы, и включает показатели, основанные на современных исследованиях в области анализа защищенности.
Разработанная система показателей защищенности включает следующие уровни: топологический уровень, уровень графа атак, уровень атакующего, уровень событий и уровень интегральных показателей. Каждый уровень включает три категории показателей: основные, стоимостные показатели и показатели 0-дня.
Взаимосвязи между уровнями определяют порядок вычисления показателей в рамках разработанного подхода и информацию, учитываемую в процессе их вычисления.
Первые три уровня относятся к статическому режиму работы системы. На топологическом уровне на основе модели системы и информации об уязвимостях и слабых местах системы рассчитываются следующие основные показатели: Уязвимость хоста, Слабость хоста, Внутренняя критичность, Внешняя критичность, Процент систем без известных критичных уязвимостей; следующие показатели 0-дня: Уязвимость хоста к атакам нулевого дня; и следующие стоимостные показатели: Ценность хоста для бизнеса. При расчете показателей используются как известные, так и модифицированные методики.
На уровне графа атак на основе графа атак, с учетом информации с предыдущего топологического уровня, рассчитываются следующие основные показатели: Критичность атакующих действий, Потенциал атаки, Ущерб от атаки; следующие показатели 0-дня: Потенциал атаки с учетом нулевого дня; и следующие стоимостные показатели: Стоимостной ущерб от атаки, Затраты на реагирование.
На уровне атакующего на основе профиля атакующего, с учетом информации с двух предыдущих уровней, рассчитываются следующие основные показатели: Уровень навыков атакующего, Профильный потенциал атаки; следующие показатели 0-дня: Профильный потенциал атаки с учетом нулевого дня; и следующие стоимостные показатели: Профильный стоимостной ущерб от атаки, Профильные затраты на реагирование. Профиль атакующего при этом включает уровень навыков атакующего и его потенциальные цели, и может корректироваться в соответствии с информацией, полученной со следующего уровня событий.
Уровень событий относится к динамическому режиму работы системы и позволяет корректировать оценки показателей в соответствии с получаемыми событиями и тем самым отслеживать появление и развитие атаки в системе, определять профиль атакующего и прогнозировать его дальнейшие действия.
На уровне событий рассчитываются следующие основные показатели: Позиция атакующего, Динамический уровень навыков атакующего, Вероятностный уровень навыков атакующего, Динамический потенциал атаки; следующие показатели 0-дня: Динамический потенциал атаки с учетом нулевого дня; и следующие стоимостные показатели: Динамический стоимостной ущерб от атаки, Динамические затраты на реагирование.
Интегральные показатели могут рассчитываться на основе показателей любого уровня на основе различных методик, что позволяет иметь оценки разной степени точности на разных уровнях работы системы. При этом сложность алгоритмов увеличивается с ростом количества учитываемой информации. На интегральном уровне рассчитываются следующие основные показатели: Уровень риска, Уровень защищенности, Поверхность атаки.

5. Разработаны формальные модели, методики функционирования и архитектуры компонентов верификации политики безопасности.

Формальные модели и программные прототипы компонентов верификации политики безопасности были созданы для решения задачи проверки сетевых информационных потоков на наличие аномалий политик безопасности. Например, один из типов аномалий, на выявление которых направлена верификация, связан с аномалией «затемнения». Наличие данной аномалии предполагает, что некоторое правило никогда не срабатывает из-за того, что имеется одно или несколько правил с более высокими приоритетами, его «перекрывающих». Аномалия свидетельствует о вероятной ошибке в политике, которую необходимо пересмотреть.
Сущность метода «проверки на модели», применяемого для обнаружения аномалий, заключается в переборе состояний, в которые может перейти система в зависимости от появляющихся информационных потоков и ответов компонента, принимающего решения о разрешении или отклонении таких запросов на основе политик.
Последовательность действий при переборе зависит от условий, которые сформулированы на языке линейной темпоральной логики и выражают корректные состояния системы. Состояние системы определяется набором значений переменных, а изменение состояния вызывается выполняющимися в ней параллельными процессами.
Процесс, который должен выполняться в очередной момент времени, выбирается случайно. Система рассматривает все возможные последовательности шагов для заданных процессов и сигнализирует о потенциальном некорректном состоянии. После этого пользователю выдается «трасса», т.е. последовательность шагов, ведущая к некорректному состоянию системы относительно заданных условий.
Основными входными данными верификации сетевых информационных потоков являются описания правил политики контроля сетевых информационных потоков и структура сети, содержащей встроенные устройства, на языке описания системы, а также выявляемые виды аномалий. На первом этапе верификации входные данные преобразуются во внутренний формат системы верификации. Затем, на втором этапе, строится общая модель системы для верификации правил разрешения/запрета информационных потоков, представленная в виде конечного автомата и инициализированная входными данными во внутреннем формате. Аномалии в модели выражены формальными утверждениями. В рамках метода «проверки на модели» эти формальные утверждения будут являться свойствами корректности, нарушение которых приводит исследуемую систему в некорректное состояние. На третьем этапе общая модель для верификации правил разрешения/запрета информационных потоков верифицируется специальными программными средствами, реализующими метод «проверки на модели». В процессе верификации выявляются все некорректные состояния системы. На завершающем этапе полученные результаты верификации интерпретируются. Если были обнаружены аномалии, то создается описание, содержащее ситуацию и информационный поток, приводящий к возникновению аномалии, а также тип аномалии.
Преимущество предложенного подхода к верификации информационных потоков – возможность гарантировать безопасность системы при условии совпадения поведения модели и реальной системы. К недостаткам можно отнести большой объем необходимых вычислительных ресурсов для анализа сложных моделей; «ложные срабатывания», то есть предупреждения об аномалиях, которых в реальной системе не будет; и неполнота, так как проверяется не реальная система, а ее модель.

6. Разработаны формальные модели, методики функционирования и архитектуры компонентов активного аудита компьютерных систем и сетей и защиты информационных и программных ресурсов от вредоносного программного обеспечения.
Основное внимание было уделено аспекту построения системы детектирования вредоносного программного обеспечения на основе методов

интеллектуального анализа данных с учетом установленных требований - устойчивости к ошибкам, инкрементальности и оперативности процедур обучения и валидации системы детектирования. Выполнение требования устойчивости к ошибкам достигается за счет выбраковки всех неоднозначных правил классификации, выведенных на каждой итерации обучения для каждого используемого набора признаков. Соблюдение требования инкрементальности обучения обеспечивается за счет выделения каждой конечной модели принятия решения в отдельный классификатор, включающийся в общую комбинированную схему принятия решения. Требование оперативности обучения обеспечивается как за счет введения процедур приоритезации отдельных групп признаков в соответствии со степенью их значимости, так и за счет использования методов комбинирования классификаторов. Предложена модель инкрементального обновления знаний об угрозах, следующая принципу периодического поступления на вход системы новых наборов заранее исследованных объектов, имеющих установленный класс вредоносности. В качестве основных групп признаков использовались как поведенческие, так и структурные особенности анализируемых объектов. В качестве базового метода классификации применялись деревья решений (далее Decision Trees, DT), основные методы метаклассификации - голосование (Voting), бустинг (Boosting) и стэкинг (Stacking). Комбинирование классификаторов производилось на основе совмещения отдельных групп признаков в рамках отдельных моделей принятия решения. Показана применимость предложенных моделей и методик детектирования потенциально вредоносных исполняемых программных модулей на основе статических позиционно-зависимых данных на примере анализа исполняемых файлов формата Portable Executable (PE32). Общие положения подхода могут быть использованы для других носителей угроз, в том числе и комбинированных. Процесс извлечения признаков основан на использовании программного средства разбора файлов данного формата (парсера). Данное программное средство способно идентифицировать программную точку входа анализируемого объекта, непрерывный физический участок (секцию) объекта, включающий точку входа и обеспечивать операцию чтения идентифицированной секции по допустимому региону относительных виртуальных адресов.

7. Разработаны формальные модели, методики функционирования и архитектуры компонентов визуализации событий и информации безопасности.
Подсистема визуализации состоит из трех основных компонентов: пользовательский интерфейс, управляющие сервисы и графические элементы.
Управляющие сервисы обеспечивают подключение и регистрацию функциональных компонент и графических элементов, поэтому условно их можно разделить на две группы: контроллер графических элементов и контроллер сервисов. Контроллер графических элементов предоставляет стандартный интерфейс по работе с потоками визуализации, поддерживающий создание и остановку графического потока, который реализуется на уровне графических элементов. Контроллер сервисов обеспечивает управление функциональными модулями. Графические элементы представляют собой библиотеку графических примитивов – графов, лепестковых диаграмм, гистограмм, карт деревьев, географических карт и т.д., и выполняют обработку входных данных, их отображение и взаимодействие пользователя непосредственно с входными данными. Важным моментом является организация взаимодействия между функциональными и графическими элементами. Необходимо реализовать достаточно гибкую связь между компонентами, обеспечив таким образом их относительную независимость друг от друга. Для этого предлагается использовать следующий сценарий взаимодействия. Когда какому-либо

функциональному модулю необходимо визуализировать данные, он запрашивает у контроллера графических элементов перечень доступных графических элементов и выбирает наиболее подходящий элемент, оценивая его свойства. Контроллер графических элементов создает экземпляр элемента и возвращает его функциональному модулю, который в свою очередь передает ему данные для отображения. Графический элемент соответствующим образом обрабатывает данные и предоставляет уже готовый экран с визуализацией и элементами ее управления (масштабирование, управление точкой обзора и т.д.). Таким образом, для реализации данного подхода, необходимо, во-первых, выработать общий формат обмена данными и, во-вторых, определить интерфейс графического объекта, позволяющий передать данные для их графической интерпретации и получить результат визуализации.
Благодаря такому решению, любое изменение во внутренней логике какого-либо элемента системы (функционального или графического) не затронет другие элементы, даже связанные с ним. Кроме того, такой подход позволит разрабатывать и тестировать компоненты независимо, что позволит повысить качество самого приложения. кроме того, при реализации графических элементов могут быть использованы различные технологии визуализации, например, Java3D, Flash , SVG и т.д.

8. Разработаны формальные модели, методики функционирования и архитектуры компонентов хранения данных о событиях безопасности. Предложенный гибридный онтологический репозиторий включает онтологическое информационное хранилище и модули для реализации конкретных механизмов логического вывода - исчисление событий и метод «проверки на модели». В общем виде основными элементами этой архитектуры являются: онтология, хранилище триплетов, редактор метаданных, транслятор, навигатор, ассоциатор, классификатор и блок вывода. Онтология в формате RDF/XML или OWL/XML содержит как логическую теорию, так и базу фактов. Хранилище триплетов (RDF Triple store) предназначено для хранения онтологий. Редактор метаданных служит для создания и редактирования логической теории. Транслятор в онтологическое представление преобразует поступающие от других интеллектуальных сервисов данные во внутренней формат. Навигатор осуществляет поиск необходимой информации, находящейся в хранилище. Ассоциатор осуществляет поиск ассоциаций между экземплярами понятий, необходимых для анализа информации и выявления корреляций различной глубины. Классификатор ресурсов является основным и наиболее эффективным по скорости инструментом логического вывода. Блок вывод является модулем логического вывода, реализующий один из двух методов вывода – на основе исчисления событий (Event Calculus) или на основе «проверки на модели» (Model checking).

9. Разработаны формальные модели, методики функционирования и архитектуры компонентов сбора и корреляции событий и информации безопасности, анализа событий безопасности и прогнозирования атакующих действий нарушителя.
Предлагаемый подход к анализу событий безопасности и прогнозированию действий нарушителя и их последствий включает следующие этапы: формирование графа атак и зависимостей сервисов на основе данных о топологии сети; учет навыков и позиции нарушителя и формирование так называемых профильных графов атак; анализ происходящих в системе событий, в том числе последовательности их возникновения (истории событий) для отслеживания текущей ситуации по безопасности; вычисление показателей защищенности на основе этих данных; прогнозирование действий нарушителя и их последствий; принятие решений по безопасности. Для представления данных по безопасности предлагается использовать протокол SCAP. Протокол включает ряд спецификаций, предназначенных для

стандартизации управления данными по безопасности. В рамках рассматриваемого подхода предлагается использовать следующие стандарты, входящие в состав SCAP: «Общее перечисление конфигураций» (Common Configuration Enumeration, CCE) для определения топологии сети, «Общее перечисление платформ» (Common Platform Enumeration, CPE), «Общие уязвимости и дефекты» (Common Vulnerabilities and Exposures, CVE) и «Общая система оценки уязвимостей» (Common Vulnerabilities Scoring System, CVSS) для определения характеристик хостов, генерации графа атак и оценивания уязвимостей.
Кроме топологии сети и характеристик хостов, входными данными являются зависимости сервисов (используются для определения распространения ущерба), модель нарушителя, события, происходящие в системе, слабые места системы, которые определяются на основе стандарта «Общее перечисление слабых мест» (Common Weaknesses Enumeration, CWE), и т.п.
К выходным данным, получаемым в результате анализа защищенности, относятся: графы атак, вычисленные показатели защищенности, прогнозируемые последующие действия нарушителя и их последствия, набор рекомендуемых контрмер.
На основе различных способов вычисления показателей защищенности, выделено два варианта работы методики анализа событий безопасности и прогнозирования действий нарушителя и их последствий: (1) статическая методика, реализующая экспресс-оценку; (2) динамическая методика, основанная на поведении защищаемой системы.
Методика включает следующие процедуры: определение уровней критичности хостов и атакующих действий, вычисление ущерба от реализации атакующих действий, определение возможных цепочек действий по графу атак, расчет на их основе ущерба от реализации угроз (определяемых заданными цепочками действий) и сложности их реализации, вычисление уровня риска для каждой из угроз, и на его основе общего уровня защищенности системы выбор контрмер.
Основной особенностью методики, основанной на поведении защищаемой системы, является тот факт, что она ориентирована на работу в реальном времени и учитывает поступление новых событий.
Основными процедурами данной методики являются: 1) генератор последовательности атаки строит последовательность действий по реализации атаки, задающих историю событий безопасности, на основе предупреждений от механизма корреляции; 2) генератор графа атак формирует граф возможных атак на основе данных об известных уязвимостях и топологии системы (этот граф служит для прогнозирования действий нарушителя и их последствий, определяя все возможные цепочки действий нарушителя); (3) компонент отображения последовательностей на граф атак отображает последовательность атаки на граф атак для определения реализуемой последовательности и позиции нарушителя на графе атак; (4) генератор графа зависимостей строит граф зависимостей сервисов на основе данных о зависимостях сервисов в анализируемой сети; (5) система оценки защищенности вычисляет набор показателей защищенности на основе графа атак, определенной позиции нарушителя, набора реализованных шагов и графа зависимостей сервисов. На основе этих данных и значений показателей определяются возможные последующие действия нарушителя, их последствия и возможные цели атаки. Затем осуществляется выбор решений по защите (контрмер).

10. Разработаны формальные модели, методики функционирования и архитектуры компонентов выработки решений по реагированию на целевые компьютерные атаки и сетей.
Предлагаемый подход основан на предложенной комплексной системе показателей защищенности, отражающих ситуацию по безопасности. Для выбора контрмер в систему показателей вводится дополнительный уровень поддержки принятия решений, базирующийся на показателях оценки

эффективности применения контрмер. Предложенная модель контрмеры включает: (1) метод и действие контрмеры; программно-аппаратную платформу; (2) индикаторы, влияние на работу, где отрицательное влияние на свойства безопасности активов выражается показателем уровня побочного ущерба; (3) название контрмеры; тип влияния на граф атак - удаление, добавление или изменение связи в графе; (4) показатели эффективности контрмеры, стоимости реализации контрмеры и уровня побочного ущерба. Основными особенностями предлагаемого подхода является использование графов атак и зависимостей сервисов, применение введенной модели контрмер и предложенных показателей защищенности, а также возможность предоставления решения по выбору контрмер в любой момент времени в зависимости от текущей информации о состоянии защищенности и событиях безопасности.

11. Разработаны формальные модели, методики функционирования и архитектуры компонентов выявления основного смыслового содержимого веб-сайтов для определения нежелательной и вредоносной информации. Рассматривались веб-страницы, принадлежащие к ряду категорий, относящихся к различным темам. Для описания других тем и относящихся к ним категорий использовалась обобщенное понятие "неизвестная тема" (unknown).
Подход к обучению системы классификации веб-страниц основан на применении методов машинного обучения для получения базовых классификаторов, необходимых для формирования общей системы классификации веб-страниц. Используя информацию, полученную на этапе обработки исходных (первичных или "сырых") данных, производится формирование списков основных ключевых слов по определенным категориям на основе структурных компонентов веб-страниц. Непосредственное обучение классификаторов происходит на основе текстовых данных, полученных в процессе анализа веб-страниц, принадлежащих к заранее определенным темам.
На основе данных, доступных из адресов веб-страниц (URL) и их форматированного текстового содержимого (HTML), предложена трехуровневая схема принятия решений. Элементы первого (начального) уровня представляют собой функциональные блоки, ориентированные на отдельные категории. Элементы второго уровня разработанной схемы используют классификаторы, ориентированные на принятие решения о принадлежности вектора описаний заданной веб-страницы одной из заданных тем (категорий) в рамках информации, получаемой при анализе отдельных структурных аспектов веб-страницы, например, данных адреса веб-страницы или элементов ее форматирования. Предсказания второго уровня используются для формирования описаний анализируемых веб-страниц, которые применяются для обучения и принятия решений элементом третьего уровня, осуществляющим формирование окончательных решений.

12. Осуществлена реализация и теоретическая и экспериментальная оценка предложенных компонентов мониторинга и управления информационной безопасностью в компьютерных сетях и системах критических инфраструктур. Реализован комплекс программных компонентов, которые предназначены для мониторинга и управления информационной безопасностью в компьютерных сетях и системах.
Получены свидетельства о государственной регистрации программ для ЭВМ, в том числе для конфигурации системы защиты встроенных устройств, верификации правил фильтрации политики безопасности, визуализации логов сервиса мобильных денежных переводов, генетической оптимизации схемы разграничения доступа в виртуальной локальной вычислительной сети, прогнозирования состояния локальной сети с помощью искусственных нейронных сетей, вычисления показателей защищенности для анализа текущего состояния информационно-телекоммуникационных систем и

поддержки принятия решений по реагированию на инциденты информационной безопасности, формирования модели нарушителя для анализа защищенности информационно-телекоммуникационных систем, верификации сетевых информационных потоков для защиты информационно-телекоммуникационных систем со встроенными устройствами, поддержки принятия решений при оценке рисков угроз информационной безопасности мультисервисных сетей связи, решения задачи оценки и прогнозирования состояния распределенных информационных систем, визуализации графов атак системы оценки защищенности компьютерных сетей, визуализации топологии компьютерной сети для мониторинга и управления безопасностью, анализа статистики и оценки качественных параметров интегрированной базы уязвимостей, реализации сервисов доступа и управления интегрированной базой уязвимостей, контроля и управления доступом в помещения на основе бесконтактных смарт-карт, классификации состояния элементов компьютерной сети при оценке рисков угроз информационной безопасности, моделирования атак для защиты информационно-телекоммуникационных систем, оценивания критичности ресурсов на основе построения модели зависимостей сервисов, оценки эффективности конфигурирования компонентов защиты систем Интернета вещей, сбора данных о системе для проектирования, верификации и тестирования компонентов защиты, обнаружения атак на основе гибридизации методов вычислительного интеллекта.

3.6 Сопоставление полученных результатов с мировым уровнем

Основные научные результаты являются новыми и оригинальными, они основываются на разработках исполнителей проекта, выполненных ранее и выполняемых в настоящее время, а также базируются на современных достижениях в области защиты информации, интеллектуального анализа данных, онтологического моделирования, разработки и применения механизмов логического вывода и др.

Все результаты, полученные в процессе выполнения проекта, соответствуют мировому уровню.

Подтверждением этого является то, что авторы проекта изложили основные результаты в статьях, опубликованных в журналах, индексируемых в международных системах цитированияWeb of Science и Scopus («Herald of the Russian Academy of Sciences», «Journal of Computer and Systems Sciences International», «Journal of Wireless Mobile Networks», «Ubiquitous Computing, and Dependable Applications», «The Scientific World Journal», «Journal of Cyber Security and Mobility», «Future internet», «Journal of Automatic Control and Computer Sciences»), в статьях, опубликованных в журналах, входящих в список ВАК Минобрнауки России и РПНЦ («Вестник Российской академии наук»,«Известия РАН. Теория и системы управления», «Информационно-управляющие системы», «Проблемы информационной безопасности. Компьютерные системы», «Безопасность информационных технологий», «Информационные технологии», «Информационные технологии и вычислительные системы», «Изв. вузов. Приборостроение», «Вопросы радиоэлектроники. Сер. СОИУ», «Информация и космос», «Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление», «Труды СПИИРАН» и др.), а также в прочих журналах и трудах конференций.

Результаты проекта были апробированы на множестве различных российских и международных конференций, в частности, на международной конференции по вычислительным наукам и инжинирингу (CSE 2015), где получена награда за лучшую статью; международной конференции IEEE «Интеллектуальное приобретение данных и продвинутые вычислительные системы» (IDAACS'2013, где также получена награда за лучшую статью, IDAACS'2015); международной конференции (Euromicro) по параллельной, распределенной и сетевой обработке информации (PDP 2013, PDP 2014, PDP 2015); международной конференции «РусКрипто» по криптологии,

стеганографии, цифровой подписи и системам защиты информации («РусКрипто 2013», «РусКрипто 2014», «РусКрипто 2015»); международном семинаре по геоинформационным системам и системам информационного слияния: проблемы среды и города (IF&GIS’ 2013); международном форуме по практической безопасности Positive Hack Days (Positive Hack Days 2013, Positive Hack Days 2014, Positive Hack Days 2015); Европейской конференции по моделированию (ECMS 2013); научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (МТСОБИ 2013, МТСОБИ 2014, МТСОБИ 2015); международной конференции по доступности, надежности и безопасности (ARES-2013, ARES-2014); международном Конгрессе по интеллектуальным системам и информационным технологиям (IS&IT’13, IS&IT’14, IS&IT’15); международной научно-практической конференции «ИнтеллектТранс» («ИнтеллектТранс-2014», «ИнтеллектТранс-2015»); Всероссийской научной конференции «Нечеткие системы, мягкие вычисления и интеллектуальные технологии» (НСМВ-2013); межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013, ИБРР-2015); Азиатской конференции по доступности, надежности и безопасности (AsiaARES 2014, AsiaARES 2015); национальной конференции по искусственному интеллекту с международным участием (КИИ-2014); Всероссийской научно-практической конференции "Актуальные проблемы защиты и безопасности" (2014 г.); международной научно-практической конференции "Теоретические и прикладные проблемы информационной безопасности" (19 июня 2014 года, г. Минск, Беларусь, 2014 г.); международной индустриальной конференции по Data Mining (ICDM 2014); IEEE международном симпозиуме по безопасности киберпространства (CSS 2014); международной конференции по мягким вычислениям и измерениям (SCM'2015); международной конференции по рискам и безопасности Интернета и систем (CRiSIS 2015); международной конференции по доверию, безопасности и приватности в вычислениях и телекоммуникациях (IEEE TrustCom 2015) и симпозиуме по современным достижениям в доверии, безопасности и приватности в вычислениях и телекоммуникациях (IEEE RATSP 2015); международном симпозиуме по интеллектуальным распределенным вычислениям (IDC 2014, IDC 2015) и др. Также получено 29 свидетельств о государственной регистрации программ для ЭВМ.

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

При выполнении проекта для исследований использовались работы в следующих областях:
(1) механизмы обеспечения информационной безопасности в компьютерных сетях (в том числе новые технологии разграничения доступа и обнаружения вторжений);
(2) методы системного анализа и теории систем в части их применения для разработки общей архитектуры и архитектуры отдельных компонентов системы интеллектуальных сервисов защиты информационных и сетевых ресурсов в современных и перспективных компьютерных системах;
(3) методы агентно-ориентированного моделирования, генерации трафика на основе моделей, эмуляции и виртуализации сетевых процессов, имитационного моделирования на уровне сетевых пакетов; в работе был использован гибридный подход к моделированию, основанный на комбинации агентно-ориентированного моделирования, генерации трафика на основе моделей, а также методов эмуляции, виртуализации и имитационного моделирования на уровне сетевых пакетов и использовании записей трафика, ранее зафиксированных в реальных сетях;
(4) методы визуального анализа информации;
(5) методы объединения (слияния) данных и информации;
(6) методы реализации логического вывода на основе исчисления событий и

«проверки на модели» (model checking) в части их применения к управлению уровнями защищенности современных компьютерных систем и сетей;
(7) методы нечетких когнитивных карт и нечеткого логического вывода, дополняющих положения теории математического программирования, массового обслуживания, случайных процессов и графов;
(8) онтологический подход к моделированию предметной области систем защиты информации в части создания и применении онтологии, охватывающей метрики защищенности, структурные элементы информационно-телекоммуникационной системы и контрмеры по обеспечению требуемого уровня защищенности;
(9) методы вывода, основанные на знаниях о выполняемых действиях и предсказании намерений и планов оппонента, а также рефлексивные процессы и модели антагонистических процессов;
(10) методы оценки защищенности и анализа рисков; основное отличие предлагаемого подхода от существующих подходов заключается в предлагаемом способе построения графа атак (применяется многоуровневое иерархическое представление стратегий действий злоумышленника) и использовании построенного общего графа атак для определения семейства различных показателей (метрик) защищенности, предназначенных для качественного анализа заданной конфигурации сети и реализуемой политики безопасности; в работе предлагается реализация методики детальной оценки защищенности, основанной на анализе сценариев атак и процессов, происходящих в анализируемой компьютерной сети;
(11) методы интеллектуального анализа данных, в том числе на базе статической и динамической информации, комбинирования классификаторов, обучения и классификации на зашумленных наборах данных; в работе предлагается использовать комбинацию следующих особенностей, позволяющих говорить об использовании интеллектуальных механизмов защиты: "многорезолюционный" способ обнаружения и сдерживания, сочетающий использование нескольких интервалов времени ("окон") наблюдения сетевого трафика и применение различных порогов для отслеживаемых параметров;
(12) методы верификации политики безопасности, т.е. проверки непротиворечивости спецификации политики безопасности за счет обнаружения и разрешения возможных аномалий и противоречий в правилах политики; особенностями предлагаемого подхода являются применение гибридной архитектуры, использующей разные математические подходы для поиска и разрешения различных типов противоречий, открытость для введения дополнительных моделей и методов верификации, использование человеко-машинных процедур разрешения противоречий;
и др.

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)

Котенко Игорь Витальевич:
- руководство проектом;
- разработка моделей и архитектур компонентов исследовательского моделирования компьютерных атак и процессов защиты от них;
- разработка моделей и архитектур компонентов анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации;
- разработка моделей и архитектур компонентов выработки решений по реагированию на целевые компьютерные атаки;
- разработка моделей и архитектур компонентов верификации политики безопасности;
- разработка моделей и архитектур компонентов визуального анализа информации безопасности;
- разработка моделей и архитектур компонентов сбора и корреляции событий

и информации безопасности, анализа событий безопасности и прогнозирования атакующих действий нарушителя;
- теоретическая и экспериментальная оценка полученных результатов.

Десницкий Василий Алексеевич:
- разработка моделей и архитектур компонентов верификации политики безопасности;
- разработка программных прототипов компонентов верификации политики безопасности;
- теоретическая и экспериментальная оценка полученных результатов.

Дойникова Елена Владимировна:
- разработка моделей и архитектур компонентов анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации;
- разработка моделей и архитектур компонентов выработки решений по реагированию на целевые компьютерные атаки;
- разработка программных прототипов компонентов анализа защищенности компьютерных систем и сетей, определения рисков безопасности информации и выработки решений по реагированию на целевые компьютерные атаки;
- теоретическая и экспериментальная оценка полученных результатов.

Комашинский Дмитрий Владимирович:
- активного аудита и защиты информационных и программных ресурсов от вредоносного программного обеспечения;
- разработка моделей и архитектур компонентов выявления основного смыслового содержимого веб-сайтов для определения нежелательной и вредоносной информации;
- разработка программных прототипов компонентов активного аудита и защиты информационных и программных ресурсов от вредоносного программного обеспечения, а также выявления основного смыслового содержимого веб-сайтов для определения нежелательной и вредоносной информации;
- теоретическая и экспериментальная оценка полученных результатов.

Новикова Евгения Сергеевна:
- разработка моделей и архитектур компонентов визуального анализа информации безопасности;
- разработка программных прототипов компонентов визуального анализа информации безопасности;
- теоретическая и экспериментальная оценка полученных результатов.

Саенко Игорь Борисович:
- разработка моделей и архитектур компонентов сбора и корреляции событий и информации безопасности, анализа событий безопасности и прогнозирования атакующих действий нарушителя;
- разработка моделей и архитектур компонентов хранения данных о событиях безопасности;
- разработка программных прототипов компонентов сбора и корреляции событий и информации безопасности, анализа событий безопасности и прогнозирования атакующих действий нарушителя а также хранения данных о событиях безопасности;
- теоретическая и экспериментальная оценка полученных результатов.

Чечулин Андрей Алексеевич:
- разработка моделей и архитектур компонентов сбора и корреляции событий и информации безопасности, анализа событий безопасности и прогнозирования атакующих действий нарушителя;
- разработка моделей и архитектур компонентов выявления основного

смыслового содержимого веб-сайтов для определения нежелательной и вредоносной информации;
- разработка программных прототипов компонентов сбора и корреляции событий и информации безопасности, анализа событий безопасности и прогнозирования атакующих действий нарушителя, а также выявления основного смыслового содержимого веб-сайтов для определения нежелательной и вредоносной информации;
- теоретическая и экспериментальная оценка полученных результатов.

Браницкий Александр Александрович:
- разработка моделей и архитектур компонентов обнаружения сетевых атак, основанных на методах интеллектуального анализа информации, в том числе иммунных систем, нейросетевой классификации, нечеткого вывода и гибридных подходов для выявления аномалий в сетевом трафике;
- разработка программных прототипов компонентов обнаружения сетевых атак, основанных на методах интеллектуального анализа информации, для поддержки принятия решений при мониторинге и управлении информационной безопасностью;
- теоретическая и экспериментальная оценка полученных результатов.

Федорченко Андрей Владимирович:
- разработка моделей и архитектур компонентов сбора и корреляции событий и информации безопасности, анализа событий безопасности и прогнозирования атакующих действий нарушителя;
- разработка программных прототипов компонентов сбора и корреляции событий и информации безопасности, анализа событий безопасности и прогнозирования атакующих действий нарушителя;
- теоретическая и экспериментальная оценка полученных результатов.

3.8.1 Количество научных работ, опубликованных в ходе выполнения Проекта (за весь период выполнения Проекта, цифрами)

253

3.8.1.1 Из них в изданиях, включенных в перечень ВАК

49

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

71

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

30

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

3

3.9 Участие в 2015 году в научных мероприятиях по тематике Проекта (каждое мероприятие с новой строки, указать названия мероприятий и тип доклада)

- 23-я Европейская (Euromicro) международная конференция по параллельной, распределенной и сетевой обработке информации (PDP 2015), Турку, Финляндия, 4-6 марта 2015 г. (И.В.Котенко, А.А.Чечулин, два секционных доклада).
- 16-я международная конференции «РусКрипто 2015» по криптологии, стеганографии, цифровой подписи и системам защиты информации, Московская область, г.Солнечногорск, 17-20 марта 2015 г. (И.В.Котенко,

В.А.Десницкий, А.А.Чечулин, Браницкий А.В., четыре секционных доклада).
- V международная научно-практическая конференция "Интеллектуальные системы на транспорте" (ИнтеллектТранс-2015). 2–3 апреля 2015 г., г. Санкт-Петербург (И.Б.Саенко, секционный доклад).
- XVIII Международная конференция по мягким вычислениям и измерениям (SCM'2015). 19-21 мая 2015 г. (И.В.Котенко, В.А.Десницкий, А.А.Чечулин, И.Б.Саенко, три секционных доклада).
- Международный форум по практической безопасности Positive Hack Days. Москва, 26-27 мая 2015 г. (И.В.Котенко, пленарный доклад, А.В.Федорченко, секционный доклад).
- 23-я Общероссийская научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, 29 июня-02 июля 2015 г. (И.Б.Саенко, секционный доклад).
- 10-я Международная конференция по рискам и безопасности Интернета и систем (CRiSIS 2015). Остров Лесбос, Греция, 20-22 июля 2015 г. (Е.В.Дойникова, секционный доклад).
- Международной конференции по доверию, безопасности и приватности в вычислениях и телекоммуникациях (IEEE TrustCom 2015) и симпозиум по современным достижениям в доверии, безопасности и приватности в вычислениях и телекоммуникациях (IEEE RATSP 2015). Хельсинки, Финляндия. 20-22 августа 2015 г. (И.В.Котенко, секционный доклад).
- Международный Конгресс по интеллектуальным системам и информационным технологиям «IS&IT'15», Дивноморское, 2-8 сентября, 2015 г. (И.В.Котенко, В.А.Десницкий, А.А.Чечулин, И.Б.Саенко, три секционных доклада).
- 8-я международная конференция IEEE «Интеллектуальное приобретение данных и продвинутые вычислительные системы» (IDAACS'2015), Варшава, Польша, 24-26 сентября 2015 г. (И.В.Котенко, А.А.Чечулин, два секционных доклада).
- Азиатская конференция по доступности, надежности и безопасности (AsiaARES 2015). Тэджон, Корея, 4-7 октября 2015 г. (И.В.Котенко, секционный доклад).
- 9-й Международный симпозиум по интеллектуальным распределенным вычислениям (IDC'2015). Гимараеш, Португалия. 7-9 октября 2015 г. (И.В.Котенко, два секционных доклада).
- Международная конференция по вычислительным наукам и инжинирингу (CSE 2015). г. Порто, Португалия. 21-23 октября 2015 г. (И.В.Котенко, два секционных доклада).
- IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. (И.В.Котенко, пленарный доклад, И.Б.Саенко, В.А.Десницкий, Е.В.Дойникова, А.А.Чечулин, А.В.Федорченко, Браницкий А.В., шесть секционных докладов).
- Международная научная школа "Управление инцидентами и противодействие целевым кибер-физическим атакам в распределенных крупномасштабных критически важных системах", Санкт-Петербург, 26–28 ноября 2015 г. (И.В.Котенко, приглашенный доклад)

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

-

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

700000,00

3.11.2. Финансовые средства, полученные в 2014 году от Фонда (указать общий объем, в руб.)

520000,00

3.11.3. Финансовые средства, полученные в 2013 году от Фонда (указать общий объем, в руб.)

400000,00

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

http://comsec.spb.ru/ru/staff/kotenko
http://comsec.spb.ru/en/staff/kotenko
http://comsec.spb.ru/ru/projects
http://comsec.spb.ru/en/projects

3.13 Библиографический список всех публикаций по проекту за весь период выполнения проекта, в порядке значимости: монографии, статьи в научных изданиях, тезисы докладов и материалы съездов, конференций и т.д.

1. Konovalov A.M., Kotenko I.V., Shorov A.V. Simulation-Based Study of Botnets and Defense Mechanisms against Them // Journal of Computer and Systems Sciences International, Vol.52, Issue 1, 2013. P.43-65. Pleiades Publishing, Ltd.. DOI: 10.1134/S1064230712060044. (WoS)
2. Igor Kotenko, Andrey Shorov, Evgenia Novikova. Simulation of Protection Mechanisms Based on "Network Nervous System" against Infrastructure Attacks // Proceedings of the 21th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013). Belfast, Northern Ireland, UK. 27th February – 1st March 2013. Los Alamitos, California. IEEE Computer Society. 2013. P.526-533. (WoS, Scopus)
3. Evgenia Novikova, Igor Kotenko. Analytical Visualization Techniques for Security Information and Event Management // Proceedings of the 21th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013). Belfast, Northern Ireland, UK. 27th February – 1st March 2013. Los Alamitos, California. IEEE Computer Society. 2013. P.519-525. (WoS, Scopus)
4. Igor Kotenko, Andrey Shorov, Andrey Chechulin, Evgenia Novikova. Dynamical Attack Simulation for Security Information and Event Management // V. Popovich et al. (eds.), Information Fusion and Geographic Information Systems (IF&GIS 2013), Lecture Notes in Geoinformation and Cartography, DOI: 10.1007/978-3-642-31833-7_14, Springer-Verlag, Berlin, Heidelberg, 2014. P.219-234. (WoS, Scopus)
5. Igor Kotenko, Olga Polubelova, Igor Saenko. Logical Inference Framework for Security Management in Geographical Information Systems // V. Popovich et al. (eds.), Information Fusion and Geographic Information Systems (IF&GIS 2013), Lecture Notes in Geoinformation and Cartography, DOI: 10.1007/978-3-642-31833-7_14, Springer-Verlag, Berlin, Heidelberg, 2014. P.203-218. (Scopus)
6. Igor Kotenko, Igor Saenko, Olga Polubelova, Andrey Chechulin. Design and Implementation of a Hybrid Ontological-Relational Data Repository for SIEM systems // Future internet, Vol. 5, No. 3, 2013. P. 355-375. ISSN 1999-5903. doi:10.3390/fi5030355. (Scopus)
7. Igor Kotenko. Experiments with simulation of botnets and defense agent teams // 27th European Conference on Modelling and Simulation (ECMS 2013). Proceedings. May 27 - May 30st, Aalesund University College, Norway. 2013. P.61-67. (WoS)
8. Igor Kotenko and Andrey Chechulin. A Cyber Attack Modeling and Impact Assessment Framework // 5th International Conference on Cyber Conflict 2013 (CyCon 2013). Proceedings. IEEE and NATO COE Publications. 4-7 June 2013, Tallinn, Estonia. 2013. P.119-142. (WoS)
9. Igor Kotenko, Igor Saenko, Olga Polubelova and Elena Doynikova. The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems

// The 2nd International Workshop on Recent Advances in Security Information and Event Management (RaSIEM 2013). In conjunction with the 8th International Conference on Availability, Reliability and Security (ARES 2013). September 2nd – 6th, 2013. Regensburg, Germany. IEEE Computer Society. 2013. P.638-645. (WoS, Scopus)
10. Igor Kotenko and Evgenia Novikova. VisSecAnalyzer: a Visual Analytics Tool for Network Security Assessment // 3rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2013). In conjunction with the 8th International Conference on Availability, Reliability and Security (ARES 2013). September 2-6, 2013, Regensburg, Germany. Lecture Notes in Computer Science (LNCS), Vol.8128. Springer. 2013, P.345-360. (WoS, Scopus)
11. Igor Kotenko and Andrey Chechulin. Computer Attack Modeling and Security Evaluation based on Attack Graphs // The IEEE 7th International Conference on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS'2013). Proceedings. Berlin, Germany, September 12-14, 2013. P.614-619. (Scopus)
12. Igor Kotenko and Elena Doynikova. Security metrics for risk assessment of distributed information systems // The IEEE 7th International Conference on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS'2013). Proceedings. Berlin, Germany, September 12-14, 2013. P.646-650. (Scopus)
13. Igor Kotenko, Elena Doynikova, Andrey Chechulin. Security metrics based on attack graphs for the Olympic Games scenario // Proceedings of the 22th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2014). Turin, Italy. 12th - 14th February, 2014. Los Alamitos, California. IEEE Computer Society. 2014. P.561-568. (WoS, Scopus)
14. Philipp Nesteruk, Lesya Nesteruk, Igor Kotenko. Creation of a Fuzzy Knowledge Base for Adaptive Security Systems // Proceedings of the 22th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2014). Turin, Italy. 12th - 14th February, 2014. Los Alamitos, California. IEEE Computer Society. 2014. P.574-577. (WoS, Scopus)
15. Igor Kotenko, Elena Doynikova. Security Assessment of Computer Networks based on Attack Graphs and Security Events // The 2014 Asian Conference on Availability, Reliability and Security (AsiaARES 2014). In conjunction with ICT-EurAsia 2014. Bali, Indonesia, April 14th – 17th, 2014. / Linawati et al. (Eds.): ICT-EurAsia 2014, Lecture Notes in Computer Science (LNCS), Vol.8407. IFIP International Federation for Information Processing (2014). Springer. 2014, P.462-471. (WoS, Scopus)
16. Igor Kotenko, Andrey Chechulin, Andrey Shorov, Dmitry Komashinsky. Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking. P. Perner (Ed.): 14th Industrial Conference on Data Mining (ICDM 2014), July 16 – 21, 2014, St. Petersburg, Russia. Lecture Notes in Artificial Intelligence (LNAI), DOI 10.1007/978-3-319-08976-8. P. 39–54. ISSN 0302-9743, ISBN 978-3-319-08975-1. (WoS, Scopus)
17. Kotenko I., Shorov A. Simulation of bio-inspired security mechanisms against network infrastructure attacks // Intelligent Distributed Computing VIII. Studies in Computational Intelligence. Springer-Verlag, Vol.570. Proceedings of 8th International Symposium on Intelligent Distributed Computing - IDC'2014. September 3-5, 2014, Madrid, Spain. Springer-Verlag. P.127-133. (WoS, Scopus)
18. Igor Kotenko, Igor Saenko. Design of Virtual Computer Networks: Data Mining by Genetic Algorithms // Intelligent Distributed Computing VIII. Studies in Computational Intelligence. Springer-Verlag, Vol.570. Proceedings of 8th International Symposium on Intelligent Distributed Computing - IDC'2014. September 3-5, 2014, Madrid, Spain. Springer-Verlag. P.95-105. (WoS, Scopus)
19. Igor Kotenko, Elena Doynikova. Security Evaluation Models for Cyber Situational Awareness // The 2014 IEEE 6th International Symposium on Cyberspace Safety and Security (CSS 2014). August 20-22, 2014, Paris, France. 2014. Los Alamitos, California. IEEE Computer Society. 2014. P.1229-1236. (WoS, Scopus)

20. Igor Kotenko, Evgenia Novikova. Visualization of Security Metrics for Cyber Situation Awareness // The 1st International Software Assurance Workshop (SAW 2014). In conjunction with the 9th International Conference on Availability, Reliability and Security (ARES 2014). September 8nd – 12th, 2014. Fribourg, Switzerland. IEEE Computer Society. 2014. P.506-513. (WoS, Scopus)
21. Evgenia Novikova, Igor Kotenko. Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services // International Cross Domain Conference and Workshops (CD-ARES 2014). September 8nd – 12th, 2014. Fribourg, Switzerland. Lecture Notes in Computer Science (LNCS), Vol.8708. Springer-Verlag. 2014, P.63-78. (WoS, Scopus)
22. 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. (WoS, Scopus)
23. Igor Kotenko, Elena Doynikova. Evaluation of Computer Network Security based on Attack Graphs and Security Event Processing // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol.5, No.3, September 2014. P.14-29. (Scopus)
24. Igor Saenko, Igor Kotenko. Design of Virtual Local Area Network Scheme based on Genetic Optimization and Visual Analysis // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol.5, No.4, December 2014. (Scopus)
25. Andrey Shorov, Igor Kotenko. The Framework for Simulation of Bio-inspired Security Mechanisms Against Network Infrastructure Attacks // The Scientific World Journal, Volume 2014 (2014), Article ID 172583, 11 pages. http://dx.doi.org/10.1155/2014/172583. (WoS, IF=1.730, Scopus)
26. I.V. Kotenko and I. B. Saenko. Creating New Generation Cybersecurity Monitoring and Management Systems // Herald of the Russian Academy of Sciences, 2014, Vol.84, No.6. P.993–1001. ISSN 1019-3316. DOI: 10.1134/S1019331614060033 (Scopus IF=0.170, WoS)
27. Igor Kotenko, Andrey Chechulin. Fast Network Attack Modeling and Security Evaluation based on Attack Graphs // Journal of Cyber Security and Mobility, Vol.3, No.1, P.27–46. (Scopus)
28. Yana Bekeneva, Konstantin Borisenko, Andrey Shorov, Igor Kotenko. Investigation of DDoS Attacks by Hybrid Simulation // The 2015 Asian Conference on Availability, Reliability and Security (AsiaARES 2015). In conjunction with ICT-EurAsia 2015. October 4th – 7th, 2015, Daejeon, Korea / ICT-EurAsia 2015, Lecture Notes in Computer Science (LNCS), Vol.9357. IFIP International Federation for Information Processing (2015). Springer. 2015, P.179-189. (WoS, Scopus)
29. 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) (принято к печати)
30. Chechulin A.A., Kotenko I.V. Real-Time Security Events Processing using an Approach based on the Attack Trees Analysis // Automatic Control and Computer Sciences, № 8, 2015, Springer, 2015. (Scopus) (принято к печати)

31. Коновалов А.М., Котенко И.В., Шоров А.В. Исследование бот-сетей и механизмов защиты от них на основе имитационного моделирования // Известия РАН. Теория и системы управления, № 1, 2013, С.45-68. (ВАК, РИНЦ)
32. Полубелова О.В., Котенко И. В. Построение онтологий уязвимостей и применение логического вывода для управления информацией и событиями безопасности // Безопасность информационных технологий, № 1, 2013, С.21-24. (ВАК, РИНЦ)
33. Котенко И.В., Саенко И.Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах //

Труды СПИИРАН. Вып.1 (24). СПб.: Наука, 2013. С.21-40. (ВАК, РИНЦ)
34. Котенко И.В., Саенко И.Б. Научный анализ и поддержка политик безопасности в киберпространстве: обзор перспективных исследований по результатам Международного семинара SA&PS4CS 2012 // Труды СПИИРАН. Вып.1 (24). СПб.: Наука, 2013. С.66-88. (ВАК, РИНЦ)
35. Котенко И.В., Саенко И.Б., Полубелова О.В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. Вып.2 (25). СПб.: Наука, 2013. С.113-134. (ВАК, РИНЦ)
36. Котенко И.В., Саенко И.Б. Математические модели, методы и архитектуры для защиты компьютерных сетей: обзор перспективных исследований по результатам Международной конференции MMM–ACNS–2012 // Труды СПИИРАН. Вып.2 (25). СПб.: Наука, 2013. С.148-170. (ВАК, РИНЦ)
37. Нестерук Ф.Г., Котенко И.В. Инструментальные средства создания нейросетевых компонент интеллектуальных систем защиты информации // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.7-25. (ВАК, РИНЦ)
38. Котенко И.В., Полубелова О.В., Чечулин А.А. Построение модели данных для системы моделирования сетевых атак на основе онтологического подхода // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.26-39. (ВАК, РИНЦ)
39. Чечулин А.А. Методика оперативного построения, модификации и анализа деревьев атак // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.40-53. (ВАК, РИНЦ)
40. Дойникова Е. В. Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.54-68. (ВАК, РИНЦ)
41. Полубелова О. В. Архитектура и программная реализация системы верификации правил фильтрации // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.79-90. (ВАК, РИНЦ)
42. Комашинский Д. В. Обнаружение и идентификация вредоносных исполняемых программных модулей с помощью методов Data Mining // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.115-125. (ВАК, РИНЦ)
43. Комашинский Д.В. Подход к выявлению вредоносных документов на основе методов интеллектуального анализа данных // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.126-135. (ВАК, РИНЦ)
44. Десницкий В.А., Котенко И.В. Конфигурирование встроенных систем защиты информации в рамках сервисов обеспечения комплексной безопасности железнодорожного транспорта // Труды СПИИРАН. Вып.7 (30). СПб.: Наука, 2013. С. 40-55. (ВАК, РИНЦ)
45. Котенко И.В., Дойникова Е.В., Чечулин А.А. Динамический перерасчет показателей защищенности на примере определения потенциала атаки // Труды СПИИРАН. Вып.7 (30). СПб.: Наука, 2013. С. 26-39. ISSN: 2078-9181. (ВАК, РИНЦ)
46. Котенко И.В., Саенко И.Б., Чернов А.В., Бутакова М.А. Построение многоуровневой интеллектуальной системы обеспечения информационной безопасности для автоматизированных систем железнодорожного транспорта // Труды СПИИРАН. Вып.7 (30). СПб.: Наука, 2013. С.7-25. (ВАК, РИНЦ)
47. Десницкий В.А. Методика верификации сетевых информационных потоков в информационно-телекоммуникационных системах со встроенными устройствами // Труды СПИИРАН. Вып.7 (30). СПб.: Наука, 2013. С. 246-257. (ВАК, РИНЦ)
48. Котенко И.В., Новикова Е.С. Визуальный анализ для оценки защищенности компьютерных сетей // Информационно-управляющие системы, 2013, № 3, С.55-61. (ВАК, РИНЦ)
49. Котенко И.В., Саенко И.Б. Перспективные модели и методы защиты компьютерных сетей и обеспечения безопасности киберпространства: обзор международных конференции MMM-ACNS-2012 и семинара SA&PS4CS 2012 // Информационно-управляющие системы, 2013, № 3, С.97-99. ISSN 1684-8853. (ВАК, РИНЦ)
50. Десницкий В.А., Котенко И.В. Проектирование защищенных встроенных устройств на основе конфигурирования // Проблемы информационной

безопасности. Компьютерные системы, № 1, 2013. С.44-54. (ВАК, РИНЦ)
51. Полубелова О.В., Котенко И.В. Методика верификации правил фильтрации методом "проверки на модели" // Проблемы информационной безопасности. Компьютерные системы, № 1, 2013. С.151-168. (ВАК, РИНЦ)
52. Новикова Е.С., Котенко И.В. Проектирование компонента визуализации для автоматизированной системы управления информационной безопасностью // Информационные технологии, № 9, 2013. С.32-36. (ВАК, РИНЦ)
53. Котенко И.В., Саенко И.Б., Чечулин А.А. Проактивное управление информацией и событиями безопасности в информационно-телекоммуникационных системах // Вопросы радиоэлектроники. Сер. СОИУ. 2014. Вып. 1. С. 170–180. (ВАК, РИНЦ)
54. Чечулин А.А., Котенко И.В. Построение графов атак для анализа событий безопасности // Безопасность информационных технологий, № 3, 2014, С.135-141. (ВАК, РИНЦ) (принято к печати)
55. Котенко И.В., Дойникова Е.В. Вычисление и анализ показателей защищенности на основе графов атак и зависимостей сервисов // Проблемы информационной безопасности. Компьютерные системы, № 2, 2014. С.19-36. (ВАК, РИНЦ)
56. 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. (ВАК, РИНЦ)
57. Чечулин А.А., Котенко И.В. Обработка событий безопасности в условиях реального времени с использованием подхода, основанного на анализе деревьев атак // Проблемы информационной безопасности. Компьютерные системы, № 3, 2014. С.56-59. (ВАК, РИНЦ)
58. Федорченко А.В., Чечулин А.А., Котенко И.В. Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения // Проблемы информационной безопасности. Компьютерные системы, № 3, 2014. С.131-135. (ВАК, РИНЦ)
59. Котенко И.В., Саенко И.Б. К новому поколению систем мониторинга и управления безопасностью // Вестник Российской академии наук, Том 84, № 11, 2014, С.993–1001. (ВАК, РИНЦ)
60. Котенко И.В., Саенко И.Б., Юсупов Р.М. Новое поколение систем мониторинга и управления инцидентами безопасности // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. СПбГПУ, 2014, № 3 (198), С.7-18. (ВАК, РИНЦ)
61. Федорченко А.В., Чечулин А.А., Котенко И.В. Построение интегрированной базы данных уязвимостей // Изв. вузов. Приборостроение, Т.57, № 10, 2014, С.62-67. ISSN 0021-3454. (ВАК, РИНЦ)
62. Дойникова Е.В., Котенко И.В. Отслеживание текущей ситуации и поддержка принятия решений по безопасности компьютерной сети на основе системы показателей защищенности // Изв. вузов. Приборостроение, Т.57, № 10, 2014, С.72-77. ISSN 0021-3454. (ВАК, РИНЦ)
63. Десницкий В.А., Котенко И.В. Использование экспертных знаний для разработки защищенных систем со встроенными устройствами // Информационные технологии и вычислительные системы, № 4, 2014, С.17-32. (ВАК, РИНЦ)
64. Федорченко А.В., Чечулин А.А., Котенко И.В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных систем и сетей // Информационно-управляющие системы, 2014, №5, С.72-79. (ВАК, РИНЦ)
65. Носков А.Н., Чечулин А.А., Тарасова Д.А. Исследование эвристических подходов к обнаружению атак на телекоммуникационные сети на базе методов интеллектуального анализа данных // Труды СПИИРАН. Вып.6 (37). СПб.: Наука, 2014. (ВАК, РИНЦ)
66. Агеев С.А., Саенко И.Б., Егоров Ю.П., Гладких А.А., Богданов А.В. Интеллектуальное иерархическое управление рисками информационной

безопасности в защищенных мультисервисных сетях специального назначения // Автоматизация процессов управления. Вып. №3 (37), 2014. ISSN 1991-2927. С.78-88. (ВАК, РИНЦ)
67. Куваев В.О., Саенко И.Б. Концептуальные основы интеграции неоднородных информационных ресурсов предприятия в едином информационном пространстве // Проблемы экономики и управления в торговле и промышленности, № 7 (007), 2014. – С. 101-104. ISSN 2309-3064. (ВАК, РИНЦ)
68. Саенко И.Б., Куваев В.О., Алышев С.В. Подход к построению системы показателей качества единого информационного пространства // Естественные и математические науки в современном мире, 2014. № 14. С. 51-56. (ВАК, РИНЦ)
69. 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)
70. Котенко И.В., Шоров А.В. Исследование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода «нервная система сети» // Проблемы информационной безопасности. Компьютерные системы, № 3, 2015. С.45-55. (ВАК, РИНЦ)
71. 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)
72. Браницкий А.А., Котенко И.В. Построение нейросетевой и иммуноклеточной системы обнаружения вторжений // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015. С.23-27. (ВАК, РИНЦ)
73. Котенко И.В., Новикова Е.С., Чечулин А.А. Визуализация метрик защищенности для мониторинга безопасности и управления инцидентами // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015. С.42-47. (ВАК, РИНЦ)
74. 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)
75. Дойникова Е.В., Котенко И.В., Чечулин А.А. Динамическое оценивание защищенности компьютерных сетей в SIEM-системах // Безопасность информационных технологий, № 3, 2015. (ВАК, РИНЦ)
76. Котенко И.В., Дойникова Е.В. Методика выбора контрмер на основе комплексной системы показателей защищенности в системах управления информацией и событиями безопасности // Информационно-управляющие системы, 2015, № 3, С.60-69. doi:10.15217/issn1684-8853.2015.3.60. (ВАК, РИНЦ)
77. Браницкий А.А., Котенко И.В. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейро-нечетких классификаторов // Информационно-управляющие системы, 2015, № 4, С.69-77. doi:10.15217/issn1684-8853.2015.4.69. (ВАК, РИНЦ)
78. Коломеец М.В., Чечулин А.А., Котенко И.В. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН. 2015. Вып. 42. С. 232-257. (ВАК, РИНЦ)
79. Куваев В.О., Чечулин А.А., Ефимов В.В., Лыжинкин К.В. Варианты построения единого информационного пространства для интеграции разнородных автоматизированных систем // Информация и космос. Научно-технический журнал, № 4, 2015. С. 83-87. (ВАК, РИНЦ)
80. Котенко И.В., Шоров А.В. Исследование биоинспирированных подходов для защиты от инфраструктурных атак на основе комплекса имитационного моделирования // Технические науки — от теории к практике, № 17-1, 2013 / «Технические науки — от теории к практике»: материалы XVII

международной заочной научно-практической конференции. Часть I. (23 января 2013 г.); Новосибирск: Изд. «СибАК», 2013. С.39-43. (РИНЦ)
81. Котенко Д.И., Котенко И.В., Саенко И.Б. Моделирование атак в больших компьютерных сетях // Технические науки — от теории к практике, № 17-1, 2013 / «Технические науки — от теории к практике»: материалы XVII международной заочной научно-практической конференции. Часть I. (23 января 2013 г.); Новосибирск: Изд. «СибАК», 2013. С.12–16. (РИНЦ)
82. Котенко И.В., Саенко И.Б. Система интеллектуальных сервисов защиты информации для критических инфраструктур // Технические науки — от теории к практике, № 17-1, 2013 / «Технические науки — от теории к практике»: материалы XVII международной заочной научно-практической конференции. Часть I. (23 января 2013 г.); Новосибирск: Изд. «СибАК», 2013. С.7-11. ISBN 978-5-4379-0205-9. (РИНЦ)
83. Котенко И.В., Нестерук Ф.Г., Шоров А.В. Гибридная адаптивная система защиты информации на основе биометафор "нервных" и нейронных сетей // Инновации в науке, № 16-1, 2013 / Инновации в науке»: материалы XVI международной заочной научно-практической конференции. Часть I. (28 января 2013 г.); Новосибирск: Изд. «СибАК», 2013. С.79-83. (РИНЦ)
84. Котенко И.В., Саенко И.Б., Дойникова Е.В. Оценка рисков в компьютерных сетях критических инфраструктур // Инновации в науке, № 16-1, 2013 / «Инновации в науке»: материалы XVI международной заочной научно-практической конференции. Часть I. (28 января 2013 г.); Новосибирск: Изд. «СибАК», 2013. С.84-88. (РИНЦ)
85. Десницкий В.А. Комбинированная защита встроенных устройств на основе конфигурирования // Инновации в науке, № 16-1, 2013 / «Инновации в науке»: материалы XVI международной заочной научно-практической конференции. Часть I. (28 января 2013 г.); Новосибирск: Изд. «СибАК», 2013. С.64-67. (РИНЦ)
86. Комашинский Д.В. Особенности применения методов интеллектуального анализа данных для задачи обнаружения разрушающих программных воздействий // Инновации в науке, № 16-1, 2013 / «Инновации в науке»: материалы XVI международной заочной научно-практической конференции. Часть I. (28 января 2013 г.); Новосибирск: Изд. «СибАК», 2013. С.74-78. (РИНЦ)
87. Новикова Е.С. Модели графического представления информации о защищенности компьютерной сети // Инновации в науке, № 16-1, 2013 / «Инновации в науке»: материалы XVI международной заочной научно-практической конференции. Часть I. (28 января 2013 г.); Новосибирск: Изд. «СибАК», 2013. С.116-120. (РИНЦ)
88. Полубелова О.В. Методика верификации правил фильтрации методом "проверки на модели" // XVI Международная заочная научно-практическая конференция "Инновации в науке". Новосибирск, 2013. С.134-138. (РИНЦ)
89. Чечулин А.А. Методика построения графов атак для систем анализа событий безопасности // Инновации в науке, № 16-1, 2013 / «Инновации в науке»: материалы XVI международной заочной научно-практической конференции. Часть I. (28 января 2013 г.); Новосибирск: Изд. «СибАК», 2013. С.156-160. (РИНЦ)
90. Скорик Ф.А., Саенко И.Б. Нейросетевая модель оценки состояния распределенной информационной системы // Инновации в науке, № 16-1, 2013 / «Инновации в науке»: материалы XVI международной заочной научно-практической конференции. Часть I. (28 января 2013 г.); Новосибирск: Изд. «СибАК», 2013. С.151-155. (РИНЦ)
91. Котенко И.В., Саенко И.Б. Предложения по онтологическому представлению и гибридному хранению данных о событиях безопасности в АСУ железнодорожного транспорта // Технические науки — от теории к практике, № 29, 2014. Новосибирск: Изд. «СибАК», 2014. С.28-32. (РИНЦ)
92. Котенко И.В., Саенко И.Б. Предложения по реализации логического вывода для управления кибербезопасностью в АСУ железнодорожного транспорта // Естественные и математические науки в современном мире.

2014. № 14. Новосибирск: Изд. «СибАК», С. 46-50. (РИНЦ)
93. Котенко И.В., Саенко И.Б. Методика верификации политик безопасности в многоуровневой интеллектуальной системе обеспечения комплексной безопасности железнодорожного транспорта // Технические науки - от теории к практике. Новосибирск: Изд. «СибАК», 2014. № 30. С. 18-22. (РИНЦ)
94. 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. (РИНЦ)
95. 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. (РИНЦ)
96. Десницкий В.А., Чечулин А.А. Обобщенная модель нарушителя и верификации информационно-телекоммуникационных систем со встроенными устройствами // Журнал «Технические науки — от теории к практике». Изд. НП "СибАК", №38, 2014, С.7-21. (РИНЦ)
97. Саенко И.Б., Куваев В.О., Бирюков М.А. Общая архитектура единой системы разграничения доступа к разнородным ресурсам в едином информационно-коммуникационном пространстве // Технические науки – от теории к практике, 2015, № 11 (47), С. 70-75. (РИНЦ)
98. Саенко И.Б., Куваев В.О., Бирюков М.А. Использование онтологий для управления разграничением доступа к разнородным ресурсам единого информационно-коммуникационного пространства // Технические науки – от теории к практике, 2015, № 11 (47), С. 76-80. (РИНЦ)
99. Левшун Д.С., Чечулин А.А. Постановка задачи построения единого хранилища мультимедийных данных из полевых этнографических экспедиций // Журнал «Технические науки — от теории к практике». Изд. НП "СибАК", №46, 2015, С. 25-30. (РИНЦ)
100. Десницкий В.А. Конфигурирование компонентов защиты встроенных устройств на основе эвристического подхода // Журнал «Технические науки — от теории к практике». Изд. НП "СибАК", №46, 2015, С.16-20. (РИНЦ)
101. Десницкий В.А. Методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами // Журнал «Технические науки — от теории к практике». Изд. НП "СибАК", №47, 2015, С.14-18. (РИНЦ)

102. D.V. Komashinskiy, I.V. Kotenko. Intelligent Data Analysis for Malware Detection (Комашинский Д.В., Котенко И.В. Интеллектуальный анализ данных для выявления вредоносных программ) // International Journal of Computing, Research Institute of Intelligent Computer Systems, Ternopil National Economic University. 2013, Vol.12, Issue 1. P.63-74. ISSN 1727-6209.
103. I.V. Kotenko, P.G. Nesteruk, A.V. Shorov. Conception of a Hybrid Adaptive Protection of Information Systems (Котенко И.В., Нестерук Ф.Г., Шоров А.В. Концепция гибридной адаптивной защиты информационных систем) // International Journal of Computing, Research Institute of Intelligent Computer Systems, Ternopil National Economic University. 2013, Vol.12, Issue 1. P.86-98. ISSN 1727-6209.
104. Igor Kotenko, Elena Doynikova. Comprehensive Multilevel Security Risk Assessment of Distributed Information Systems // International Journal of Computing, Research Institute of Intelligent Computer Systems, Ternopil National Economic University. 2013, Vol.12, Issue 3. ISSN 1727-6209.
105. Котенко И.В., Саенко И.Б. Международная конференция “Математические модели, методы и архитектуры для защиты компьютерных сетей” (MMM-ACNS-2012) и Международный семинар “Научный анализ и поддержка политик безопасности в киберпространстве” (SA&PS4CS 2012) // Защита информации. Инсайд, 2013, № 1, С.8-9.
106. Котенко И.В., Саенко И.Б. Интеллектуальные сервисы защиты информации в компьютерных системах и сетях // Защита информации. Инсайд, 2013, № 2, С.32-41.

107. Maksim Kolomeec, Andrey Chechulin, Igor Kotenko. Methodological Primitives for Phased Construction of Data Visualization Models // Journal of Internet Services and Information Security (JISIS), Vol. 5, No. 4 (November 2015). http://www.jisis.org: Submission: October 23, 2015.

108. Котенко И.В. Моделирование атак, анализ защищенности и визуализация в SIEM-системах // Пятнадцатая Международная конференция "РусКрипто'2013". Московская область, г.Солнечногорск, 28-30 марта 2013 г. http://www.ruscrypto.ru/
109. Чечулин А.А., Котенко И.В. Построение графов атак для корреляции событий безопасности // Пятнадцатая Международная конференция "РусКрипто'2013". Московская область, г.Солнечногорск, 28-30 марта 2013 г. http://www.ruscrypto.ru/
110. Десницкий В.А., Котенко И.В., Чечулин А.А. Проектирование защищенных информационных систем со встроенными устройствами // Пятнадцатая Международная конференция "РусКрипто'2013". Московская область, г.Солнечногорск, 28-30 марта 2013 г. http://www.ruscrypto.ru/
111. Комашинский Д.В., Чечулин А.А, Котенко И.В., Шоров А.В. Категорирование Web-сайтов для систем блокирования Web-страниц с неприемлемым содержимым // Пятнадцатая Международная конференция "РусКрипто'2013". Московская область, г.Солнечногорск, 28-30 марта 2013 г. http://www.ruscrypto.ru/
112. Котенко И.В. Моделирование атак, вычисление метрик защищенности и визуализация в перспективных SIEM-системах // Международный форум по практической безопасности Positive Hack Days. Москва. 23-24 мая 2013 г. http://www.phdays.ru
113. Дойникова Е.В., Котенко И.В. Оценка защищенности компьютерных сетей на основе графов атак с использованием многоуровневой системы показателей // Методы и технические средства обеспечения безопасности информации. Материалы 22-й научно-технической конференции. 8 - 11 июля 2013 года. Санкт-Петербург. Издательство Политехнического университета. 2013. С.18-20.
114. Котенко И.В., Саенко И.Б., Дойникова Е.В., Полубелова О.В. Применение онтологии метрик защищенности для принятия решений по обеспечению кибербезопасности // Методы и технические средства обеспечения безопасности информации. Материалы 22-й научно-технической конференции. 8 - 11 июля 2013 года. Санкт-Петербург. Издательство Политехнического университета. 2013. С.32-33.
115. Шоров А.В., Чечулин А.А., Котенко И.В. Категорирование веб-сайтов для блокирования веб-страниц с неприемлемым содержимым защищенности для принятия решений по обеспечению кибербезопасности // Методы и технические средства обеспечения безопасности информации. Материалы 22-й научно-технической конференции. 8 - 11 июля 2013 года. Санкт-Петербург. Издательство Политехнического университета. 2013. С.75-77.
116. Десницкий В.А. Верификация информационных потоков в процессе разработки защищенных систем со встроенными устройствами // Методы и технические средства обеспечения безопасности информации. Материалы 22-й научно-технической конференции. 8 - 11 июля 2013 года. Санкт-Петербург. Издательство Политехнического университета. 2013. С.17-18.
117. Нестерук Ф.Г. Разработка адаптивного сервиса защиты информации // Методы и технические средства обеспечения безопасности информации. Материалы 22-й научно-технической конференции. 8 - 11 июля 2013 года. Санкт-Петербург. Издательство Политехнического университета. 2013. С.36-37.
118. Новикова Е.С. Методика визуального анализа событий системы мобильных платежей // Методы и технические средства обеспечения безопасности информации. Материалы 22-й научно-технической конференции. 8 - 11 июля 2013 года. Санкт-Петербург. Издательство Политехнического университета. 2013. С.37-39.

119. Полубелова О.В. Использование онтологий в системе поддержки принятия решений о выборе контрмер // Методы и технические средства обеспечения безопасности информации. Материалы 22-й научно-технической конференции. 8 - 11 июля 2013 года. Санкт-Петербург. Издательство Политехнического университета. 2013. С.41-42.
120. Чечулин А.А. Распознавание нарушителей на основе анализа деревьев атак // Методы и технические средства обеспечения безопасности информации. Материалы 22-й научно-технической конференции. 8 - 11 июля 2013 года. Санкт-Петербург. Издательство Политехнического университета. 2013. С.141-142.
121. Саенко И.Б., Котенко И.В., Полубелова О.В., Дойникова Е.В. Применение онтологии метрик защищенности для выработки контрмер по обеспечению безопасности компьютерных сетей // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'13». Научное издание в 4-х томах. М.: Физматлит, 2013. Т. 2. С.372-377. ISBN 978-5-9221-1479-0.
122. Саенко И.Б., Котенко И.В., Морозов И.В. Применение генетических алгоритмов для разграничения доступа в геоинформационных системах // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'13». Научное издание в 4-х томах. М.: Физматлит, 2013. Т. 2. С.58-63. ISBN 978-5-9221-1479-0.
123. Котенко И.В., Саенко И.Б. О построении многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г. Материалы конференции. СПб.: СПОИСУ, 2013. С.107-108.
124. Десницкий В.А., Котенко И.В. Конфигурирование встроенных систем защиты в рамках сервисов многоуровневой интеллектуальной системы комплексной безопасности железнодорожного транспорта // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г. Материалы конференции. СПб.: СПОИСУ, 2013. С.91-92.
125. Котенко И.В., Новикова Е.С. Подход к построению системы визуального анализа для управления безопасностью интеллектуальной информационной системы железнодорожного комплекса России // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г. Материалы конференции. СПб.: СПОИСУ, 2013. С.106-107.
126. Котенко И.В., Саенко И.Б., Полубелова О.В., Дойникова Е.В. Онтология показателей защищенности компьютерной сети как основа выработки контрмер // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г. Материалы конференции. СПб.: СПОИСУ, 2013. С.108-109.
127. Шоров А.В., Чечулин А.А., Котенко И.В. Категорирование веб-сайтов для систем блокирования веб-сайтов с неприемлемым содержимым на основе анализа текстовой и графической информации // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г. Материалы конференции. СПб.: СПОИСУ, 2013. С. 129-130.
128. Котенко И.В. Интеллектуальные сервисы защиты информации в системах мониторинга и управления безопасностью критически важных инфраструктур // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г.
129. Чечулин А.А. Применение аналитического моделирования для повышения уровня защищенности распределенных информационных систем // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г. Материалы конференции. СПб.: СПОИСУ, 2013. С. 127-128.

130. Десницкий В.А. Верификация информационных потоков в системах со встроенными устройствами // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г. Материалы конференции. СПб.: СПОИСУ, 2013. С.92-93.
131. Десницкий В.А. Методика конфигурирования безопасного встроенного устройства // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г. Материалы конференции. СПб.: СПОИСУ, 2013. С.93-94.
132. Дойникова Е.В. Подход к анализу защищенности распределенных информационных систем на основе системы показателей защищенности // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г. Материалы конференции. СПб.: СПОИСУ, 2013. С.94-95.
133. Нестерук Ф.Г. Тенденции развития адаптивных систем защиты информации // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г. Материалы конференции. СПб.: СПОИСУ, 2013. С.117-118.
134. Новикова Е.С. Выявление аномальной активности в системе мобильных денежных переводов с помощью методов визуального анализа // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г. Материалы конференции. СПб.: СПОИСУ, 2013. С.120.
135. Полубелова О.В. Стратегии разрешения аномалий фильтрации межсетевых экранов // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г. Материалы конференции. СПб.: СПОИСУ, 2013. С.62-63.
136. Саенко И.Б., Куваев В.О. Об интеллектуальной системе разграничения доступа к ресурсам единого информационного пространства для разнородных автоматизированных систем // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). 23-25 октября 2013 г. Материалы конференции. СПб.: СПОИСУ, 2013. С.105-106.
137. Куваев В.О., Саенко И.Б. Разграничение доступа к ресурсам единого информационного пространства в ходе их интеграции в автоматизированных системах специального назначения // Материалы 22-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 08-12 июля 2013 г. Санкт-Петербург. Издательство Политехнического университета. С. 85-86.
138. Агеев С. А., Саенко И.Б. Интеллектуальные методы для управления безопасностью защищённых мультисервисных сетей связи // Материалы 22-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 08-12 июля 2013 г. Санкт-Петербург. Издательство Политехнического университета. С. 51-52.
139. Скорик Ф.А., Саенко И.Б. Применение технологии «размытого спектра» для обеспечения безопасности беспроводных сетей // Материалы 22-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 08-12 июля 2013 г. Санкт-Петербург. Издательство Политехнического университета. С. 74-75.
140. Котенко И.В., Саенко И.Б. О задачах обеспечения кибербезопасности в инфраструктурах "электронного города" на основе методов искусственного интеллекта // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.618-622. ISBN 978-5-91995-042-4.
141. Чечулин А.А., Котенко И.В. Разработка системы защиты пользователей от нежелательной информации в сети Интернет // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.642-647. ISBN 978-5-

91995-042-4.
142. Котенко И.В., Чечулин А.А. Применение технологии обработки больших данных для защиты сетевой инфраструктуры // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.614-617. ISBN 978-5-91995-042-4.
143. Федорченко А. В., Чечулин А.А., Котенко И.В. Интегрированная база данных уязвимостей в системе оценки защищенности компьютерных сетей // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.638-641. ISBN 978-5-91995-042-4.
144. 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.
145. Дойникова Е.В. Оценивание защищенности информационных систем и реагирование на инциденты информационной безопасности с учетом текущей ситуации по безопасности // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.601-604. ISBN 978-5-91995-042-4.
146. Саенко И.Б., Куваев В.О. О применении методов искусственного интеллекта для разграничения доступа к ресурсам единого информационного пространства разнородных автоматизированных систем // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.631-637. ISBN 978-5-91995-042-4.
147. Агеев С.А., Саенко И.Б. Управление рисками информационной безопасности защищенной мультисервисной сети специального назначения на основе интеллектуальных мультиагентов // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.556-562. ISBN 978-5-91995-042-4.
148. Котенко И.В., Саенко И.В., Чечулин А.А. Проактивное управление информацией и событиями безопасности в сетях NGN // Материалы семинара Международного союза электросвязи «Переход развивающихся стран с существующих сетей на сети нового поколения (NGN): технические, экономические, законодательные и политические аспекты», Санкт-Петербург, СПб ГУТ им Бонч-Бруевича. 23–25 июня 2014 года.
149. Котенко И.В., Новикова Е.С. Модели и методики визуального анализа данных для решения задач компьютерной безопасности // Шестнадцатая Международная конференция “РусКрипто’2014”. Московская область, г.Солнечногорск, 25-28 марта 2014 г. http://www.ruscrypto.ru/
150. Чечулин А.А., Котенко И.В.Обработка событий безопасности в условиях реального времени с использованием подхода, основанного на анализе деревьев атак // Шестнадцатая Международная конференция “РусКрипто’2014”. Московская область, г.Солнечногорск, 25-28 марта 2014 г. http://www.ruscrypto.ru/
151. 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/
152. Федорченко А.В., Чечулин А.А., Котенко И.В.Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения // Шестнадцатая Международная конференция “РусКрипто’2014”. Московская область, г.Солнечногорск, 25-28 марта 2014 г. http://www.ruscrypto.ru/
153. Котенко И.В., Саенко И.Б. О построении многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем железнодорожного транспорта //

Интеллектуальные системы на транспорте: Материалы IV международной научно-практической конференции «ИнтеллектТранс-2014». – СПб.: ПГУПС, 2014. С.196-203.
154. Котенко И.В., Юсупов Р.М. Системы мониторинга и управления кибербезопасностью нового поколения для защиты информации в критически важных инфраструктурах // XVII-я Всероссийская научно-практическая конференция "Актуальные проблемы защиты и безопасности". Санкт-Петербург, 1 - 4 апреля 2014 г.
155. Котенко И.В., Новикова Е.С. Визуальная аналитика на страже информационной безопасности // Международный форум по практической безопасности Positive Hack Days. Москва. 21-22 мая 2014 г. http://www.phdays.ru
156. Саенко И.Б., Котенко И.В. Основы построения перспективных систем мониторинга и управления безопасностью для защиты критически важных объектов информатизации // Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.
157. Федорченко А.В., Чечулин А.А., Котенко И.В. Интегрированная база данных уязвимостей // Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.
158. Чечулин А.А. Анализ и классификация возможных изменений, происходящих в компьютерной сети и их влияние на деревья атак // Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь,. 2014.
159. Нестерук Ф. Г. Специфика двухуровневой организации адаптивных систем защиты информации // Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.
160. Дойникова Е.В. Вычисление показателей защищенности в системах мониторинга и управления безопасностью // Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.
161. 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.
162. Котенко И.В., Саенко И.Б. Об архитектуре многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте // 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.97-98.
163. 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.
164. 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.

165. 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.
166. 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.
167. Федорченко А.В. Анализ уязвимостей по временным характеристикам на основе открытой базы данных X-Force // 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.104-105.
168. Дойникова Е.В. Подход к оцениванию защищенности на основе графов атак в системах управления информацией и событиями безопасности // 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.90-91.
169. Агеев С.А., Саенко И.Б. Интеллектуальные методы управления рисками информационной безопасности мультисервисных сетей связи // 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.59-60.
170. Куваев В.О., Саенко И.Б. Подход к решению задачи разграничения доступа в разнородном информационном пространстве // 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.33-34.
171. Котенко И.В., Саенко И.Б. Система логического вывода и верификации политик безопасности в автоматизированных системах железнодорожного транспорта // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'14». Научное издание в 4-х томах. М.: Физматлит, 2014. Т.2. С.271-276. 978-5-9221-1572-8.
172. Саенко И.Б., Котенко И.В. Генетический подход к проектированию виртуальных компьютерных сетей на основе генетических алгоритмов // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'14». Научное издание в 4-х томах. М.: Физматлит, 2014. Т.1. С.35-40. ISBN 978-5-9221-1572-8.
173. Котенко И.В., Саенко И.Б. Интеллектуальная система мониторинга и управления инцидентами кибербезопасности // Четырнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2014 (24–27 сентября 2014 года, г. Казань, Россия): Труды конференции. Т.3. Казань: Изд-во РИЦ «Школа», 2014. С.219-227.
174. Дойникова Е.В., Котенко И.В. Анализ и применение показателей защищенности в SIEM-системах на основе графов атак и зависимостей сервисов // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). Труды конференции. СПб.: СПОИСУ, 2014.
175. Новожилов Д.А., Чечулин А.А. Методы определения основного языка веб-страниц // XIV Санкт-Петербургская Международная Конференция "Региональная информатика-2014" ("РИ-2014"). Материалы конференции. СПб., 2014. С.155-156.
176. Чечулин А.А., Комашинский Д.В. Решение задачи классификации сайтов на иностранных языках в сети Интернет // XIV Санкт-Петербургская

Международная Конференция "Региональная информатика-2014" ("РИ-2014"). Материалы конференции. СПб., 2014. С.169-170.
177. Чечулин А.А., Котенко И.В. Программный прототип компонента аналитического моделирования атак для систем управления информацией и событиями безопасности в автоматизированных системах управления РЖД // XIV Санкт-Петербургская Международная Конференция "Региональная информатика-2014" ("РИ-2014"). Материалы конференции. СПб., 2014. С.170-171.
178. 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"). Материалы конференции. СПб., 2014. С.130.
179. 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"). Материалы конференции. СПб., 2014. С.131.
180. Дойникова Е.В., Котенко И.В. Оценивание защищенности в автоматизированных системах управления РЖД // XIV Санкт-Петербургская Международная Конференция "Региональная информатика-2014" ("РИ-2014"). Материалы конференции. СПб., 2014. С.132-133.
181. Дойникова Е.В. Поддержка принятия решений по выбору защитных мер в информационных системах на основе комплекса показателей защищенности // XIV Санкт-Петербургская Международная Конференция "Региональная информатика-2014" ("РИ-2014"). Материалы конференции. СПб., 2014. С.132.
182. Федорченко А.В. Методы интеграции баз уязвимостей для улучшения анализа защищенности компьютерных систем // XIV Санкт-Петербургская Международная Конференция "Региональная информатика-2014" ("РИ-2014"). Материалы конференции. СПб., 2014. С.165-166.
183. Федорченко А.В. Обзор механизмов корреляции событий безопасности в SIEM-системах // XIV Санкт-Петербургская Международная Конференция "Региональная информатика-2014" ("РИ-2014"). Материалы конференции. СПб., 2014. С.166.
184. Агеев С.А., Саенко И.Б. Оценка и управление рисками информационной безопасности в защищенных мультисервисных сетях на основе методов искусственного интеллекта // XIV Санкт-Петербургская Международная Конференция "Региональная информатика-2014" ("РИ-2014"). Материалы конференции. СПб., 2014. С.116-117.
185. Котенко И.В., Саенко И.Б. Поддержка принятия решений по безопасности информации в АСУ железнодорожного транспорта на основе онтологического моделирования данных // XIV Санкт-Петербургская Международная Конференция "Региональная информатика-2014" ("РИ-2014"). Материалы конференции. СПб., 2014. С.144.
186. Котенко И.В., Саенко И.Б. Модели и методы визуального анализа больших объемов данных и событий безопасности автоматизированных систем железнодорожного транспорта // XIV Санкт-Петербургская Международная Конференция "Региональная информатика-2014" ("РИ-2014"). Материалы конференции. СПб., 2014. С.143.
187. Левшун Д.С., Чечулин А.А. Построение классификационной схемы существующих методов корреляции событий безопасности // XIV Санкт-Петербургская Международная Конференция "Региональная информатика-2014" ("РИ-2014"). Материалы конференции. СПб., 2014. С.148-149.
188. Брюханов А.В., Архипов Ю.А., Лепнев П.А., Чечулин А.А., Котенко И.В. Решение задачи формирования списков информационных объектов и их связей для визуализации данных при мониторинге и управлении информационной безопасностью // Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014

г. СПб.: Изд-во СПбГЭТУ «ЛЭТИ». 2014. С.65-69.
189. Чечулин А.А., Котенко И.В., Дойникова Е.В. Методика анализа истории событий безопасности, прогнозирования действий нарушителя и их последствий // Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014 г. СПб.: Изд-во СПбГЭТУ «ЛЭТИ». 2014. С.69-72.
190. 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». 2014. С.73-77.
191. Безродный И.В., Смирнов Д.Б., Саенко И.Б., Котенко И.В., Волков А.А. Основы технологии агрегации, нормализации и анализа данных для мониторинга безопасности сетей «Интернет вещей» // Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014 г. СПб.: Изд-во СПбГЭТУ «ЛЭТИ». 2014. С.77-81.
192. Полушин В.Ю., Малоземов Д.Г., Саенко И.Б., Чечулин А.А., Зорохович С.В. Программно-аппаратный стенд генерации наборов тестовых гетерогенных данных для моделирования сети «Интернет вещей» // Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014 г. СПб.: Изд-во СПбГЭТУ «ЛЭТИ». 2014. С.81-85.
193. 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/
194. 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/
195. Смирнов Д.Б., Чечулин А.А. Корреляция данных безопасности в сетях «Интернет вещей» // Семнадцатая Международная конференция “РусКрипто’2015”. Московская область, г.Солнечногорск, 17-20 марта 2015 г. http://www.ruscrypto.ru/
196. Котенко И.В. Вычисление, визуализация и анализ метрик защищенности для мониторинга безопасности и управления инцидентами в SIEM-системах // Международный форум по практической безопасности Positive Hack Days. Москва. 26-27 мая 2015 г. http://www.phdays.ru
197. Котенко И.В., Саенко И.Б. Генетический подход к проектированию виртуальной частной сети в защищенном информационном пространстве // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'15, 2015, Том 2. С.320-325.
198. 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.
199. 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.
200. Саенко И.Б., Котенко И.В. Адаптивное изменение политик и схем разграничения доступа к ресурсам единого информационного пространства // 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.127-128.
201. Котенко И.В., Саенко И.Б., Чечулин А.А. Разработка систем управления информацией и событиями безопасности нового поколения // 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.123-124.
202. Браницкий А.А., Котенко И.В. Методы комбинирования бинарных классификаторов для задач обнаружения и классификации сетевых атак // 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.68.
203. Дойникова Е.В., Котенко И.В. Выбор защитных мер для управления защищенностью компьютерных сетей на основе комплексной системы показателей // 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.114-115.
204. Новиков И.М., Котенко И.В. Определение функциональной логики веб-приложений по данным сетевого трафика // 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.91-92.
205. Чечулин А.А., Проноза А.А. Классификация и анализ типов связей в компьютерных сетях для их последующей визуализации // 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.132-133.
206. Проноза А.А., Чечулин А.А. Модель извлечения данных разнородной структуры об информационных объектах компьютерной сети для подсистемы визуализации систем управления событиями и информацией безопасности // 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.125-127.
207. Агеев С.А., Васильев Д.В., Саенко И.Б. Управление безопасностью защищенной мультисервисной сети специального назначения // 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.106-107.
208. 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.
209. 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.
210. Дойникова Е.В. Генератор сценариев атак на основе классификации шаблонов атак CAPEC // 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.71-72.
211. Федорченко А.В Комбинированный процесс корреляции событий безопасности в SIEM-системах // 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.102-103.
212. Саенко И.Б., Котенко И.В. Модели и методы оценки эффективности

функционирования системы разграничения доступа к ресурсам информационного пространства // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 85-86.
213. Коломеец М.В., Чечулин А.А., Котенко И.В. Визуализация параметров безопасности компьютерных сетей с помощью диаграммы Вороного // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 73-74.
214. 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.
215. Дешевых Е. А., Ушаков И.А., Котенко И.В. Обзор средств и платформ обработки больших данных для задач мониторинга информационной безопасности // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 67.
216. Дубровин Н.Д., Ушаков И.А., Котенко И.В. Реализация прототипа на базе Hadoop для анализа больших данных // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 69-70.
217. Крылов К.Ю., Ушаков И.А., Котенко И.В. Анализ методик применения концепции больших данных для мониторинга безопасности компьютерных сетей // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 75-76.
218. 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.
219. 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.
220. 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.
221. 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.
222. Дойникова Е.В. Применение графов зависимостей сервисов в рамках задачи анализа защищенности компьютерных сетей для оценивания критичности ресурсов системы и обоснованного выбора защитных мер // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 68-69.
223. Новожилов Д.А., Чечулин А.А. Разработка программных средств поддержки проведения экспериментов по классификации веб-сайтов // IX Санкт-Петербургская межрегиональная конференция "Информационная

безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 80-81.
224. 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.

225. Котенко И.В., Десницкий В.А. Конфигуратор системы защиты встроенных устройств. Федеральная служба по интеллектуальной собственности. Свидетельство о государственной регистрации программы для ЭВМ № 2013612691. Зарегистрировано в Реестре программ для ЭВМ 11.03.2013 г.
226. Полубелова О.В., Котенко И.В. Верификатор правил фильтрации политики безопасности. Федеральная служба по интеллектуальной собственности. Свидетельство о государственной регистрации программы для ЭВМ № 2013612707. Зарегистрировано в Реестре программ для ЭВМ 11.03.2013 г.
227. Новикова Е.С., Котенко И.В. Система визуализации логов сервиса мобильных денежных переводов. Федеральная служба по интеллектуальной собственности. Свидетельство о государственной регистрации программы для ЭВМ № 2013660999. Зарегистрировано в Реестре программ для ЭВМ 26.11.2013 г.
228. Саенко И.Б., Нестерук Ф.Г. Решение задачи генетической оптимизации схемы разграничения доступа в виртуальной локальной вычислительной сети. Федеральная служба по интеллектуальной собственности. Свидетельство о государственной регистрации программы для ЭВМ № 2013618914. Зарегистрировано в Реестре программ для ЭВМ 23.09.2013.
229. Саенко И.Б., Скорик Ф.А., Нестерук Ф.Г. Решение задачи прогнозирования состояния локальной сети с помощью искусственных нейронных сетей. Федеральная служба по интеллектуальной собственности. Свидетельство о государственной регистрации программы для ЭВМ № 2013618915. Зарегистрировано в Реестре программ для ЭВМ 23.09.2013.

230. Котенко И.В., Дойникова Е.В., Чечулин А.А. Вычисление показателей защищенности для анализа текущего состояния информационно-телекоммуникационных систем и поддержки принятия решений по реагированию на инциденты информационной безопасности. Свидетельство № 2014661026. Зарегистрировано в Реестре программ для ЭВМ 22.10.2014.
231. Котенко И.В., Чечулин А.А. Формирование модели нарушителя для анализа защищенности информационно-телекоммуникационных систем. Свидетельство № 2014661028. Зарегистрировано в Реестре программ для ЭВМ 22.10.2014.
232. Десницкий В.А., Котенко И.В. Верификация сетевых информационных потоков для защиты информационно-телекоммуникационных систем со встроенными устройствами. Свидетельство № 2014661027. Зарегистрировано в Реестре программ для ЭВМ 22.10.2014.
233. Саенко И.Б., Агеев С.А., Чечулин А.А. Поддержка принятия решений при оценке рисков угроз информационной безопасности мультисервисных сетей связи. Свидетельство № 2014660775. Зарегистрировано в Реестре программ для ЭВМ 15.10.2014.
234. Саенко И.Б., Скорик Ф.А., Чечулин А.А. Решение задачи оценки и прогнозирования состояния распределенных информационных систем. Свидетельство № 2014660856. Зарегистрировано в Реестре программ для ЭВМ

235. Котенко И.В., Чечулин А.А. Компонент визуализации графов атак системы оценки защищенности компьютерных сетей. Свидетельство № 2015615640. Зарегистрировано в Реестре программ для ЭВМ 22.05.2015.
236. Котенко И.В., Чечулин А.А. Компонент визуализации топологии

компьютерной сети для мониторинга и управления безопасностью информационно-телекоммуникационных систем. Свидетельство № 2015615773. Зарегистрировано в Реестре программ для ЭВМ 22.05.2015.
237. Коломеец М.В., Чечулин А.А., Котенко И.В. Сервер системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт. Свидетельство № 2015662190. Зарегистрировано в Реестре программ для ЭВМ 18.11.2015.
238. Федорченко А.В., Чечулин А.А., Котенко И.В. Компонент анализа статистики и оценки качественных параметров интегрированной базы уязвимостей. Свидетельство № 2015662208. Зарегистрировано в Реестре программ для ЭВМ 18.11.2015.
239. Саенко И.Б., Чечулин А.А., Агеев С.А., Котенко И.В. Классификатор состояния элементов компьютерной сети при оценке рисков угроз информационной безопасности. Свидетельство № 2015662186. Зарегистрировано в Реестре программ для ЭВМ 18.11.2015.
240. Чечулин А.А., Котенко И.В. Компонент моделирования атак для защиты информационно-телекоммуникационных систем. Свидетельство № 2015619128. Зарегистрировано в Реестре программ для ЭВМ 25.11.2015.
241. Федорченко А.В., Котенко И.В. Сервисы доступа и управления интегрированной базой уязвимостей для систем мониторинга и управления безопасностью информационно-телекоммуникационных систем. Свидетельство № 2015615366. Зарегистрировано в Реестре программ для ЭВМ 15.05.2015.
242. Дойникова Е.В., Котенко И.В. Компонент оценивания критичности ресурсов на основе построения модели зависимостей сервисов при тестировании компонентов защиты в сетях Интернета вещей. Свидетельство № 2015615374. Зарегистрировано в Реестре программ для ЭВМ 24.03.2015.
243. 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.
244. Браницкий А.А., Котенко И.В. Адаптивная система обнаружения атак на основе гибридизации методов вычислительного интеллекта. Свидетельство № 2015662189. Зарегистрировано в Реестре программ для ЭВМ 18.11.2015.
245. 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.
246. Саенко И.Б., Браницкий А.А. Программно-инструментальный стенд визуализации и оценки качества проектирования виртуальных компьютерных сетей для поддержки принятия решений при мониторинге и управлении информационной безопасностью. Свидетельство № 2015615772. Зарегистрировано в Реестре программ для ЭВМ 22.05.2015.
247. 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.
248. Десницкий В.А. Генератор отчетных форм анализа защищенности систем Интернета вещей. Свидетельство № 2015662184. Зарегистрировано в Реестре программ для ЭВМ 18.11.2015.
249. Дойникова Е.В., Чечулин А.А. Генератор случайных последовательностей атакующих действий для тестирования сетей Интернета вещей. Свидетельство № 2015615368. Зарегистрировано в Реестре программ для ЭВМ 15.05.2015.
250. Федорченко А.В., Чечулин А.А. Интегрированная база уязвимостей для систем мониторинга и управления безопасностью информационно-телекоммуникационных систем. Свидетельство № 2015621655. Зарегистрировано в Реестре баз данных 17.11.2015.

251. Коломеец М.В., Чечулин А.А. Клиент системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт. Свидетельство № 2015662136. Зарегистрировано в Реестре программ для ЭВМ 17.11.2015.
252. Левшун Д.С., Чечулин А.А. Прошивка встроенного устройства системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт. Свидетельство № 2015662137. Зарегистрировано в Реестре программ для ЭВМ 17.11.2015.
253. Саенко И.Б., Чечулин А.А., Куваев В.О., Барыкин Н.А. Программное средство оценки оперативности доступа к ресурсам единого информационно-коммуникационного пространства. Свидетельство № 2015662574. 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 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 настоящем проекте основные усилия были сосредоточены на исследовании наиболее важных проблем построения интеллектуальных сервисов мониторинга и управления информационной безопасностью в критически важных инфраструктурах, в недостаточной степени исследованных с точки зрения получения фундаментальных теоретических и практических результатов в области защиты информации.

Проведен детальный анализ состояния современных исследований в области построения интеллектуальных сервисов защиты информации в критически важных инфраструктурах. В качестве основных тенденций создания интеллектуальных сервисов мониторинга и управления информационной безопасностью в критически важных инфраструктурах выделены: разработка надёжных и устойчивых средств обеспечения осведомлённости пользователей о безопасности; совершенствование механизмов распределённого управления безопасностью для адаптивного конфигурирования политик безопасности; достижение более высокой масштабируемости, обеспечивающей требуемый рост производительности при увеличении скорости поступления и количества обрабатываемых данных; использование инновационных моделей прогнозирования безопасности, позволяющих осуществлять проактивную обработку инцидентов и событий безопасности; децентрализация сбора и обработки событий безопасности и др.

Разработаны формальная постановка задачи исследования и основные требования к интеллектуальным сервисам мониторинга и управления информационной безопасностью. К числу новых компонентов системы мониторинга и управления информационной безопасностью, предложенных в проекте, относятся: компонент гибридного хранения данных о событиях безопасности, компонент моделирования атак и анализа защищенности, компонент визуализации, универсальный транслятор событий, высоконадежная шина событий, прогностический анализатор безопасности, масштабируемый процессор событий, система поддержки принятия решений и реагирования.

Разработаны формальные модели, методики функционирования и архитектуры компонентов исследовательского моделирования компьютерных атак и процессов защиты от них. Эти модели, методики и прототипы основаны на построении и анализе графов атак, позволяющих, с одной стороны, оценить защищенность компьютерной сети от атак, а с другой – участвовать в анализе событий безопасности для выявления наиболее вероятных трасс атак и, как следствие, наиболее вероятных нарушителей. Основной особенностью, отличающей предложенные модели и методики от существующих, является способ использования графов атак и учета текущих событий безопасности для идентификации фрагмента графа атак.

Разработаны формальные модели, методики функционирования и архитектуры компонентов анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации. Предлагаемый подход к анализу защищенности и определению рисков безопасности основывается на иерархической системе показателей защищенности, специфицирующей различные уровни представления компьютерной системы, и включает показатели, основанные на современных исследованиях в области анализа защищенности. Разработанная система показателей защищенности включает следующие уровни: топологический уровень, уровень графа атак, уровень атакующего, уровень событий и уровень интегральных показателей. Каждый уровень включает три категории показателей: основные, стоимостные показатели и показатели 0-дня.

Разработаны формальные модели, методики функционирования и архитектуры компонентов верификации политики безопасности. Формальные модели и программные прототипы компонентов верификации политики безопасности были созданы для решения задачи проверки сетевых информационных потоков на наличие аномалий политик безопасности. Сущность метода «проверки на модели», применяемого для обнаружения

аномалий, заключается в переборе состояний, в которые может перейти система в зависимости от появляющихся информационных потоков и ответов компонента, принимающего решения о разрешении или отклонении таких запросов на основе политик.

Разработаны формальные модели, методики функционирования и архитектуры компонентов активного аудита компьютерных систем и сетей и защиты информационных и программных ресурсов от вредоносного программного обеспечения. Основное внимание было уделено аспекту построения системы детектирования вредоносного программного обеспечения на основе методов интеллектуального анализа данных с учетом установленных требований - устойчивости к ошибкам, инкрементальности и оперативности процедур обучения и валидации системы детектирования. Выполнение требования устойчивости к ошибкам достигается за счет выбраковки всех неоднозначных правил классификации, выведенных на каждой итерации обучения для каждого используемого набора признаков. Соблюдение требования инкрементальности обучения обеспечивается за счет выделения каждой конечной модели принятия решения в отдельный классификатор, включающийся в общую комбинированную схему принятия решения. Требование оперативности обучения обеспечивается как за счет введения процедур приоритезации отдельных групп признаков в соответствии со степенью их значимости, так и за счет использования методов комбинирования классификаторов.

Разработаны формальные модели, методики функционирования и архитектуры компонентов визуализации событий и информации безопасности. Подсистема визуализации состоит из трех основных компонентов: пользовательский интерфейс, управляющие сервисы и графические элементы. Управляющие сервисы обеспечивают подключение и регистрацию функциональных компонент и графических элементов, поэтому условно их можно разделить на две группы: контроллер графических элементов и контроллер сервисов. Контроллер графических элементов предоставляет стандартный интерфейс по работе с потоками визуализации, поддерживающий создание и остановку графического потока, который реализуется на уровне графических элементов. Контроллер сервисов обеспечивает управление функциональными модулями. Графические элементы представляют собой библиотеку графических примитивов – графов, лепестковых диаграмм, гистограмм, карт деревьев, географических карт и т.д., и выполняют обработку входных данных, их отображение и взаимодействие пользователя непосредственно с входными данными.

Разработаны формальные модели, методики функционирования и архитектуры компонентов хранения данных о событиях безопасности. Предложенный гибридный онтологический репозиторий включает онтологическое информационное хранилище и модули для реализации конкретных механизмов логического вывода - исчисление событий и метод «проверки на модели». В общем виде основными элементами этой архитектуры являются: онтология, хранилище триплетов, редактор метаданных, транслятор, навигатор, ассоциатор, классификатор и блок вывода.

Разработаны формальные модели, методики функционирования и архитектуры компонентов сбора и корреляции событий и информации безопасности, анализа событий безопасности и прогнозирования атакующих действий нарушителя. Предлагаемый подход к анализу событий безопасности и прогнозированию действий нарушителя и их последствий включает следующие этапы: формирование графа атак и зависимостей сервисов на основе данных о топологии сети; учет навыков и позиции нарушителя и формирование так называемых профильных графов атак; анализ происходящих в системе событий, в том числе последовательности их возникновения (истории событий) для отслеживания текущей ситуации по безопасности; вычисление показателей защищенности на основе этих данных; прогнозирование действий нарушителя и их последствий; принятие решений по безопасности.

Разработаны формальные модели, методики функционирования и архитектуры компонентов выработки решений по реагированию на целевые компьютерные атаки и сетей. Предлагаемый подход основан на предложенной комплексной системе показателей защищенности, отражающих ситуацию по безопасности. Для выбора контрмер в систему показателей вводится дополнительный уровень поддержки принятия решений, базирующийся на показателях оценки эффективности применения контрмер. Основными особенностями предлагаемого подхода является использование графов атак и зависимостей сервисов, применение введенной модели контрмер и предложенных показателей защищенности, а также возможность предоставления решения по выбору контрмер в любой момент времени в зависимости от текущей информации о состоянии защищенности и событиях безопасности.

Разработаны формальные модели, методики функционирования и архитектуры компонентов выявления основного смыслового содержимого веб-сайтов для определения нежелательной и вредоносной информации. На основе данных, доступных из адресов веб-страниц (URL) и их форматированного текстового содержимого (HTML), предложена трехуровневая схема принятия решений. Элементы первого (начального) уровня представляют собой функциональные блоки, ориентированные на отдельные категории. Элементы второго уровня разработанной схемы используют классификаторы, ориентированные на принятие решения о принадлежности вектора описаний заданной веб-страницы одной из заданных тем (категорий) в рамках информации, получаемой при анализе отдельных структурных аспектов веб-страницы, например, данных адреса веб-страницы или элементов ее форматирования. Предсказания второго уровня используются для формирования описаний анализируемых веб-страниц, которые применяются для обучения и принятия решений элементом третьего уровня, осуществляющим формирование окончательных решений.

Осуществлена реализация и теоретическая и экспериментальная оценка предложенных компонентов мониторинга и управления информационной безопасностью в компьютерных сетях и системах критических инфраструктур. Получены свидетельства о государственной регистрации программ для ЭВМ, в том числе для конфигурации системы защиты встроенных устройств, верификации правил фильтрации политики безопасности, прогнозирования состояния локальной сети с помощью искусственных нейронных сетей, вычисления показателей защищенности для анализа текущего состояния информационно-телекоммуникационных систем и поддержки принятия решений по реагированию на инциденты информационной безопасности, формирования модели нарушителя для анализа защищенности информационно-телекоммуникационных систем и др.

Теоретическая и экспериментальная оценка предложенных компонентов мониторинга и управления информационной безопасностью базировалась на реализации следующих этапов работы: формирование модели сети (эксперименты проводились для сетей различного объема и различной структуры зависимостей сервисов); задание параметров (моделей атакующего, критичностей, и т.п.); формирование графа атак; анализ графа атак; сбор и корреляции событий и информации безопасности; визуализация событий и информации безопасности; анализ событий безопасности и прогнозирование атакующих действий нарушителя; выработка контрмер. Для оценки использовались свойства, характеризующие приспособленность разработанных моделей, методик и реализованных на их основе исследовательских прототипов к выполнению оценки защищенности

Аннотации публикаций

1. Konovalov A.M., Kotenko I.V., Shorov A.V. Simulation-Based Study of Botnets and Defense Mechanisms against Them // Journal of Computer and Systems Sciences International, Vol.52, Issue 1, 2013. P.43-65. Pleiades Publishing, Ltd.. DOI: 10.1134/S1064230712060044. (WoS)

Рассматривается подход к исследованию бот-сетей и механизмов защиты от них, основанный на имитационном моделировании с помощью специальной программной среды моделирования, разработанной авторами статьи. Описывается архитектура разработанной среды моделирования, включая библиотеки, необходимые для создания моделей бот-сетей и механизмов защиты. Приводятся данные экспериментов.

2. Igor Kotenko, Andrey Shorov, Evgenia Novikova. Simulation of Protection Mechanisms Based on "Network Nervous System" against Infrastructure Attacks // Proceedings of the 21th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013). Belfast, Northern Ireland, UK. 27th February – 1st March 2013. Los Alamitos, California. IEEE Computer Society. 2013. P.526-533. (WoS, Scopus)

Работа посвящена анализу механизма защиты компьютерной сети "нервная система компьютерной сети", основанного на био-инспирированном подходе. Для исследования данного механизма предложено использовать имитационное моделирование. В работе представлена архитектура системы защиты компьютерной сети, основанной на механизме "нервная система компьютерной сети", описаны алгоритмы ее функционирования и проведены эксперименты. Полученные в ходе выполнения эксперимента результаты были использованы для оценки эффективности механизма "нервная система компьютерной сети" для защиты от инфраструктурных атак.

3. Evgenia Novikova, Igor Kotenko. Analytical Visualization Techniques for Security Information and Event Management // Proceedings of the 21th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013). Belfast, Northern Ireland, UK. 27th February – 1st March 2013. Los Alamitos, California. IEEE Computer Society. 2013. P.519-525. (WoS, Scopus)

В работе представляется архитектура компонента визуализации системы управления информационной безопасностью (SIEM-системы). SIEM-системы позволяют получить обобщенное видение безопасности информационной системы. Предложенная архитектура позволяет легко расширять функциональность системы и интегрировать различные технологии для разработки графических элементов. Для иллюстрации подхода был разработан прототип компонента, который предоставляет графический интерфейс компоненту аналитического моделирования атак.

4. Igor Kotenko, Andrey Shorov, Andrey Chechulin, Evgenia Novikova. Dynamical Attack Simulation for Security Information and Event Management // V. Popovich et al. (eds.), Information Fusion and Geographic Information Systems (IF&GIS 2013), Lecture Notes in Geoinformation and Cartography, DOI: 10.1007/978-3-642-31833-7_14, Springer-Verlag, Berlin, Heidelberg, 2014. P.219-234. (WoS, Scopus)

В работе представляется подход к динамическому моделированию атак и механизмов защиты, предназначенный для использования в системах управления информационной безопасностью (SIEM-системы). Для демонстрации подхода разработан прототип компонента и проведены эксперименты.

5. Igor Kotenko, Olga Polubelova, Igor Saenko. Logical Inference Framework for Security Management in Geographical Information Systems // V. Popovich et al. (eds.), Information Fusion and Geographic Information Systems (IF&GIS 2013), Lecture Notes in Geoinformation and Cartography, DOI: 10.1007/978-3-642-31833-7_14, Springer-Verlag, Berlin, Heidelberg, 2014. P.203-218. (Scopus)

Разработка программных средств реализации логического вывода на основе знаний о безопасности информации и событий является перспективным направлением исследований для обеспечения безопасности в крупных информационных системах, включая распределенные геоинформационные системы. Платформы, которые используют логические языки и системы логического вывода, предоставляют администраторам мощные и гибкие средства, которые обеспечивают верификацию политик безопасности, создание эффективных контрмер против компьютерных атак и поддержание требуемого уровня безопасности. В статье излагается новый подход для разработки и осуществления системы логического вывода для управления информацией и событий безопасности. Рассматриваются общая архитектура этой системы, а также детали архитектуры и реализация конкретных модулей логического вывода, основанные на исчислении событий, методе «проверки на моделях» и онтологическом представлении данных в репозитории.

6. Igor Kotenko, Igor Saenko, Olga Polubelova, Andrey Chechulin. Design and Implementation of a Hybrid Ontological-Relational Data Repository for SIEM systems // Future internet, Vol. 5, No. 3, 2013. P. 355-375. ISSN 1999-5903. doi:10.3390/fi5030355. (Scopus)

Технология безопасности информации и событий управления (SIEM) становится одним из наиболее важных направлений прикладных исследований в области безопасности компьютерной сети. Общая функциональность SIEM-систем в значительной степени зависит от качества решений, реализованных на уровне хранения данных, которые предназначены для представления гетерогенных событий безопасности, их хранения в хранилище данных и извлечения соответствующих данных для аналитических модулей SIEM систем. В статье обсуждаются ключевые вопросы проектирования и реализации гибридного хранилища данных SIEM-системы, которое сочетает в себе данные реляционных и онтологических представлений. На основе анализа существующих SIEM-систем и стандартов, в качестве основного компонента хранилища выбирается онтологический подход и приводится пример онтологической модели данных уязвимостей. Предлагается гибридная архитектура хранилища для реализации в SIEM-системах . Поскольку большая часть работ, выполняемых в хранилище SIEM-системы, основана на реляционной модели данных, статья посвящена гибридному подходу к реализации онтологического компонента. Для проверки хранилища использованы оценки, предназначенные для моделирования атак и анализа безопасности, которые включают показатели онтологической и реляционной модели данных.

7. Igor Kotenko. Experiments with simulation of botnets and defense agent teams // 27th European Conference on Modelling and Simulation (ECMS 2013). Proceedings. May 27 - May 30st, Aalesund University College, Norway. 2013. P.61-67. (WoS)

В статье предлагается подход к многоагентному моделированию бот-сетей и механизмов защиты от них. Основное внимание в статье уделяется представлению улучшенной среды агентно-ориентированного моделирования на примере моделирования бот-сетей, а также экспериментированию с этой среды для анализа различных бот-сетей и механизмов защиты. Эксперименты демонстрируют возможности среды моделирования для исследования различных этапов жизненного цикла бот-сетей и эффективности различных механизмов защиты.

8. Igor Kotenko and Andrey Chechulin. A Cyber Attack Modeling and Impact Assessment Framework // 5th International Conference on Cyber Conflict 2013 (CyCon 2013). Proceedings. IEEE and NATO COE Publications. 4-7 June 2013, Tallinn, Estonia. 2013. P.119-142. (WoS)

Статья содержит описание программного комплекса, предназначенного для аналитического моделирования атак и оценки защищенности на основе моделей. В статье представлен подход к оперативному построению моделей и набор показателей безопасности, наиболее эффективно отражающих состояние защищенности.

9. Igor Kotenko, Igor Saenko, Olga Polubelova and Elena Doynikova. The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems // The 2nd International Workshop on Recent Advances in Security Information and Event Management (RaSIEM 2013). In conjunction with the 8th International Conference on Availability, Reliability and Security (ARES 2013). September 2nd – 6th, 2013. Regensburg, Germany. IEEE Computer Society. 2013. P.638-645. (WoS, Scopus)

Анализ безопасности компьютерной сети является серьезной проблемой. Многие метрики безопасности были предложены для этой цели, но их эффективное использование для быстрой и надежной оценки безопасности и выработки контрмер в SIEM-системах остается важной проблемой. Использование онтологий для представления информации безопасности в SIEM-системах во многом способствует успеху этой задачи. Однако большинство работ по онтологическому представлению данных о безопасности не принимают во внимание онтологии показателей безопасности. В настоящей статье предлагается новый подход с использованием метрик безопасности, который базируется на их онтологическом представлении и служит для всеобъемлющей оценки защищенности и последующей выработки контрмер. Новизна предлагаемого подхода заключается в том, что онтология метрик безопасности рассматривается как основной компонент системы поддержки принятия контрмер. Предложенные решения тестируются на конкретном примере.

10. Igor Kotenko and Evgenia Novikova. VisSecAnalyzer: a Visual Analytics Tool for Network Security Assessment // 3rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2013). In conjunction with the 8th International Conference on Availability, Reliability and Security (ARES 2013). September 2-6, 2013, Regensburg, Germany. Lecture Notes in Computer Science (LNCS), Vol.8128. Springer. 2013, P.345-360. (WoS, Scopus)

В работе представлен общий подход к визуализации в SIEM-системах, который позволяет включать различные технологии визуализации и легко расширять функциональные возможности приложений. Чтобы проиллюстрировать данный подход, разработан компонент визуализации VisSecAnalyzer. В статье продемонстрированы его возможности для задач моделирования атак и оценки защищенности.

11. Igor Kotenko and Andrey Chechulin. Computer Attack Modeling and Security Evaluation based on Attack Graphs // The IEEE 7th International Conference on “Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications” (IDAACS'2013). Proceedings. Berlin, Germany, September 12-14, 2013. P.614-619. (Scopus)

В статье рассматривается подход к моделированию компьютерных атак и оценки защищенности, который предлагается использовать в системах мониторинга и управления безопасностью. Подход основан на моделировании поведения злоумышленника, формирования общего графа атак, обработки текущих предупреждений в реальном времени, модификации графов атак, расчете различных показателей безопасности и обеспечении процедуры оценки защищенности.

12. Igor Kotenko and Elena Doynikova. Security metrics for risk assessment of distributed information systems // The IEEE 7th International Conference on “Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications” (IDAACS'2013). Proceedings. Berlin, Germany, September 12-14, 2013. P.646-650. (Scopus)

В статье рассмотрены основные вопросы и рекомендации по использованию методов оценки риска на основе анализа статических, динамических и исторических сведений. Предложена система показателей защищенности и методы их расчета. Предлагаемые методы основаны на графах атак и зависимостях сервисов. Они позволяют оценить характеристики защищенности для различных сетевых топологий, злоумышленников и атак, а также комплексные свойства и характеристики защищенности, которые рассчитываются на основе анализа "затраты-прибыль" и уязвимостей "нулевого дня".

13. Igor Kotenko, Elena Doynikova, Andrey Chechulin. Security metrics based on attack graphs for the Olympic Games scenario // Proceedings of the 22th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2014). Turin, Italy. 12th - 14th February, 2014. Los Alamitos, California. IEEE Computer Society. 2014. P.561-568. (WoS, Scopus)

Анализ угроз безопасности и расчет показателей защищенности является важной задачей систем мониторинга и управления информационной безопасностью. В статье рассматривается методика расчета показателей безопасности на базе графов атак и зависимостей сервисов. Методика использует несколько аспектов оценки или уровней предметной области (топологический, уровень графа атак, уровень злоумышленника, уровень событий и уровень системы) и позволяет осуществлять настройку в соответствии с различными параметрами работы системы мониторинга и управления информационной безопасностью. Рассматривается также применение этой методики для предметной области "Олимпийских игр".

14. Philipp Nesteruk, Lesya Nesteruk, Igor Kotenko. Creation of a Fuzzy Knowledge Base for Adaptive Security Systems // Proceedings of the 22th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2014). Turin, Italy. 12th - 14th February, 2014. Los Alamitos, California. IEEE Computer Society. 2014. P.574-577. (WoS, Scopus)

Для создания следующего поколения адаптивных систем безопасности должны быть разработаны мощные интеллектуальные компоненты. В статье описывается нечеткая база знаний, специфицирующая связи между угрозами и механизмами защиты. Создание этой нечеткой базы знаний осуществляется с использованием Fuzzy Logic Toolbox пакета Mathworks MATLAB. Цель состоит в том, чтобы повысить эффективность реакций системы защиты на различные угрозы путем минимизации весов нейронных сетей. В статье демонстрируется методика создания такой нечеткой базы знаний для улучшения эффективности механизмов защиты на основе мониторинга и коррекции правил защиты.

15. Igor Kotenko, Elena Doynikova. Security Assessment of Computer Networks based on Attack Graphs and Security Events // The 2014 Asian Conference on Availability, Reliability and Security (AsiaARES 2014). In conjunction with ICT-EurAsia 2014. Bali, Indonesia, April 14th – 17th, 2014. / Linawati et al. (Eds.): ICT-EurAsia 2014, Lecture Notes in Computer Science (LNCS), Vol.8407. IFIP International Federation for Information Processing (2014). Springer. 2014, P.462-471. (WoS, Scopus)

Оценивание защищенности является важной задачей для современных компьютерных сетей. В статье предлагается методика оценивания защищенности на основе графов атак, применимая в современных системах управления информацией и событиями безопасности (Security Information and Events Management, SIEM). Она основана на таксономии показателей защищенности и различных методиках вычисления показателей защищенности, отличающихся в зависимости от данных о текущих событиях безопасности. Предлагаемые показатели формируют основу для отслеживания ситуации по защищенности, и позволяют отразить текущую ситуацию, в том числе развитие атак, источники и цели атак, характеристики атакующих. Продемонстрировано применение предложенной методики на тестовом примере.

16. Igor Kotenko, Andrey Chechulin, Andrey Shorov, Dmitry Komashinsky. Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking. P. Perner (Ed.): 14th Industrial Conference on Data Mining (ICDM 2014), July 16 – 21, 2014, St. Petersburg, Russia. Lecture Notes in Artificial Intelligence (LNAI), DOI 10.1007/978-3-319-08976-8. P. 39–54. ISSN 0302-9743, ISBN 978-3-319-08975-1. (WoS, Scopus)

В статье рассматривается проблема автоматической категоризации веб-сайтов для систем, используемых для блокировки веб-страниц, содержащих неприемлемое содержимое. Авторы применяют методики анализа текста, html тэгов, URL адресов и другой информации методами машинного обучения и интеллектуального анализа данных (Data Mining). Кроме того, предлагаются методики анализа сайтов, предоставляющих информацию на разных языках. Представлена архитектура и алгоритмы системы сбора, хранения и анализа данных, требующихся для классификации сайтов по определенным категориям. Также представлены результаты экспериментов по анализу веб-сайтов разных категорий. Выполнена оценка качества классификации. Разработанная по результатом данной работы система классификации реализована в системах анализа веб-содержимого F-Secure.

17. Kotenko I., Shorov A. Simulation of bio-inspired security mechanisms against network infrastructure attacks // Intelligent Distributed Computing VIII. Studies in Computational Intelligence. Springer-Verlag, Vol.570. Proceedings of 8th International Symposium on Intelligent Distributed Computing - IDC'2014. September 3-5, 2014, Madrid, Spain. Springer-Verlag. P.127-133. (WoS, Scopus)

Рассматривается развитие подхода к моделированию механизмов защиты от инфраструктурных атак на основе биологической метафоры. Представлена спецификация модели атак и механизмов защиты дается. Предложены алгоритмы реализации атак и механизмов защиты. Детально рассмотрена среда для моделирования механизмов безопасности на основе биологической метафоры, представлены эксперименты, которые демонстрируют возможности разработанной системы моделирования.

18. Igor Kotenko, Igor Saenko. Design of Virtual Computer Networks: Data Mining by Genetic Algorithms // Intelligent Distributed Computing VIII. Studies in Computational Intelligence. Springer-Verlag, Vol.570. Proceedings of 8th International Symposium on Intelligent Distributed Computing - IDC'2014. September 3-5, 2014, Madrid, Spain. Springer-Verlag. P.95-105. (WoS, Scopus)

Предлагается подход и его программная реализация для проектирования виртуальных компьютерных сетей на основе генетических алгоритмов

19. Igor Kotenko, Elena Doynikova. Security Evaluation Models for Cyber Situational Awareness // The 2014 IEEE 6th International Symposium on Cyberspace Safety and Security (CSS 2014). August 20-22, 2014, Paris, France. 2014. Los Alamitos, California. IEEE Computer Society. 2014. P.1229-1236. (WoS, Scopus)

В статье рассматриваются методики измерения и вычисления показателей защищенности на основе графов атак и зависимостей сервисов. Методики основаны на нескольких уровнях оценивания (топологическом, графа атак, атакующего, событий и системы) и таких важных аспектах, как атаки нулевого дня и стоимостные характеристики атак. Они позволяют оценить текущую ситуацию по защищенности, в том числе определить уязвимые и слабые места системы, выявить опасные события, параметры проходящих и возможных кибер-атак, намерения атакующих, вычислить интегральные показатели защищенности и определить возможные защитные меры.

20. Igor Kotenko, Evgenia Novikova. Visualization of Security Metrics for Cyber Situation Awareness // The 1st International Software Assurance Workshop (SAW 2014). In conjunction with the 9th International Conference on Availability, Reliability and Security (ARES 2014). September 8nd – 12th, 2014. Fribourg, Switzerland. IEEE Computer Society. 2014. P.506-513. (WoS, Scopus)

Одним из важных направлений исследований в области ситуационной осведомленности является реализация методов визуальной аналитики, которые могут быть эффективно применены при работе с большими данных по безопасности в критических приложениях. В статье рассматривается методика визуальной аналитики для отображения множества метрик безопасности, используемых для оценки общего состояния безопасности сети и оценки эффективности механизмов защиты. Методика призвана помочь в решении задач в области безопасности, которые важны для систем мониторинга управления событиями (SIEM). Предложенный подход подходит для отображения показателей безопасности больших сетей и поддерживает исторический анализ данных. Чтобы продемонстрировать и оценить полезность предложенной методики был реализован прототип приложения для сценария Олимпийских игр.

21. Evgenia Novikova, Igor Kotenko. Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services // International Cross Domain Conference and Workshops (CD-ARES 2014). September 8nd – 12th, 2014. Fribourg, Switzerland. Lecture Notes in Computer Science (LNCS), Vol.8708. Springer-Verlag. 2014, P.63-78. (WoS, Scopus)

Мобильные сервисы денежных переводов (МСДП) в настоящее время развернуты на многих рынках по всему миру и широко используется для внутренних и международных денежных переводов. Тем не менее, они могут быть использованы для отмывания денег и других незаконных финансовых операций. В статье рассматривается интерактивный подход, который позволяет представить поведение абонентов МСДП в соответствии с их деятельностью по выполнению транзакций. Предложенное визуальное представление о поведении пользователей МСДП, основанное на методике визуализации RadViz, помогает определить группы с аналогичным поведением и выбросы. Рассматривается несколько приложений, соответствующих отмыванию денег и мошенничеству. Они используются для оценки эффективности предложенного подхода, а также для представления и обсуждения результатов экспериментов.

22. 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. (WoS, Scopus)

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.

23. Igor Kotenko, Elena Doynikova. Evaluation of Computer Network Security based on Attack Graphs and Security Event Processing // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol.5, No.3, September 2014. P.14-29. (Scopus)

В статье рассматривается проблема оценивания защищенности. Предлагается подход к оцениванию защищенности на основе графов атак, который может применяться в системах управления информацией и событиями безопасности (Security Information and Events Management, SIEM). Ключевой особенностью подхода является применение разработанной системы показателей защищенности, основанной на классификации входных данных, используемых для вычисления показателей. Входные данные включают в том числе информацию о событиях безопасности от SIEM-системы. Предлагаемые показатели создают основу для отслеживания ситуации по защищенности системы путем отражения развития атак, их источников и целей, и характеристик атакующих. Демонстрируется применение предложенной методики на тестовом примере.

24. Igor Saenko, Igor Kotenko. Design of Virtual Local Area Network Scheme based on Genetic Optimization and Visual Analysis // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol.5, No.4, December 2014. (Scopus)

В статье рассатривается подход к генетической оптимизации схемы виртуальной локальной вычислительной сети с использованием разработанного инструментария – средства проектирования схемы VLAN. Авторы предлагают формальную постановку задачи оптимизации схемы VLAN, решение которой может улучшить надежность и безопасность функционирования корпоративной компьютерной сети. В статье показано, что рассматриваемая проблема является одной из форм булевой матричной факторизации. В предложенном генетическом алгоритме был реализован ряд усовершенствований, касающихся формирования начальной популяции, вида функции пригодности, кодирования хромосом и выполнения операций скрещивания и мутации. Средство проектирования схемы VLAN позволяет решать проблему с помощью генетического алгоритма, формировать визуальное представление хода решения задачи и обеспечивает оценку генетического алгоритма. Экспериментальные результаты подтвердили высокую эффективность предложенного генетического алгоритма.

25. Andrey Shorov, Igor Kotenko. The Framework for Simulation of Bio-inspired Security Mechanisms Against Network Infrastructure Attacks // The Scientific World Journal, Volume

2014 (2014), Article ID 172583, 11 pages. http://dx.doi.org/10.1155/2014/172583. (WoS, IF=1.730, Scopus)

В статье представляется биоинспирированный подход под названием " нервная система сети " и методы моделирования инфраструктурных атак и механизмов защиты, основанных на предлагаемом подходе. Механизмы защиты на основе этого подхода включают распределенные процедуры сбора и обработки информации, которые координируют деятельность основных устройств компьютерной сети, идентифицируют атаки и определяют необходимые контрмеры. Атаки и механизмы защиты специфицируются в виде структурных моделей на основе теоретико-множественного подхода. Демонстрируется среда моделирования механизмов защиты, основанных на биологической метафоре, описываются эксперименты, показывающие эффективность механизмов защиты.

26. I.V. Kotenko and I. B. Saenko. Creating New Generation Cybersecurity Monitoring and Management Systems // Herald of the Russian Academy of Sciences, 2014, Vol.84, No.6. P.993–1001. ISSN 1019-3316. DOI: 10.1134/S1019331614060033 (Scopus IF=0.170, WoS)

В статье рассматривается технология управления событиями и информацией безопасности – новое интенсивно развивающееся направление в области кибербезопасности, которое обладает достаточно большим потенциалом как в отношении обнаружения угроз, так и с точки зрения выработки контрмер, обеспечивающих требуемый уровень безопасности информационных инфраструктур. Системы мониторинга и управления кибербезопасностью, ориентированные на эту технологию, предполагают оперативный сбор, хранение и последующую аналитическую обработку данных о событиях, связанных с безопасностью.

27. Igor Kotenko, Andrey Chechulin. Fast Network Attack Modeling and Security Evaluation based on Attack Graphs // Journal of Cyber Security and Mobility, Vol.3, No.1, P.27–46. (Scopus)

В статье предлагается подход к моделированию сетевых атак и оцениванию защищенности, применимый к системам управления информацией и событиями безопасности (Security Information and Events Management, SIEM). Он основан на моделировании сети и поведения злоумышленников, построении графов атак, обработке текущих предупреждений для дополнения частичных графов атак в режиме, близком к реальному времени, вычислении различных показателей защищенности и предоставлении процедур оценивания защищенности. Новизна предлагаемого подхода состоит в применении особых алгоритмов построения, модификации и анализа графов атак, направленных на быструю оценку безопасности. Это позволяет использовать подход в SIEM системах, которые функционируют в режиме, близком к реальному времени. Выделяется архитектура компонента моделирования атак и оценки защищенности (Attack Modeling and Security Evaluation Component, AMSEC), как одного из основных компонентов SIEM систем. Определны основные компоненты и методики моделирования атак и оценки защищенности. Представлен прототип AMSEC.

28. Yana Bekeneva, Konstantin Borisenko, Andrey Shorov, Igor Kotenko. Investigation of DDoS Attacks by Hybrid Simulation // The 2015 Asian Conference on Availability, Reliability and Security (AsiaARES 2015). In conjunction with ICT-EurAsia 2015. October 4th – 7th, 2015, Daejeon, Korea / ICT-EurAsia 2015, Lecture Notes in Computer Science (LNCS), Vol.9357. IFIP International Federation for Information Processing (2015). Springer. 2015, P.179-189. (WoS, Scopus)

В настоящее время защита от распределенных атак типа "отказ в обслуживании" (DDoS) является одной из важнейших задач в области компьютерной безопасности. В статье рассматривается среда моделирования DDoS-атак различных типов, основанная на использовании комбинации имитационного подхода и реальных программно-аппаратных стендов. В работе описаны архитектура системы и серия экспериментов для моделирования DDoS-атак на транспортном уровне и уровне приложений. Представлены экспериментальные результаты и проведен их анализ.

29. 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)

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.

30. Chechulin A.A., Kotenko I.V. Real-Time Security Events Processing using an Approach based on the Attack Trees Analysis // Automatic Control and Computer Sciences, № 8, 2015, Springer, 2015. (Scopus)

В настоящей работе рассмотрен подход, позволяющий повысить скорость обработки событий безопасности с помощью деревьев атак. Особенностью предложенной методики является возможность получения за ограниченное время необходимых решений, причем обоснованность этих решений повышается с увеличением предоставляемого времени. Использование программных средств, основанных на применении данной методики, приведет к возможности выполнять аналитическое моделирование в современных средствах защиты, работающих в режиме, близком к реальному времени.

31. Коновалов А.М., Котенко И.В., Шоров А.В. Исследование бот-сетей и механизмов защиты от них на основе имитационного моделирования // Известия РАН. Теория и системы управления, № 1, 2013, С.45-68. (ВАК, РИНЦ)

Для защиты от бот-сетей необходимо иметь инструменты, позволяющие исследовать процессы, которые происходят на всех этапах жизненного цикла бот-сетей (распространение, управление, выполнение атаки), а также механизмы защиты, которые могут противодействовать бот-сетям. Предлагается подход к исследованию бот-сетей и механизмов защиты от них, основанный на имитационном моделировании с помощью специальной программной среды моделирования, разработанной авторами статьи. Описывается архитектура разработанной среды моделирования, включая библиотеки, необходимые для создания моделей бот-сетей и механизмов защиты. Приводятся данные экспериментов, демонстрирующие возможности среды моделирования для исследования различных этапов функционирования бот-сети, а также эффективности соответствующих механизмов защиты от бот-сетей.

32. Полубелова О.В., Котенко И. В. Построение онтологий уязвимостей и применение логического вывода для управления информацией и событиями безопасности // Безопасность информационных технологий, № 1, 2013, С.21-24. (ВАК, РИНЦ)

В системах управления информацией и событиями безопасности (SIEM) важным аспектом, влияющим на скорость обработки и качество анализа данных, является способ их представления и хранения. Для этой цели в работе предлагается использовать один из популярных в настоящее время стандартов в области безопасности SCAP. Как правило, при построении модели данных на основе этого стандарта для SIEM-систем применяется реляционный поход. Он является не лучшим решением для сложной модели с большим количеством связей, которая в процессе управления безопасностью должна подвергаться разностороннему и глубокому анализу. В качестве альтернативы в работе для представления информации и событий безопасности предлагается использовать онтологический подход. Приводится пример построения онтологии для модели уязвимостей и атак на основе стандарта CVE (MITRE). Для хранения данных используется хранилище триплетов на базе сервера Virtuoso компании OpenLink software.

33. Котенко И.В., Саенко И.Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. Вып.1 (24). СПб.: Наука, 2013. С.21-40. (ВАК, РИНЦ)

В статье приводится описание общей архитектуры системы интеллектуальных сервисов защиты информации (СИСЗИ), предназначенной для использования в критически важных инфраструктурах, а также входящих в ее состав компонентов. В общей архитектуре СИСЗИ выделяются три уровня: данных, событий и прикладной. Рассматриваются структурная и функциональная модели общей архитектуры СИСЗИ, позволяющие определить основные функциональные механизмы для выделенных уровней. В качестве основных компонентов СИСЗИ, для которых приводится более детальное описание их архитектурного построения, рассматриваются модуль управления корреляцией событий, прогностический анализатор безопасности, компонент моделирования атак и поведения системы защиты, компонент поддержки решений и реагирования, модуль визуализации и репозиторий.

34. Котенко И.В., Саенко И.Б. Научный анализ и поддержка политик безопасности в киберпространстве: обзор перспективных исследований по результатам Международного семинара SA&PS4CS 2012 // Труды СПИИРАН. Вып.1 (24). СПб.: Наука, 2013. С.66-88. (ВАК, РИНЦ)

В статье приводится аналитический обзор докладов ведущих зарубежных и отечественных специалистов в области обеспечения безопасности компьютерных сетей, сделанных на втором Международном семинаре "Научный анализ и поддержка политик безопасности в киберпространстве" (SA&PS4CS 2012), проходившем в Санкт-Петербурге 20 октября 2012 года. Основными темами выступлений семинара являлись обнаружение, распознавание и определение различных видов деятельности злоумышленников, реагирование на атаки и вторжения в киберпространстве, включая информационные операции национального уровня, идентификация новых перспективных технологий, способов, методов и средств обеспечения взаимодействия в области поддержки политик безопасности в киберпространстве.

35. Котенко И.В., Саенко И.Б., Полубелова О.В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. Вып.2 (25). СПб.: Наука, 2013. С.113-134. (ВАК, РИНЦ)

В статье приводится анализ наиболее известных и развитых в настоящее время систем хранения данных в части их использования для построения репозитория перспективных систем мониторинга и управления безопасностью информации (SIEM–систем). Анализу подвергаются реляционные СУБД, XML–базы данных и хранилища триплетов. Предложена и прокомментирована реляционная схема данных, интегрирующая аналитические модули SIEM–системы. Приведена классификация и характеристика известных средств построения и использования XML–баз данных. Среди хранилищ триплетов сделан выбор в пользу системы Virtuoso, обеспечивающей гибридный подход к построению репозитория в перспективных SIEM–системах, который был апробирован на решении задач моделирования атак и анализа защищенности.

36. Котенко И.В., Саенко И.Б. Математические модели, методы и архитектуры для защиты компьютерных сетей: обзор перспективных исследований по результатам Международной конференции MMM–ACNS–2012 // Труды СПИИРАН. Вып.2 (25). СПб.: Наука, 2013. С.148-170. (ВАК, РИНЦ)

В статье приводится аналитический обзор перспективных направлений исследований по результатам докладов ведущих зарубежных и отечественных специалистов в области обеспечения безопасности компьютерных сетей, сделанных на шестой Международной конференции «Математические модели, методы и архитектуры для защиты компьютерных сетей» (MMM–ACNS–2012), проходившей в Санкт-Петербурге с 17 по 19 октября 2012 года. На секциях конференции были рассмотрены актуальные вопросы, связанные с предотвращением, обнаружением и реагированием на вторжения, противодействием вредоносному программному обеспечению, прикладной криптографией и протоколами безопасности, разграничением доступа и защитой информации, управлением событиями и информацией безопасности, моделированием защиты информации и безопасностью облачных вычислений, политиками безопасности.

37. Нестерук Ф.Г., Котенко И.В. Инструментальные средства создания нейросетевых компонент интеллектуальных систем защиты информации // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.7-25. (ВАК, РИНЦ)

На рынке инструментальных средств создания нейросетевых интеллектуальных систем представлено большое количество программных средств, что объясняется многоплановостью задач интеллектуальной обработки информации. В работе предлагается обзор инструментальных средств, применимых для создания нейросетевых компонент интеллектуальных систем защиты информации

38. Котенко И.В., Полубелова О.В., Чечулин А.А. Построение модели данных для системы моделирования сетевых атак на основе онтологического подхода // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.26-39. (ВАК, РИНЦ)

В статье рассматривается задача построения модели данных на основе онтологического подхода для системы моделирования сетевых атак, являющейся частью SIEM-системы. Приводится общая схема данных для данной системы, построенная на базе SCAP-протокола. Выполнен анализ релевантных работ, в которых рассматриваются использование онтологий для различных систем защиты информации. Более подробно в работе рассматривается построение онтологий для SCAP-протокола. В качестве примера реализации модели данных для системы моделирования сетевых атак предлагается онтология для представления модели уязвимостей.

39. Чечулин А.А. Методика оперативного построения, модификации и анализа деревьев атак // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.40-53. (ВАК, РИНЦ)

Применение методик моделирования сетевых атак является перспективным направлением в области защиты информации. В статье рассматривается подход к аналитическому моделированию сетевых атак на основе деревьев атак. Новизна предлагаемой методики заключается в возможности ее применения в системах, работающих в режиме близком к реальному времени. В статье рассмотрены основные модели предметной области и элементы алгоритмов формирования и модификации деревьев атак.

40. Дойникова Е. В. Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.54-68. (ВАК, РИНЦ)

В данной работе рассматриваются основные направления исследований в области показателей защищенности и вводится сформированная на их основе классификация показателей. Кроме того, предлагается многоуровневый подход к оценке защищенности, включающий систему показателей защищенности и методики их расчета, основанные на графах атак и зависимостях сервисов. Данный подход позволяет оценивать различные аспекты защищенности системы с учетом ее топологии, режима работы, исторических данных об инцидентах и другой информации.

41. Полубелова О. В. Архитектура и программная реализация системы верификации правил фильтрации // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.79-90. (ВАК, РИНЦ)

В статье описывается общая архитектура системы верификации правил фильтрации межсетевого экрана, а также рассматриваются аспекты программной реализации этой системы. Реализация выполнена на основе применения метода "проверки на модели" (Model Checking). В качестве верификатора используется программная система SPIN. Также был разработан пользовательский интерфейс, который позволяет загружать данные о верифицируемой системе, правила политики фильтрации, управлять процессом верификации, а также в удобном виде представлять ее результаты. Кроме того, в предлагаемой системе реализована возможность применить различные стратегии разрешения аномалий.

42. Комашинский Д. В. Обнаружение и идентификация вредоносных исполняемых программных модулей с помощью методов Data Mining // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.115-125. (ВАК, РИНЦ)

Исследование затрагивает проблему улучшения основных характеристик систем обнаружения и идентификации вредоносных исполняемых файлов на основе методов Data Mining. Определяется общая структура процессов построения и эксплуатации систем данного класса. На ее основе уточняется перечень нефункциональных требований к подобным системам. Задача работы определяется в виде поиска эффективных моделей представления исполняемых объектов, позволяющих получать компактные и информативные вектора описаний анализируемых объектов. Излагается суть предлагаемых подходов к обнаружению и выявлению вредоносных программ на основе статической позиционно-зависимой информации и низкоуровневых динамических признаков. Представляется архитектура разработанной системы выявления вредоносных программ и результаты практической проверки разработанных моделей представления.

43. Комашинский Д.В. Подход к выявлению вредоносных документов на основе методов интеллектуального анализа данных // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.126-135. (ВАК, РИНЦ)

Работа посвящена проблеме безопасности файловых объектов формата Portable Document Format. Обобщаются существующие практики, нацеленные на выявление вредоносных документов. Формируется набор основных групп статических признаков вредоносных и безопасных документов. Собранные данные используются для построения системы автоматической классификации новых, ранее неизвестных документов, на основе методов интеллектуального анализа данных (Data Mining). Анализ результатов использования отдельных групп признаков позволяет сформировать новую модель представления документов, основанную на описании взаимосвязей и содержания их основных структурных элементов. Применение полученной модели позволяет оптимизировать целевую функцию систем обнаружения вредоносных документов в базисе требований к точности принятия решения и времени анализа.

44. Десницкий В.А., Котенко И.В. Конфигурирование встроенных систем защиты информации в рамках сервисов обеспечения комплексной безопасности железнодорожного транспорта // Труды СПИИРАН. Вып.7 (30). СПб.: Наука, 2013. С. 40-55. (ВАК, РИНЦ)

В работе представлены концепция разработки комбинированной защиты встроенных устройств, применимая в процессе разработки механизмов защиты информации систем и сервисов обеспечения комплексной безопасности железнодорожного транспорта. Предлагаются модель процесса конфигурирования компонентов защиты встроенных устройств, а также методика конфигурирования, разработанные с учетом экспертных знаний в предметной области информационной безопасности встроенных устройств. Цель конфигурирования – найти такую конфигурацию защиты, которая реализует все необходимые требования защиты и ограничения со стороны платформы устройства, удовлетворяет заданным критериям ресурсопотребления и не содержит известных видов несовместимостей компонентов защиты.

45. Котенко И.В., Дойникова Е.В., Чечулин А.А. Динамический перерасчет показателей защищенности на примере определения потенциала атаки // Труды СПИИРАН. Вып.7 (30). СПб.: Наука, 2013. С. 26-39. ISSN: 2078-9181. (ВАК, РИНЦ)

Анализ информационных рисков и вычисление показателей защищенности являются важными задачами для систем управления информацией и событиями безопасности (Security Information and Events Management, SIEM). Они позволяют определить текущую ситуацию в области защищенности и необходимые контрмеры. Данная статья рассматривает методику вычисления показателей защищенности во времени, близком к реальному, и демонстрирует ее применение на примере перерасчета потенциала атаки.

46. Котенко И.В., Саенко И.Б., Чернов А.В., Бутакова М.А. Построение многоуровневой интеллектуальной системы обеспечения информационной безопасности для автоматизированных систем железнодорожного транспорта // Труды СПИИРАН. Вып.7 (30). СПб.: Наука, 2013. С.7-25. (ВАК, РИНЦ)

В статье рассматриваются особенности построения и функционирования автоматизированных систем железнодорожного транспорта. В качестве основных отличительных факторов выделены достаточно большое многообразие и разнородность таких систем, их взаимная связность и связность с сетями общего пользования и сильная разнородность внутренних пользователей. Представлена и рассмотрена архитектура многоуровневой системы обеспечения информационной безопасности, которая предложена для защиты информации в автоматизированных системах железнодорожного транспорта. Для хранения данных о безопасности в многоуровневой интеллектуальной системе защиты предложено использование гибридного онтологического репозитория. Для интеллектуальных сервисов анализа данных, находящихся на верхнем уровне рассматриваемой системы защиты, предложены формальные постановки задачи. Анализ этих постановок показал, что разработка интеллектуальных сервисов управления корреляцией, анализа защищенности и моделирования атак следует относить к задачам анализа. Интеллектуальные сервисы поддержки принятия решений и визуального анализа данных относятся к задачам синтеза.

47. Десницкий В.А. Методика верификации сетевых информационных потоков в информационно-телекоммуникационных системах со встроенными устройствами // Труды СПИИРАН. Вып.7 (30). СПб.: Наука, 2013. С. 246-257. (ВАК, РИНЦ)

В работе представлена методика верификации сетевых информационных потоков информационно-телекоммуникационных систем со встроенными устройствами. Цель методики – оценка защищенности разрабатываемой системы и проверка соответствия информационных потоков в реальной системе заданным политикам. Проводимая верификация базируется на методе «проверки на модели» с использованием программного средства SPIN. Верификация информационных потоков проводится на начальных этапах проектирования и обеспечивает более раннее обнаружение противоречий в используемой политике безопасности и несоответствий топологии сети требованиям информационно-телекоммуникационной системы.

48. Котенко И.В., Новикова Е.С. Визуальный анализ для оценки защищенности компьютерных сетей // Информационно-управляющие системы, 2013, № 3, С.55-61. (ВАК, РИНЦ)

Анализируются методики визуального анализа защищенности компьютерных сетей. Описывается компонент визуализации системы оценки защищенности компьютерной сети, отличающийся от других систем тем, что позволяет графически представлять как отчеты сканеров уязвимостей, так и результаты моделирования атак, благодаря чему пользователь системы может соотнести потенциальные причины нарушения безопасности с возможными последствиями их эксплуатации злоумышленником.

49. Котенко И.В., Саенко И.Б. Перспективные модели и методы защиты компьютерных сетей и обеспечения безопасности киберпространства: обзор международных конференции MMM-ACNS-2012 и семинара SA&PS4CS 2012 // Информационно-управляющие системы, 2013, № 3, С.97-99. ISSN 1684-8853. (ВАК, РИНЦ)

На основе анализа докладов международной конференции "Математические модели, методы и архитектуры для защиты компьютерных сетей" (MMM-ACNS-2012) и 2-го международного семинара «Научный анализ и поддержка политик безопасности в киберпространстве» (SA&PS4CS 2012) анализируются перспективные модели, методы и архитектуры для защиты компьютерных сетей.

50. Десницкий В.А., Котенко И.В. Проектирование защищенных встроенных устройств на основе конфигурирования // Проблемы информационной безопасности. Компьютерные системы, № 1, 2013. С.44-54. (ВАК, РИНЦ)

В работе предложена модель процесса проектирования защищенных встроенных устройств на основе комбинирования отдельных компонентов защиты. Вводится понятие конфигурации, которая представляет собой набор компонентов защиты, способных предоставить устройству некоторый защитный функционал. Путем анализа свойств компонентов защиты формируется множество допустимых конфигураций, из которых на основе критериев оптимальности выбираются наиболее эффективные. Представлена архитектура программного средства конфигурирования на основе UML-диаграмм, а также приведен демонстрационный пример встроенного устройства, позволяющий показать применимость разработанной модели на практике.

51. Полубелова О.В., Котенко И.В. Методика верификации правил фильтрации методом “проверки на модели” // Проблемы информационной безопасности. Компьютерные системы, № 1, 2013. С.151-168. (ВАК, РИНЦ)

В статье предлагается методика верификации правил фильтрации межсетевых экранов для обнаружения аномалий фильтрации, основанная на применении метода “проверки на модели” (Model Checking). Представляются основные компоненты, на которых базируется предлагаемая методика, модели компьютерной сети, межсетевого экрана и аномалий фильтрации, а также алгоритмы обнаружения аномалий. Рассматриваются аспекты реализации системы верификации, а также результаты проведенных экспериментов.

52. Новикова Е.С., Котенко И.В. Проектирование компонента визуализации для автоматизированной системы управления информационной безопасностью // Информационные технологии, № 9, 2013. С.32-36. (ВАК, РИНЦ)

В статье представляются результаты проектирования подсистемы визуализации автоматизированной систем управления информационной безопасностью. Исследуются механизмы визуализации в современных системах управления информационной безопасностью. Описываются архитектура подсистемы визуализации, позволяющая расширять графический функционал системы и использовать различные технологии для реализации графических элементов. Приводится описание реализации системы, иллюстрирующего предложенный подход.

53. Котенко И.В., Саенко И.Б., Чечулин А.А. Проактивное управление информацией и событиями безопасности в информационно-телекоммуникационных системах // Вопросы радиоэлектроники. Сер. СОИУ. 2014. Вып. 1. С. 170–180. (ВАК, РИНЦ)

В статье рассматриваются вопросы построения проактивных систем управления и мониторинга безопасности информации для современных информационно-телекоммуникационных систем. Обсуждаются решения, полученные в ключевых областях, связанных с построением репозитория и анализом событий безопасности на основе моделирования сетевых атак.

54. Чечулин А.А., Котенко И.В. Построение графов атак для анализа событий безопасности // Безопасность информационных технологий, № 3, 2014, С.135-141. (ВАК, РИНЦ)

В настоящей работе предложен подход к использованию системы моделирования атак для повышения точности и оперативности обнаружения атак в общем потоке событий. Рассмотренные в статье задачи являются составными элементами общей системы управления инцидентами и событиями. Кроме того, предложенный подход позволяет после обнаружения атаки вычислить вероятные характеристики нарушителя (такие как, уровень знаний, технические возможности, цели, и т.д.), предсказать возможные направления развития атаки и возможные действия нарушителя, которые предшествовали проведению основной атаки (захват управления над сетевым оборудованием, кража паролей и т.д.). Результатом работы системы моделирования атак также могут быть следующие характеристики: (1) слабые места в топологии сети (хосты, через которые проходит наибольшее число графов атак); (2) выбранные контрмеры, позволяющие снизить вероятность максимального количества графов атак; (3) возможные последствия реализации контрмер, учитывающие зависимости сервисов.

55. Котенко И.В., Дойникова Е.В. Вычисление и анализ показателей защищенности на основе графов атак и зависимостей сервисов // Проблемы информационной безопасности. Компьютерные системы, № 2, 2014. С.19-36. (ВАК, РИНЦ)

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".

56. 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. (ВАК, РИНЦ)

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".

57. Чечулин А.А., Котенко И.В. Обработка событий безопасности в условиях реального времени с использованием подхода, основанного на анализе деревьев атак // Проблемы информационной безопасности. Компьютерные системы, № 3, 2014. С.56-59. (ВАК, РИНЦ)

В статье представлен подход, позволяющий использовать аналитическое моделирование атак в системах защиты информации, работающих в режиме, близком к реальному времени.

58. Федорченко А.В., Чечулин А.А., Котенко И.В. Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения // Проблемы информационной безопасности. Компьютерные системы, № 3, 2014. С.131-135. (ВАК, РИНЦ)

В статье представлен анализ открытых баз данных уязвимостей. Приведена статистика и выявлены тенденции обнаружения уязвимостей в программно-аппаратном обеспечении основных разработчиков.

59. Котенко И.В., Саенко И.Б. К новому поколению систем мониторинга и управления безопасностью // Вестник Российской академии наук, Том 84, № 11, 2014, С.993–1001. (ВАК, РИНЦ)

В статье обобщены основные результаты проекта MASSIF по построению систем управления событиями и информацией безопасности, а также рассмотрены возможные сценарии применения этих разработок.

60. Котенко И.В., Саенко И.Б., Юсупов Р.М. Новое поколение систем мониторинга и управления инцидентами безопасности // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. СПбГПУ, 2014, № 3 (198), С.7-18. (ВАК, РИНЦ)

Обоснована технологическая необходимость разработки нового поколения систем мониторинга и управления инцидентами безопасности, основанных на технологии управления информацией и событиями безопасности. Приведены типовая архитектура и основные решения по построению отдельных модулей таких систем, осуществляющих устойчивый сбор данных о событиях безопасности, их универсальную трансляцию, масштабируемую обработку, гибридное онтологическое хранение и многофункциональную визуализацию, а также межуровневую корреляцию событий, моделирование атак и прогностический анализ безопасности. Сформулированы предложения по применению таких систем в предметных областях, касающихся обеспечения безопасности в критических инфраструктурах.

61. Федорченко А.В., Чечулин А.А., Котенко И.В. Построение интегрированной базы данных уязвимостей // Изв. вузов. Приборостроение, Т.57, № 10, 2014, С.62-67. ISSN 0021-3454. (ВАК, РИНЦ)

Представлены результаты исследования открытых баз данных уязвимостей и описание процесса их интеграции для применения в системах оценивания защищенности компьютерных сетей. Предлагаются модель процесса формирования и структура интегрированной базы уязвимостей, а также описание и анализ разработанного прототипа.

62. Дойникова Е.В., Котенко И.В. Отслеживание текущей ситуации и поддержка принятия решений по безопасности компьютерной сети на основе системы показателей защищенности // Изв. вузов. Приборостроение, Т.57, № 10, 2014, С.72-77. ISSN 0021-3454. (ВАК, РИНЦ)

Рассматривается подход к отслеживанию текущей ситуации по защищенности компьютерной сети и поддержке принятия решений по реагированию на инциденты безопасности, основанный на использовании предлагаемой системы показателей защищенности и разработанных моделей и алгоритмов их расчета. Ключевой особенностью подхода является учет разноплановой информации при вычислении показателей защищенности, что позволяет более точно отразить текущую ситуацию по безопасности компьютерной сети.

63. Десницкий В.А., Котенко И.В. Использование экспертных знаний для разработки защищенных систем со встроенными устройствами // Информационные технологии и вычислительные системы, № 4, 2014, С.17-32. (ВАК, РИНЦ)

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.

64. Федорченко А.В., Чечулин А.А., Котенко И.В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных систем и сетей // Информационно-управляющие системы, 2014, №5, С.72-79. (ВАК, РИНЦ)

Произведен разбор и сравнение форматов открытых баз уязвимостей, а так же форматов словарей продуктов и показателей, характеризующих уязвимости. Собрана статистика обнаруженных уязвимостей в распространенных операционных системах и веб-браузерах, а также получено распределение уязвимых продуктов основных разработчиков программного обеспечения за последние 10 лет.

65. Носков А.Н., Чечулин А.А., Тарасова Д.А. Исследование эвристических подходов к обнаружению атак на телекоммуникационные сети на базе методов интеллектуального анализа данных // Труды СПИИРАН. Вып.6 (37). СПб.: Наука, 2014. (ВАК, РИНЦ)

Анализ методик систем обнаружения сетевых атак является перспективным направлением в области защиты сетей и сетевых систем. В статье рассматривается подход к оценке алгоритмов и механизмов обнаружения атак. Новизна предлагаемой методики заключается в возможности создания самообучающихся систем для обнаружения вторжения. В статье рассмотрены основные элементы алгоритмов обнаружения атак.

66. Агеев С.А., Саенко И.Б., Егоров Ю.П., Гладких А.А., Богданов А.В. Интеллектуальное иерархическое управление рисками информационной безопасности в защищенных мультисервисных сетях специального назначения // Автоматизация процессов управления. Вып. №3 (37), 2014. ISSN 1991-2927. С.78-88. (ВАК, РИНЦ)

Рассматриваются основные подходы построения интеллектуальных методов и алгоритмов, синтезированных на их основе, оценки и управления рисками информационной безопасности защищенных мультисервисных сетей (ЗМС). Показана необходимость применения интеллектуальных методов управления ЗМС. Разработана и исследована математическая модель оценки риска информационной безопасности ЗМС.

67. Куваев В.О., Саенко И.Б. Концептуальные основы интеграции неоднородных информационных ресурсов предприятия в едином информационном пространстве // Проблемы экономики и управления в торговле и промышленности, № 7 (007), 2014. – С. 101-104. ISSN 2309-3064. (ВАК, РИНЦ)

В статье излагаются концептуальные основы интеграции неоднородных информационных ресурсов предприятия в едином информационном пространстве. Формулируются формализованные постановки задач, необходимые для эффективной интеграции информационных ресурсов.

68. Саенко И.Б., Куваев В.О., Алышев С.В. Подход к построению системы показателей качества единого информационного пространства // Естественные и математические науки в современном мире, 2014. № 14. С. 51-56. (ВАК, РИНЦ)

В статье приводится описание системы показателей качества, предназначенной для оценки единого информационного пространства. Выделяются наиболее существенные характеристики и предлагаются показатели для их оценки.

69. 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.

70. Котенко И.В., Шоров А.В. Исследование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода «нервная система сети» // Проблемы информационной безопасности. Компьютерные системы, № 3, 2015. С.45-55. (ВАК, РИНЦ)

Развивается подход к имитационному моделированию механизмов защиты от инфраструктурных атак на основе биологической метафоры. Дана спецификация моделей инфраструктурных атак и механизмов защиты от них с помощью теоретико-множественного подхода. Представлены алгоритмы реализации атак и

механизмов защиты. Детально рассмотрена среда моделирования механизмов защиты на основе биологической метафоры «нервная система сети». Произведена оценка основных показателей эффективности реализованной среды моделирования.

71. 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.

72. Браницкий А.А., Котенко И.В. Построение нейросетевой и иммуноклеточной системы обнаружения вторжений // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015. С.23-27. (ВАК, РИНЦ)

В статье рассматриваются методы обнаружения и классификации аномальных образцов сетевых соединений с использованием аппарата искусственных нейронных сетей и эволюционной модели иммунной системы.

73. Котенко И.В., Новикова Е.С., Чечулин А.А. Визуализация метрик защищенности для мониторинга безопасности и управления инцидентами // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015. С.42-47. (ВАК, РИНЦ)

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.

74. 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

75. Дойникова Е.В., Котенко И.В., Чечулин А.А. Динамическое оценивание защищенности компьютерных сетей в SIEM-системах // Безопасность информационных технологий, № 3, 2015. (ВАК, РИНЦ)

В статье предлагается подход к оцениванию защищенности компьютерных сетей, основанный на графах атак, и предназначенный для систем управления информацией и событиями безопасности. Основной особенностью подхода является применение разноуровневой системы показателей защищенности, определяющей профиль защищаемой системы в зависимости от характера применяемых для расчета показателей данных и методик вычисления показателей. Это позволяет корректировать оценку защищенности в режиме, близком к реальному времени, распознавать предыдущие и прогнозировать последующие шаги атак, определять цели и характеристики атакующих. На основе предлагаемого подхода реализован прототип системы оценивания защищенности и проведен анализ его функционирования на нескольких сценариях атак.

76. Котенко И.В., Дойникова Е.В. Методика выбора контрмер на основе комплексной системы показателей защищенности в системах управления информацией и событиями безопасности // Информационно-управляющие системы, 2015, № 3, С.60-69. doi:10.15217/issn1684-8853.2015.3.60. (ВАК, РИНЦ)

В статье предлагается методика выбора контрмер в процессе управления информацией и событиями безопасности. Разработанная методика основана на предложенной авторами комплексной системе показателей защищенности, отражающих ситуацию по безопасности в системе. Для выбора контрмер в систему показателей вводится дополнительный уровень поддержки принятия решений, базирующийся на показателях оценки эффективности применения контрмер. Основными особенностями предлагаемого подхода является использование графов атак и зависимостей сервисов, применение введенной в статье модели контрмер и предложенных показателей защищенности, а также возможность предоставления решения по выбору контрмер в любой момент времени в зависимости от текущей информации о состоянии защищенности и событиях безопасности.

77. Браницкий А.А., Котенко И.В. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейро-нечетких классификаторов // Информационно-управляющие системы, 2015, № 4, С.69-77. doi:10.15217/issn1684-8853.2015.4.69. (ВАК, РИНЦ)

В статье предложена обобщенная схема комбинирования классификаторов для обнаружения сетевых атак. На ее основе разработано программное средство, которое позволяет анализировать сетевой трафик на наличие аномальной сетевой активности.

78. Коломеец М.В., Чечулин А.А., Котенко И.В. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН. 2015. Вып. 42. С. 232-257. (ВАК, РИНЦ)

В статье рассматриваются основные методологические примитивы на примере поэтапного построения модели визуализации с заранее подготовленными данными, с целью сформировать комплексное видение процесса создания модели и влияющих на неё аспектов. Приводится классификация примитивов и их связи между собой в соответствии с этапами построения модели. Рассматриваются библиотеки визуализации на популярных языках программирования.

79. Куваев В.О., Чечулин А.А., Ефимов В.В., Лыжинкин К.В. Варианты построения единого информационного пространства для интеграции разнородных автоматизированных систем // Информация и космос. Научно-технический журнал, № 4, 2015. С. 83-87. (ВАК, РИНЦ)

В статье рассматриваются возможные варианты построения единого информационного пространства, объединяющего информационные ресурсы разнородных автоматизированных систем. Приведены классификационные признаки построения единого информационного пространства. Предложена система показателей качества, полученная при подходе, в котором на информационные средства распространяются результаты анализа стандартов и исследований в области оценки качества программных средств. Проводится анализ номенклатуры качества программного обеспечения, следующих действующих стандартов: отечественном стандарте ГОСТ Р ИСО/МЭК 9126-93 и пакете международных стандартов ISO 9126. Предложенный подход к построению системы показателей качества единого информационного пространства задает основу для анализа и синтеза вариантов построения единого информационного пространства в условиях строгого учета предъявляемых к нему требований. Предложена методика оценки качества единого информационного пространства.