Форма 501. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ

1.1 Номер проекта

13-01-00843

1.2 Руководитель проекта (фамилия, имя, отчество)

Котенко Игорь Витальевич

1.3 Название проекта

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

1.4 Код и название конкурса

А Инициативный

1.5 Год представления отчета

2013

1.6 Вид Отчета (цифра 1 – итоговый; цифра 2 - этап 2013 г.)

2

1.7 Аннотация (не более 1 стр.; описать содержание фактически проделанной за отчетный период работы и полученные результаты: для итоговых отчетов – за весь период работы над проектом, для промежуточных – за 2013 год)

Проведен детальный анализ состояния современных исследований в области построения интеллектуальных сервисов защиты информации в критически важных инфраструктурах. Разработаны формальная постановка задачи исследования, основные требования и формальные модели компонентов исследовательского моделирования компьютерных атак и процессов защиты от них, анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации. Проведены исследования в области разработки компонента визуализации, предназначенного для реализации нового поколения функций визуального анализа информации безопасности, а также перспективных компонентов хранения данных о событиях безопасности. Разработан гибридный онтологический репозиторий, обеспечивающий моделирование данных о событиях и политиках безопасности. Предложена архитектура исследовательских макетов моделирования компьютерных атак и процессов защиты от них, анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации. Выполнена первоначальная экспериментальная оценка полученных результатов с помощью исследовательских прототипов и компьютерного моделирования. Получены свидетельства о государственной регистрации программ для ЭВМ для конфигуратора системы защиты встроенных устройств, верификатора правил фильтрации политики безопасности, системы визуализации логов сервиса мобильных денежных переводов, компонента генетической оптимизации схемы разграничения доступа в виртуальной локальной вычислительной сети и компонента прогнозирования состояния локальной сети с помощью искусственных нейронных сетей.

1.8 Полное название организации, предоставляющей условия для выполнения работ по Проекту физическим лицам (использовать только официально утвержденное название)

Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Форма 503. 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 (в порядке значимости)

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

3.4 Объявленные ранее цели проекта на 2013 год

Основные цели проекта на 2013 год сводились к следующему:
1) детальный анализ состояния современных исследований в области построения интеллектуальных сервисов защиты информации в критически важных инфраструктурах, в том числе в исследовательском моделировании компьютерных атак и процессов защиты от них, анализе защищенности компьютерных систем и сетей и определении рисков безопасности информации;
2) разработка формальной постановки задачи исследования, основных требований и формальных моделей компонентов исследовательского моделирования компьютерных атак и процессов защиты от них, анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации;
3) разработка архитектуры исследовательских макетов моделирования компьютерных атак и процессов защиты от них, анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации;
4) проведение первоначальной экспериментальной оценки полученных результатов с помощью исследовательских прототипов и компьютерного моделирования.

3.5 Степень достижения поставленных в проекте целей

Все задачи, запланированные в проекте на 2013 год, выполнены полностью. Дополнительно проведены исследования в области разработки компонента визуализации, предназначенного для реализации нового поколения функций визуального анализа информации безопасности, а также перспективных компонентов хранения данных о событиях безопасности, и разработан гибридный онтологический репозиторий, обеспечивающий моделирование данных о событиях и политиках безопасности.

3.6 Полученные в 2013 году важнейшие результаты

1. Проведен детальный анализ состояния современных исследований в области построения интеллектуальных сервисов защиты информации в критически важных инфраструктурах.

2. Разработаны формальная постановка задачи исследования, основные требования и формальные модели компонентов исследовательского моделирования компьютерных атак и процессов защиты от них, анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации.
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 (например, Apache, MySQL и т.д.).

3. Проведены исследования в области разработки компонента визуализации, предназначенного для реализации нового поколения функций визуального анализа информации безопасности.
Архитектура подсистемы 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.

4. Проведены исследования в области разработки перспективных компонентов хранения данных о событиях безопасности и разработан гибридный онтологический репозиторий, обеспечивающий моделирование данных о событиях и политиках безопасности.

Выполнена классификация и характеристика известных средств построения и использования XML–баз данных, в которой выделены такие классы, как «естественные» (natural) и «встроенные» (embedded), и хранилищ триплетов. Среди отечественных XML-баз данных особое внимание обращено на СУБД Sedna, которая относится к первому классу. Среди хранилищ триплетов сделан выбор в пользу комплексных систем хранения триплетов, сочетающих возможности всех трех типов моделей данных и обеспечивающих гибридный подход к построению репозитория в перспективных системах разграничения доступа.

Предложенный гибридный онтологический репозиторий включает онтологическое информационное хранилище и модули для реализации конкретных механизмов логического вывода - исчисление событий и метод «проверки на моделях».

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).

Модуль исчисления событий использует процедуру абдуктивного вывода CIFF, реализованную в CIFF 4.0 с использованием SICStus Prolog. Как один из вариантов, в процедуре CIFF используется предметно-независимая аксиоматика, состоящая из пяти аксиом. Имея в качестве входа формулу, которая выражает противоречивое состояние системы, процедура абдуктивного вывода определяет последовательность событий, которая приводит систему к этому состоянию. В качестве исходных данных модуль исчисления событий использует следующие данные: описание защищаемой системы, описание политик безопасности и описание аномалий (конфликтов). В качестве результата функционирования этого модуля выдаются данные об итогах верификации политик разграничения доступа и модифицированные правила, которые позволяют разрешить конфликты.

Метод “проверки на модели” позволяет исследовать пространство состояний, покрывающих с некоторой степенью точности, все возможные пути спецификации системы. “Проверка на модели” позволяет продемонстрировать, что специфицированная система (программа) обладает желаемыми свойствами, изучая все возможные пути выполнения программы, а если свойства не выполняются, то предоставляет контрпримеры с нарушением свойств. Для реализации этого метода разработан алгоритм проведения логического вывода, входными данными которого являются описания системы, политик и противоречий. Выходными данными являются: результаты верификации “да/нет”, информация о найденных противоречиях, включающая их тип, правила, применение которых к ним приводит, а также изменения, которые надо внести в правила, чтобы политика разграничения доступа стала непротиворечивой. Работа алгоритма происходит в два этапа. На первом этапе осуществляется поиск пересечений между условиями правила разграничения доступа, на втором — определяется тип аномалии.

Данный подход был успешно апробирован на решении ряда задач, связанных с моделирования атак и анализом защищенности информационных и телекоммуникационных систем от несанкционированного доступа.

5. Разработана архитектура исследовательских макетов моделирования компьютерных атак и процессов защиты от них, анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации.

Для реализации предложенного подхода была построена распределенная архитектура, основанная на следующих программных продуктах: сервер приложений Apache Tomcat, СУБД Virtuoso, сканер безопасности MaxPatrol, Nmap или Nessus. Элементы исследовательских макетов были реализованы как сервисы, запущенные на сервере приложений. Макеты моделирования компьютерных атак и процессов защиты от них, анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации включают в себя следующие функциональные подсистемы: подсистему хранения исходных данных; генератор модели

компьютерной сети и нарушителей; генератор деревьев атак, работающий в режиме построения и модификации; подсистему анализа данных и определения рисков безопасности информации.

6. Проведена первоначальная экспериментальная оценка полученных результатов с помощью исследовательских прототипов и компьютерного моделирования. Получены свидетельства о государственной регистрации программ для ЭВМ для конфигуратора системы защиты встроенных устройств, верификатора правил фильтрации политики безопасности, системы визуализации логов сервиса мобильных денежных переводов, компонента генетической оптимизации схемы разграничения доступа в виртуальной локальной вычислительной сети и компонента прогнозирования состояния локальной сети с помощью искусственных нейронных сетей.

Для оценки использовались свойства, характеризующие приспособленность разработанных моделей, методик и реализованных на их основе исследовательских прототипов к выполнению оценки защищенности. В работе рассмотрены такие свойства как оперативность, обоснованность и ресурсопотребление, а также их показатели. При проведении экспериментов по очереди выполнялись этапы методики для случайных компьютерных сетей, каждый хост которых содержал уязвимости, позволяющие получить максимальные права доступа. Эксперименты показали, что самым затратным с точки зрения оперативности является этап формирования возможных атакующих действий для всех хостов компьютерной сети. Временные затраты на другие этапы не превышают нескольких секунд.

Время выполнения складывается из продолжительности ее этапов и зависит от топологии сети. Для экспериментов использовались модели, сформированные на основе реальных компьютерных сетей с добавлением случайных элементов. В качестве платформы для проведения экспериментов использовался ЭВМ с установленной ОС Windows 7 Service Pack 1 x64 на базе четырехядерного процессора Intel i5 2,3 ГГц с 4 Гб оперативной памяти. Результаты экспериментов представляют собой усредненные величины. Анализ полученных данных позволяет судить о том, что время, необходимое на построение и анализ деревьев атак для компьютерной сети, состоящей из 1000 хостов, не превышает 2 минут, а время для полного обновления 10% хостов этой сети (т.е. 100 хостов) не превышает 10 секунд. Причем, если изменение затрагивает только отдельные модели (например, обновление программного обеспечения на хостах), необходимое время значительно сокращается.

3.7 Степень новизны полученных результатов

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.

3.8 Сопоставление полученных результатов с мировым уровнем

Все результаты, полученные в процессе выполнения 2013 года проекта, соответствуют мировому уровню. Авторы проекта опубликовали полученные результаты в нескольких журналах, сборниках и трудах конференций, а также апробировали результаты на множестве различных российских и международных конференций, в частности, на 21-й международной конференции (Euromicro) по параллельной, распределенной и сетевой обработке информации (PDP 2013), Белфаст, 27 февраля – 1 марта 2013 г.; 15-й международной конференции «РусКрипто 2013» по криптологии, стеганографии, цифровой подписи и системам защиты информации, Московская область, г.Солнечногорск, 28-30 марта 2013 г.; 6-м Международном семинаре по геоинформационным системам и системам информационного слияния: проблемы среды и города (IF&GIS’ 2013), Санкт-Петербург, 12-15 мая 2013 г.; Международном форуме по практической безопасности Positive Hack Days, Москва, 23-24 мая 2013 г.; 27-й Европейской конференции по моделированию (ECMS 2013), Олесунн, Норвегия, 27-30 мая 2013 г.; 22-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, 08-12 июля 2013 г.; Международной конференции по доступности, надежности и безопасности (ARES-2013), Регенсбург, Германия, 2–6 сентября 2013 г.; Международном Конгрессе по интеллектуальным системам и информационным технологиям «IS&IT’13», Дивноморское, 2-8 сентября, 2013 г.; 7-й международной конференции IEEE «Интеллектуальное приобретение данных и продвинутые вычислительные системы» (IDAACS'2013), Берлин, 12-14 сентября 2013 г.; 5-й Всероссийской научной конференции «Нечеткие системы, мягкие вычисления и интеллектуальные технологии» (НСМВ-2013), г. Сочи, 14-17 октября 2013 г.; VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013), 23-25 октября 2013 г.

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

В качестве базиса 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;
(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;
(11) методы интеллектуального анализа данных, в том числе на базе статической и динамической информации, комбинирования классификаторов, обучения и классификации на зашумленных наборах данных;
и др.

3.10.1.1 Количество научных работ, опубликованных в ходе выполнения Проекта (для Отчетов по продолжающимся Проектам – за 2013 год, для итоговых Отчетов – за весь период выполнения Проекта, цифрами)

94

3.10.1.2 Из них включенных в перечень ВАК

32

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

12

3.10.2 Количество научных работ, подготовленных в ходе выполнения проекта и принятых к печати в 2013 году (цифрами)

5

3.11 Участие в научных мероприятиях по тематике Проекта, которые проводились при финансовой поддержке Фонда (указать только количество мероприятий – цифрами

4

3.12 Участие в экспедициях по тематике Проекта, которые проводились при финансовой поддержке Фонда (указать только количество экспедиций – цифрами)

0

3.13 Финансовые средства, полученные от РФФИ (указать общий объем, в руб.)

400000,00

3.14 Адреса (полностью) ресурсов в Интернете, подготовленных авторами по данному проекту, например, http://www.somewhere.ru/mypub.html (если адресов несколько – для них последовательно заполняются подпункты 3.14.1; 3.14.2 и т.д.)

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

3.15 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. (к отчету за второй год выполнения проекта – список публикаций за два года, к отчету за третий год выполнения проекта – список за три года)

1. 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. ISSN 0002-3388.

2. 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., ISSN 1064-2307. DOI: 10.1134/S1064230712060044.

3. 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.

4. 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.

5. 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. (принято в печать)

6. 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. (принято в печать)

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

24. Чечулин А.А. Методика оперативного построения,

модификации и анализа деревьев атак // Труды СПИИРАН. Вып.3 (26). СПб.: Наука, 2013. С.40-53.

25. 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.

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

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. Котенко И.В., Новикова Е.С. Визуальный анализ для оценки защищенности компьютерных сетей // Информационно-управляющие системы, 2013, № 3, С.55-61. ISSN 1684-8853.

34. 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.

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

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

37. Новикова Е.С., Котенко И.В. Проектирование компонента визуализации для автоматизированной системы управления информационной безопасностью // Информационные технологии, № 9, 2013. С.32-36. ISSN 1684-6400.

38. 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.

39. Котенко И.В., Саенко И.Б. Интеллектуальные сервисы защиты информации в компьютерных сетях и системах // Защита информации. Инсайд, 2013, № 2, С.32-41.

40. Котенко И.В., Шоров А.В. Механизмы защиты компьютерных сетей от инфраструктурных атак на основе биоинспирированного подхода «нервная система сети» // Вопросы защиты информации,

№ 2, 2013. С.57-66.

41. Котенко И.В., Новикова Е.С. Методики визуального анализа в системах управления безопасностью компьютерных сетей // Вопросы защиты информации, № 3, 2013. С.33-42.

42. Комашинский Д.В., Котенко И.В. Методы интеллектуального анализа данных для выявления вредоносных программных объектов: обзор современных исследований // Вопросы защиты информации, № 4, 2013. С.21-33.

43. Котенко И.В., Саенко И.Б. Предложения по созданию многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте // Вестник Ростовского государственного университета путей сообщения, 2013, № 3. С. 69-79. ISSN 0201-727X.

44. Котенко И.В., Саенко И.Б., Юсупов Р.М. Перспективные модели и методы защиты компьютерных сетей // Вестник РАН, том 83, № 5, 2013. С.84-85.

45. Котенко И.В., Чечулин А.А. Применение графов атак для оценки защищенности компьютерных сетей и анализа событий безопасности // Системы высокой доступности, № 3 (9), 2013. С.103-111.

46. Десницкий В.А., Котенко И.В., Чечулин А.А. Верификация информационных потоков для проектирования защищенных информационных систем со встроенными устройствами // Системы высокой доступности, № 3 (9), 2013. С.112-118.

47. Комашинский Д.В., Котенко И.В., Чечулин А.А., Шоров А.В. Автоматизированная система категорирования веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Системы высокой доступности, № 3 (9), 2013. С.119-127.

48. 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. ISBN 978-5-4379-0205-9.

49. 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. ISBN 978-5-4379-0205-9.

50. 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.

51. 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. ISBN 978-5-4379-0210-3.

52. 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. ISBN 978-5-4379-0210-3.

53. 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. ISBN 978-5-4379-0210-3.

54. 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. ISBN 978-5-4379-0210-3.

55. 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. ISBN 978-5-4379-0210-3.

56. 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. ISBN 978-5-4379-0210-3.

57. 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. ISBN 978-5-4379-0210-3.

58. 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. ISBN 978-5-4379-0210-3.

59. 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/

60. 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/

61. 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/

62. 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/

63. 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

64. 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.

65. 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.

66. 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.

67. 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.

68. 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.

69. 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.

70. 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.

71. 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.

72. 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.

73. 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.

74. 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.

75. 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.

76. 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.

77. 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.

78. 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.

79. 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.

80. 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.

81. 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.

82. 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.

83. 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.

84. 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.

85. 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.

86. 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.

87. 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.

88. Агеев С.А., Саенко И.Б., Егоров Ю.П., Зозуля Е.И. Адаптивные алгоритмы оценивания интенсивности потока в мультисервисных сетях связи // Автоматизация процессов управления. Вып.1(31), 2013. С.3-11.

89. 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.

90. 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.

91. 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.

92. 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.

93. 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.

94. 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.

95. 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.

96. 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.

97. 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. (принято в печать)

98. 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. (принято в печать)

99. Чечулин А.А., Котенко И.В. Построение графов атак для анализа событий безопасности // Безопасность информационных технологий, № 1, 2014. (принято в печать)

3.16 Приоритетное направление развития науки, технологий и техники РФ, которому, по мнению исполнителей, соответствуют результаты данного проекта (выбрать номер пункта по Приложению или «не очевидно»)

Информационно-телекоммуникационные системы

3.17 Критическая технология РФ, которой, по мнению исполнителей, соответствуют результаты данного проекта (выбрать номер пункта по Приложению или «не очевидно»)

Технологии информационных, управляющих, нвигационных систем

3.18 Основное направление технологической модернизации экономики России, которому, по мнению исполнителей, соответствуют результаты данного проекта (выбрать номер пункта по Приложению или «не очевидно»)

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