НОМЕР ПРОЕКТА **11-07-00435**		УЧЕТНАЯ КАРТОЧКА
НАЗВАНИЕ ПРОЕКТА **Разработка и исследование математических моделей и методов анализа и синтеза систем разграничения доступа к информационным и сетевым ресурсам в современных и перспективных компьютерных системах и сетях на основе создания и применения средств искусственного интеллекта**		
ОБЛАСТЬ ЗНАНИЯ **07 - инфокоммуникационные технологии и вычислительные системы**		КОД(Ы) КЛАССИФИКАТОРА **07-235 07-241 07-298 07-956 01-217**
КОД И НАЗВАНИЕ КОНКУРСА **а - Инициативные проекты**		
ФАМИЛИЯ, ИМЯ, ОТЧЕСТВО РУКОВОДИТЕЛЯ ПРОЕКТА **Саенко Игорь Борисович**		ТЕЛЕФОН РУКОВОДИТЕЛЯ ПРОЕКТА **(812)3282642**
ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ, предоставляющей условия для выполнения работ по Проекту физическим лицам **Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук**		
ОБЪЕМ СРЕДСТВ, ФАКТИЧЕСКИ ПОЛУЧЕННЫХ ЗА 2013 г. **420000 руб.**		
СОСТАВ НАУЧНОГО КОЛЛЕКТИВА, ВЫПОЛНЯВШЕГО РАБОТЫ ПО ПРОЕКТУ В 2013 ГОДУ		
ЧИСЛО ЧЛЕНОВ НАУЧНОГО КОЛЛЕКТИВА, ВКЛЮЧАЯ РУКОВОДИТЕЛЯ **9**	ЧИСЛО ЧЛЕНОВ НАУЧНОГО КОЛЛЕКТИВА, ИМЕЮЩИХ УЧЕНУЮ СТЕПЕНЬ **6**	ЧИСЛО НАУЧНОГО КОЛЛЕКТИВА В ВОЗРАСТЕ ДО 35 ЛЕТ ВКЛЮЧИТЕЛЬНО **7**
ФИО члена научного коллектива		
Чечулин Андрей Алексеевич		
Шоров Андрей Владимирович		
Десницкий Василий Алексеевич		
Комашинский Дмитрий Владимирович		
Дойникова Елена Владимировна		
Полубелова Ольга Витальевна		
Нестерук Филипп Геннадьевич		
Новикова Евгения Сергеевна		
СОСТАВ НАУЧНОГО КОЛЛЕКТИВА, КОТОРЫЙ БУДЕТ ВЫПОЛНЯТЬ РАБОТЫ ПО ПРОЕКТУ В 2014 ГОДУ		
ЧИСЛО ЧЛЕНОВ НАУЧНОГО КОЛЛЕКТИВА, ВКЛЮЧАЯ РУКОВОДИТЕЛЯ **0**	ЧИСЛО ЧЛЕНОВ НАУЧНОГО КОЛЛЕКТИВА, ИМЕЮЩИХ УЧЕНУЮ СТЕПЕНЬ **0**	ЧИСЛО НАУЧНОГО КОЛЛЕКТИВА В ВОЗРАСТЕ ДО 35 ЛЕТ ВКЛЮЧИТЕЛЬНО **0**
ФИО члена научного коллектива		
ПОДПИСЬ РУКОВОДИТЕЛЯ ПРОЕКТА		ДАТА **23.12.2013**

ОТЧЕТ ЗА 2013 ГОД ПО ПРОЕКТУ РФФИ 11-07-00435-а

Статус отчета: подписан

Дата подписания: 23.12.2013

Подписал: Саенко Игорь Борисович

Отчет распечатан: 23.12.2013

Форма 501. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ

1.1. Номер проекта
11-07-00435

1.2. Руководитель проекта
Саенко Игорь Борисович

1.3. Название проекта
Разработка и исследование математических моделей и методов анализа и синтеза систем разграничения доступа к информационным и сетевым ресурсам в современных и перспективных компьютерных системах и сетях на основе создания и применения средств искусственного интеллекта

1.4. Вид конкурса
а - Инициативные проекты

1.5. Год представления отчета
2014

1.6. Вид отчета
итоговый (2011-2013)

1.7. Аннотация
Разработаны теоретические основы решения задач интеллектуального анализа данных (Data Mining) при синтезе схем разграничения доступа с помощью усовершенствованных генетических алгоритмов, которые были протестированы для предметных областей виртуальных локальных сетей, ролевых схем разграничения доступа и геоинформационных систем. Разработаны общая архитектура и архитектуры отдельных компонентов системы интеллектуальных сервисов для разграничения доступа к информационным и сетевым ресурсам в современных и перспективных компьютерных системах и сетях. Проведено исследование математических моделей и методов реализации интеллектуальных механизмов логического ввода на знаниях о событиях доступа в системах разграничения доступа современных и перспективных компьютерных систем и сетей. Разработаны модели и методы интеллектуализации управления разграничением доступа к информационным и коммуникационным ресурсам в защищенных мультисервисных сетях. Проведено исследование моделей и методов оценивания показателей доступности информационных и сетевых ресурсов в современных и перспективных компьютерных системах и сетях и разработана онтология метрик защищенности информационных и сетевых ресурсов от несанкционированного доступа. Разработана общая архитектура многоуровневой интеллектуальной системы разграничения доступа для АСУ железнодорожного транспорта. Проведена экспериментальная оценка полученных результатов.

1.8. Полное название организации, где выполняется проект
Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук

"Исполнители проекта согласны с опубликованием (в печатной и электронной формах) научных отчетов и перечня публикаций по проекту"

Подпись руководителя проекта

Форма 503. РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1. Номер проекта
11-07-00435

3.2. Название проекта
Разработка и исследование математических моделей и методов анализа и синтеза систем разграничения доступа к информационным и сетевым ресурсам в современных и перспективных компьютерных системах и сетях на основе создания и применения средств искусственного интеллекта

3.3. Коды классификатора, соответствующие содержанию фактически проделанной работы
07-235 07-241 07-298 07-956 01-217

3.4. Объявленные ранее (в исходной заявке) цели проекта на 2013 год
Основные цели проекта на 2013 год определялись как дальнейшее совершенствование, реализация и экспериментальная оценка элементов научно-методологического обеспечения систем разграничения доступа в следующих научных направлениях: 1) совершенствование генетических алгоритмов оптимизации и реализованных на их основе методов решения проблемы «извлечения ролей» и методик синтеза схем ролевого разграничения доступа; 2) разработка алгоритмов, моделей, методов и методик построения отдельных интеллектуальных сервисов разграничения доступа к информационным и сетевым ресурсам на основе технологии SIEM, в частности, сервисов внутреннего представления, хранения и визуализации событий доступа; 3) разработка частных постановок задач, подходов к построению интеллектуальных моделей и методов управления разграничением доступа в защищенных мультисервисных сетях. Для достижения этих целей планировалось решение следующих задач: 1) разработка и тестирование эволюционных алгоритмов, моделей и методов для новых предметных областей разграничения доступа к информационным и сетевым ресурсам в современных и перспективных компьютерных системах и сетях; 2) разработка общей архитектуры и архитектуры отдельных компонентов системы для интеллектуальных сервисов разграничения доступа к информационным и сетевым ресурсам в современных и перспективных компьютерных системах и сетях; 3) исследование и разработка математических моделей и методов реализации интеллектуальных механизмов логического ввода на знаниях о событиях, происходящих в системах разграничения доступа, для современных и перспективных компьютерных систем и сетей; 4) исследование и разработка моделей и методов интеллектуализации управления разграничением доступа к информационным и коммуникационным ресурсам в защищенных мультисервисных сетях; 5) исследование и разработка моделей и методов оценивания показателей доступности информационных и сетевых ресурсов в современных и перспективных компьютерных системах и сетях; 6) экспериментальная оценка полученных результатов.

3.5. Степень выполнения поставленных в проекте задач
Все задачи, запланированные в проекте на 2013 год, а также в целом на весь период выполнения проекта, выполнены полностью. Дополнительно проведены исследования в области адаптации и применения моделей и методов мониторинга и управления событиями разграничения доступа в информационных и аналитических системах АСУ железнодорожного транспорта.

3.6. Полученные за отчетный период важнейшие результаты
1. В ходе разработки и тестирования эволюционных алгоритмов, моделей и методов для новых предметных областей формирования схем разграничения доступа к информационным и сетевым ресурсам в современных и перспективных компьютерных системах и сетях был разработан новый фундаментальный теоретический результат, заключающийся в обосновании и детализации подхода к решению NP-полных задач интеллектуального анализа данных (Data Mining), возникающих при синтезе схем разграничения доступа, с помощью усовершенствованных генетических алгоритмов. На основании обобщения результатов, полученных в течение первых двух лет проекта, была сформулирована обобщенная концептуальная постановка задачи синтеза схемы разграничения доступа, которая в конечной итоге сводится к нахождению оптимального мультипликативного разбиения исходной булевой матрицы, описывающей отношение между множествами субъектов и объектов доступа, на две булевы матрицы-сомножителя, которые при выполнении над ними операции матричного умножения дают в результате исходную матрицу. Критерием оптимизации данной задачи является минимизация варьируемого количества строк и столбцов в искомых матрицах. К данной постановке задачи в конечном итоге сводятся такие рассмотренные ранее в проекте проблемы, как задача синтеза ролевой схемы разграничения доступа, известная как «проблема извлечения ролей» (Role Mining Problem), задача синтеза схемы разграничения доступа в виртуальной локальной сети с учетом признаков общего доступа на контролируемых ресурсах, задача формирования схемы разграничения доступа к слоям в геоинформационной системе и задача минимизации количества виртуальных локальных подсетей при заданной матрице смежности этих подсетей. В последней задаче осуществляется поиск одной единственной матрицы - матрицы инциденций, определяющей принадлежность хостов виртуальным подсетям. В качестве второго сомножителя в этом случае используется транспонированное представление искомой матрицы. Все рассмотренные задачи относятся к классу NP-полных. Усовершенствованные генетические алгоритмы, разработанные в проекте, отличаются тем, что (1) в качестве генов хромосом в них используются столбцы искомых матриц, (2) применяется мульти-хромосомное механизмы для операций скрещивания мутации и (3) вводится в рассмотрения дополнительная управляющая хромосома.
2. При разработке общей архитектуры и архитектуры отдельных компонентов системы интеллектуальных сервисов для разграничения доступа к информационным и сетевым ресурсам в современных и перспективных компьютерных системах и сетях были в первую очередь исследованы перспективные системы хранения данных о событиях разграничения доступа, позволяющие разработать гибридный онтологический репозиторий, обеспечивающий моделирование данных о событиях и политиках разграничения доступа в дополнение к реляционным базам данных в виде XML-баз данных и в виде триплетов «субъект-предикат-объект». В ходе исследований в этой области была проведена классификация и дана характеристика известных средств построения и использования

XML–баз данных, в которой выделены такие классы, как «естественные» (natural) и «встроенные» (embedded). Среди отечественных XML-баз данных особое внимание обращено на СУБД Sedna, которая относится к первому классу. Среди хранилищ триплетов был сделан выбор в пользу комплексных систем хранения триплетов, сочетающих возможности всех трех типов моделей данных и обеспечивающих гибридный подход к построению репозитория для систем разграничения доступа. Данный подход был успешно апробирован на решении ряда задач, связанных с моделирования атак, направленных на нарушение схем и политик разграничения доступа, и анализом защищенности от несанкционированного доступа (НСД) информационных и телекоммуникационных систем. Кроме репозитория, к числу новых компонентов такой системы, являющейся прототипом перспективной интеллектуальной системы разграничения доступа, предложенных в проекте, относятся компонент визуализации, прогностический анализатор безопасности и система поддержки принятия решений и реагирования.Компонент визуализации предназначен для реализации в интеллектуальной системе разграничения доступа, в целях повышения эффективности анализа данных и принятия решений, возможности визуального анализа информации о разграничении доступа. Его архитектура состоит из слоя графических примитивов, слоя управляющих сервисов и интерфейсного слоя. Управляющие сервисы осуществляют выбор графических шаблонов представления информации в соответствии с требованиями пользователей по обеспечению необходимой степени детализации информации. Прогностический анализатор безопасности использует в качестве входных данных политики разграничения доступа, модели их обработки, требования защищенности от НСД и данные о событиях разграничения доступа, поступающие в систему в реальном масштабе времени. Целью его функционирования является оказание помощи в принятии важнейших решений, касающихся выработки контрмер по противодействию атакам и угрозам реализации НСД, которые воздействуют на информационно-телекоммуникационную систему в текущий момент времени.Система поддержки принятия решений и реагирования позволяет осуществлять конфигурирование политик разграничения доступа внешних систем, вызываемых соответствующими средствами (например, Apache, MySQL и т.д.). При этом не требуется знание правил конфигурирования других средств, а достаточно правил конфигурирования самого компонента.

3. В ходе исследования и разработки математических моделей и методов реализации интеллектуальных механизмов логического ввода на знаниях о событиях и политиках разграничения доступа был предложен подход для разработки и реализации системы логического вывода. Была предложена общая архитектура этой системы, включающая онтологическое информационное хранилище и модули для реализации конкретных механизмов логического вывода - исчисления событий и метода «проверки на моделях». В общем виде основными элементами этой архитектуры являются: онтология, хранилище триплетов, редактор метаданных, транслятор, навигатор, ассоциатор, классификатор и ризонер (reasoner). 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 данные, поступающие от других интеллектуальных сервисов, 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 опертивным инструментом логического вывода. Ризонер является модулем логического вывода, реализующий один из двух методов вывода – на основе исчисления событий (Event Calculus) или на основе «проверки на модели» (Module 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 информационно-телекоммуникационной системы, описание политик разграничения доступа 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. Метод «проверки на модели» позволяет доказать, что специфицированная система (программа) обладает желаемыми свойствами, за счет изучения всех возможных путей 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.

4. При исследовании и разработке моделей и методов интеллектуализации управления разграничением доступа к информационным и коммуникационным ресурсам в защищенных мультисервисных сетях (ЗМС) разработана концептуальная модель интеллектуальной системы управления безопасностью ЗМС и предложены адаптивные алгоритмы для оценки трафика в ЗМС. Предложенная концептуальная модель рассматривает систему управления безопасностью ЗМС как многоуровневую иерархическую структуру, в которой на каждом уровне иерархии имеется интеллектуальный слой координации решений. К числу задач, решаемых интеллектуальными слоями, относятся: 1) оперативная координация взаимодействия задач управления как на одном абстрактном уровне управления, так и между уровнями; 2) повышение оперативности получения объективной

количественной и качественной информации о состоянии ЗМС и ее элементов; 3) повышение оперативности распределения телекоммуникационных ресурсов для обеспечения пользователей услугами связи с требуемым качеством; 4) уменьшение времени реакции на угрозы безопасности; 5) своевременное реагирование на изменение целевых сетевых задач. Интеллектуализацию предполагается реализовать на основе методов нечетких когнитивных карт, а также методов нечетких логических выводов. При этом классические методы оптимизации сетевого управления не отрицаются, а дополняются, позволяя учитывать лимит времени на обработку информации (как правило, неполной и нечеткой) о состоянии сетевых элементов и ЗМС в целом и снизить размерность оптимизационных задач, что, как следствие, улучшает оперативность выработки решений по управлению ЗМС. Предлагаемый подход не отрицает, а дополняет их в условиях лимита времени на обработку информации в условиях неполной и нечеткой информации о состоянии сетевых элементов и ЗМС СН в целом, позволяет снизить размерность оптимизационных задач и, как следствие, улучшить оперативность выработки решений по управлению ЗМС СН.Разработанные алгоритмы оценивания сетевого трафика в ЗМС подразделяются на два вида. К первому виду относится модифицированный алгоритм стохастической аппроксимации, ко второму – алгоритм оценивания в «скользящем окне». Модифицированный алгоритм стохастической аппроксимации отличается от классического тем, что в нем для коэффициентов шагов алгоритма задается постоянное значение, лежащее в диапазоне от 0 до 1. В этом случае алгоритм оценивания позволяет отслеживать изменения значения интенсивности, а не сходиться к определённому её значению. В результате данный алгоритм может успешно применяться для оценки нестационарных интенсивностей. Основной задачей в этом случае является нахождение компромиссного решения между скоростью и точностью оценивания, для которой сформулирована формальная постановка задачи и предложен метод решения. В алгоритме оценивания в «скользящем окне» в еще большей степени сокращается анализируемая выборка значений, ограничиваясь последними N значениями, где N – размер окна. Проведенная экспериментальная оценка показала, что предложенные алгоритмы обеспечивают значительно меньшую ошибку оценивания, чем классические.

5. При исследовании и разработке моделей и методов оценивания показателей доступности информационных и сетевых ресурсов в современных и перспективных компьютерных системах и сетях была разработана многоуровневая система метрик защищенности от НСД в условиях вредоносного воздействия и предложен подход к их онтологическому представлению и использованию. Метрики защищенности образуют отдельный класс в предлагаемой онтологии. Кроме этого класса, в онтологию входят классы, отражающие структурные элементы информационно-телекоммуникационной системы, и контрмеры (меры по противодействию). Связи, установленные в онтологии между классами структурных элементов, метрик и контрмер, позволяют реализовать процедуру логического вывода, основанную на дескрипционной логике и позволяющую в реальном (или в близком к реальному) масштабе времени получить следующие сведения: 1) о нападении на основе некоторых экземпляров метрик атак; 2) об обнаружении ресурсов, на которые направлены атаки, на основе экземпляров системных метрик; 3) о внутренней корреляции показателей; 4) о возможных контрмерах, принимая во внимание различные стоимостные метрики.

6. Для экспериментальной оценки полученных результатов был разработан ряд программных прототипов, для двух из которых были получены свидетельства о государственной регистрации программ для ЭВМ.

7. В ходе дополнительно проведенных исследований в области адаптации и применения моделей и методов мониторинга и управления событиями разграничения доступа в информационных и аналитических системах АСУ железнодорожного транспорта (ЖТ) была получены следующие результаты: 1) проведен анализ особенностей построения и функционирования АСУ ЖТ, показавший, что все автоматизированные системы ЖТ можно разделить на три уровня иерархии – корпоративный, дорожный и линейно-узловой; 2) разработана общая архитектура многоуровневой интеллектуальной системы разграничения доступа для АСУ ЖТ, включающая уровень традиционных средств разграничения доступа, уровень интеллектуальных сервисов сбора и хранения данных о разграничении доступа и уровень интеллектуальных сервисов анализа данных о разграничении доступа; 3) разработаны формальные постановки задач для разработки отдельных интеллектуальных сервисов этой системы.

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, эволюционного моделирования, оптимизации сложных систем, 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 6-м Международном семинаре по геоинформационным системам и системам информационного слияния: проблемы среды и города (IF&GIS’ 2013), Санкт-Петербург, 12-15 мая, 2013; Международной конференции по доступности, надежности и безопасности (ARES-2013), Регенсбург, Германия, 2–6 сентября 2013; 7-й международной конференции IEEE «Интеллектуальное приобретение данных и продвинутые вычислительные системы» (IDAACS'2013), Берлин, 12-14 сентября 2013 года; 21-й международной конференции (Euromicro) по параллельной, распределенной и сетевой обработке информации (PDP 2013), Белфаст, Февраль, 2013; 22-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, 08-12 июля 2013 г.; Международного Конгресса по интеллектуальным системам и информационным технологиям «IS&IT’13», Дивноморское, сентябрь, 2013; VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность

регионов России (ИБРР-2013), 23-25 октября 2013 г.; 5-й Всероссийской научной конференции «Нечеткие системы, мягкие вычисления и интеллектуальные технологии» (НСМВ-2013), 14-17 октября 2013 г., г. Сочи.

3.9. Методы и подходы, использованные в ходе выполнения проекта

В ходе выполнения проекта получили дальнейшее развитие следующие методы и подходы:
(1) методы теории оптимизации в части формирования обобщенной формализованной постановки задачи синтеза схем разграничения доступа и сведения ее к NP-полной задаче мультипликативного разбиения булевых матриц;
(2) методы био-инспирированной оптимизации сложных систем в части разработки усовершенствованных генетических алгоритмов оптимизации, которые ориентированы на масштабируемое решение задач интеллектуального анализа данных (Data Mining) при больших размерностях задачи;
(3) методы генетической оптимизации в применении к новым областям разграничения доступа, в частности, для минимизации количества подсетей в виртуальной локальной вычислительной сети;
(4) методы системного анализа и теории систем в части их применения для разработки общей архитектуры и архитектуры отдельных компонентов системы интеллектуальных сервисов разграничения доступа к информационным и сетевым ресурсам в современных и перспективных компьютерных системах;
(5) методы реализации логического вывода на основе исчисления событий и «проверки на модели» (model checking) в части их применения к управлению уровнями защищенности от несанкционированного доступа к информационным и сетевым ресурсам в современных компьютерных системах и сетях;
(6) методы нечетких когнитивных карт и нечетких логических выводов, дополняющих положения теорий математического программирования, массового обслуживания, случайных процессов и графов, в части разработки сервисов интеллектуализации управления разграничением доступа к информационным и сетевым ресурсам защищенных мультисервисных сетей;
(7) онтологический подход к моделированию предметной области системы разграничения доступа в современных и перспективных компьютерных системах и сетях в части создания и применении онтологии, охватывающей метрики защищенности от несанкционированного доступа, структурные элементы информационно-телекоммуникационной системы и контрмеры по обеспечению требуемого уровня защищенности;
(8) подход к управлению защищенностью от несанкционированного доступа информационных и сетевых ресурсов сложной мультидоменной автоматизированной системы на основе разработки и применения интеллектуальных сервисов разграничения доступа.

3.10.1.1. Количество научных работ, опубликованных в ходе выполнения проекта

111

3.10.1.2. Из них включенных в перечень ВАК

25

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)

11

3.10.2. Количество научных работ, подготовленных в ходе выполнения проекта и принятых к печати в 2013 г.

2

3.11. Участие в научных мероприятиях по тематике проекта, которые проводились при финансовой поддержке Фонда

3

3.12. Участие в экспедициях по тематике проекта, проводимых при финансовой поддержке Фонда

0

3.13. Финансовые средства, полученные от РФФИ

420000 руб.

3.14. Адреса (полностью) ресурсов в Internet, подготовленных авторами по данному проекту

http://www.comsec.spb.ru/saenko/

3.15. Библиографический список всех публикаций по проекту

1. Котенко И.В., Саенко И.Б., Юсупов Р.М. Защита информационных ресурсов в компьютерных сетях // Вестник РАН, т.81, №8, август 2011. С.746-747.
2. Котенко И.В., Саенко И.Б., Юсупов Р.М. Научный анализ и поддержка политик безопасности в киберпространстве // Вестник РАН, т.81, №9, сентябрь 2011. С. 844-845.
3. Котенко И.В., Саенко И.Б., Юсупов Р.М. Перспективные модели и методы защиты компьютерных сетей // Вестник РАН, т.83. №5. С. 463.
4. Агеев С.А., Бушуев А.С., Егоров Ю.П., Саенко И.Б. Концепция автоматизации управления информационной безопасностью в защищенных мультисервисных сетях специального назначения // Автоматизация процессов управления. Вып.1(23), 2011. С.50-57.
5. Агеев С.А., Саенко И.Б., Егоров Ю.П., Гладких А.А. К разработке комплекса математических моделей управления защищённой мультисервисной сетью // Автоматизация процессов управления. Вып.3(29), 2012. С.8-18.
6. 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.
7. Десницкий В.А., Чечулин А.А. Модели процесса построения безопасных встроенных систем // Системы высокой доступности, №2, т.7, 2011. С.97-101.
8. Саенко И.Б., Котенко И.В. Генетическая оптимизация схем ролевого доступа к информации // Системы высокой доступности, №2, т.7, 2011. С.112-116.

9. Полубелова О.В., Котенко И. В., Саенко И.Б., Чечулин А.А. Применение онтологий и логического вывода для управления информацией и событиями безопасности системы // Системы высокой доступности, №2, т.8, 2012. С.100-108.
10. Агеев С.А., Шерстюк Ю.М., Саенко И.Б., Полубелова О.В. Концептуальные основы автоматизации управления защищенными мультисервисными сетями // Проблемы информационной безопасности. Компьютерные системы. №3, 2011. С. 30-39.
11. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2012. № 2. С.57-68.
12. Синещук Ю.И., Филиппов А.Г., Терехин С.Н., Николаев Д.В., Саенко И.Б. Структурно-логический метод анализа безопасности потенциально опасных объектов // Труды СПИИРАН. 2011. Вып.2(17). С.55-69.
13. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2012. Вып.1(20). С.27-56.
14. Кий А.В., Копчак Я.М., Саенко И.Б., Козленко А.В. Динамическое управление доступом к информационным ресурсам в критически важных инфраструктурах на основе анализа информационных профилей пользователей // Труды СПИИРАН. 2012. Вып.2(21). С.5-20.
15. Козленко А.В., Авраменко В.С., Саенко И.Б., Кий А.В. Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности // Труды СПИИРАН. 2012. Вып.2(21). С.41-55.
16. Котенко И.В., Саенко И.Б. Построение интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. 2012. Вып.3(22). С.84-100.
17. Демидов А.А., Никифоров О.Г., Саенко И.Б. Разработка концепции обеспечения информационной безопасности информационно-телекоммуникационных систем органов государственной власти // Труды СПИИРАН. 2012. Вып.3(22). С.71-83.
18. Котенко Д.И., Котенко И.В., Саенко И.Б. Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы // Труды СПИИРАН. 2012. Вып.3(22). С.5-30.
19. Котенко Д.И., Котенко И.В., Саенко И.Б. Методика итерационного моделирования атак в больших компьютерных сетях // Труды СПИИРАН. 2012. Вып.4(23). С.50-79.
20. Котенко И.В., Саенко И.Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. Вып.1(24). С.21-40.
21. Котенко И.В., Саенко И.Б., Полубелова О.В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. 2013. Вып.2(25). С.113-134.
22. 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. 2013. Вып.7(30). С.7-25.
23. Саенко И.Б., Нижегородов А.В. Анализ проблемы управления доступом в автоматизированных системах на основе оценки защищенности баз данных // Журнал "В мире научных открытий". Математика. Механика. Информатика. Выпуск 8(22), 2012. Красноярск. Изд-во «Научно-инновационный центр». С.11-21.
24. Агеев С.А., Саенко И.Б. Концептуальное моделирование управления доступом к информации в ключевой системе информационной инфраструктуры // Проблемы управления рисками в техносфере: научно-аналитический журнал, СПбУ ГПС МЧС России. №4(20), 2011. С.92-96.
25. 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(51). С.68-78.
26. Саенко И.Б., Нижегородов А.В. Анализ состояния развития систем защиты баз знаний // Материалы IV Всероссийской научно-практической конференции с международным участием "Научное творчество XXI века", апрель 2011 г. Приложение к журналу «В мире научных открытий», выпуск 2. Красноярск. Издательство «Научно-инновационный центр». С.86.
27. Котенко И.В., Саенко И.Б. SIEM-системы для управления информацией и событиями безопасности // «Защита информации. Инсайд». №5, 2012. С.2-12.
28. Котенко И.В., Саенко И.Б. Интеллектуальные сервисы защиты информации в компьютерных системах и сетях // «Защита информации. Инсайд». №2, 2013. С.32-41.
29. Котенко Д.И., Котенко И.В., Саенко И.Б. Моделирование атак в больших компьютерных сетях // Технические науки - от теории к практике, №17-1, 2013. С.12–16.
30. Котенко И.В., Саенко И.Б. Система интеллектуальных сервисов защиты информации для критических инфраструктур // Технические науки - от теории к практике, №17-1. С.7-11.
31. Котенко И.В., Саенко И.Б., Дойникова Е.В. Оценка рисков в компьютерных сетях критических инфраструктур // Инновации в науке, №16-1. С.84-88.
32. Скорик Ф.А., Саенко И.Б. Нейросетевая модель оценки состояния распределенной информационной системы // Инновации в науке, №16-1. С.151-155.
33. Kotenko I., Polubelova O., Sheshulin A., Saenko I. Design and Implementation of a Hybrid Ontological-Relational Data Repository for SIEM Systems // Future Internet, 2013, №5, Pp. 355-375; doi:10.3390/fi50x000x. www.mdpi.com/journal/futureinternet
34. Komashinskiy D., Kotenko I. Intelligent Data Analysis for Malware Detection // International Journal of Computing, 2013, №12(1), Pp. 63-74.
35. Igor Saenko, Igor Kotenko. Genetic Algorithms for Role Mining Problem // Proc. of the 19th International Euromicro Conference on Parallel, Distributed and Network-based Processing. Ayia Napa, Cyprus, 9-11 February 2011. P. 646-650.
36. Igor Saenko, Igor Kotenko. Design and Performance Evaluation of Improved Genetic Algorithm for Role Mining Problem // Proc. of the 20th International Euromicro Conference on Parallel, Distributed and

Network-based Processing. Garching, Germany, 15-17 February 2012. P.269-274.
37. Igor Kotenko, Olga Polubelova, Igor Saenko. Hybrid Data Repository Development and Implementation for Security Information and Event Management // Proc. of the 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing. Work in Progress. Garching, Germany, 15-17 February 2012.
38. Kotenko I., Polubelova O., Saenko I. Hybrid Data Repository Development and Implementation for Security Information and Event Management // Proc. of the Work in Progress Session 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing. Garching/Munich, February 2012.
39. Novikova E., Kotenko I.. Analytical Visualization Techniques for Security Information and Event Management // Proc. of 21st International Euromicro Conference on Parallel, Distributed, and Network-Based Processing, 2013. Belfast, Ireland. P. 519-525.
40. Kotenko I., Polubelova O., Saenko I. Data Repository for Security Information and Event Management in service infrastructures // Proceedings of 9th International Joint Conference on e-Business and Telecommunications (ICETE 2012). International Conference on Security and Cryptography (SECRYPT 2012). Rome, Italy, 24–27 July, 2012. Pp.308-313.
41. Polubelova O., Saenko I., Kotenko I. The Ontological Approach for SIEM Data Repository Implementation // 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing. Besancon, France, September 11-14, 2012. Los Alamitos, California. IEEE Computer Society. 2012. P. 761-766.
42. Kotenko I., Polubelova O., Saenko I. Logical Inference Framework for Security Management in Geographical Information Systems // Proceedings of the 6th International Workshop on Information Fusion and Geographical Information Systems: Environmental and Urban Challenges (IF&GIS' 2013). St.Petersburg, Russia, May 12-15, 2013. Lecture Notes in Geoinformation and Cartography. Berlin: Springer-Verlag. August 31, 2013.
43. Kotenko I., Saenko I., Polubelova O., Doynikova E. The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems // Proc. of 2013 International Conference on Availability, Reliability and Security (ARES - 2013). September 2-6, 2013. University of Regensburg. Regensburg, Germany. 2013. DOI 10.1109/ARES.2013.84. Pp.638-645.
44. Kotenko I., Doynikova E. Security metrics for risk assessment of distributed information systems // Proc. IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. Berlin, Germany, September 12-14, 2013. P.646-650.
45. Саенко И.Б., Агеев С.А. Основы математического моделирования задач управления защищенными мультисервисными сетями // Международный конгресс по информатике: информационные системы и технологии. Материалы международного научного конгресса, Республика Беларусь, Минск, 31 октября – 3 ноября 2011 года, в 2 ч. Ч.1 / редкол. : С.В. Абламейко (отв. ред.) [и др.]. - Минск: БГУ, 2011. С.282-287.
46. Дойникова Е.В., Жадан О.П., Саенко И.Б. Об актуальных задачах управления системами ролевого разграничения доступа к информации в едином информационном пространстве // Сборник научных трудов SWorld. По материалам международной научно-практической конференции «Научные исследования и их практическое применение. Современное состояние и пути развития – 2011». Том 3. Технические науки. Одесса: Черноморье, 2011. С.82-83.
47. Саенко И.Б., Нижегородов А.В. Необходимость создания систем защиты баз знаний // Сборник научных трудов SWorld. По материалам международной научно-практической конференции «Современные направления теоретических и прикладных исследований - 2011». Том 3. Технические науки. Одесса: Черноморье, 2011. С.76-78.
48. Саенко И.Б., Нижегородов А.В., Кабанов А.С. О необходимости создания единой системы управления доступом к информационным ресурсам в автоматизированных системах // Сборник научных трудов SWorld. Материалы международной научно-практической конференции «Современные направления теоретических и прикладных исследований '2012». – Выпуск 1. Том 4. Одесса: КУПРИЕНКО, 2012. С.28-30.
49. Скорик Ф.А., Саенко И.Б., Шоров А.В. Метод определения ограничений масштабирования ресурсов в ГРИД-системах // Интеллект и наука: труды XI Международной научно-практической конференции, (г. Железноводск, 28-29 апреля 2011 г.). Красноярск: ИПК СФУ, 2011. С.133-134.
50. Саенко И.Б., Нижегородов А.В., Ключко Н.Ю. Необходимость защиты баз данных в современном обществе // Современные исследования социальных проблем: Материалы III Общероссийской научно-практической конференции с международным участием. Вып.1. Красноярск: Научно-инновационный центр, 2011. С.224-225.
51. Полубелова О.В., Саенко И.Б., Котенко И.В. Разработка методов представления данных и логического вывода для управления информацией и событиями безопасности // Часть 5-й Российской мультиконференции по проблемам управления (МКПУ-2012) - конференция «Информационные технологии в управлении» (ИТУ-2012). 09–11 октября 2012 г. Материалы конференции. СПб. 2012. С.723-728.
52. Агеев С.А., Саенко И.Б. О межуровневой координации показателей функционирования защищенной мультисервисной сети промышленного назначения // Седьмая Международная научно-техническая конференция «Информационные технологии в промышленности» (ITI-2012): тезисы докладов (30–31 октября 2012 года, Минск). Минск: ОИПИ НАН Беларуси, 2012. С.101-102.
53. Саенко И.Б., Нижегородов А.В. Влияние защищенности информационных ресурсов на комплексную безопасность критических инфраструктур // Безопасность в чрезвычайных ситуациях: сборник научных трудов IV Всероссийской научно-практической конференции. СПб.: Изд-во Политехн. ун-та, 2012. С.151-154.
54. Саенко И.Б., Котенко И.В. Применение генетических алгоритмов в оптимизационных задачах разграничения доступа к информации // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'12». Научное издание в 4-х томах. М.: Физматлит, 2012. Т. 1. С.40-45.

55. Полубелова О.В., Котенко И.В., Саенко И.Б. Онтологический подход к построению интеллектуальных сервисов хранения и обработки событий безопасности //Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'12». Научное издание в 4-х томах. М.: Физматлит, 2012. Т. 2. С.394-399.
56. 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.
57. 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.
58. Саенко И.Б., Котенко И.В. Метод генетической оптимизации схем ролевого доступа к информации // Тринадцатая Международная конференция «РусКрипто-2011». Московская область, г. Солнечногорск, 30 марта-2 апреля 2011 г. [Электронный ресурс]. http://www.ruscrypto.ru/sources/conference/rc2011.
59. Полубелова О.В., Саенко И.Б. Применение онтологического подхода и логического вывода для управления информацией и событиями безопасности // Четырнадцатая международная конференция «РусКрипто-2012», Московская область, Солнечногорск, 29-30 марта 2012 года. [Электронный ресурс]. http://www.ruscrypto.org/sources/conference/rc2012/.
60. Саенко И.Б., Морозов И.В. Проблема разграничения доступа к информации в современных геоинформационных системах // 66-я научно-техническая конференция, посвященная Дню радио. 19–29 апреля 2011 г. Труды конференции. Санкт-Петербург, 2011. С.84-85.
61. Круглов С.Н., Саенко И.Б., Сидоров А.А. Метод оптимизации схемы ролевого доступа к информации // 66-я научно-техническая конференция, посвященная Дню радио. 19–29 апреля 2011 г. Труды конференции. Санкт-Петербург, 2011. С.85-86.
62. Саенко И.Б., Нижегородов А.В., Ключко Н.Ю. Анализ SQL-инъекций как вида программных атак на базы данных // 66-я научно-техническая конференция, посвященная Дню радио. 19–29 апреля 2011 г. Труды конференции. Санкт-Петербург, 2011. С.87-88.
63. Саенко И. Б., Сидоров А.А., Круглов С.Н. Применение генетических алгоритмов для решения задачи «извлечения ролей» в RBAC-системах // Материалы Юбилейной 20-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 27 июня -1 июля 2011 г. Санкт-Петербург. Издательство Политехнического университета. С.89-90.
64. Саенко И. Б., Полубелова О.В., Котенко И.В. Разработка информационного хранилища системы управления информацией и событиями безопасности для гетерогенной инфраструктуры // Материалы Юбилейной 20-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 27 июня -1 июля 2011 г. Санкт-Петербург. Издательство Политехнического университета. С.41-42.
65. Агеев С.А., Полубелова О.В. Методы управления безопасностью информации в защищенных мультисервисных сетях // Материалы Юбилейной 20-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 27 июня -1 июля 2011 г. Санкт-Петербург. Издательство Политехнического университета. С.122-124.
66. Морозов И.В., Чечулин А.А. Разграничение доступа к информации в геоинформационных системах // Методы и технические средства обеспечения безопасности информации. Материалы Юбилейной 20-й научно-технической конференции. 27 июня - 01 июля 2011 года. Санкт-Петербург. Издательство Политехнического университета. 2011. С.34-36.
67. Десницкий В.А. Модель унифицированного процесса построения безопасных встроенных систем // Методы и технические средства обеспечения безопасности информации. Материалы Юбилейной 20-й научно-технической конференции. 27 июня - 1 июля 2011 года. Санкт-Петербург. Издательство Политехнического университета. 2011. С.15-16.
68. Полубелова О.В. Верификация правил фильтрации политики безопасности методом «проверки на модели» // Методы и технические средства обеспечения безопасности информации. Материалы Юбилейной 20-й научно-технической конференции. 27 июня - 1 июля 2011 года. Санкт-Петербург. Издательство Политехнического университета. 2011. С.87-88.
69. Комашинский Д.В. Комбинирование методов классификации и кластеризации для детектирования и идентификации malware // Методы и технические средства обеспечения безопасности информации. Материалы Юбилейной 20-й научно-технической конференции. 27 июня - 1 июля 2011 года. Санкт-Петербург. Издательство Политехнического университета. 2011. С.136-137.
70. Саенко И.Б., Полубелова О.В., Агеев С.А. Предложения по концептуальному моделированию подсистемы управления защитой информации в защищённых мультисервисных сетях // Информационная безопасность регионов России (ИБРР-2011). VII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 26-28 октября 2011 г.: Материалы конференции / СПОИСУ. СПб., 2011. С.93-94.
71. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Методы и средства построения репозитория системы управления информацией и событиями безопасности в критической информационной инфраструктуре // Информационная безопасность регионов России (ИБРР-2011). VII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 26-28 октября 2011 г.: Материалы конференции / СПОИСУ. СПб., 2011. С.79-80.
72. Саенко И.Б., Котенко И.В. Усовершенствованный генетический алгоритм для решения задачи «извлечения ролей» в RBAC-системах // Информационная безопасность регионов России (ИБРР-2011). VII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 26-28 октября 2011 г.: Материалы конференции / СПОИСУ. СПб., 2011.С.92-93.
73. Полубелова О.В. Решения по разработке репозитория в SIEM системе на основе онтологического подхода // Информационная безопасность регионов России (ИБРР-2011). VII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 26-28 октября 2011 г.: Материалы конференции /

СПОИСУ. СПб., 2011. С.89.
74. Шоров А.В. Архитектура механизма защиты от инфраструктурных атак на основе подхода «нервная система сети» // Информационная безопасность регионов России (ИБРР-2011). VII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 26-28 октября 2011 г.: Материалы конференции / СПОИСУ. СПб., 2011. С.157-158.
75. Полубелова О.В. Применение линейной темпоральной логики для верификации правил фильтрации политики безопасности методом «проверки на модели» // Информационная безопасность регионов России (ИБРР-2011). VII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 26-28 октября 2011 г.: Материалы конференции / СПОИСУ. СПб., 2011. С.88-89.
76. Саенко И.Б., Котенко И.В., Полубелова О.В. Применение онтологического подхода для построения модели уязвимостей на основе стандарта SCAP // Материалы 21-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 24 июня -29 июня 2012 г. Санкт-Петербург. Издательство Политехнического университета. С.74-76.
77. Агеев С.А., Саенко И.Б. О моделях координации управления защищенными мультисервисными сетями // Материалы 21-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 24 июня -29 июня 2012 г. Санкт-Петербург. Издательство Политехнического университета. С.39-40.
78. Нижегородов А.В., Саенко И.Б. Управление безопасностью информационно-телекоммуникационных систем при создании единой системы управления доступом к информационным ресурсам // Материалы 21-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 24 июня -29 июня 2012 г. Санкт-Петербург. Издательство Политехнического университета. С.65-67.
79. Агеев С.А., Саенко И.Б., Зозуля Е.И Методы межуровневой координации критериев функционирования защищенной мультисервисной сети // Региональная информатика (РИ-2012). Юбилейная XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции / СПОИСУ. СПб, 2012. С.77-78.
80. Крутов Д.С., Саенко И.Б. Информационный подход к созданию многоаспектной системы защиты информации // Региональная информатика (РИ-2012). Юбилейная XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. / СПОИСУ. СПб, 2012. С.103-104.
81. Морозов И.В., Саенко И.Б. Разграничение доступа к информации в геоинформационной системе // Региональная информатика (РИ-2012). Юбилейная XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. / СПОИСУ. СПб, 2012. С.111.
82. Нижегородов А.В., Саенко И.Б. О создании систем защиты облачных информационных систем // Региональная информатика (РИ-2012). Юбилейная XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. / СПОИСУ. СПб, 2012. С.114.
83. Десницкий В.А. Анализ подходов к построению anytime-алгоритмов для решения вычислительно сложных задач // Региональная информатика (РИ-2012). Юбилейная XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. / СПОИСУ. СПб, 2012. С.90-91.
84. Десницкий В.А. Конфигурирования безопасных встроенных устройств на основе нефункциональных свойств защиты // Региональная информатика (РИ-2012). Юбилейная XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. / СПОИСУ. СПб, 2012. С.91-92.
85. Десницкий В.А. Использование anytime-алгоритмов для моделирования атак и оценки защищенности в SIEM-системах // Региональная информатика (РИ-2012). Юбилейная XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. / СПОИСУ. СПб, 2012. С.92-93.
86. Дойникова Е.В., Котенко И.В. Комплексный подход к формированию системы показателей защищенности для оценки рисков и реагирования на компьютерные вторжения // Региональная информатика (РИ-2012). Юбилейная XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. / СПОИСУ. СПб, 2012. С.94-95.
87. Полубелова О.В. Применение линейной темпоральной логики для верификации правил фильтрации политики безопасности методом «проверки на модели» // Региональная информатика (РИ-2012). Юбилейная XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. / СПОИСУ. СПб, 2012. С.121.
88. Чечулин А.А., Котенко И.В. Построение графов атак на основе моделей нарушителей и данных об уязвимостях и шаблонах атак // Региональная информатика (РИ-2012). Юбилейная XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. / СПОИСУ. СПб, 2012. С.129-130.
89. Чечулин А.А., Десницкий В.А. Анализ сетевых информационных потоков в задаче анализа встроенных систем // Региональная информатика (РИ-2012). Юбилейная XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. / СПОИСУ. СПб, 2012. С.129.
90. Чечулин А.А. Распознавание цели нарушителя на основе анализа событий безопасности и графов атак // Региональная информатика (РИ-2012). Юбилейная XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. / СПОИСУ. СПб, 2012. С.130-131.
91. Шоров А.В. Использование биоинспирированного подхода «нервная система сети» для защиты компьютерных сетей от инфраструктурных атак // Региональная информатика (РИ-2012). Юбилейная

XII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26 октября 2012 г.: Материалы конференции. / СПОИСУ. СПб, 2012. С.132.
92. Котенко И.В., Саенко И.Б., Дойникова Е.В., Полубелова О.В. Применение онтологии метрик защищенности для принятия решений по обеспечению кибербезопасности // Материалы 22-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 08-12 июля 2013 г. Санкт-Петербург. Издательство Политехнического университета. С. 32-34.
93. 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.
94. 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.
95. 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.
96. Десницкий В.А. Верификация информационных потоков в процессе разработки защищенных систем со встроенными устройствами // Материалы 22-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 08-12 июля 2013 г. Санкт-Петербург. Издательство Политехнического университета. С. 66-67.
97. Дойникова Е.В., Котенко И.В. Оценка защищенности компьютерных сетей на основе графов атак с использованием многоуровневой системы показателей // Материалы 22-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 08-12 июля 2013 г. Санкт-Петербург. Издательство Политехнического университета.
98. Котенко И.В., Нестерук Ф.Г. Разработка адаптивного сервиса защиты информации // Материалы 22-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 08-12 июля 2013 г. Санкт-Петербург. Издательство Политехнического университета. С.111.
99. Чечулин А.А. Распознавание нарушителей на основе анализа деревьев атак // Материалы 22-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 08-12 июля 2013 г. Санкт-Петербург. Издательство Политехнического университета. С.75-77.
100. Саенко И.Б., Куваев В.О. Об интеллектуальной системе разграничения доступа к ресурсам единого информационного пространства для разнородных автоматизированных систем // Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)». СПб.: СПОИСУ, 2013. С.65–66.
101. Котенко И.В., Саенко И.Б. О построении многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте // Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)». СПб.: СПОИСУ, 2013. С.107–108.
102. Котенко И.В., Саенко И.Б., Полубелова О.В., Дойникова Е.В. Онтология показателей защищенности компьютерной сети как основа выработки контрмер // Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)». СПб.: СПОИСУ, 2013. С.108–109.
103. Десницкий В.А. Верификация информационных потоков в системах со встроенными устройствами // Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)». СПб.: СПОИСУ, 2013. С.92.
104. Дойникова Е.В. Подход к анализу защищенности распределенных информационных систем на основе системы показателей защищенности // Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)». СПб.: СПОИСУ, 2013. С.94-95.
105. Нестерук Ф.Г. Тенденции развития адаптивных систем защиты информации // Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)». СПб.: СПОИСУ, 2013. С.117-118.
106. Котенко И.В., Новикова Е.С. Подход к построению системы визуального анализа для управления безопасностью интеллектуальной информационной системы железнодорожного комплекса России // Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)». СПб.: СПОИСУ, 2013. С.106-107.
107. Новикова Е.С. Выявление аномальной активности в системе мобильных денежных переводов с помощью методов визуального анализа// Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)». СПб.: СПОИСУ, 2013. С.120.
108. Чечулин А.А. Применение аналитического моделирования для повышения уровня защищенности распределенных информационных систем // Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)». СПб.: СПОИСУ, 2013. С. 127-128.
109. 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 // Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)». СПб.: СПОИСУ, 2013. С.129-130.
110. 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.
111. 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.

3.16. Приоритетное направление развития науки, технологий и техники РФ, в котором, по мнению исполнителей, могут быть использованы результаты данного проекта
безопасность и противодействие терроризму

3.17. Критическая технология РФ, в которой, по мнению исполнителей, могут быть использованы результаты данного проекта
Технологии информационных, управляющих, навигационных систем

3.18. Основное направление технологической модернизации экономики России, которому, по мнению исполнителей, соответствуют результаты данного проекта
Стратегические информационные технологии, включая вопросы создания суперкомпьютеров и разработки программного обеспечения

Подпись руководителя проекта