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 **07-241 07-235 07-276 07-298 07-341 07-941 07-961 01-202 01-217**
ВИД КОНКУРСА **а - Инициативные проекты**		
ФАМИЛИЯ, ИМЯ, ОТЧЕСТВО РУКОВОДИТЕЛЯ ПРОЕКТА **Саенко Игорь Борисович**		ТЕЛЕФОН РУКОВОДИТЕЛЯ ПРОЕКТА **(812)3282642**
ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ, ГДЕ РЕАЛИЗУЕТСЯ ПРОЕКТ **Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук**		
ОБЪЕМ СРЕДСТВ, ФАКТИЧЕСКИ ПОЛУЧЕННЫХ ЗА 2012 г. **405000 руб.**	ОБЪЕМ ФИНАНСИРОВАНИЯ, ЗАПРАШИВАЕМЫЙ НА СЛЕДУЮЩИЙ ГОД **600000 руб.**	
ЧИСЛО УЧАСТНИКОВ ПРОЕКТА (включая руководителя) **10**	ЧИСЛО УЧАСТНИКОВ, ИМЕЮЩИХ УЧЕНУЮ СТЕПЕНЬ **4**	ЧИСЛО МОЛОДЫХ (до 35 лет включительно) УЧАСТНИКОВ **9**
Чечулин Андрей Алексеевич		
Шоров Андрей Владимирович		
Нестерук Филипп Геннадьевич		
Десницкий Василий Алексеевич		
Комашинский Дмитрий Владимирович		
Дойникова Елена Владимировна		
Степашкин Михаил Викторович		
Полубелова Ольга Витальевна		
Коновалов Алексей Михайлович		
ПОДПИСЬ РУКОВОДИТЕЛЯ ПРОЕКТА		ДАТА ПОДАЧИ ОТЧЕТА **14.01.2013**

ОТЧЕТ ЗА 2012 ГОД ПО ПРОЕКТУ РФФИ 11-07-00435-а

Статус отчета: зарегистрирован

Дата подписания: 14.01.2013

Подписал: Саенко Игорь Борисович

Дата регистрации: 14.01.2013

Отчет распечатан: 14.01.2013

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
2013

1.6. Вид отчета
этап 2012 года

1.7. Аннотация
Разработаны методы и алгоритмы адаптации и совершенствования эволюционных моделей первоначального построения и оперативного управления схемами разграничения доступа к информационным и сетевым ресурсам в современных и перспективных компьютерных системам и сетях, основанные на усовершенствованных генетических алгоритмах. Существенной особенностью этих алгоритмов является проведение дополнительной базовой операции в виде локальной оптимизации структур хромосом после выполнения операции кроссовера. Разработана концепция построения и функционирования системы интеллектуальных сервисов разграничения доступа к информационным и сетевым ресурсам в компьютерных системах и сетях на основе технологии управления информацией и событиями безопасности (SIEM), обеспечивающей реализацию более высоких требований по производительности и адекватности принимаемых решений. Выполнена программная апробация отдельных компонентов системы интеллектуальных сервисов разграничения доступа, основанных на принципах SIEM технологии. Проведено исследование вопросов реализации в системах разграничения доступа функций внутреннего представления, логического вывода и визуализации данных о событиях доступа, реализуемых информационным хранилищем SIEM системы в перспективных компьютерных системах и сетях, и сформирована обобщенная методика его построения. Сформированы частные постановки задач, моделей и методов синтеза защищенных мультисервисных сетей на отдельных уровнях управления разграничением доступа к информационным и сетевым ресурсам. Проведена экспериментальная оценка полученных результатов.

1.8. Полное название организации, где реализуется 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) аннотаций научных отчетов и перечня публикаций по проекту в авторской редакции"

Подпись руководителя проекта

Форма 502. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ НА АНГЛИЙСКОМ ЯЗЫКЕ

2.1. Номер проекта
11-07-00435

2.2. Руководитель проекта
Saenko Igor Borisovich

2.3. Название проекта
Research and development of mathematical models and methods of analysis and synthesis of restricting access to information and network resources in a modern and advanced computer systems and networks through the creation and application of artificial intelligence

2.4. Год представления отчета
2013

2.5. Вид отчета
этап 2012 года

2.6. Аннотация
The methods and algorithms for the adaptation and improvement of evolutionary models of initial construction and operational management schemas of access differentiation to information and communication resources in modern and perspective computer systems and networks based on improved genetic algorithms are developed. A significant feature of these algorithms is to carry out an additional basic operation as a local optimization of the structures of chromosomes after crossover. The concept of construction and operation of the system of intelligent services for an access to information and network resources in computer systems and networks based on security information and events management (SIEM) technology that provides a higher performance requirements and the adequacy of decisions is developed. Software testing for individual components of intelligent security access services' system based on the principles of SIEM technology is completed. A study of the issues of the realization in access differentiation systems the functions of internal representation, inference and visualization of access event information that are implemented in SIEM system repositories in advanced computer systems and networks is completed. The generalized technique formed the repository is build. Private setting, models and methods of synthesis of protected multiservice networks at the individual levels of differentiation of access to information and communication resources are formed. An experimental evaluation of the results is done.

2.7. Полное название организации, где реализуется проект
Saint-Petersburg Institute for Informatics and Automation of Russian Academy of Sciences

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(в порядке значимости)
07-241 07-235 07-276 07-298 07-341 07-941 07-961 01-202 01-217

3.4. Объявленные ранее цели проекта на 2012 год
Основными целями проекта на 2012 год являлись: (1) разработка методов и алгоритмов адаптации и совершенствования эволюционных моделей первоначального построения и оперативного управления схемами разграничения доступа в современных и перспективных компьютерных системах и сетях; (2) разработка концепции построения и функционирования системы интеллектуальных сервисов разграничения доступа к информационным и сетевым ресурсам в компьютерных системах и сетях на основе технологии управления информацией и событиями безопасности (SIEM); (3) исследование вопросов реализации компонентов системы интеллектуальных сервисов разграничения доступа к информационным и сетевым ресурсам, основанных на принципах SIEM технологии; (4) исследование вопросов реализации в системах разграничения доступа перспективных компьютерных систем и сетей функций внутреннего представления, логического вывода и визуализации данных о событиях доступа, реализуемых информационным хранилищем; (5) формирование обобщенной методики построения информационного хранилища данных о событиях доступа в перспективных компьютерных системах и сетях; (6) формирование частных постановок задач, моделей и методов синтеза защищенных мультисервисных сетей на отдельных уровнях управления разграничением доступа к информационным и телекоммуникационным ресурсам; (7) экспериментальная оценка полученных результатов.

3.5. Степень выполнения поставленных в проекте задач
Все задачи, запланированные в проекте на второй год, выполнены полностью. Дополнительно проведен анализ подходов к оцениванию защищенности компьютерных систем и сетей от несанкционированного доступа к информации.

3.6. Полученные важнейшие результаты
1. В ходе разработки методов и алгоритмов адаптации и совершенствования эволюционных моделей первоначального построения и оперативного управления схемами разграничения доступа в современных и перспективных компьютерных системах и сетях были проведены исследования, направленные на дальнейшее совершенствование эволюционных алгоритмов ролевого разграничения доступа и их применение в других предметных областях. Были выявлены недостатки предложенного ранее генетического алгоритма для решения проблемы «извлечения ролей», которые заключались в резком падении производительности алгоритма при больших размерностях задачи, когда количество пользователей для системы разграничения доступа превышает несколько сотен человек. Причиной этого оказались недостаточная гибкость и избыточность информационных структур, используемых в генетических алгоритмах в качестве «хромосом». В предложенном усовершенствованном генетическом алгоритме для решения проблемы «извлечения ролей» удалось существенно снизить эту избыточность за счет использования «информационных хромосом» переменной длины, отказа от использования «управляющей хромосомы» и введения дополнительной базовой операции в виде локальной оптимизации структур хромосом особей-потомков, полученных в результате выполнения модернизированной операции кроссовера. Проведенная экспериментальная оценка усовершенствованного генетического алгоритма оптимизации ролевой схемы разграничения доступа показала существенный выигрыш в его производительности при больших размерностях задачи. Кроме того, данный подход был апробирован в других задачах синтеза схем разграничения доступа, в частности, в задаче синтеза виртуальной локальной вычислительной сети, в которой дополнительно в качестве переменных используется вектор булевых значений, определяющих наличие флага общего доступа на соответствующем информационном ресурсе.
2. Разработанная концепция построения и функционирования системы интеллектуальных сервисов разграничения доступа к информационным и сетевым ресурсам в компьютерных системах и сетях на основе технологии управления информацией и событиями безопасности (SIEM) представляет собой систему взглядов на обеспечение санкционированного доступа к информации за счет применения интеллектуальных сервисов и механизмов разграничения доступа. Эта концепция предназначена для заказчиков, разработчиков и пользователей современных и перспективных компьютерных систем и сетей, в которых осуществляется обработка, хранение и представление информации, требующей защиты от несанкционированного доступа, и является методологической базой нормативно-технических и методических документов, направленных на решение задач выработки технических заданий на построение, создание и сертификацию систем интеллектуальных сервисов разграничения доступа. Концепция содержит систему основных определений, в которой введены и обоснованы такие новые определения, как сервис разграничения доступа, интеллектуализация разграничения доступа, система интеллектуальных сервисов разграничения доступа (СИСРД), интеллектуальная система разграничения доступа (ИСРД) и система интеллектуализации разграничения доступа (СИРД). Определено место СИСРД в СИРД и в ИСРД как в системах более высокого уровня. Кроме того, в этой концепции определены принципы интеллектуализации разграничения доступа к информационным и сетевым ресурсам, цели и задачи СИРД, особенности компьютерных систем и объектов как объектов интеллектуализации разграничения доступа к информационным и сетевым ресурсам, механизмы интеллектуализации разграничения доступа к информационным и сетевым ресурсам, общая архитектура и требования к компонентам СИРД.

3. При исследовании вопросов реализации компонентов системы интеллектуальных сервисов разграничения доступа к информационным и сетевым ресурсам, основанных на принципах SIEM технологии, были проанализированы сервисы сбора, преобразования и хранения информации о событиях доступа, сервисы моделирования атак и поведения системы разграничения доступа, сервисы поддержки принятия решений в области обеспечения санкционированного доступа и сервисы визуализации информации о событиях доступа. Для реализации интеллектуальных сервисов сбора, преобразования и хранения информации были выявлены достоинства и недостатки существующих инструментальных средств и предложено онтологическое представление данных, а в качестве инструментария для их реализации предложено использовать гибридное инструментальное средство. Для реализации интеллектуальных сервисов моделирования атак и поведения системы разграничения доступа предлагается подход, основанный на моделировании объекта доступа, поведения злоумышленника, генерации общего графа атак, вычислении различных показателей доступности и предоставлении всеобъемлющих процедур анализа доступности. В качестве базиса для построения моделей используется набор стандартов для общего перечисления, выражения и отчетности по информации, связанной с доступом к информации. Данные стандарты позволяют создать единое, обновляемое и согласованное хранилище данных, необходимое для построения и анализа графов или деревьев атак. Для реализации интеллектуальных сервисов поддержки принятия решений по разграничению доступа представляется оптимальным подход, согласно которому лицо, принимающее решение, итеративно создает желаемые уровни для целей или изменяет верхние и нижние границы через графический интерфейс и, таким образом, снижает набор вариантов-кандидатов. Достоинство данного подхода лежит не только в производимом выборе, но и понимании ситуации по разграничению доступа, которое получается на каждом уточняющем шаге его оценки. Для реализации интеллектуальных сервисов визуализации выделены следующие классы графов, которые можно использовать для их построения: простые диаграммы; диаграммы с накоплением; схемы полигонов; диаграммы рассеивания; графы параллельных координат; графы связей; карты; карты деревьев. Каждый из этих графов имеет разные возможности и подчеркивает конкретные аспекты данных. Наиболее специфичными оказались схемы полигонов и графы параллельных координат.
4. При исследовании вопросов реализации в системах разграничения доступа перспективных компьютерных систем и сетей функций внутреннего представления, логического вывода и визуализации данных о событиях доступа, реализуемых информационным хранилищем, были выявлены базовые интеллектуальные функции, которые включают в себя: фильтрацию поступающих данных о событиях доступа; преобразование их во внутренний универсальный формат; агрегирование и корреляцию данных; хранение данных о событиях доступа. Показано, что известные простые форматы не могут удовлетворять следующим требованиям интеллектуальных сервисов разграничения доступа: поддержке структурированного представления информации; использованию меток времени; обеспечению иерархической структуры для представления информации. Обосновано, что наиболее перспективным решением в этой области является онтологический подход к представлению данных, который предполагает использование специального формализованного описания предметной области, основанного, как правило, на дескрипционной логике, и получившего название онтологии. Суть онтологического подхода заключается в том, что вначале выделяется набор базовых понятий данной предметной области. Затем строятся связи между концептами, т.е. задаются отношения между базовыми понятиями. Следующим этапом обработки данных о событиях доступа является корреляция событий, под которой понимается сопоставление различной информации об одинаковых событиях или явлениях, полученных от различных источников, с целью устранения имеющейся в них неопределенности и/или получения новой достоверной информации о доступе. Процесс корреляции информации тесно связан с процессом получения новой информации на основе анализа хранимых онтологий в условиях их неполноты и противоречивости. Данные о событиях доступа, прошедшие все вышеописанные процедуры обработки, помещаются в репозиторий. В качестве базовой архитектуры репозитория целесообразно использовать архитектуру SOA (архитектуру, ориентированную на сервисы), которая реализуется как набор web-сервисов, используемых для доступа к данным в репозитории. Онтологический подход позволяет реализовать в репозитории современных и перспективных компьютерных систем и сетей подсистему логического вывода решений по разграничения доступа, основанную на онтологии. В настоящее время для этой цели получает широкое распространение язык OWL (Web Ontology Language). Кроме OWL, для логического вывода используется SWRL (Semantic Web Rule Language). Для визуализации данных о событиях доступа предложена архитектура компонента, в котором выделяются три уровня: пользовательский интерфейс; управляющие сервисы, состоящие из контроллера графических элементов; менеджера сервисов, осуществляющих управление низкоуровневыми элементами модели графическими элементами и другими сервисами.
5. При формировании обобщенной методики построения информационного хранилища данных о событиях доступа в перспективных компьютерных системах и сетях учтен предложенный онтологический подход к представлению данных. В соответствии с принципами SOA доступ к информации осуществляется с использованием веб-сервисов. При этом архитектура SOA является концептом распределенной информационной среды, которая объединяет воедино различные программные модули и приложения, основанные на хорошо определенных интерфейсах, и обеспечивает их взаимодействие. В соответствии с принципами SOA архитектура репозитория разделяется на три основных слоя: слоя хранения, слоя представления и слоя сервисов. Слой хранения включает различные виды хранилищ, такие, как реляционное, триплетов и XML-ориентированное. Слой представления охватывает все элементы, которые обеспечивают взаимодействие пользователя с ИСРД. Этот механизм может быть реализован в виде командной строки или текстового меню, однако для него наиболее предпочтителен графический интерфейс, разработанный как тонкий клиент (Windows, Swing API и другие) или основанный на HTML. Слой сервисов является дополнительным слоем между слоем представления и слоем хранения и позволяет абстрагировать взаимодействие между одним или многими бизнес-объектами, потоками и сервисами посредством промежуточного интерфейса API. Разработанная методика позволяет создавать

онтологию в виде совокупности схемы данных TBox (Terminology box) и самих данных – ABox (Assertion box). Согласно данной методике описание объектов и событий доступа представляет собой последовательность программно-аппаратных компонентов, соединенных логическими операторами (AND, OR, NOT AND, NOT OR), которые преобразуются в наборы аксиом, отображающих логику взаимосвязей концептов.
6. При формировании частных постановок задач, моделей и методов синтеза защищенных мультисервисных сетей на отдельных уровнях управления разграничением доступа к информационным и телекоммуникационным ресурсам разработан и предложен к использованию порядок и обобщенный метод разработки взаимоувязанных математических моделей, который справедлив и для этапа эксплуатации. Первым этапом разработки моделей является формулировка целевого предназначения ЗМС и формулировка требований к ее системе управления. Второй этап образуют разработка содержательной модели, разработка концептуальной модели, разработка и определение функциональных и статистических взаимосвязей характеристик и определение функциональных взаимосвязей между компонентами математического комплекса моделирования. Третьим этапом разработки являются: планирование проведения верификации разработанного комплекса моделей; подготовка исходных данных для верификации разработанного комплекса; верификация комплекса; анализ экспериментальных результатов; выработка рекомендаций. На уровне оперативного управления разграничением доступа выполнены постановки следующих задач: планирования разработки ЗМС и её системы управления и синтеза топологии ЗМС. На уровне оперативно-технического управления разграничением доступа сделаны постановки задач: оптимального распределения ресурсов; оптимизации и управления маршрутизацией; оптимизации распределения и управления потоками; оптимизации управления устойчивостью; оптимизации управления доступом. На уровне технологического управления разработаны постановки следующих задач: сетевого мониторинга; оптимального управления сетевыми элементами.
7. В ходе экспериментальной оценки полученных результатов для усовершенствованного алгоритма генетической оптимизации ролевой схемы доступа было выявлено существование зависимости производительности алгоритма от показателя критичности ролей, характеризующего требуемую схему ролевого доступа. Экспериментальная апробация и оценка решений по онтологическому моделированию и реализации репозитория событий доступа подтвердили правомерность предположений об эффективности гибридной реализации и сервисно-ориентированной архитектуре информационного хранилища.
8. Дополнительно проведенный анализ подходов к оцениванию защищенности компьютерных систем и сетей от несанкционированного доступа к информации показал, во-первых, сложность и важность задачи анализа защищенности для систем разграничения доступа, во-вторых, необходимость разработки алгоритмов и методик оценивания защищенности, способных давать нужную оценку как в off-line, так и в on-line режимах, в-третьих, необходимость учета и использования метрик доступа к информации, характеризующих топологию сети, злоумышленника, атакующие действия, а также интегральные свойства.

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 второго 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 20-й международной конференции (Euromicro) по параллельной, распределенной и сетевой обработке информации (PDP 2012), Мюнхен, Февраль, 2012; секции работ в развитии (Work in Progress) 20-й международной конференции (Euromicro) по параллельной, распределенной и сетевой обработке информации (PDP 2012), Мюнхен, Февраль, 2012; IV Всероссийской научно-практической конференции «Безопасность в чрезвычайных ситуациях», Санкт-Петербург, март, 2012; Международной научно-практической конференции «Современные направления теоретических и прикладных исследований '2012», Украина, Одесса, март, 2012; 14-й международной конференции «РусКрипто-12», Московская обл., март, 2012; 9-ой международной объединенной конференции по электронной коммерции и коммуникациям (e-Business and Telecommunications) (ICETE 2012), Италия, Рим, июль, 2012; Международной конференции по безопасности и криптографии (SECRYPT 2012 Италия, Рим, июль, 2012; Конгрессе по интеллектуальным системам и информационным технологиям «IS&IT'12», Дивноморское, сентябрь, 2012; 21-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, июнь, 2012; 2-ой Семинар по безопасности систем и программной нажедности (Security of System & Software resiLiency) (3SL-2012), Бесансьон, Франция, ноябрь, 2012; 5-й Российской мультиконференции по проблемам управления (МКПУ-2012) - конференции "Информационные технологии в управлении" (ИТУ-2012), Санкт-Петербург, октябрь, 2012; Седьмой Международной научно-технической конференции «Информационные технологии в промышленности» (ITI*2012), Беларусь, Минск, октябрь, 2012; Юбилейной XII Санкт-Петербургской международной конференции «Региональная информатика (РИ-2012), октябрь, 2012.

3.9. Методы и подходы, использованные в ходе выполнения проекта

В ходе выполнения проекты получили дальнейшее развитие следующие методы и подходы:
(1) методы теории оптимизации в части формирования формализованных постановок задач синтеза схем разграничения доступа и применения генетических алгоритмов оптимизации для их решения;
(2) методы эволюционного моделирования сложных систем в части разработки усовершенствованных генетических алгоритмов оптимизации, которые ориентированы на повышение своего быстродействия

при больших размерностях задачи;
(3) методы генетической оптимизации в применении к новым областям разграничения доступа, в частности, для синтеза виртуальных локальных вычислительных сетей;
(4) методы интеллектуального анализа данных в части разработки усовершенствованного алгоритма для решения проблемы Role Mining Problem;
(5) методы теорий математического программирования, массового обслуживания, случайных процессов и графов в части формирования частных постановок задач для управления разграничением доступа в защищенных мультисервисных сетях;
(6) онтологический подход к моделированию предметной области системы разграничения доступа в современных и перспективных компьютерных системах и сетях;
(7) методы проектирования и реализации гибридного информационного хранилища данных о событиях доступа на основе сервисно-ориентированной архитектуры;
(8) подход к динамическому управлению разграничением доступа, ориентированный на учет и совместную обработку информационных профилей пользователей, а также событий доступа и шаблонов инцидентов;
(9) методы системного анализа и теории систем в части их применения для разработки концепции интеллектуализации разграничения доступа в компьютерных системах и сетях.

3.10.1.1. Количество научных работ, опубликованных в ходе выполнения проекта
40

3.10.1.2. Из них включенных в перечень ВАК
10

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 2012 г.
2

3.11. Участие в научных мероприятиях по тематике проекта, которые проводились при финансовой поддержке Фонда
2

3.12. Участие в экспедициях по тематике проекта, проводимых при финансовой поддержке Фонда 0

3.13. Финансовые средства, полученные от РФФИ
405000 руб.

3.15. Адреса (полностью) ресурсов в Internet, подготовленных авторами по данному проекту
http://www.comsec.spb.ru/saenko/

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

1. Котенко И.В., Саенко И.Б., Юсупов Р.М. Защита информационных ресурсов в компьютерных сетях // Вестник РАН, том 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, том 81, № 9, сентябрь 2011. С. 844-845.
3. 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.
4. Десницкий В.А., Чечулин А.А. Модели процесса построения безопасных встроенных систем // Системы высокой доступности, № 2, т.7, 2011. С.97-101.
5. Саенко И.Б., Котенко И.В. Генетическая оптимизация схем ролевого доступа к информации // Системы высокой доступности, №2, т.7, 2011. С.112-116.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.

14. 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.
15. 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. Издательство «Научно-инновационный центр». С.11-21.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. Котенко И.В., Саенко И.Б. SIEM-системы для управления информацией и событиями безопасности // «Защита информации. Инсайд». №5, 2012. С.2-12.
22. Igor Saenko, Igor Kotenko. Genetic Algorithms for Role Mining Problem // Proceeding of the 19th International Euromicro Conference on Parallel, Distributed and Network-based Processing. Ayia Napa, Cyprus, 9-11 February 2011. P. 646-650.
23. Igor Saenko, Igor Kotenko. Design and Performance Evaluation of Improved Genetic Algorithm for Role Mining Problem // // Proceeding of the 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing. Garching, Germany, 15-17 February 2012.
24. Igor Kotenko, Olga Polubelova, Igor Saenko. Hybrid Data Repository Development and Implementation for Security Information and Event Management // // Proceeding of the 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing. Work in Progress. Garching, Germany, 15-17 February 2012.
25. 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.
26. Saenko I., Kotenko I. Design and Performance Evaluation of Improved Genetic Algorithm for Role Mining Problem // Proceeding of the 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing (PDP 2012). P.269-274.
27. Kotenko I., Polubelova O., Saenko I. Hybrid Data Repository Development and Implementation for Security Information and Event Management // Proceeding of the Work in Progress Session 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing (PDP 2012). Garching/Munich, February 2012.
28. 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.
29. 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.
30. 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.
31. Саенко И.Б., Нижегородов А.В. Необходимость создания систем защиты баз знаний // Сборник научных трудов по материалам международной научно-практической конференции «Современные направления теоретических и прикладных исследований - 2011». Том 3. Технические науки. Одесса: Черноморье, 2011. С.76-78.
32. 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.
33. 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.
34. 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.
35. 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.
36. 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.
37. 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.
38. 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.
39. 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.
40. 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.
41. Полубелова О.В., Саенко И.Б. Применение онтологического подхода и логического вывода для управления информацией и событиями безопасности // Четырнадцатая международная конференция «РусКрипто-12», Московская область, Солнечногорск, 29-30 марта 2012 года. [Электронный ресурс]. http://www.ruscrypto.org/sources/conference/rc2012/.
42. 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.
43. 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.
44. 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.
45. 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.
46. 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.
47. 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.
48. 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.
49. 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.
50. 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.
51. 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.
52. 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.
53. 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.

54. 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.
55. Полубелова О.В. Решения по разработке репозитория в SIEM системе на основе онтологического подхода // VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2011). 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.89.
56. Шоров А.В. Архитектура механизма защиты от инфраструктурных атак на основе подхода «нервная система сети» // VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2011). 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.157-158.
57. Полубелова О.В. Применение линейной темпоральной логики для верификации правил фильтрации политики безопасности методом «проверки на модели» // VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2011). 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.88-89.
58. 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.
59. 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.
60. 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.
61. 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.
62. 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.
63. 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.
64. 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.
65. 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.
66. 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.
67. 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.
68. 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.
69. 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.
70. 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.
71. 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.
72. 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.
73. 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.

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

безопасность и противодействие терроризму

3.18. Критическая технология РФ, в которой, по мнению исполнителей, соответствуют результаты данного проекта

Технологии информационных, управляющих, навигационных систем

3.19. 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