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 - создание и развитие ИВТР для фундаментальных исследований**		КОД(Ы) КЛАССИФИКАТОРА **07-811 01-217 01-202 01-203**
ВИД КОНКУРСА **а - Инициативные проекты**		
ФАМИЛИЯ, ИМЯ, ОТЧЕСТВО РУКОВОДИТЕЛЯ ПРОЕКТА **Саенко Игорь Борисович**		ТЕЛЕФОН РУКОВОДИТЕЛЯ ПРОЕКТА **(812)3282642**
ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ, ГДЕ ВЫПОЛНЯЕТСЯ ПРОЕКТ **Учреждение Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН**		
ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ, ЧЕРЕЗ КОТОРУЮ ОСУЩЕСТВЛЯЕТСЯ ФИНАНСИРОВАНИЕ **Учреждение Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН**		
ЧИСЛО УЧАСТНИКОВ ПРОЕКТА (включая руководителя) **10**	ЧИСЛО УЧАСТНИКОВ, ИМЕЮЩИХ УЧЕНУЮ СТЕПЕНЬ **3**	ЧИСЛО МОЛОДЫХ (до 35 лет включительно) УЧАСТНИКОВ **7**
Степашкин Михаил Викторович		
Тишков Артем Валерьевич		
Полубелова Ольга Витальевна		
Десницкий Василий Алексеевич		
Сидельникова Екатерина Викторовна		
Чечулин Андрей Алексеевич		
Комашинский Дмитрий Владимирович		
Резник Сергей Александрович		
Шоров Андрей Владимирович		
ПОДПИСЬ РУКОВОДИТЕЛЯ ПРОЕКТА		ДАТА ПОДАЧИ ОТЧЕТА **12.12.2011**

ОТЧЕТ ЗА 2011 ГОД ПО ПРОЕКТУ РФФИ 11-07-00435-а

Статус отчета: подписан

Дата последнего изменения: 12.12.2011

Отчёт создал: Саенко Игорь Борисович

Отчет распечатан: 12.12.2011

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
2012

1.6. Вид отчета
этап 2011 года

1.7. Аннотация
Проведен анализ эффективности построения систем разграничения доступа к информации в автоматизированных информационных и телекоммуникационных системах при применении разнородных средств и механизмов защиты. Разработан новый подход к оценке схем разграничения доступа, основанный на комплексном применении традиционных математических и интеллектуальных моделей и методов. Существенным отличием рассматриваемого подхода является тот факт, что в нем используется расширенная система показателей эффективности, в которую включаются не только показатели конфиденциальности, но также показатели доступности и целостности информационных и телекоммуникационных ресурсов. Осуществлена разработка формальной постановки задачи синтеза схем разграничения доступа к информации, основанных на совместном применении дискреционных, мандатных и ролевых средств и механизмов доступа к неоднородным распределенным базам данных, геоинформационным системам, мультимедийным базам данных и другим информационным ресурсам. Исследованы вопросы применения теории эволюционного моделирования для решения поставленной задачи синтеза на основе использования специально разработанных генетических алгоритмов оптимизации. Выполнена разработка концептуальной модели многоуровневого управления безопасностью в защищенных мультисервисных сетях, в которой критерии безопасности на различных уровнях взаимно увязываются с другими. Для динамического управления разграничением доступа к информации предложено использование подхода, применяемого в системах управления информацией и событиями безопасности. Выполнена первоначальная экспериментальная оценка полученных результатов.

1.8. Полное название организации, где выполняется проект
Учреждение Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН

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

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
2012

2.5. Вид отчета
этап 2011 года

2.6. Аннотация
The effectiveness analysis of the information access differentiation system construction in the automated information and telecommunication systems in applying different protection means and mechanisms is driven. A new approach to evaluating access schemas based on integrated application of traditional mathematical and intellectual models and methods is developed. The essential difference of this approach is that it uses the enhanced system performance, which includes not only confidency, but also performance indicators of the availability and integrity of information and telecommunication resources. The formal task of synthesis information access schemes, based on the joint application of discretionary, mandatory and role-based tools and mechanisms for access to heterogeneous distributed databases, geographical information systems, multimedia databases and other information resources is completed to develop. The issues of the application of the evolutionary modeling theory for the solution the task of synthesis using specially designed genetic optimization algorithms are studied. The development of a conceptual model of multilevel security management in protected multiservice networks, in which the criteria of safety at various levels are linked with others, is completed. To dynamically manage permissions to the information it is requested the approach which is used in security information and event management systems. The initial experimental evaluation of the results is performed.

2.7. Полное название организации, где выполняется 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
07-811 01-217 01-202 01-203

3.4. Объявленные ранее цели проекта на 2011 год
Основными целями проекта на 2011 год являлись: (1) разработка и исследование моделей и методов анализа эффективности построения систем разграничения доступа к информации в автоматизированных информационных и телекоммуникационных системах при применении разнородных средств и механизмов защиты; (2) разработка и исследование моделей и методов синтеза схем разграничения доступа к информации, основанных на совместном применении дискреционных, мандатных и ролевых средств и механизмов доступа к неоднородным распределенным базам данных, геоинформационным системам, мультимедийным базам данных и другим информационным ресурсам; (3) разработка и исследование моделей и методов синтеза схем разграничения доступа, основанных на использовании средств построения виртуальных компьютерных сетей и других сетевых механизмов управления доступом в компьютерных системах и сетях; (4) разработка и исследование моделей и методов динамического управления разграничением доступа к информации на основе формирования и анализа информационных образов, профилей поведения и аномальных действий пользователей.

3.5. Степень выполнения поставленных в проекте задач
Все задачи, запланированные в проекте на первый год, выполнены полностью. Дополнительно проведен анализ уровня развития и практического применения технологии управления информацией и событиями безопасности.

3.6. Полученные за отчетный период важнейшие результаты
1. Для анализа эффективности построения систем разграничения доступа к информации в автоматизированных информационных и телекоммуникационных системах при применении разнородных средств и механизмов защиты обоснован и разработан новый подход, основанный на комплексном применении традиционных математических и интеллектуальных моделей и методов. Данному подходу свойственен ряд характерных особенностей. Во-первых, он выделяет в системе защиты информации в автоматизированных информационных и телекоммуникационных системах новый архитектурный уровень – интеллектуальных сервисов защиты. Во-вторых, он ориентирует решение задачи синтеза систем разграничения доступа вначале на создание методами традиционной математики формальной оптимизационной постановки задачи, а затем на ее решение интеллектуальными методами. В-третьих, для решения задач синтеза систем разграничения доступа он предусматривает использование усовершенствованных генетических алгоритмов как наиболее эффективного метода решения дискретных оптимизационных задач очень большой размерности. Наконец, предложенный подход имеет наивысшую эффективность в критически важных инфраструктурах, где наибольшую значимость имеют не внешние, а внутренние угрозы безопасности информации, а задачи синтеза систем разграничения доступа отличаются очень высокой размерностью. Тот факт, что данный подход можно применять не только на этапе тестирования, но также на этапах проектирования и эксплуатации анализируемых компьютерных сетей и систем, также является его несомненным достоинством и преимуществом.Существенным отличием рассматриваемого подхода от других релевантных является тот факт, что в нем используется расширенная система показателей эффективности. В данную систему, в отличие от других подходов, включаются не только показатели конфиденциальности, но также показатели доступности и целостности информационных и телекоммуникационных ресурсов. Между этими показателями существует антагонистическая взаимосвязь, которая обусловливает многокритериальный характер задач синтеза рациональных схем доступа в автоматизированных информационных и телекоммуникационных системах. К числу областей, в которых наиболее остро стоит задача оценки эффективности построения схем разграничения доступа, относятся базы данных и знаний коллективного пользования в крупных корпоративных автоматизированных системах, где количество пользователей составляет от нескольких десятков до нескольких тысяч, а количество регламентируемых защищаемых ресурсов достигает уровня в нескольких десятков тысяч или даже миллионов. К категории такого рода автоматизированных систем относятся информационные и телекоммуникационные системы критически важных (ключевых) инфраструктур. Разработка методов решения задачи синтеза или реконфигурирования схем разграничения доступа в таких инфраструктурах в реальном или близком к реальном масштабе времени приобретает исключительно важное значение.
2. Разработанные модели и методы синтеза схем разграничения доступа к информации, основанных на совместном применении дискреционных, мандатных и ролевых средств и механизмов доступа к неоднородным распределенным базам данных, геоинформационным системам, мультимедийным базам данных и другим информационным ресурсам, позволяют обеспечить реальный масштаб времени при принятии решения по построению схем разграничения доступа в информационных и телекоммуникационных системах критически важных инфраструктур. В соответствии с применяемым в проекте подходом к оценке эффективности схем разграничения доступа, разработанные модели и методы синтеза сочетают в себе применение традиционных математических методов для формализованной постановки задачи в виде оптимизационной задачи и применение методов искусственного интеллекта для нахождения ее рационального решения в отводимые временные

сроки. Для оптимизационной постановки задачи предложена целевая функция, в которой в качестве основных переменных величин используются бинарные матрицы. Данные матрицы отображают схему разграничения доступа. Так, например, в случае ролевой схемы разграничения доступа такими матрицами являются матрица «пользователи - роли» и «роли - ресурсы». Целевая функция постановки задачи отражает степень выполнения требований по конфиденциальности и доступности ресурсов. В частности, в качестве целевой функции для ролевой схемы доступа предложено применять взвешенную свертку элементов бинарной матрицы, определяющей расхождение требуемой и реальной матриц «пользователи - ресурсы». Для других моделей доступа (дискреционной, мандатной, комбинированной) целевые функции также основываются на использовании бинарных переменных матриц и / или векторов.Для решения оптимизационной задачи предложено использование метода генетических алгоритмов, которые составляют основное содержание теории эволюционного моделирования. Достоинством генетических алгоритмов является то, что они относятся к классу эвристических алгоритмов оптимизации, позволяющих получить оптимальное или близкое к оптимальному решение в реальном масштабе времени или близком к нему. Однако традиционные генетические алгоритмы оптимизации оказываются непригодными по ряду причин. В этой связи были разработанные специальные усовершенствования отдельных элементов и процедур традиционного генетического алгоритма с сохранением общей логики выполнения последнего. Для ролевой схемы доступа к числу таких усовершенствований относятся следующие: применение не одной, а трех хромосом, одна из которых является управляющей, а две остальные - информационные; применение в качестве генов информационных хромосом столбцов искомых бинарных переменных матриц; модификация операций кроссинговера и мутации особей в популяции генетического алгоритма и другие. Для других моделей доступа для генетического алгоритма оптимизации также предложены необходимые усовершенствования. Предложенные решения в построении этих генетических алгоритмов имеют фундаментальное значение для науки и техники, так как они вносят значительный вклад в теорию эволюционного моделирования и открывают новые классы полихромосомных (имеющих более одной хромосомы), самоуправляемых (управляемых хромосомами) и сложно структурированных (генами хромосом являются объекты со сложной структурой) генетических алгоритмов.Разработанные генетические алгоритмы оптимизации ролевых схем разграничения доступа являются новым и эффективным средством решения известной проблемы RMP (Role Mining Problem), впервые сформулированной в 2003 году Кюлманом (Kuhlmann). С момента ее первого формулирования были предложены разные подходы к ее решению: графовый, стоимостной, вероятностный, кластерный, семантический, булево-матричный. Однако только разработанные генетические алгоритмы являются универсальным средством решения проблемы RMP, обладающим достаточно хорошей производительностью и масштабируемостью.Разработан программный макет в среде универсального языка программирования Delphi, который позволил провести экспериментальную оценку разработанного генетического алгоритма на предмет его вычислительной сложности и производительности. Проведенная с его помощью оценка показала достаточно высокую эффективность разработанного алгоритма как метода синтеза схем разграничения доступа к информационным ресурсам.

3. Для синтеза схем разграничения доступа, основанных на использовании средств построения виртуальных компьютерных сетей и других сетевых механизмов управления доступом в компьютерных системах и сетях, также предложено использование генетических алгоритмов оптимизации как базового метода синтеза. Однако многоуровневая архитектура построения автоматизированных систем управления современными телекоммуникационными системами дополнительно требует комплексного подхода к управлению безопасностью таких систем, при котором взаимно увязываются вопросы управления на следующих уровнях: оперативном, оперативно-техническом, технологическом и уровне отдельных сетевых элементов. Телекоммуникационные системы, в которых реализовано многоуровневое управление безопасностью и обеспечивается выполнение жестких требований по разграничению доступа (защите от несанкционированного доступа) к разнородным услугам и ресурсам получили название защищенных мультисервисных сетей (ЗМС). Для синтеза систем управления доступом в ЗМС разработана концептуальная многоуровневая модель управления безопасностью, в которой критерии безопасности на различных уровнях взаимно увязываются с другими критериями (устойчивости, пропускной способности и т.д.). Предложенная концептуальная модель является основой для разработки частных оптимизационных моделей для каждого уровня управления ЗМС, разработка и анализ которых является задачей следующего этапа проекта.

4. Для динамического управления разграничением доступа к информации на основе формирования и анализа информационных образов, профилей поведения и аномальных действий пользователей предложено использование подхода, применяемого в системах управления информацией и событиями безопасности. Системы такого рода называются SIEM-системами (Security Information and Event Management) и представляют собой новое и достаточно перспективное направление в области обеспечения и управления безопасностью информацией в автоматизированных информационно-телекоммуникационных системах. Исследования в области применения SIEM-систем для динамического управления разграничением доступа к информации проводились в области обоснования архитектуры SIEM-системы нового поколения и построения информационного хранилища SIEM-системы нового поколения, в котором содержатся в едином внутреннем формате и подлежат обработке моделями анализа и принятия решения SIEM-системы следующие данные: записи журналов аудита разнородных источников событий безопасности информационно-телекоммуникационной системы (серверы, рабочие станции, антивирусные приложения, системы аутентификации, сетевые устройства и т.д.); шаблоны информационных образов, профилей поведения и аномальных действий пользователей; политики безопасности организации; обобщенные данные о состоянии отдельных элементов и всей системы в целом; результаты моделирования и прогнозирования поведения пользователей, нарушителей и состояния защищаемой системы. К числу дополнительных механизмов функционирования, предложенных для SIEM-системы нового поколения в дополнение к традиционно выделяемым (нормализации, классификации, фильтрации, корреляции, приоритезации), относятся

такие функциональные процессы, как моделирование, межуровневая корреляция событий, выработка предупреждений и принятие решений на реконфигурацию и визуализация событий безопасности.
5. Дополнительно к поставленным на 2011 год задачам проекта был проведен: анализ известных стандартов в области XML-ориентированного представления событий безопасности (таких, как Common Event Expression, Common Base Event, Distributed Audit Service и Common Information Model), анализ существующих решений по построению SIEM-систем, выработанных мировыми лидерами в этой области (OSSIM, AccelOps от Cisco, QRadar от Q1 Labs, Prelude, ArcSight, IBM Tivoli и Novel Sentinel), анализ XML-ориентированных языков представления и обработки событий безопасности (RDFS, OWL, SWRL, SPARQL, Event calculus и SPIN), анализ XML-ориентированных СУБД (Apache XIndice, BaseX, Sedna и другие) и систем хранения триплетов (AllegroGraph, BigOWLIM, PelletDb, Virtuoso и другие). Результаты проведенного анализа в этих предметных областях позволили предложить в качестве базовой архитектуры для построения информационного хранилища SIEM системы нового поколения «сервис-ориентированную» архитектуру (SOA). В качестве подхода к построению внутренней информационной структуры хранилища предложен онтологический подход, поддерживаемый языками RDFS и OWL. Для обработки запросов к информационному хранилищу предложены языки SPARQL, Event calculus и SPIN. В качестве инструментального средства построения информационного хранилища предложено применение системы хранения триплетов Virtuoso, эффективно сочетающей возможности обработки реляционных данных, XML-ориентированных данных и триплетов.

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, XML-ориентированного представления данных и др.

3.8. Сопоставление полученных результатов с мировым уровнем

Все результаты, полученные в процессе выполнения первого 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 19-й Европейской (Euromicro) международной конференции по параллельной, распределенной и сетевой обработке информации (PDP 2011). Айа-Напа, Кипр, 9-11 февраля 2011 г.; Тринадцатой конференции «РусКрипто'2011» по криптологии, стеганографии, цифровой подписи и системам защиты информации. Московская область, г.Солнечногорск, 30 марта – 2 апреля 2011 г.; XX Общероссийской научно-технической конференции "Методы и технические средства обеспечения безопасности информации" (МТСОБИ 2011), 27 июня - 1 июля 2011 года, Санкт-Петербург; VII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2011), 26-28 октября 2011 г.; IV Всероссийской научно-практической конференции с международным участием "Научное творчество XXI века", Красноярск, апрель 2011 г.; III Общероссийской научно-практической конференции с международным участием «Современные исследования социальных проблем». Красноярск, 2011 г.; 66-я научно-технической конференции, посвященной Дню радио, Санкт-Петербург, 19–29 апреля 2011 г.; Международной научно-практической конференции «Современные направления теоретических и прикладных исследований '2011», Одесса, 2011 г.; XI Международной научно-практической конференции «Интеллект и наука», Железноводск, 28-29 апреля 2010 г.; Международном конгрессе по информатике «Информационные системы и технологии - CSIST'2011», Республика Беларусь, Минск, 31 октября - 3 ноября 2011 г. и др.

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 оптимизации схем разграничения доступа и применения генетических алгоритмов для из решения;
(2) методы эволюционного моделирования сложных систем в части разработки новых классов генетических алгоритмов (полихромосомных, самоуправляемых и сложно структурированных), которые в первую очередь ориентированы на оптимизацию ролевых схем доступа, однако также могут быть использованы для структурной и параметрической оптимизации сложных объектов и систем в других областях;
(3) методы моделирования и анализа дискреционного, мандатного, ролевого и основанных на них прочих механизмов контроля и управления доступом в части обоснования критериев их оптимизации, учитывающих требования по конфиденциальности и доступности к информационным и сетевым ресурсам;
(4) методы интеллектуального анализа данных в части решения проблемы Role Mining Problem и других аналогичных NP-полных проблем;
(5) методы теории массового обслуживания, теории случайных процессов и теории графов в части формирования постановок задач в рамках многоуровневой концептуальной модели управления разграничением доступа в защищенных мультисервисных сетях;
(6) онтологический подход к XML-ориентированному внутреннему представлению знаний в SIEM системах нового поколения для критически важных инфраструктур;
(7) методы логического вывода, фильтрации, классификации и межуровневой корреляции на XML-ориентированных данных, применяемые в информационном хранилище SIEM системы нового поколения;
(8) подход к динамическому управлению разграничением доступа, ориентированный на совместную обработку событий безопасности, шаблонов, информационных профилей и политик безопасности с использование SIEM технологии;
(9) гибридный подход к построению информационного хранилища SIEM системы нового поколения,

реализующий принципы SOA и рационально сочетающий возможности реляционных СУБД, XML-ориентированных СУБД и систем хранения триплетов.

3.10.1.1. Количество научных работ, опубликованных в ходе выполнения проекта
32

3.10.1.2. Из них включенных в перечень ВАК
8

3.10.1.3. Из них включенных в системы цитирования (Web of science, Scopus, Web of Knowledge, Astrophysics, PubMed, Mathematics, Chemical Abstracts, Springer, Agris, GeoRef)
12

3.10.2. Количество научных работ, подготовленных в ходе выполнения проекта и принятых к печати в 2011 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

3.13. Финансовые средства, полученные от РФФИ
310000 руб.

3.14. Вычислительная техника и научное оборудование, приобретенные на средства Фонда

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

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. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. 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.
32. 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.
33. 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.
34. 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.

3.17. Приоритетное направление развития науки, технологий и техники РФ, в котором, по мнению

исполнителей, могут быть использованы результаты данного проекта
безопасность и противодействие терроризму

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

3.19. Основное направление технологической модернизации экономики России, в котором, по мнению исполнителей, могут быть использованы результаты завершенного проекта
Стратегические информационные технологии, включая вопросы создания суперкомпьютеров и разработки программного обеспечения

Подпись руководителя проекта