Форма 501. **КРАТКИЙ НАУЧНЫЙ ОТЧЕТ**

1.1. Номер проекта

14-07-00697

1.2. Руководитель проекта

Саенко Игорь Борисович

1.3. Название Проекта

Модели и методы разграничения доступа к ресурсам единого информационно-коммуникационного пространства разнородных автоматизированных систем, основанные на технологии искусственного интеллекта

1.4. Код и название Конкурса

А - Конкурс инициативных научно-исследовательских проектов 2014 года

1.5. Год представления Отчета

2014

1.6. Вид Отчета (*цифра 2- этап 2014 г.)*

2

1.7. Аннотация

Проведен анализ состояния исследований в области построения систем контроля и разграничения доступа к информационным и телекоммуникационным ресурсам и анализ угроз информационной безопасности ЕИКП разнородных автоматизированных систем. В качестве модели угроз несанкционированного доступа в ЕИКП разработана модель виртуального разбиения локальной компьютерной сети, позволяющая находить минимальное разделение локальной сети на виртуальные подсети, обеспечивающее заданную матрицу логической связности узлов сети. Сформирована общая формальная постановка задачи исследования, определяющая исходные данные, критерии и допущения. Определены требования по безопасности, достоверности и производительности единой системы разграничения доступа в ЕИКП. Определены два подхода к разработке единой системы разграничения доступа в ЕИКП, связанные с (1) использованием онтологий и (2) постановкой и решением оптимизационных задач для схем разграничения доступа. Для решения оптимизационных задач предложены усовершенствованные генетические алгоритмы, отличающиеся рядом инноваций. Предложена обобщенная методика поддержки принятия решений по разграничению доступа к ресурсам ЕИКП. Сформулированы новые постановки задач по адаптивному изменению политик и схем разграничения доступа к разнородным ресурсам ЕИКП. Проведена экспериментальная оценка полученных результатов.

1.8. 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

*Форма 503.*РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1. Номер Проекта

14-07-00697

3.2. Название Проекта

Модели и методы разграничения доступа к ресурсам единого информационно-коммуникационного пространства разнородных автоматизированных систем, основанные на технологии искусственного интеллекта

3.3. Коды классификатора, соответствующие содержанию фактически проделанной работы

07-241, 07-235, 07-956, 01-224

3.4. Объявленные ранее цели Проекта на 2014 год

Основными целями проекта на 2014 год являлись:

(1) анализ состояния исследований в области построения систем контроля и разграничения доступа к информационным и телекоммуникационным ресурсам ЕИКП разнородных автоматизированных систем;

(2) анализ угроз информационной безопасности ЕИКП разнородных автоматизированных систем и выработка предложений по моделированию угроз несанкционированного доступа к информационным и телекоммуникационным ресурсам ЕИКП;

(3) общая формальная постановка задачи исследования и обоснование основных требований и критериев по безопасности, производительности, достоверности и другим квалификационным свойствам;

(4) исследование вопросов реализации моделей, методов и алгоритмов основанного на знаниях представления, верификации и оптимизации политик и схем разграничения доступа к информационным и телекоммуникационным ресурсам ЕИКП разнородных автоматизированных систем;

(5) разработка обобщенной методики поддержки принятия решений по разграничению доступа к ресурсам ЕИКП на основе логического вывода на знаниях и визуализации данных о политиках, схемах и событиях доступа;

(6) исследование вопросов реализации моделей и методов адаптации политик и схем разграничения доступа к изменениям условий и режимов функционирования ЕИКП;

(7) экспериментальная оценка полученных результатов.

3.5. Степень достижения поставленных в Проекте целей

Все задачи, запланированные в проекте на первый год, выполнены полностью. Дополнительно выработаны предложения по интеллектуальному иерархическому управлению политиками и схемами разграничения доступа в защищенных мультисервисных сетях.

3.6. Полученные в 2014 году важнейшие результаты

1. В ходе анализа состояния исследований в области построения систем контроля и разграничения доступа к информационным и телекоммуникационным ресурсам ЕИКП разнородных автоматизированных систем был рассмотрен и изучен основные отечественные и зарубежные работы по данной тематике. Анализ позволил сформулировать следующие выводы: (1) решения по построению систем контроля и разграничения доступа

к информационным и телекоммуникационным ресурсам ЕИКП достаточно чувствительны к решениям, связанным непосредственно с построением самого ЕИКП; (2) теория построения ЕИКП как таковая в настоящее время находится в состоянии своего зарождения, в результате чего возникает необходимость в обосновании возможных вариантов построения ЕИКП; (3) вопросам создания систем контроля и разграничения доступа к информационным и телекоммуникационным ресурсам ЕИКП в литературе по построению ЕИКП и по разграничению доступа в информационно-коммуникационных системах уделяется чрезвычайно мало внимания, ошибочно предполагая, что для построения такого рода систем в интегрированном ЕИКП вполне достаточно использовать решения, разработанные для традиционных информационных и телекоммуникационных систем. Большинство отечественных работ, посвященных тематике построения ЕИКП, рассматривают только функциональные аспекты, определяя, каковы преимущества имеет ЕИКП в функциональном плане и каким образом можно эти преимущества реализовать и использовать для повышения эффективности функционирования системы управления в целом. В то же время в зарубежных работах при построении ЕИКП предлагается ориентироваться на новую парадигму «пространство данных» (data space), которая является дальнейшим развитием парадигмы «хранилище данных» (data warehouse), а последняя в свою очередь – развитием парадигмы «база данных» (data base). Хранилище данных в структурном плане отличается от базы данных тем, что интегрирует многомерные аналитические базы данных совместно с транзакционными реляционными базами. Пространство данных в структурном плане отличается от хранилища тем, что интегрирует данные, содержащиеся в хранилищах, совместно с электронными информационными ресурсами, хранящимися отдельно от хранилищ и баз данных в произвольных узлах инфо-коммуникационной сети. Для интеграции ресурсов в ЕИКП применяются различные методы (консолидации, федерализации, распространения) и технологии (ETL, EII, EAI, CDI).

2. В ходе анализа угроз информационной безопасности ЕИКП разнородных автоматизированных систем было выявлено, что все множество угроз разделяется на две группы: внутренние и внешние. При этом характер внешних угроз и специфика защиты от них не сильно отличаются от того, как проявляются эти вопросы в традиционных инфо-коммуникационных системах. Поэтому для защиты от внешних угроз являются вполне применимыми методы и средства, используемые для защиты, например, компьютерных сетей от программных атак. Однако особое внимание в ЕИКП следует обращать на внутренние угрозы информационной безопасности, исходящие от лояльных внутренних пользователей, и защиту от этих угроз. Связано это с тем, что при интеграции систем разграничения доступа, имеющихся в различных автоматизированных системах, в единую систему разграничения доступа ЕИКП возможно возникновение избыточных разрешающих либо запрещающих правил политик разграничения доступа. В качестве модели угроз несанкционированного доступа в ЕИКП была разработана модель виртуального разбиения локальной компьютерной сети, позволяющая находить такое минимальное разделение локальной сети на виртуальные подсети, при котором удовлетворяется заданная матрица логической связности узлов сети между собой. Показано, что постановка задачи поиска минимального количества виртуальных подсетей имеет вид A=X*XT, где A – требуемая матрица логической связности, X – искомая матрица принадлежности узлов к виртуальных подсетям, XT – транспонированная матрица X. Данная постановка задачи является одной из разновидностей задач булевой матричной факторизации и относится к классу NP-полных.

3. При формировании общей формальной постановки задачи исследования был

определен состав исходных данных и критерии формирования единой системы разграничения доступа в ЕИКП. Исходные данные составляют: (1) множества пользователей в каждой автоматизированной системе, подлежащей интеграции в ЕИКП; (2) множества ресурсов в каждой автоматизированной системе, доступ к которым разграничивается; (3) частные схемы разграничения доступа, применяемые в каждой автоматизированной системе, определяемые полномочия по доступу пользователей автоматизированной системы к ресурсам автоматизированной системы. Частные схемы разграничения доступа являются разнородными в том смысле, что, с одной стороны, они могут базироваться на различных моделях доступа (в качестве основных рассматриваются дискреционная, мандатная и ролевая модели доступа), а с другой – охватывать различные ресурсы и разных пользователей. Критерии задачи определяют степень соблюдения единой системой разграничения доступа ЕИКП правил частных политик разграничения доступа, изначально установленных в каждой из интегрируемых автоматизированных систем. Дополнительными условиями постановки задачи (допущениями) являются теоретико-множественные выражения, определяющие, что общее множество пользователей единой системы разграничения доступа ЕИКП формируется путем объединения частных множеств пользователей отдельных автоматизированных систем, а также общее множество ресурсов единой системы разграничения доступа ЕИКП формируется путем объединения частных множеств ресурсов. При этом допускается, что частные множества пользователей и, соответственно, ресурсов могут пересекаться и иметь общие элементы. К числу основных требований по безопасности относится требование полного совпадения частных схем разграничения доступа и так называемой «проекции» единой схемы разграничения доступа ЕИКП по соответствующей автоматизированной системе. Данная «проекция» является новым понятием, введенным в ходе исследований по настоящему проекту. «Проекция» единой схемы разграничения доступа по соответствующей автоматизированной системе получается из единой схемы путем удаления из нее всех пользователей и ресурсов, которые отсутствуют в автоматизированной системе, а также всех связанных с ними дополнительных элементов (ролей, связей, полномочий и т.д.). Требования по достоверности и производительности единой системы разграничения доступа в ЕИКП сводятся к тому, что изменение единой схемы разграничения доступа в случае изменения множеств пользователей, ресурсов и/или полномочий должно производиться и завершаться до наступления новых изменений в этих множествах.

4. При исследовании вопросов реализации моделей, методов и алгоритмов основанного на знаниях представления, верификации и оптимизации политик и схем разграничения доступа к ресурсам ЕИКП были выявлены два подхода к построению таких моделей, методов и алгоритмов. Первый подход основан на использовании онтологий. Второй подход заключается в формировании оптимизационной постановки задачи и применении для ее решения методов биоинспирированной оптимизации (в частности, усовершенствованных генетических алгоритмов). Первый подход рассматривается как обладающий большей степенью универсальности. Однако он предполагает, что изначально в каждой из интегрируемых автоматизированных систем разграничение доступа осуществляется с использованием частных онтологий. Такое предположением не всегда справедливо на практике. Второй подход является менее универсальным и требует для каждого конкретного случая интеграции автоматизированных систем в ЕИКП формировать целевые функции и критерии оптимизации. Однако при данном подходе в проекте разработан ряд усовершенствований, позволяющих успешно применять для решения данных

задач метод генетической оптимизации. К числу таких усовершенствований, разработанных и предложенных в ходе текущих исследований, относятся: (1) применение мульти-хромосомного кодирования возможных решений; (2) использование сложных объектов (в частности, столбцов искомых булевых матриц) в качестве генов хромосом; (3) введение в рассмотрение дополнительных хромосом (управляющих), предотвращающих появление недействительных решений и ускоряющих, тем самым, работу алгоритма; (4) двумерное скрещивание родительских хромосом, кодирующих переменные, выраженные в матричной форме; (5) генерация специального вида особей для начальной популяции (в частности, для задачи поиска виртуальных подсетей – это генерация и ввод в состав начальной популяции тривиальных решений задачи, в которых в каждой виртуальной подсети находится всего два компьютера).

5. Предложена обобщенная методика поддержки принятия решений по разграничению доступа к ресурсам ЕИКП на основе логического вывода на знаниях и визуализации данных о политиках, схемах и событиях доступа. Методика содержит следующие этапы: (1) предварительный; (2) основной; (3) заключительный. На предварительном этапе формируется единая база знаний о разграничении доступа в онтологическом формате (формате RDF) путем интеграции частных онтологий разграничения доступа отдельных автоматизированных систем. На основном этапе для определения возможности доступа пользователя к конкретному ресурсу запускается механизм логического вывода, результат которого, с одной стороны, показывает, доступен ресурс пользователю или нет, а с другой ¬– каковы полномочия пользователя в случае доступности ресурса. На заключительном этапе формируется визуальная модель представления данных, отражающая доступность ресурса и характер предоставленных пользователю полномочий по отношению как заданного ресурса, так и других, соседних, ресурсов.

6. В ходе исследования вопросов реализации моделей и методов адаптации политик и схем разграничения доступа к изменениям условий и режимов функционирования ЕИКП были сформулированы постановки задачи адаптивного изменения политик и схем разграничения доступа к разнородным ресурсам. Показано, что в случае схем разграничения доступа к телекоммуникационным ресурсам (на примере виртуальных подсетей) постановка задачи сводится к поиску минимума для DX при заданной DA и матрице X, которые связаны друг с другом уравнением вида X*XT+DA=(X+DX)(X+DX)T. Данное матричное уравнение чрезвычайно затруднительно решать традиционными способами, особенно для большой размерности X. Предлагается использовать для ее решения эвристические методы, в частности, генетический подход, по аналогии с решением задачи A=X*XT. Для адаптивного изменения политик и схем разграничения доступа к информационным ресурсам также сформулирована постановка задачи, заключающаяся в поиске минимума для (DX+DY) при заданных DA, X и Y, связанных уравнением X*Y+DA= (X+DX)(Y+DY). Данное матричное уравнение также предлагается решать эвристически на основе генетических алгоритмов.

7. Для экспериментальной оценки полученных результатов был разработан инструментальный стенд, позволяющий, с одной стороны, решать оптимизационные задачи для проектирования схем разграничения доступа к неоднородным информационным и телекоммуникационным ресурсам, а с другой – осуществлять визуальный анализ хода поиска оптимального решения. На данном стенде были проведены серии экспериментов, позволившие найти зависимости оптимальных параметров генетических алгоритмов от

размерностей решаемых задач. Программный компонент инструментального стенда «Решение задачи оценки и прогнозирования состояния распределенных информационных систем» был зарегистрирован в Реестре программ для ЭВМ Федеральной службы по интеллектуальной собственности, о чем получено свидетельство о государственной регистрации программы для ЭВМ №2014660856.

8. Дополнительно был разработан метод интеллектуального иерархического управления политиками и схемами разграничения доступа в защищенных мультисервисных сетях. Данный метод основан на нечеткой оценке рисков нарушения политик и схем разграничения доступа в защищенных мультисервисных сетях на различных уровнях иерархической модели управления сетями. Разработанная программа «Поддержка принятия решений при оценке рисков угроз информационной безопасности мультисервисных сетей связи» была зарегистрирована в Реестре программ для ЭВМ Федеральной службы по интеллектуальной собственности, о чем получено свидетельство о государственной регистрации программы для ЭВМ №2014660775. С ее помощью была исследована математическая модель оценки рисков несанкционированного доступа в защищенных мультисервисных сетях.

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 от несанкционированного доступа, 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 изложили основные результаты в 5 статьях, опубликованных в журналах, индексируемых в международных базах цитирования WoS и Scopus, в 5 статьях, опубликованных в журналах, входящих в список ВАК, а также в прочих журналах и трудах конференций, а также апробировали результаты на множестве различных российских и международных конференций, в частности, на 8-м международном симпозиуме по интеллектуальным распределенным вычислениям (IDC-2014), Мадрид, Испания, сентябрь, 2014; 6-м международном симпозиуме по безопасности и защите киберпространства (CSS 2014), Париж, Франция, август, 2014; Шестнадцатой Международной конференции «РусКрипто -2014», Московская обл., март, 2014; IV международной научно-практической конференции «ИнтеллектТранс-2014», Санкт-Петербург, апрель, 2014; Международном форуме по практической безопасности Positive Hack Days, Москва, май, 2014; Международной научно-практической конференции «Теоретические и прикладные проблемы информационной безопасности», Минск, Республика Беларусь, июнь, 2014; Четырнадцатой национальной конференции по искусственному интеллекту с международным участием КИИ-2014, Казань, сентябрь, 2014; Конгрессе по интеллектуальным системам и информационным технологиям «IS&IT’14», Дивноморское, Краснодарский край, сентябрь, 2014; 23-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, июнь-июль, 2014; Семинаре Международного союза электросвязи «Переход развивающихся стран с существующих сетей на сети нового поколения (NGN): технические, экономические, законодательные и

политические аспекты», Санкт- Петербург, июнь 2014; 6-й Российской мультиконференции по проблемам управления (МКПУ-2014) - конференции «Информационные технологии в управлении» (ИТУ-2014), Санкт-Петербург, октябрь, 2014; XIV Санкт-Петербургской международной конференции «Региональная информатика (РИ-2014), октябрь, 2014.

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 формализованных постановок задач синтеза схем разграничения доступа к разнородным информационным и телекоммуникационным ресурсам 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 задач адаптивного изменения схем разграничения доступа к информационным и телекоммуникационным ресурсам;

(4) методы интеллектуального анализа данных в части разработки усовершенствованного алгоритма для решения проблемы нахождения минимального множества виртуальных подсетей;

(5) метод интеллектуального иерархического управления разграничением доступа в защищенных мультисервисных сетях;

(6) онтологический подход к управлению разграничением доступа к разнородным ресурсам ЕИКП;

(7) 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 по Проекту, опубликованных в 2014 году

35

3.10.1.2 Из них в изданиях, включенных в перечень ВАК

5

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

4

3.10.2. Количество научных работ, подготовленных в ходе выполнения Проекта и принятых к печати в 2014 году (цифрами)

2

3.11. Участие в 2014 году в научных мероприятиях по тематике Проекта

1. 8-й международный симпозиум по интеллектуальным распределенным вычислениям (IDC-2014), Мадрид, Испания, сентябрь, 2014;

2. 6-й международный симпозиум по безопасности и защите киберпространства (CSS 2014), Париж, Франция, август, 2014;

3. Шестнадцатая Международная конференция «РусКрипто-2014», Московская обл., март, 2014;

4. IV международная научно-практическая конференция «ИнтеллектТранс-2014», Санкт-Петербург, апрель, 2014;

5. Международный форум по практической безопасности Positive Hack Days, Москва, май, 2014;

6. Международная научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности», Минск, Республика Беларусь, июнь, 2014;

7. Четырнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2014, Казань, сентябрь, 2014;

8. Конгресс по интеллектуальным системам и информационным технологиям «IS&IT-14», Дивноморское, Краснодарский край, сентябрь, 2014;

9. 23-я научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, июнь-июль, 2014;
10. Семинар Международного союза электросвязи «Переход развивающихся стран с существующих сетей на сети нового поколения (NGN): технические, экономические, законодательные и политические аспекты», Санкт-Петербург, июнь 2014;

11. 6-я Российская мультиконференция по проблемам управления (МКПУ-2014) - конференция «Информационные технологии в управлении» (ИТУ-2014), Санкт-Петербург, октябрь, 2014;

12. XIV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2014), октябрь, 2014.

3.12. Участие в 2014 году в экспедициях по тематике Проекта, которые проводились при финансовой поддержке Фонда

нет

3.13. Финансовые средства, полученные в 2014 году от РФФИ (в руб.)

500000,00

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

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

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

http://www.comsec.spb.ru/en/papers

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

3.15. Библиографический список всех публикаций по Проекту, опубликованных в 2014 году, в порядке значимости: монографии, статьи в научных изданиях, тезисы докладов и материалы съездов, конференций и т.д.

1. Igor Kotenko, Igor Saenko. A Genetic Approach for Virtual Computer Network Design // Intelligent Distributed Computing VIII. Studies in Computational

Intelligence. Springer-Verlag, Vol.570. Proceedings of 8th International Symposium on Intelligent Distributed Computing - IDC'2014. September 3-5, 2014, Madrid, Spain. Springer-Verlag. P.95-105. (WoS, Scopus).

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

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

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

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

6. Igor Kotenko, Igor Saenko. Improved genetic algorithms for solving the optimization tasks in access scheme design for computer networks // International Journal of Bio-Inspired Computation, 2014 (Scopus, WoS).

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

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

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

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

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

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

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

14. Котенко И.В., Саенко И.Б. Предложения по реализации логического вывода для управления кибербезопасностью в АСУ железнодорожного транспорта // Естественные и математические науки в современном мире. 2014. № 14. Новосибирск: Изд. «СибАК», С. 46-50.

15. Котенко И.В., Саенко И.Б. Методика верификации политик безопасности в многоуровневой интеллектуальной системе обеспечения комплексной безопасности железнодорожного транспорта // Технические науки - от теории к практике. Новосибирск: Изд. «СибАК», 2014. № 30. С. 18-22.

16. Десницкий В.А., Чечулин А.А. Обобщенная модель нарушителя и верификации информационно-телекоммуникационных систем со встроенными устройствами // Технические науки - от теории к практике. Новосибирск: Изд. «СибАК», 2014. №38, С.7-21.

17. Саенко И.Б., Куваев В.О. О применении методов искусственного интеллекта для разграничения доступа к ресурсам единого информационного пространства разнородных автоматизированных систем // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.631-637. ISBN 978-5-91995-042-4.

18. Куваев В.О., Саенко И.Б. Подход к решению задачи разграничения доступа в разнородном информационном пространстве // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.33-34.

19. Котенко И.В., Саенко И.Б. О задачах обеспечения кибербезопасности в инфраструктурах «электронного города» на основе методов искусственного интеллекта // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.618-622. ISBN 978-5-91995-042-4.

20. Десницкий В.А. Верификация сетевых информационных потоков систем со встроенными устройствами на основе экспертных знаний // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.596-600. ISBN 978-5-91995-042-4.

21. Агеев С.А., Саенко И.Б. Управление рисками информационной безопасности защищенной мультисервисной сети специального назначения на основе интеллектуальных мультиагентов // Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С.556-562. ISBN 978-5-91995-042-4.

22. Котенко И.В., Новикова Е.С. Модели и методики визуального анализа данных для решения задач компьютерной безопасности // Шестнадцатая Международная конференция «РусКрипто-2014». Московская область, г.Солнечногорск, 25-28 марта 2014 г. http://www.ruscrypto.ru/

23. Котенко И.В., Саенко И.Б. О построении многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем железнодорожного транспорта // Интеллектуальные системы на транспорте: Материалы IV международной научно-практической конференции «ИнтеллектТранс-2014». – СПб.: ПГУПС, 2014. С.196-203.

24. Котенко И.В., Новикова Е.С. Визуальная аналитика на страже

информационной безопасности // Международный форум по практической безопасности Positive Hack Days. Москва. 21-22 мая 2014 г. http://www.phdays.ru

25. Саенко И.Б., Котенко И.В. Основы построения перспективных систем мониторинга и управления безопасностью для защиты критически важных объектов информатизации // Международная научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности». 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.

26. Нестерук Ф. Г. Специфика двухуровневой организации адаптивных систем защиты информации // Международная научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности». 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.С. 227-231.

27. Котенко И.В., Саенко И.Б. Об архитектуре многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.97-98.

28. Агеев С.А., Саенко И.Б. Интеллектуальные методы управления рисками информационной безопасности мультисервисных сетей связи // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.59-60.

29. Котенко И.В., Саенко И.Б. Система логического вывода и верификации политик безопасности в автоматизированных системах железнодорожного транспорта // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT-14». Научное издание в 4-х томах. М.: Физматлит, 2014. Т.2. С.271-276. 978-5-9221-1572-8.

30. Саенко И.Б., Котенко И.В. Генетический подход к проектированию виртуальных компьютерных сетей на основе генетических алгоритмов // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT-14». Научное издание в 4-х томах. М.: Физматлит, 2014. Т.1. С.35-40. ISBN 978-5-9221-1572-8.

31. Котенко И.В., Саенко И.Б. Интеллектуальная система мониторинга и управления инцидентами кибербезопасности // Четырнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2014 (24–27 сентября 2014 года, г. Казань, Россия): Труды конференции. Т.3. Казань: Изд-во РИЦ «Школа», 2014. С.219-227.

32. Дойникова Е.В., Котенко И.В. Оценивание защищенности в автоматизированных системах управления РЖД // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.132-133.

33. Дойникова Е.В. Поддержка принятия решений по выбору защитных мер в информационных системах на основе комплекса показателей защищенности // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.132.

34. Агеев С.А., Саенко И.Б. Оценка и управление рисками информационной безопасности в защищенных мультисервисных сетях на основе методов

искусственного интеллекта // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.116-117.

35. Котенко И.В., Саенко И.Б. Поддержка принятия решений по безопасности информации в АСУ железнодорожного транспорта на основе онтологического моделирования данных // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.144.

36. Котенко И.В., Саенко И.Б. Модели и методы визуального анализа больших объемов данных и событий безопасности автоматизированных систем железнодорожного транспорта // XIV Санкт-Петербургская Международная Конференция «Региональная информатика-2014» (РИ-2014). Материалы конференции. СПб., 2014. С.143.

37. Котенко И.В., Саенко И.В., Чечулин А.А. Проактивное управление информацией и событиями безопасности в сетях NGN // Материалы семинара Международного союза электросвязи «Переход развивающихся стран с существующих сетей на сети нового поколения (NGN): технические, экономические, законодательные и политические аспекты», Санкт- Петербург, СПб ГУТ им Бонч-Бруевича. 23–25 июня 2014 года.

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

Информационно-телекоммуникационные системы

3.17. Критическая технология РФ, которой, по мнению исполнителей, соответствуют 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.