*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**
2015

**1.6. Вид Отчета** (*этап 2015 г.)*
2

**1.7. Содержательная научная часть отчета, публикуемая на сайте Фонда**
Выполнена разработка и проведено тестирование эволюционных алгоритмов, моделей и методов для новых предметных областей разграничения доступа к информационным и телекоммуникационным ресурсам в ЕИКП, которыми являются: (1) виртуальные локальные вычислительные сети и (2) виртуальные частные сети и (3) ролевые схемы доступа к информации в критических инфраструктурах. Произведено обоснование и выполнена разработка общей архитектуры единой системы разграничения доступа к ресурсам ЕИКП, а также ее компонентов, распределенных по трем уровням общей архитектуры: (1) локальному уровню, (2) уровню интеграции данных и (3) аналитическому уровню. Проведено исследование и выполнена разработка моделей и методов использования онтологий, лежащих в основе построения центрального хранилища единой системы разграничения доступа к разнородным ресурсам ЕИКП. Проведено исследование и выполнена разработка моделей и методов адаптивного изменения политик и схем разграничения доступа к разнородным информационным и телекоммуникационным ресурсам ЕИКП, основанных на решении задач булевой матричной факторизации. Проведено исследование и выполнена разработка моделей и методов оценки эффективности функционирования единой системы разграничения доступа к разнородным информационным и телекоммуникационным ресурсам в ЕИКП. Осуществлена 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 2015 год**
Полученные на первом этапе проекта результаты показали перспективность и высокую эффективность следующих моделей и методов, разрабатываемых для построения систем разграничения доступа к разнородным информационным и телекоммуникационным ресурсам ЕИКП: (1) усовершенствованных генетических алгоритмов оптимизации и реализованных на их основе методов интеграции разнородных схем разграничения доступа, включая схемы ролевого доступа и схемы разграничения виртуальных подсетей; (2) моделей и методов использования онтологий для управления разграничением доступа к разнородным ресурсам ЕИКП; (3) постановок задач адаптивного изменения политик и схем разграничения доступа к разнородным информационным и телекоммуникационным ресурсам ЕИКП. Поэтому основные цели очередного годичного этапа определяются как дальнейшее совершенствование, реализация и экспериментальная оценка элементов научно-методологического обеспечения систем разграничения доступа в указанных выше научных направлениях.

**3.5. Полученные в 2015 году важнейшие результаты**
1. Выполнены разработка и тестирование эволюционных алгоритмов, моделей и методов для новых предметных областей разграничения доступа к информационным и телекоммуникационным ресурсам в ЕИКП. При этом рассматривались следующие сценарии: (1) виртуальные локальные вычислительные сети (VLAN, virtual local area networks); (2) виртуальные частные сети (VPN, virtual private networks) в защищенном информационном пространстве; (3) ролевые схемы доступа (RBAC, Role-based access control) к базам данных критических инфраструктур. Для предметных областей VLAN и RBAC были разработаны унифицированные эвристические алгоритмы на основе метода генетической оптимизации. По сути, эти алгоритмы отличались друг от друга видом функции пригодности (fitness function), зависящий от вида целевой функции в постановке задачи, а также структурой хромосом, которыми обладали особи в популяции алгоритма. Для области VLAN особи имели одну хромосому, генами которой являлись столбцы матрицы требуемой логической связности компьютеров в сети. Для RBAC особи имели по три хромосомы, из которых две отражали связи между пользователями, ролями и ресурсами, а третья являлась служебной, предназначенной для обеспечения логической целостности хромосом. Кроме того, для скрещивания в случае RBAC применялся мульти-хромосомный подход, а в случае VLAN – двумерное скрещивание, повышающее результативность и оперативность работы алгоритма. В остальном работа алгоритмов была одинаковой. Для предметной области VPN был разработан генетический алгоритм, в котором функция пригодности рассчитывалась как взвешенная сумма частных нормированных показателей эффективности функционирования сети VPN. Частными показателями эффективности

являлись показатели пропускной способности, устойчивости и стоимости эксплуатации сети. Расчет частных показателей эффективности производится на основании аналитических зависимостей, полученных в результате применения теории массового обслуживания и теории графов. На основании теории массового обслуживания были выведены выражения для расчета показателя пропускной способности составного VPN-канала с N транзитами. На основании теории графов была предложен высоко оперативный матричный метод расчета минимального количества транзитов в информационном направлении. Исходными данными являлись: параметры входных потоков, интенсивности обслуживания крипто-маршрутизаторов, пропускные способности IP-каналов, требования по пропускной способности, устойчивости и стоимости. Генами хромосом в генетическом алгоритме являются элементы, располагающиеся выше главной диагонали матрицы логической связности узлов сети VPN. Тестирование разработанных алгоритмов проводилось на разработанном программно-инструментальном стенде, позволяющем автоматически генерировать требуемые схемы доступа для различных размерностей задач, управлять параметрами алгоритмов, а также проводить оценку и визуальный анализ хода решения задач с помощью разработанных алгоритмов.

2. Произведена разработка общей архитектуры и архитектуры отдельных компонентов единой системы разграничения доступа (ЕСРД) к разнородным информационным и телекоммуникационным ресурсам в ЕИКП. При этом учитывалось, что ЕИКП является не только системой, обеспечивающая требуемую защищенность информационных и сетевых ресурсов, но и средством интеграции разнородных ресурсов. Разработанная общая архитектура ЕСРД включает три уровня своего построения: (1) локальный уровень; (2) уровень интеграции данных; (3) аналитический уровень. Локальный уровень ЕСРД образуют локальные системы разграничения доступа (ЛСРД) отдельных автоматизированных систем, ресурсы которых интегрируются в ЕИКП. Формальное задание ЛСРД обеспечивается с помощью локальных схем и политик разграничения доступа отображением декартова произведения множества пользователей и множества ресурсов локальной автоматизированной системы на множество полномочий. Вид этого отображения зависит от используемых в ЛСРД моделей управления доступом. На уровне интеграции данных ЕСРД осуществляется формирование единых схем и политик разграничения доступа. Формально задача их построения сводится к тому, чтобы сформировать отображение декартова произведения множества пользователей и множества ресурсов всего ЕИКП на множество полномочий. При этом должно выполняться условие, заключающееся в том, что проекция ЕСРД по локальным множествам пользователей, ресурсов и полномочий должна приводить к соответствующей ЛСРД. Обосновано основное противоречие построения ЕСРД, которое обусловлено тремя факторами. Во-первых, один и тот же пользователь может являться пользователем различных локальных систем. С другой стороны, один и тот же контролируемый ресурс может являться общим для различных локальных систем. Наконец, полномочия доступа между этим пользователем и ресурсом в различных локальных системах могут быть также различными. В силу существования данного противоречия решение задачи построения ЕСРД не является тривиальным. В результате основным компонентом ЕСРД на уровне интеграции данных является центральное хранилище схем разграничения и политик доступа, которое должно обеспечивать возможность хранения данных как в SQL-формате, так и в форматах, обеспечивающих применение методов искусственного интеллекта, а именно XML- и RDF-форматах. Обосновано, что в основу построения центрального хранилища ЕСРД целесообразно положить

онтологический подход. На аналитическом уровне основными компонентами являются ЕСРД компонента анализа и компонент принятия решений. Необходимость в данных компонентах обусловлена Компонент анализа решает задачу обеспечения целостности и непротиворечивости ЕСРД. Компонент принятия решений решает задачу формирования адекватных изменений схем и политик ЕСРД при появлении изменений в ЛСРД, причем выполняемых с минимальными затратами. Последнее условие необходимо для обеспечения разрешимости основного противоречия построения ЕСРД.

3. Произведены исследование и разработка моделей и методов использования онтологий для управления разграничением доступа к разнородным ресурсам ЕИКП. При этом выявлено, что онтология как средство поддержки логического вывода может быть использована для многих современных моделей доступа, таких как RBAC, ABAC (Attributes Based Access Control) и других. Показано, что в качестве базисной онтологии ЕСРД может выступать онтология предметной области, политику доступа которой можно рассматривать как совокупность правил оперирования объектами, представленными в данной онтологии. При этом данные правила не составляют суть самих объектов или процессов с их участием, а являются лишь отображением корректных действий субъектов доступа ЕИКП по отношению к объектам доступа. Предложена формальная модель управления доступом в виде онтологической модели, которая позволяет полностью описать семантику базовых понятий управления доступа к сервисам ЕИКП. Семантическая модель инвариантна относительно форматов представления описаний прав доступа к сервисам, что позволяет ее использовать как конечными пользователями, так и автоматизированными анализаторами. В состав онтологической модели ЕСРД включена собственная подсистема доступа, содержащая формальные записи политик доступа к сервисам, семантика которых определена онтологической моделью. Подсистема доступа обеспечивает управление доступом к сервисам на основе RBAC и возможность делегирования полномочий управления доступа к объектам доступа.

4. Выполнены исследование и разработка моделей и методов решения задач адаптивного изменения политик и схем разграничения доступа к разнородным информационным и телекоммуникационным ресурсам ЕИКП. Выявлены факторы, обусловливающие необходимость своевременной и адекватной корректировки (изменения, реконфигурации) политик и схем разграничения доступа к ресурсам ЕИП. В качестве критерия решения задачи предложено условие минимизации трудозатрат администратора безопасности на выполнение работ по переходу к новой схеме разграничения доступа с сохранением уровней конфиденциальности и доступности информации, обеспечиваемых предыдущей схемой доступа. Сформированы формальные постановки задач изменения схемы доступа к ресурсам ЕИП для сценариев RBAC и VLAN, которые основываются на решении задачи булевой матричной факторизации. Показано, что поставленные задачи являются NP-полными. Для их решения разработаны генетические алгоритмы, в которых в качестве генов хромосом используются столбцы искомых булевых матриц, а скрещивание хромосом родительских особей выполняется в двумерном режиме. Для реализации предложенных алгоритмов разработаны программные прототипы.

5. Исследованы и разработаны модели и методы оценки эффективности функционирования ЕСРД к разнородным информационным и телекоммуникационным ресурсам ЕИКП. Обоснована специфика моделей и методов, обусловленная тем, что ЕСРД, с одной стороны, должна обеспечивать сохранение значений функциональных показателей

разграничения доступа, имеющихся у отдельных субъектов доступа (пользователей либо автоматизированных систем) до их вхождения в информационное пространство, а с другой – обеспечивать поддержание значений новых функциональных показателей, характеризующих эффективность доступа одних субъектов доступа к ресурсам других субъектов доступа. При этом ЕСРД должна обеспечивать комплексирование различных моделей разграничения доступа (дискреционной, мандатной, ролевой и т.д.), присущих отдельным субъектам доступа, и возможность сохранения исходной модели разграничения доступа при выполнении операции проекции ЕСРД на отдельный субъект доступа. Разработанные модели и методы оценки эффективности функционирования ЕСРД основаны на принципах имитационного моделирования попыток несанкционированного доступа, а также автоматической генерации объектов и полномочий доступа. В качестве показателей эффективности функционирования системы разграничения доступа в них используются значения количества ошибок первого и второго рода, совершаемых за заданный период модельного времени, а также рассчитываемая на их основе вероятность реализации несанкционированного доступа. В ходе автоматической генерации объектов и полномочий доступа учитываются заданные плотности распределения значений последних, а также общие количественные ограничения. Кроме того, используются различные алгоритмы поиска рациональных вариантов построения системы разграничения доступа. В частности, одним из разновидностей реализованных алгоритмов являются генетические алгоритмы оптимизации схем разграничения доступа к информационным и коммуникационным ресурсам, которые позволяют решать NP-полные задачи оптимизации, встречающиеся при формировании схем RBAC, VLAN и VPN. Разработан подход к использованию предложенных моделей и методов оценки эффективности функционирования ЕСРД, позволяющий не только проводить оценку ЕСРД по предложенным показателям, но и обнаруживать «узкие места» формируемой системы разграничения доступа в интересах повышения обоснованности принимаемых решений по обеспечению защищенности ЕИКП от несанкционированного доступа.

6. Предложена классификация вариантов построения ЕИКП в целях интеграции разнородных автоматизированных систем, обоснованы показатели качества функционирования ЕИКП и сделана сравнительная оценка различных вариантов построения ЕИКП. Выявлена специфика формирования и оценки функционирования ЕСРД для различных вариантов построения ЕИКП.

7. Разработаны предложения по повышению защищенности от несанкционированного доступа к информационным и сетевым ресурсам в мультисервисных сетях ЕИКП на основе методов нечеткого логического вывода. Предложен подход к обнаружению аномалий в схемах разграничения доступа ЕИКП на основе комплексного использования нечеткого кластерного анализа согласно алгоритму «горной» кластеризации и нечеткого логического вывода по Мамдани.

8. Произведена экспериментальная оценка полученных результатов с использованием разработанного программно-инструментальный стенда. Стенд позволяет не только вычислять значения показателей эффективности проектируемых схем разграничения доступа для различных сценариев (VLAN, VPN, RBAC и т.д.), но и осуществлять визуальный анализ хода поиска оптимального решения. Проведенные на стенде эксперименты показали, что разработанные модели, методы и алгоритмы обладают высокими значениями частных показателей эффективности (точности, оперативности, достоверности). Найденные на стенде экспериментальные

зависимости могут найти широкое применение на практике. Разработанные программные средства «Программно-инструментальный стенд визуализации и оценки качества проектирования виртуальных компьютерных сетей для поддержки принятия решений при мониторинге и управлении информационной безопасностью» и «Программное средство оценки оперативности доступа к ресурсам единого информационно-коммуникационного пространства» зарегистрированы в Реестре программ для ЭВМ Федеральной службы по интеллектуальной собственности (свидетельства о государственной регистрации программы для ЭВМ №№ 2015615772, 2015662574).

**3.6. Сопоставление полученных результатов с мировым уровнем**

Все результаты, полученные в процессе выполнения второго года проекта, соответствуют мировому уровню. Авторы проекта изложили основные результаты в 3 статьях, опубликованных в журналах, индексируемых в международных базах цитирования (журналы «Automatic Control and Computer Sciences» и «Journal of Internet Services and Information Security»), в 10 статьях, опубликованных в журналах, входящих в список ВАК Минобрнауки России (журналы «Информационно-управляющие системы», «Проблемы информационной безопасности. Компьютерные системы», «Безопасность информационных технологий», «Информационные технологии и вычислительные системы», «Информация и космос», «Труды СПИИРАН»), а также в прочих журналах и трудах конференций, а также апробировали результаты на множестве различных российских и международных конференций, в частности, на Семнадцатой Международной конференции ―РусКрипто’2015‖, Московская область, г. Солнечногорск, март 2015 года; Международном форуме по практической безопасности Positive Hack Days, Москва, май, 2015 года; 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, июнь-июль 2015 года; Международном конгрессе по интеллектуальным системам и информационным технологиям (IS-IT’15), Дивноморское, Россия, сентябрь 2015 года; LI Международной научно-практической конференции «Технические науки - от теории к практике», Новосибирск, октябрь 2015 года; IX Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России» (ИБРР-2015), Санкт-Петербург, октябрь 2015 года; LII Международной научно-практической конференции «Технические науки - от теории к практике», Новосибирск, ноябрь 2015 года.

**3.7.1. 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 усовершенствования работы 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 виртуальным локальным вычислительным сетям ЕИКП ; (4) методы интеллектуального анализа данных в части разработки эвристических алгоритмов для решения проблемы оперативной и корректной реконфигурации схемы доступа в виртуальной локальной вычислительной сети; (5) метод нечеткого логического вывода применительно к мультисервисным сетям ЕИКП; (6)

онтологический подход к построению единой системы разграничения 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.

**3.7.2. Вклад каждого члена коллектива в выполнение Проекта в 2015 году**

Десницкий Василий Алексеевич:
- выявление факторов, определяющих специфику построения систем разграничения доступа в информационно-телекоммуникационных сетях;
- разработка и исследование моделей и методов оценки эффективности функционирования ЕСРД к разнородным информационным и телекоммуникационным ресурсам ЕИКП по критерию ресурсопотребления;
- разработка модели конфигурирования схем разграничения доступа в критических информационных инфраструктурах;
- анализ сценариев применения моделей и методов построения систем разграничения доступа в информационно-телекоммуникационных сетях;
- экспериментальная оценка полученных результатов.

Дойникова Елена Владимировна:
- разработка методики оценка эффективности конфигурирования схем разграничения доступа как компонентов систем защиты вычислительных систем;
- формирование комплексной системы показателей качества построения систем разграничения доступа в ЕИКП;
- разработка и исследование моделей и методов оценки эффективности функционирования ЕСРД к разнородным информационным и телекоммуникационным ресурсам ЕИКП на основе комплексной системы показателей;
- экспериментальная оценка полученных результатов.

Комашинский Дмитрий Владимирович:
- разработка системы классификации вариантов построения ЕИП.

Новикова Евгения Сергеевна:
- разработка методов визуализации показателей защищенности ресурсов ЕИКП от несанкционированного доступа.

Саенко Игорь Борисович:
- разработка и тестирование эволюционных алгоритмов, моделей и методов для новых предметных областей разграничения доступа к информационным и телекоммуникационным ресурсам в ЕИКП;
- разработка общей архитектуры и архитектуры отдельных компонентов ЕСРД к разнородным информационным и телекоммуникационным ресурсам в ЕИКП;
- исследование и разработка моделей и методов использования онтологий для управления разграничением доступа к разнородным ресурсам ЕИКП;
- исследование и разработка моделей и методов решения задач адаптивного изменения политик и схем разграничения доступа к разнородным информационным и телекоммуникационным ресурсам ЕИКП;
- исследование и разработка моделей и методов оценки эффективности функционирования ЕСРД к разнородным информационным и телекоммуникационным ресурсам ЕИКП;
- разработка подходов к классификации вариантов построения ЕИКП,
- разработка предложений по повышению защищенности от несанкционированного доступа к информационным и сетевым ресурсам в мультисервисных сетях ЕИКП на основе методов нечеткого логического вывода;
- разработка подхода к обнаружению аномалий в схемах разграничения

доступа ЕИКП;
- разработка программно-инструментального стенда для визуализации и оценки качества проектирования виртуальных компьютерных сетей для поддержки принятия решений при мониторинге и управлении информационной безопасностью;
- разработка программного средства оценки оперативности доступа к ресурсам ЕИКП;
- экспериментальная оценка полученных результатов.
Чечулин Андрей Алексеевич:
- разработка методов визуализации показателей защищенности ресурсов ЕИКП от несанкционированного доступа;
- разработка подхода к оценке эффективности системы разграничения доступа на основе анализа и моделирования деревьев атак и корреляции событий безопасности;
- разработка системы показателей качества построения ИЕКП;
- разработка предложений по классификации вариантов построения ЕИКП для интеграции разнородных автоматизированных систем и их сравнительной оценке;
- постановка задачи для построения центрального хранилища для ЕСРД к ресурсам ЕИКП;
- разработка архитектуры компонента контроля и управления доступом к ресурсам информационно-телекоммуникационной сети;
- экспериментальная оценка полученных результатов.
Браницкий Александр Александрович:
- разработка подходов к использованию методов нейросетевой классификации и нечеткого вывода для выявления аномалий в системах разграничения доступа к информационным и сетевым ресурсам вычислительных систем;
- разработка программно-инструментального стенда для визуализации и оценки качества проектирования виртуальных компьютерных сетей для поддержки принятия решений при мониторинге и управлении информационной безопасностью;
- экспериментальная оценка полученных результатов.
Федорченко Андрей Владимирович:
- разработка подхода к оценке эффективности системы разграничения доступа на основе анализа и моделирования комбинированного процесса корреляции событий безопасности.

**3.8.1. Количество научных работ по Проекту, опубликованных в 2015 году**
40

**3.8.1.1. Из них в изданиях, включенных в перечень ВАК**
10

**3.8.1.2. Из них в изданиях, включенных в библиографическую базу данных РИНЦ**
18

**3.8.1.3. Из них в изданиях, включенных в международные системы цитирования (библиографические и реферативные базы научных публикаций)**
3

**3.8.2. Количество научных работ, подготовленных в ходе выполнения Проекта и принятых к печати в 2015 году**
2

**3.9. Участие в 2015 году в научных мероприятиях по тематике Проекта**
1. Семнадцатая Международная конференция ―РусКрипто’2015‖, Московская область, г. Солнечногорск, март 2015 года (секционные доклады).

2. Международный форум по практической безопасности Positive Hack Days, Москва, май, 2015 года (секционные доклады).
3. 24-й научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, июнь-июль 2015 года (секционные доклады).
4. Международный конгресс по интеллектуальным системам и информационным технологиям (IS-IT'15), Дивноморское, Россия, сентябрь 2015 года (1 пленарный, 2 секционных доклада).
5. LI Международная научно-практическая конференция «Технические науки - от теории к практике», Новосибирск, октябрь 2015 года;
6. IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015), октябрь 2015 года (секционные доклады).
7. LII Международная научно-практическая конференция «Технические науки - от теории к практике», Новосибирск, ноябрь 2015 года.

**3.10. Участие в 2015 году в экспедициях по тематике Проекта, которые проводились при финансовой поддержке Фонда**

не было

**3.11. Финансовые средства, полученные в 2015 году от Фонда *(в руб.)***

600000,00

**3.12. 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/

**3.13. Библиографический список всех публикаций по Проекту, опубликованных в 2015 году, в порядке значимости: монографии, статьи в научных изданиях, тезисы докладов и материалы съездов, конференций и т.д.**

1. Саенко И.Б., Котенко И.В. Применение средств генетической оптимизации и визуального анализа для формирования схем доступа в виртуальных локальных вычислительных сетях // Информационные технологии и вычислительные системы, № 1, 2015, С.33-46.
2. Куваев В.О., Чечулин А.А., Ефимов В.В., Лыжинкин К.В. Варианты построения единого информационного пространства для интеграции разнородных автоматизированных систем // Научно-технический журнал «Информация и космос», № 4, 2015. С.83-87.
3. Котенко И.В., Новикова Е.С., Чечулин А.А. Визуализация метрик защищенности для мониторинга безопасности и управления инцидентами // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015. С.42-47.
4. М.В. Коломеец, А.А. Чечулин, И.В. Котенко. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН. 2015. Вып. 42. С. 232-257.
5. Браницкий А.А., Котенко И.В. Построение нейросетевой и иммуноклеточной системы обнаружения вторжений // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015. С. 23-27.
6. Котенко И.В., Чечулин А.А., Комашинский Д.В. Автоматизированное категорирование веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Проблемы информационной безопасности. Компьютерные системы, № 2, 2015. С.69-79.
7. Браницкий А.А., Котенко И.В. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейро-нечетких классификаторов // Информационно-управляющие системы, 2015, № 4. С.69-77.

8. Десницкий В.А., Котенко И.В. Формирование экспертных знаний для разработки защищенных систем со встроенными устройствами // Проблемы информационной безопасности. Компьютерные системы, № 4, 2015. С. 35-41.
9. Котенко И.В., Дойникова Е.В. Методика выбора контрмер на основе комплексной системы показателей защищенности в системах управления информацией и событиями безопасности // Информационно-управляющие системы, 2015, № 3, С.60-69.
10. Дойникова Е.В., Котенко И.В., Чечулин А.А. Динамическое оценивание защищенности компьютерных сетей в SIEM-системах // Безопасность информационных технологий, № 3, 2015. (принято к печати).
11. Desnitsky V.A., Kotenko I.V. Design and Verification of Secure Systems with Embedded Devices on the basis of Expert Knowledge // Automatic Control and Computer Sciences, № 8, 2015, Springer, 2015 (принято к печати).
12. Chechulin A.A., Kotenko I.V. Real-Time Security Events Processing using an Approach based on the Attack Trees Analysis // Automatic Control and Computer Sciences, № 8, 2015, Springer, 2015.
13. Maksim Kolomeec, Andrey Chechulin, Igor Kotenko. Methodological Primitives for Phased Construction of Data Visualization Models // Journal of Internet Services and Information Security (JISIS), Vol. 5, No. 4 (November 2015).
14. Саенко И.Б., Куваев В.О., Бирюков М.А. Использование онтологий для управления разграничением доступа к разнородным ресурсам единого информационно-коммуникационного пространства // Технические науки – от теории к практике, 2015, № 11 (47), С. 76-80.
15. Саенко И.Б., Куваев В.О., Бирюков М.А. Общая архитектура единой системы разграничения доступа к разнородным ресурсам в едином информационно-коммуникационном пространстве // Технические науки – от теории к практике, 2015, № 11 (47), С. 70-75.
16. Десницкий В.А. Методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами // Журнал «Технические науки — от теории к практике». Изд. НП «СибАК», №47, 2015, С.14-18.
17. Десницкий В.А., Дойникова Е.В. Архитектура и оценка эффективности программного средства конфигурирования компонентов защиты систем со встроенными устройствами // Журнал «Технические науки — от теории к практике». Изд. НП «СибАК», №47, 2015, С.9-13.
18. Левшун Д.С., Чечулин А.А. Постановка задачи построения единого хранилища мультимедийных данных из полевых этнографических экспедиций // Журнал «Технические науки — от теории к практике». Изд. НП «СибАК», №46, 2015, С. 25-30.
19. Котенко И.В., Саенко И.Б. Генетический подход к проектированию виртуальной частной сети в защищенном информационном пространстве // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'15, 2015, Том 2. С.320-325.
20. Десницкий В.А. Модели процесса разработки комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'15, 2015, Том 2. С. 113-118.
21. Чечулин А.А. Классификация и модели представления связей между объектами в компьютерных сетях // Труды конгресса по интеллектуальным системам и информационным технологиям IS-IT'15, 2015, Том 2. С. 165-170.
22. Саенко И.Б., Котенко И.В. Адаптивное изменение политик и схем разграничения доступа к ресурсам единого информационного пространства // Материалы 24-й научно-технической конференции «Методы и

технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.127-128.
23. Агеев С.А., Васильев Д.В., Саенко И.Б. Управление безопасностью защищенной мультисервисной сети специального назначения // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.106-107.
24. Котенко И.В., Саенко И.Б., Чечулин А.А. Разработка систем управления информацией и событиями безопасности нового поколения // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.123-124.
25. Десницкий В.А. Методика оценки ресурсопотребления компонентов защиты информационно-телекоммуникационных систем со встроенными устройствами // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.69-70.
26. Дойникова Е.В., Котенко И.В. Выбор защитных мер для управления защищенностью компьютерных сетей на основе комплексной системы показателей // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.114-115.
27. Федорченко А.В Комбинированный процесс корреляции событий безопасности в SIEM-системах // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.102-103.
28. Проноза А.А., Чечулин А.А. Модель извлечения данных разнородной структуры об информационных объектах компьютерной сети для подсистемы визуализации систем управления событиями и информацией безопасности // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.125-127.
29. Чечулин А.А., Проноза А.А. Классификация и анализ типов связей в компьютерных сетях для их последующей визуализации // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 29 июня-02 июля 2015 г. Санкт-Петербург. Издательство Политехнического университета. 2015. С.132-133.
30. Саенко И.Б., Котенко И.В. Модели и методы оценки эффективности функционирования системы разграничения доступа к ресурсам информационного пространства // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 85-86.
31. Коломеец М.В., Чечулин А.А., Котенко И.В. Визуализация параметров безопасности компьютерных сетей с помощью диаграммы Вороного // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 73-74.
32. Левшун Д.С., Чечулин А.А., Коломеец М.В., Котенко И.В. Архитектура системы контроля и управления доступом в помещения на основе

бесконтактных смарт-карт // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 76.
33. Браницкий А.А. Методы вычислительного интеллекта для обнаружения и классификации аномалий в сетевом трафике // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 61-62.
34. Дойникова Е.В. Применение графов зависимостей сервисов в рамках задачи анализа защищенности компьютерных сетей для оценивания критичности ресурсов системы и обоснованного выбора защитных мер // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 68-69.
35. Федорченко А.В. Правило-ориентированный метод корреляции событий безопасности в SIEM-системах // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 86-87.
36. Новожилов Д.А., Чечулин А.А. Разработка программных средств поддержки проведения экспериментов по классификации веб-сайтов // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 80-81.
37. Чечулин А.А. Математические модели и алгоритмы моделирования атак и выработки контрмер в режиме, близком к реальному времени // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 90.
38. Смирнов Д.Б., Чечулин А.А. Корреляция данных безопасности в сетях «Интернет вещей» // Семнадцатая Международная конференция ―РусКрипто'2015‖. Московская область, г.Солнечногорск, 17-20 марта 2015 г. http://www.ruscrypto.ru/
39. Саенко И.Б., Браницкий А.А. Программно-инструментальный стенд визуализации и оценки качества проектирования виртуальных компьютерных сетей для поддержки принятия решений при мониторинге и управлении информационной безопасностью. Свидетельство № 2015615772. Зарегистрировано в Реестре программ для ЭВМ 22.05.2015.
40. Саенко И.Б., Чечулин А.А., Куваев В.О., Барыкин Н.А. Программное средство оценки оперативности доступа к ресурсам единого информационно-коммуникационного пространства. Свидетельство № 2015662574. Зарегистрировано в Реестре программ для ЭВМ 16.11.2015.

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

Информационно-телекоммуникационные системы

**3.15. Критическая технология РФ, которой, по мнению исполнителей, соответствуют результаты данного проекта** Технологии информационных, управляющих, навигационных систем

**3.16. 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.