Основные результаты проекта РФФИ 10-01-00826-а

Название проекта
Математические модели и методы комплексной защиты от сетевых атак и вредоносного программного обеспечения в компьютерных сетях и системах, основывающиеся на гибридном многоагентном моделировании компьютерного противоборства, верифицированных адаптивных политиках безопасности и проактивном мониторинге на базе интеллектуального анализа данных

Основные цели проекта - разработка, прототипирование, теоретическая и экспериментальная оценка моделей и методов комплексной защиты от сетевых атак и вредоносного программного обеспечения, основанных на гибридном многоагентном моделировании компьютерного противоборства, реализации адаптивного управления верифицированными политиками безопасности, анализе защищенности ресурсов компьютерных сетей и систем, а также проактивном мониторинге состояния и поведения защищаемых ресурсов на базе интеграции различных методов интеллектуального анализа данных.

Основные результаты проекта, существенно повышающие эффективность защиты информации в компьютерных системах:
1. Детальный анализ состояния исследований в области моделирования компьютерного противоборства, обнаружения и реагирования против сетевых атак и вредоносного программного обеспечения, а также оценки защищенности ресурсов компьютерных сетей и систем.
2. Формальная постановка задачи исследования, основные требования и формальные модели компонентов гибридного моделирования компьютерного противоборства и механизмов защиты, реализующих обнаружение и реагирование против сетевых атак и вредоносного программного обеспечения, а также анализ защищенности ресурсов компьютерных сетей и систем. Предлагаемый подход к моделированию заключается в интеграции моделей и методов агентно-ориентированного моделировании, использования записей трафика, генерации трафика на основе моделей систем защиты, приложений и вредоносных программ и систем, применении методов эмуляции и виртуализации сетевых процессов и имитационного моделирования на уровне сетевых пакетов. Подход базируется на использовании иерархии макро- и микро-уровневых моделей компонентов реализации атаки (эксплоитов, сетевых червей, ботов, бот-сети в целом и др.) и механизмов защиты от них (аналитических, основанных на имитации сетевых пакетов, базирующихся на эмуляции), а также реальных сетей (имитационных стендов) небольшого размера.
3. Формальные модели и программные прототипы компонентов моделирования сложных распределенных сетевых атак и механизмов защиты от них (на примере функционирования бот-сетей и защиты от бот-сетей). Предложен новый комбинированный подход и формальные модели для исследовательского моделирования бот-сетей и механизмов защиты от них в глобальной сети Интернет, основанный на использовании многоагентных технологий и имитационного моделирования на уровне сетевых пакетов. Подход основан на выделении двух классов подсистем (команд) агентов, воздействующих на информационно-телекоммуникационные сети, как взаимосвязанное множество объектов (ресурсов) различных типов, и друг друга: подсистемы (команды) агентов нападения или бот-сети (для реализации распределенных скоординированных компьютерных атак); подсистемы (команды) агентов защиты (для препятствования вторжениям, многоуровневого сбора информации, обнаружения вторжений, введения злоумышленников в заблуждение, предсказания их намерений и действий и реагирования на вторжения). Разработан комплекс моделей и алгоритмов моделирования и на их основе предложена архитектура среды моделирования. Архитектура среды моделирования имеет иерархическую структуру, состоящую из четырех уровней.
4. Формальные модели и программные прототипы компонентов автоматического обнаружения и реагирования против сетевых атак на основе комбинированного анализа сетевого трафика. Предложенный подход к автоматическому обнаружению и реагированию против сетевых атак заключается в реализации следующих подзадач: определение наиболее эффективных механизмов защиты; выбор наиболее важных характеристик трафика и классификация трафика по этим характеристикам; определение метрик эффективности обнаружения; объединение механизмов защиты. Последняя задача включала разработку формальных моделей и алгоритмов выбора оптимального механизма защиты для каждого из классов трафика, а также исследование и реализацию алгоритмов для объединения механизмов защиты.
5. Формальные модели и программные прототипы компонентов детектирования вредоносного программного обеспечения на основе методов интеллектуального анализа данных. В контексте исследований рассматривались вопросы выявления наиболее значимых аспектов, использование которых позволяет строить потенциально эффективные средства принятия решения на основе методов кластеризации и классификации; определения процедур выбора оптимальных наборов статических и динамических признаков, характеризующих выбранные аспекты потенциально опасных объектов; обоснования эффективности тех или иных методов комбинирования элементов принятия решения в контексте использования набора выбранных аспектов и формирования общей методологии разработки системы детектирования и идентификации вредоносного программного обеспечения в рамках определенных требований.
6. Формальные модели и программные прототипы компонентов анализа защищенности и оценки рисков безопасности ресурсов компьютерных сетей и систем. Система анализа защищенности выполняет анализ защищенности путем имитации действий нарушителя, построения и анализа дерева атак. Основными функциями

системы анализа являются: загрузка и отображение в графическом виде (в виде графа) спецификации анализируемой системы; задание параметров, определяющих модель нарушителя; задание требуемых значений показателей защищенности; формирование и анализ (расчет множества показателей защищенности) дерева атак; ведение журналов регистрации событий; формирование отчетов и др.

7. Формальные модели и программные прототипы компонентов верификации политики безопасности. Модели верификации политики безопасности представляются через множество шагов по выполнению этапов верификации правил политики безопасности и алгоритмов обнаружения и разрешения аномалий фильтрации на основе метода "проверки на модели", а также множества отдельных моделей (компьютерной сети, межсетевого экрана и аномалий фильтрации), которые позволяют верифицировать компьютерную систему, защищенную межсетевым экраном и разрешать все обнаруженные аномалии, при соблюдении требований к методике верификации.

8. Формальные модели и программные прототипы компонентов проектирования безопасных встроенных систем. Целью проведенных исследований являлось построение модели унифицированного формирования процесса построения встроенных систем (ВС). Проектирование ВС осуществляется путем решения многокритериальной оптимизационной задачи, при которой выбор нужных компонентов защиты производится с учетом значений их показателей ресурсопотребления, степени предоставляемой защиты, энергопотребления, стоимости и других характеристик. Результатом использования данной модели является нахождение такой комбинации компонентов защиты, при которой реализуются все необходимые требования к ВС и найденная комбинация является наиболее эффективной с точки зрения оптимальности того или иного набора показателей ВС.

9. Теоретическая и экспериментальная оценка предложенных моделей и методов комплексной защиты. Авторами настоящей работы используется и разрабатывается многоуровневая инструментальная среда имитационного моделирования сетевых процессов для приложений в области защиты информации,, позволяющая выполнять оценку предложенных моделей и методов комплексной защиты. Среда представляет собой программный комплекс, включающий в качестве нижнего уровня систему моделирования дискретных событий, реализованный на языке низкого уровня, а так же ряд компонентов, реализующих сущности более высокого уровня. Нижний слой обеспечивает возможность моделирования хронологически упорядоченных последовательностей событий, распространяющихся в сетевых структурах. Промежуточные слои на базе нижнего слоя реализуют сущности, относящиеся к специфике сети Интернет, в том числе основанные на дискретных событиях модели протоколов и типовых сетевых приложений. Промежуточные слои являются базисом для построения слоев более высокого уровня, таких как, например, слой абстракции уровня интеллектуальных агентов и ряда других. Все модули и компоненты системы моделирования находятся во взаимодействии с подсистемой ввода/вывода и, таким образом, посредством данной подсистемы осуществляют обмен данными с внешними источниками данных и с оператором системы. Каждый слой реализован в виде отдельной библиотеки функций с документированным интерфейсом, посредством которого обеспечивается возможность взаимодействия с данной библиотекой со стороны прочих компонент. Проведенный комплекс экспериментов для решения различных задач моделирования процессов киберпротивоборства включал исследование действий бот-сети и противодействующих им механизмов защиты на этапах распространения бот-сети, управления бот-сетью (реконфигурирования и подготовки к атаке) и выполнения атаки. Была выполнена также теоретическая и экспериментальная оценка всех предложенных моделей и методов комплексной защиты информации.

НОМЕР ПРОЕКТА **10-01-00826**		УЧЕТНАЯ КАРТОЧКА
НАЗВАНИЕ ПРОЕКТА **Математические модели и методы комплексной защиты от сетевых атак и вредоносного программного обеспечения в компьютерных сетях и системах, основывающиеся на гибридном многоагентном моделировании компьютерного противоборства, верифицированных адаптивных политиках безопасности и проактивном мониторинге на базе интеллектуального анализа данных**		
ОБЛАСТЬ ЗНАНИЯ **01 - математика, информатика, механика**		КОД(Ы) КЛАССИФИКАТОРА **01-217 01-202 07-235**
ВИД КОНКУРСА **а - Инициативные проекты**		
ФАМИЛИЯ, ИМЯ, ОТЧЕСТВО РУКОВОДИТЕЛЯ ПРОЕКТА **Котенко Игорь Витальевич**		ТЕЛЕФОН РУКОВОДИТЕЛЯ ПРОЕКТА **(812)3282642**
ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ, ГДЕ РЕАЛИЗУЕТСЯ ПРОЕКТ **Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук**		
ЧИСЛО УЧАСТНИКОВ ПРОЕКТА (включая руководителя) **10**	ЧИСЛО УЧАСТНИКОВ, ИМЕЮЩИХ УЧЕНУЮ СТЕПЕНЬ **4**	ЧИСЛО МОЛОДЫХ (до 35 лет включительно) УЧАСТНИКОВ **9**
Коновалов Алексей Михайлович		
Чечулин Андрей Алексеевич		
Шоров Андрей Владимирович		
Десницкий Василий Алексеевич		
Комашинский Дмитрий Владимирович		
Дойникова Елена Владимировна		
Полубелова Ольга Витальевна		
Нестерук Филипп Геннадьевич		
Новикова Евгения Сергеевна		
ПОДПИСЬ РУКОВОДИТЕЛЯ ПРОЕКТА		ДАТА ПОДАЧИ ОТЧЕТА **14.01.2013**

Форма 501. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ

1.1. *Номер проекта*
10-01-00826

1.2. *Руководитель проекта*
Котенко Игорь Витальевич

1.3. *Название проекта*
Математические модели и методы комплексной защиты от сетевых атак и вредоносного программного обеспечения в компьютерных сетях и системах, основывающиеся на гибридном многоагентном моделировании компьютерного противоборства, верифицированных адаптивных политиках безопасности и проактивном мониторинге на базе интеллектуального анализа данных

1.4. *Вид конкурса*
а - Инициативные проекты

1.5. *Год представления отчета*
2013

1.6. *Вид отчета*
итоговый (2010-2012)

1.7. *Аннотация*
В результате работы над проектом разработаны и исследованы модели и методы комплексной защиты от сетевых атак и вредоносного программного обеспечения в компьютерных сетях и системах. Получены следующие основные результаты, существенно повышающие эффективность защиты информации в компьютерных системах:
(1) детальный анализ состояния исследований в области моделирования компьютерного противоборства, обнаружения и реагирования против сетевых атак и вредоносного программного обеспечения, а также оценки защищенности ресурсов компьютерных сетей и систем;
(2) формальная постановка задачи исследования, основные требования и формальные модели компонентов гибридного моделирования компьютерного противоборства и механизмов защиты, реализующих обнаружение и реагирование против сетевых атак и вредоносного программного обеспечения, а также анализ защищенности ресурсов компьютерных сетей и систем;
(3) формальные модели и программные прототипы компонентов моделирования сложных распределенных сетевых атак и механизмов защиты от них (на примере функционирования бот-сетей и защиты от бот-сетей);
(4) формальные модели и программные прототипы компонентов автоматического обнаружения и реагирования против сетевых атак на основе комбинированного анализа сетевого трафика;
(5) формальные модели и программные прототипы компонентов детектирования вредоносного программного обеспечения на основе методов интеллектуального анализа данных;
(6) формальные модели и программные прототипы компонентов анализа защищенности и оценки рисков безопасности ресурсов компьютерных сетей и систем;
(7) формальные модели и программные прототипы компонентов верификации политики безопасности;
(8) формальные модели и программные прототипы компонентов проектирования безопасных встроенных систем;
(9) теоретическая и экспериментальная оценка предложенных моделей и методов комплексной защиты.

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

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

Подпись руководителя проекта

Форма 502. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ НА АНГЛИЙСКОМ ЯЗЫКЕ

2.1. *Номер проекта*
10-01-00826

2.2. *Руководитель проекта*
Kotenko Igor Vitalevich

2.3. *Название проекта*
Mathematical models and methods of integrated protection against network attacks and malware in computer networks and systems based on hybrid multi-agent modeling and simulation of computer counteraction, verified adaptive security policies and proactive monitoring by data mining

2.4. *Год представления отчета*
2013

2.5. *Вид отчета*
итоговый (2010-2012)

2.6. *Аннотация*
As the result of the project we developed and investigated the models and methods of integrated protection against network attacks and malware in computer networks and systems.The following results, significantly improving the efficiency of information security in computer systems, were obtained:
(1) detailed analysis of state-of-the-art in the field of computer counteraction simulation, detection and reaction against network attacks and malware as well as the security evaluation of computer networks and systems;
(2) formal statement of the research problem, the basic requirements and the formal models of the components for the hybrid simulation of computer counteraction and the protection mechanisms realizing the detection and reaction against network attacks and malware, and also the security evaluation of computer networks and systems;
(3) formal models and software prototypes of components for simulation of complex distributed network attacks and defense mechanisms against them (through an example of botnets and protection against botnets);
(4) formal models and software prototypes of components to automatically detect and respond against network attacks based on combined analysis of network traffic;
(5) formal models and software prototypes of components for detection of malicious software on the basis of data mining methods;(6) formal models and software prototypes of components for security analysis and security risk assessment of computer network and system resources;
(7) formal models and software prototypes of components for security policy verification;
(8) formal models and software prototypes of components for design of secured embedded systems;
(9) theoretical and experimental evaluation of the proposed models and methods of integrated protection.

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

Подпись руководителя проекта

Форма 503. РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1. *Номер проекта*10-01-00826

3.2. *Название проекта*

Математические модели и методы комплексной защиты от сетевых атак и вредоносного программного обеспечения в компьютерных сетях и системах, основывающиеся на гибридном многоагентном моделировании компьютерного противоборства, верифицированных адаптивных политиках безопасности и проактивном мониторинге на базе интеллектуального анализа данных

3.3. *Коды классификатора, соответствующие содержанию фактически проделанной работы(в порядке значимости)*

01-217 01-202 07-235

3.4. *Объявленные ранее цели проекта на 2012 год*

Основными целями проекта на 2012 год являлось продолжение работ по разработке, прототипированию, теоретической и экспериментальной оценке моделей и методов комплексной защиты от сетевых атак и вредоносного программного обеспечения, основанных на гибридном многоагентном моделировании компьютерного противоборства, реализации адаптивного управления верифицированными политиками безопасности, анализе защищенности ресурсов компьютерных сетей и систем, а также проактивном мониторинге состояния и поведения защищаемых ресурсов на базе интеграции различных методов интеллектуального анализа данных.Основными частными целями проекта на 2012 год являлись:
1. Уточнение и доработка формальных моделей и программных прототипов компонентов моделирования сложных распределенных сетевых атак и механизмов защиты от них (на примере функционирования бот-сетей и защиты от бот-сетей).
2. Уточнение и доработка формальных моделей и программных прототипов компонентов автоматического обнаружения и реагирования против сетевых атак на основе комбинированного анализа сетевого трафика.
3. Уточнение и доработка формальных моделей и программных прототипов компонентов детектирования вредоносного программного обеспечения на основе методов интеллектуального анализа данных.
4. Уточнение и доработка формальных моделей и программных прототипов компонентов анализа защищенности и оценки рисков безопасности ресурсов компьютерных сетей и систем.
5. Разработка формальных моделей и программных прототипов компонентов верификации политики безопасности.
6. Разработка формальных моделей и программных прототипов компонентов проектирования безопасных встроенных систем.
7. Продолжение исследований по теоретической и экспериментальной оценке предложенных моделей и методов комплексной защиты от сетевых атак и вредоносного программного обеспечения.

3.5. *Степень выполнения поставленных в проекте задач*

Все задачи, запланированные в проекте, выполнены полностью.

3.6. *Полученные важнейшие результаты*

Важнейшие результаты, полученные за отчетный период, таковы:
1. Детальный анализ состояния исследований в области моделирования компьютерного противоборства, обнаружения и реагирования против сетевых атак и вредоносного программного обеспечения, а также оценки защищенности ресурсов компьютерных сетей и систем.
Основные работы, которые являются базой для моделирования компьютерного противоборства, сосредоточены в области агентно-ориентированного моделирования вида имитационного моделирования, суть которого заключается в представлении сущностей предметной области в виде отдельных автономных интеллектуальных агентов. Множество интеллектуальных агентов, имея простые собственные функции, в процессе функционирования могут включаться (или самоорганизовываться) в системы с существенно более сложным поведением. Данная область знаний представлена широким спектром работ различных исследователей, среди которых следует выделить теоретические подходы теорию разделяемых планов, теорию совместных намерений, гибридный подход, а так же ряд программных реализаций сред многоагентного моделирования. Для оптимизации функционирования команд агентов были предложены различные комбинации следующих методов и моделей: (1) традиционные BDI-модели (BDI belief-desire-intention), определяемые схемами функционирования агентов, обуславливаемыми зависимостями предметной области; (2) методы распределенной оптимизации на основе ограничений, использующие локальные взаимодействия при поиске локального или глобального оптимума; (3) методы распределенного принятия решений на основе частично-наблюдаемых Марковских сетей, позволяющие реализовать координацию командной работы при наличии неопределенности в действиях и наблюдениях; (4) теоретико-игровые модели и модели аукциона, фокусирующиеся на координации различных команд агентов, использующих "рыночные (аукционные)" механизмы принятия решений.За основу предлагаемого подхода к обнаружению сетевых атак было принято использование нескольких семейств механизмов, в том числе базирующихся на следующих методиках: методике "дросселирования/регулирования вирусов" ("Virus Throttling") и ее модификации; методиках, основанных на анализе неудачных соединений (Failed Connection, FC); методиках, использующих метод "порогового случайного прохождения" (Threshold Random Walk, TRW); методиках ограничения интенсивности соединений на основе кредитов доверия (Credit Based Rate Limiting, CB), а также гибридных методиках, комбинирующие различные методы обнаружения.Подходы, применяемые для обнаружения вредоносного программного обеспечения основываются на реализации одного из конкретных методов анализа приложений: статического, динамического или гибридного. Метод

анализа, применяемый в том или ином конкретном подходе, определяется тем, каким образом производится сбор информации, необходимой для принятия решения о вредоносности приложения. В общем случае, статический анализ использует синтаксические или структурные свойства исследуемого объекта. Методы динамического анализа ориентированы на обнаружение фактов, свидетельствующих о наличии вредоносной функциональности приложения при его выполнении или после выполнения. Гибридные методы объединяют преимущества двух вышеупомянутых типов анализа, обеспечивая применение в процессе поиска элементов вредоносности как статической, так и поведенческой информации.

2. Формальная постановка задачи исследования, основные требования и формальные модели компонентов гибридного моделирования компьютерного противоборства и механизмов защиты, реализующих обнаружение и реагирование против сетевых атак и вредоносного программного обеспечения, а также анализ защищенности ресурсов компьютерных сетей и систем.

Предлагаемый подход к моделированию заключается в интеграции моделей и методов агентно-ориентированного моделировании, использования записей трафика, генерации трафика на основе моделей систем защиты, приложений и вредоносных программ и систем, применении методов эмуляции и виртуализации сетевых процессов и имитационного моделирования на уровне сетевых пакетов. Подход базируется на использовании иерархии макро- и микро-уровневых моделей компонентов реализации атаки (эксплоитов, сетевых червей, ботов, бот-сети в целом и др.) и механизмов защиты от них (аналитических, основанных на имитации сетевых пакетов, базирующихся на эмуляции), а также реальных сетей (имитационных стендов) небольшого размера. Предлагаемый подход и разрабатываемый инструментарий моделирования и эмуляции могут использоваться для анализа текущих и будущих сетевых атак и механизмов защиты, "проигрывания" сценариев кибератак и киберзащиты, анализа защищенности систем защиты, а также применяться для расследований инцидентов, связанных с использованием бот-сетей и сетевых атак. При моделировании сетевых процессов используются модели следующих элементов: топологии сети, каналов передачи данных, протоколов, приложений, узлов, трафика. В зависимости от целей моделирования данные модели представляются с той или иной точностью.

3. Формальные модели и программные прототипы компонентов моделирования сложных распределенных сетевых атак и механизмов защиты от них (на примере функционирования бот-сетей и защиты от бот-сетей).

Предложен новый комбинированный подход и формальные модели для исследовательского моделирования бот-сетей и механизмов защиты от них в глобальной сети Интернет, основанный на использовании многоагентных технологий и имитационного моделирования на уровне сетевых пакетов. Подход основан на выделении двух классов подсистем (команд) агентов, воздействующих на информационно-телекоммуникационные сети, как взаимосвязанное множество объектов (ресурсов) различных типов, и друг друга: (1) подсистемы (команды) агентов нападения или бот-сети (для реализации распределенных скоординированных компьютерных атак); (2) подсистемы (команды) агентов защиты (для препятствования вторжениям, многоуровневого сбора информации, обнаружения вторжений, введения злоумышленников в заблуждение, предсказания их намерений и действий и реагирования на вторжения).Разработан комплекс моделей и алгоритмов моделирования и на их основе предложена архитектура среды моделирования. Архитектура среды моделирования имеет иерархическую структуру, состоящую из четырех уровней. Первый уровень реализуется посредством системы моделирования дискретных событий общего назначения. На втором уровне используется библиотека компонент моделирования вычислительных сетей, основанных на коммутации сетевых пакетов. Третий уровень предоставляет инструменты для создания сетевых топологий статистически идентичных топологиям реальных вычислительных сетей, включает модели реалистичного сетевого трафика, моделируемого на пакетном уровне. Непосредственное моделирование предметной области осуществляется на четвертом уровне, на котором представлены модели сетевых приложений, относящиеся к работе бот-сетей различных типов. На основе данной архитектуры реализована многоуровневая программная инструментальная среда моделирования, включающая систему моделирования дискретных событий общего назначения (на основе системы имитационного моделирования OMNeT++), компонент моделирования сетевых протоколов и вычислительных сетей, основанных на коммутации сетевых пакетов (на базе библиотека компонент INET Framework), компонент моделирования реалистичных вычислительных сетей (посредством библиотеки ReaSE) и библиотеку BOTNET Foundation Classes, содержащую модели сетевых приложений, относящиеся к работе бот-сетей и механизмов противодействия им. На основе предложенного подхода и формальных моделей для исследовательского моделирования бот-сетей и механизмов защиты от них предложена реализация биоинспирированного подхода, называемого "нервная система сети". Система защиты, построенная на основе данного подхода, включает два основных компонента — сервер "нервной системы сети" и узел "нервной системы сети". Серверы устанавливаются в различных подсетях и реализуют большую часть процессов обработки и анализа информации, а также координацию действий близлежащих сетевых устройств. Узлы служат для сбора, первоначальной обработки и передачи информации о состоянии сети серверам и работают на основе маршрутизаторов. Серверы находятся в разных подсетях и обмениваются информацией о состоянии своих подсетей. Таким образом, на основе метафоры "нервной системы сети" предложена адаптивная сетевая инфраструктура, обеспечивающая получение информации, ее передачу на специальный сервер и принятие решений, исходя из сложившейся ситуации.

4. Формальные модели и программные прототипы компонентов автоматического обнаружения и реагирования против сетевых атак на основе комбинированного анализа сетевого трафика.
Предложенный подход к автоматическому обнаружению и реагированию против сетевых атак заключается в реализации следующих подзадач: (1) определение наиболее эффективных механизмов защиты; (2) выбор наиболее важных характеристик трафика и классификация трафика по этим характеристикам; (3) определение метрик эффективности обнаружения; (4) объединение механизмов защиты. Последняя задача включала разработку формальных моделей и алгоритмов выбора оптимального механизма защиты для каждого из классов трафика, а также исследование и реализацию алгоритмов для объединения механизмов защиты.Основными требованиями к компонентам автоматического обнаружения и реагирования против сетевых атак являются: (1) точность работы (определяется по количеству ошибок классификации первого и второго рода); (2) своевременность (определятся по скорости реакции системы на поступающую информацию); (3) автоматизация. Это требование тесно связано со своевременностью. Система защиты должна требовать минимального участия администратора для принятия решений; (4) обнаружение атак, растянутых во времени. Предложено использование комбинированной схемы, использующей отдельные классификаторы или группы классификаторов, ориентированные на обнаружение определенных типов атак, для принятия решения о блокировании опасных хостов в сети. Полученная в результате использования данного подхода комбинированная схема обнаружения сетевого сканирования использует три уровня классификаторов: (1) классификаторы, принимающие решение о наличии или отсутствии в исследуемом трафике подозрительных участков, (2) аспектные классификаторы, которые на основе данных полученных от классификаторов 1-го уровня, принимают решение о наличии или отсутствии сканирующих последовательностей разных типов в исследуемом трафике и (3) общий классификатор, принимающий решение о том, является ли исследуемый трафик вредоносным или нет. Особенностью классификаторов 1-го уровня в этой схеме, является то, что каждый из них использует группу параметров, характерных для различных типов подозрительной сетевой активности. Этот подход позволяет добавлять новые типы обнаруживаемого сканирования без переобучения всей системы – достаточно добавить новый классификатор 1-го уровня (или модифицировать уже существующий) и переобучить соответствующие классификаторы 2-го и 3-го уровней.

5. Формальные модели и программные прототипы компонентов детектирования вредоносного программного обеспечения на основе методов интеллектуального анализа данных.
Основным принципом формирования систем детектирования и идентификации вредоносного программного обеспечения в работе является принцип комбинирования отдельных элементов принятия решения, ориентирующихся на отдельные структурные и функциональные аспекты потенциально опасных объектов, в иерархическую структуру, вырабатывающую конечное решение о классе анализируемого объекта. В контексте практических изысканий рассматривались вопросы (1) выявления наиболее значимых аспектов, использование которых позволяет строить потенциально эффективные средства принятия решения на основе методов кластеризации и классификации; (2) определения процедур выбора оптимальных наборов статических и динамических признаков, характеризующих выбранные аспекты потенциально опасных объектов; (3) обоснования эффективности тех или иных методов комбинирования элементов принятия решения в контексте использования набора выбранных аспектов и (4) формирования общей методологии разработки системы детектирования и идентификации вредоносного программного обеспечения в рамках определенных требований.Исследованы устойчивые и потенциально эффективные паттерны обработки исходных данных и применения отдельных методов классификации, кластеризации и поиска ассоциативных правил. В частности, проведенные исследования показали, что применение позиционно-зависимых признаков, извлекаемых на этапе статического анализа исполняемых файлов, является достаточно эффективным при использовании методов интеллектуального анализа данных, относящихся к группам классификаторов, использующих генерацию правил и построение деревьев решений. Наиболее эффективным показал себя метод RandomForest, интегрирующий в себя общие принципы улучшения качества классификации за счет реализации принципов обобщения результатов работы нескольких сущностей, ответственных за принятие решения.Показана и обоснована необходимость учета значимости отдельных областей (регионов) анализируемых объектов и данных, находящихся в них. Данный подход не гарантирует абсолютной точности детектирования вредоносного программного обеспечения, но, в силу показанных особенностей, может быть эффективен на определенных фазах процесса принятия решения о способе дальнейшей обработки объекта и при построении средств детектирования отдельных семейств исполняемых программ. В качестве очевидного примера можно привести задачу автоматизации обнаружения и идентификации использованных средств обфускации или защиты исполняемых файлов, что позволит обеспечить четкую автоматическую процедуру генерации правил детектирования и тем самым предоставляет возможность более корректно определить путь дальнейшего анализа объекта (каким образом настроить средства динамического анализа, каким участкам исследуемого объекта следует уделить внимание в дальнейшем при подтверждении факта его обфускации и т.д.).Разработана обобщенная методика построения элементов общей схемы принятия решения о степени вредоносности и зашумленности (искаженности) анализируемых объектов. В этой связи определены особенности задач, решаемых в процессе применения средств интеллектуального анализа данных для детектирования вредоносного программного обеспечения, в том числе задач выделения списка потенциально значимых признаков, определения процедуры выявления наиболее значимых признаков, выбора метода классификации, оценки качества созданной модели детектирования, определения используемых инструментальных средств.В

рамках проектирования отдельных средств выявления зашумленных данных предлагается в общей архитектуре системы детектирования вредоносного программного обеспечения использовать отдельные элементы, служащие для выявления зашумленных данных, представляемых отдельными трактами принятия решения и, как следствие, ориентированные на отдельные группы заведомо зашумленных данных, используемых при обучении. Разработаны модели улучшения прогностической функции принятия решения, основанных на методах интеллектуального анализа данных, и модели комбинирования отдельных элементов принятия решения за счет формирования иерархических (пошаговых) схем и схем голосования. Очевидно, что традиционно узкая направленность отдельных частных подходов к детектированию вредоносного программного обеспечения позволяет произвести достаточно точную оценку их эффективности для поставленных исследователями условий. Вместе с тем, она же ограничивает применимость предлагаемых моделей детектирования вредоносного программного обеспечения на практике. Поэтому предлагаемые модели улучшения прогностической функции принятия решения основываются на следующих элементах принятия решения: (1) использовании максимального количества объектов фокусной группы (семейства) вредоносного программного обеспечения или уточнении (последовательном ограничении) целевого семейства объектов с последующим ограничением группы фокуса используемого классификатора; (2) обобщении всей доступной информации о специфических признаках вредоносного программного обеспечения и применении дополнительных «резервных» механизмов принятия решения о вредоносности объектов, не попадающих в конкретную фокусную группу; (3) включении в процесс обучения нескольких классификаторов и использовании механизма обобщения результатов их работы, т.е. реализации комбинированных классификаторов. Модель комбинирования отдельных элементов принятия решения основывается на так называемом «многоходовом» подходе к детектированию, основанном на последовательном уточнении значимых структурных и функциональных аспектов анализируемого объекта. Первым необходимым шагом в процессе принятия решения является получение ответа на вопрос о том, является ли проверяемый объект защищенным каким-либо средством обфускации. Далее, в зависимости от результата предыдущего шага, объект передается последующему элементу модели, обученному именно на такой группе объектов, которая соответствует результату предыдущего шага принятия решения.Предложенная итоговая решающая модель классификации представляет собой иерархический метаклассификатор, производящий на начальных уровнях принятия решения уточнение структурных свойств объекта с последующим выделением наиболее эффективной для обработки конкретного объекта модели классификации по заданным категориям.Для начального сокращения размерности пространства признаков использовался фильтрующий метод выделения значимых признаков на основе значения относительного коэффициента усиления, в качестве базового метода классификации использовался метод дерева решений.

6. Формальные модели и программные прототипы компонентов анализа защищенности и оценки рисков безопасности ресурсов компьютерных сетей и систем.

Предлагаемый подход к анализу защищенности является развитием подхода к анализу защищенности компьютерных сетей (КС), предложенного ранее – получили свое развитие модели анализируемой КС, атакующих действий и нарушителя. Расширение модели анализируемой КС позволило при построении дерева атак учитывать атакующие действия, требующие физического доступа нарушителя в контролируемую зону, например, нарушение IP-связности путем физического отключения сетевого кабеля. Расширение модели нарушителя включает в себя определение ресурсов, направленных на реализацию уязвимостей санкционированных пользователей (в первую очередь, финансовые ресурсы).Разработанные прототипы состоят из следующих программных средств: (1) Конструктор спецификаций анализируемых систем; (2) Система анализа защищенности; (3) Компонент обновления базы данных (БД) уязвимостей.Конструктор спецификаций анализируемых систем (спецификации представляются в формате XML) реализует следующие основные функции: загрузка спецификации системы из файла, сохранение ее в файл; задание, модификация метаданных спецификации (название, дата и время создания и др.); создание, модификация и удаление объектов (санкционированных пользователей и вычислительных платформ – рабочих станций, серверов, коммутаторов и т.п.); задание и модификация метаданных объектов (имя, местоположение, уровень критичности и т.п.); создание, модификация и удаление связей (IP-связей между ВП; связей, описывающих доступ санкционированных пользователей) и др. Система анализа защищенности выполняет анализ защищенности путем имитации действий нарушителя, построения и анализа дерева атак. Основными функциями системы анализа являются: загрузка и отображение в графическом виде (в виде графа) спецификации анализируемой системы; задание параметров, определяющих модель нарушителя; задание требуемых значений показателей защищенности; формирование и анализ (расчет множества показателей защищенности) дерева атак; ведение журналов регистрации событий; формирование отчетов и др.Компонент обновления БД уязвимостей предназначен для внесения во внутреннюю БД, используемую системой анализа защищенности, сведений о новых уязвимостях.Вычисление метрик защищенности часто требует детального анализа всех элементов модели защищаемой сети, что неприемлемо для оценки защищенности в реальном времени. Такой анализ может занять длительное время, в результате чего точные значения обобщенных метрик (например, оценка уровня защищенности) могут быть доступны лишь через некоторое время после начала расчета. Для решения этой проблемы предложено использовать anytime-алгоритмы. В рамках anytime-алгоритма задача расчета уровня защищенности представляется в виде ряда алгоритмов с разной вычислительной сложностью. Для этого, в первую очередь, изменяется полнота входных данных. Для расчета алгоритмы используются (по усложнению модели защищаемой

компьютерной сети): (1) список отдельных хостов без учета топологии; при использовании данного варианта предполагается, что нарушитель имеет удаленный доступ ко всем хостам в сети; (2) упрощенная модель топологии сети (подсети сгруппированы по уровням критичности и представлены в виде интегральных моделей). При этом уязвимости групп считаются как сумма уязвимостей отдельных хостов в них; (3) полная модель сети, включающая отдельные модели для каждого объекта в защищаемой компьютерной сети.Аналогично, применение anytime-алгоритмов может быть связано с недоступностью в текущий момент полной информации о сети, что влечет возможность вычисления оценки для некоторого подмножества хостов.

7. Формальные модели и программные прототипы компонентов верификации политики безопасности.
Модели верификации правил фильтрации политики безопасности представляются через множество шагов по выполнению этапов верификации правил политики безопасности и алгоритмов обнаружения и разрешения аномалий фильтрации на основе метода "проверки на модели", а также множества отдельных моделей (компьютерной сети, межсетевого экрана и аномалий фильтрации), которые позволяют верифицировать компьютерную систему, защищенную межсетевым экраном и разрешать все обнаруженные аномалии, при соблюдении требований к методике верификации.Предлагаемая модель компьютерной сети предназначена для представления структуры сети, ее основных элементов и сетевых процессов. Она включает в себя два базовых компонента: топологию сети и генерируемый в сети трафик. Для задачи верификации правил фильтрации из общей топологии выделяется расположение хостов и межсетевых экранов в сети. При генерации трафика все адресное пространство сокращается до минимума, необходимого для выявления всех возможных аномалий, при этом рассматриваются только хосты, которые специфицированы в правилах фильтрации. При решении задачи ограничения диапазона сетевых адресов используется методика сегментации правил политики безопасности. Модель межсетевого экрана предназначена для представления межсетевого экрана и алгоритмов его работы. Основными компонентами этой модели являются сетевые идентификаторы, заданные наборы правил фильтрации, а также алгоритм обработки сетевого трафика. Модель аномалий фильтрации задана набором свойств аномалии, определяющей ее тип, а также распространяется ли она на всю сеть или действует только на правила одного хоста. Под аномалиями подразумевается несоответствие в задании правил политики безопасности и (или) описании сети, из-за которого одно или более правил политики никогда не будут активированы.Для реализации моделей используется программное средство "проверки на модели" SPIN. В процессе верификации выявляются все некорректные состояния системы. На завершающем этапе полученные результаты верификации интерпретируются. Если были обнаружены аномалии, то пользователь получает адреса межсетевых экранов и правила, приводящие к возникновению аномалии, а также тип аномалии. Преимуществами данного подхода являются его высокий уровень абстракции при представлении данных и возможность исследовать динамическое поведение системы. К недостаткам относится вычислительная сложность подхода.

8. Формальные модели и программные прототипы компонентов проектирования безопасных встроенных систем.
Целью проведенных исследований является построение модели унифицированного формирования процесса построения встроенных систем (ВС), обладающего двумя следующими особенностями. Для повышения защищенности ВС от возможных атак, требования к безопасности должны рассматриваться и учитываться разработчиками на каждой стадии процесса. Также, важнейшей особенностью разрабатываемого процесса является его частичная автоматизация. Необходимость автоматизации вытекает из потребности сократить время, затрачиваемое на выполнение таких действий, которые повторяются циклически и требуют ручного участия и контроля со стороны разработчиков ВС. Основными задачами, являющимися предметом исследований в отчетный период, являлись построение абстрактной модели ВС и построение конфигурационной модели ВС.Абстрактная модель (АМ) представляет обобщенное представление встроенных систем и отражает основные аспекты безопасности, характерные для широкого круга ВС. АМ описывает граф, представляющий дерево важнейших свойств ВС в качестве входных данных процесса. Дерево отображает как основные свойства безопасности, так и операционные свойства, которые напрямую не характеризуют безопасность ВС, но, влияют на нее косвенно. Для свойств безопасности рассматривается также классификация объектов, на которые направлена защита. Каждому свойству придается некоторая бинарная характеристика, как например наличие или отсутствие какой-либо структурной или поведенческой особенности, или же важность или несущественность свойства. Производится также ранжирования свойств, то есть определение для свойства более широкого диапазона его возможных значений, а также формируются критерии оценки некоторых из свойств, включающие специализированные показатели.В зависимости от типа встроенной системы разработчиками ВС задается определенный набор общих требований к ВС, а также требований к безопасности ВС. Предложен способ построения защищенных ВС на основе комбинирования отдельных компонентов защиты. Причем комбинирование осуществляется путем решения многокритериальной оптимизационной задачи, при которой выбор нужных компонентов защиты производится с учетом значений их показателей ресурсопотребления, степени предоставляемой защиты, энергопотребления, стоимости и других характеристик. Результатом использования данной модели является нахождение такой комбинации компонентов защиты, при которой реализуются все необходимые требования к ВС и найденная комбинация является наиболее эффективной с точки зрения оптимальности того или иного набора показателей ВС.Программно-техническое средство «Конфигуратор», реализованное в

работе, осуществляет процесс конфигурирования и предназначено на достижение следующих целей: построение программного средства для решения задач конфигурирования существующих сложных информационных систем и коммуникационных сетей; демонстрация процесса конфигурирования и работы отдельных его функций; получение экспериментальных данных для сравнения эффективности предлагаемого подхода с другими существующими подходами и реализованными программно-техническими решениями; применение полученных экспериментальных данных в дальнейших исследованиях и программных прототипах. Средство включает следующие основные функции: функцию конфигурирования, которая согласно заданным ограничениям и списку заданных компонентов защиты выдает оптимальную конфигурацию; функции проверки эффективности выбранной конфигурации и сравнения эффективности двух заданных конфигураций.

9. Теоретическая и экспериментальная оценка предложенных моделей и методов комплексной защиты.
Авторами настоящей работы используется и разрабатывается многоуровневая инструментальная среда имитационного моделирования сетевых процессов для приложений в области защиты информации. Среда представляет собой программный комплекс, включающий в качестве нижнего уровня систему моделирования дискретных событий, реализованный на языке низкого уровня, а так же ряд компонентов, реализующих сущности более высокого уровня. Нижний слой обеспечивает возможность моделирования хронологически упорядоченных последовательностей событий, распространяющихся в сетевых структурах. Промежуточные слои на базе нижнего слоя реализуют сущности, относящиеся к специфике сети Интернет, в том числе основанные на дискретных событиях модели протоколов и типовых сетевых приложений. Промежуточные слои являются базисом для построения слоев более высокого уровня, таких как, например, слой абстракции уровня интеллектуальных агентов и ряда других. Все модули и компоненты системы моделирования находятся во взаимодействии с подсистемой ввода/вывода и, таким образом, посредством данной подсистемы осуществляют обмен данными с внешними источниками данных и с оператором системы. Каждый слой реализован в виде отдельной библиотеки функций с документированным интерфейсом, посредством которого обеспечивается возможность взаимодействия с данной библиотекой со стороны прочих компонент.Проведенный комплекс экспериментов для решения различных задач моделирования процессов киберпротивоборства включал исследование действий бот-сети и противодействующих им механизмов защиты на этапах распространения бот-сети, управления бот-сетью (реконфигурирования и подготовки к атаке) и выполнения атаки. Для защиты от бот-сети на фазе распространения, реализуемой посредством распространения сетевых червей, были проанализированы методики, базирующиеся на Virus Throttling и Failed Connection. Для защиты от бот-сети на фазе управления были исследованы методы обнаружения IRC-ориентированных бот-сетей на базе метрики “заселенности” (Relationship) отдельных IRC-каналов, метрики распределения времени отклика на широковещательных запрос (Response), а так же метрики синхронности (Synchronization) группового поведения бот-сетей. Также исследовались методы, работающие на разных этапах защиты от DDoS-атак, в том числе SAVE (Source Address Validity Enforcement Protocol), SIM (Source IP Address Monitoring) и Hop-count filtering.Реализация результатов работы приведет к повышению показателей эффективности моделирования защиты ресурсов информационно-телекоммуникационных сетей и разработке новых методов защиты от инфраструктурных атак на информационно-телекоммуникационные сети.Эксперименты для оценки компонентов автоматического обнаружения и реагирования против сетевых атак на основе комбинированного анализа сетевого трафика позволили оценить эффективность работы отдельных и комбинированных механизмов обнаружения атак. По полученным данным можно судить о том, что использование предложенных методов комбинирования, а также настройка параметров для отдельных механизмов защиты в зависимости от статистических показателей трафика позволяет существенно улучшить эффективность работы этих механизмов.Основной целью экспериментов с компонентами детектирования вредоносного программного обеспечения на основе методов интеллектуального анализа данных была проверка базового предположения работы, что определенные статические свойства анализируемых программных приложений определяют их поведенческие особенности. Для проверки предположения были проведены практические эксперименты на наборах вредоносных и безопасных исполняемых файлов формата PE32. Начальный эксперимент был проведен с целью получения дерева решений, относящего исследуемый объект к одной из двух базовых категорий (опасен / неопасен) на всей обучающей выборке. Серия контрольных экспериментов проводилась на расширенном наборе категорий, который помимо двух базовых, включал в себя категории, определяемые значениями некоторых статических атрибутов, доступных из структуры исполняемых файлов. В зависимости от значений базовых и дополнительных категорий объектов, обучающая выборка была разбита на более мелкие группы. Сравнение результатов экспериментов показало, что совместное применение статических и динамических атрибутов позволяет значительно повысить показатели точности для отдельных групп вредоносных приложений, в среднем упростить решающие модели за счет снижения количества используемых ими поведенческих признаков и существенно уменьшить объем базовой выборки поведенческих признаков за счет исключения из нее признаков, наличие которых корелировало с включенными в рассмотрение статическими категориями. Наиболее эффективными статическими атрибутами в рамках данной модели показали себя поля SubSystem, Characteristics заголовков формата PE32 и обобщенные данные о типе компилятора, используемого при получении исполняемого файла. Было показано, что при использовании методов классификации на основе деревьев решений (decision tree, DT) и k ближайших соседей (k nearest neighbors, k-NN) и использовании некоторых групп атрибутов, характеризующих количественные и качественные характеристики их

содержимого, представляется возможным достичь достаточно высокой точности детектирования (вплоть до 99%) вредоносных документов. Продемонстрирован подход к оптимизации показателей детектирования вредоносных документов за счет комбинирования классификаторов, обученных на отдельных группах структурных признаков за счет применения методов голосования (Vote) и стекинга (Stacking). Эксперименты проводились с использованием среды Rapid Miner 5.0.Оценка разработанных компонентов анализа защищенности и рисков безопасности ресурсов компьютерных сетей и систем включали эксперименты с несколькими тестовыми сетями, различным местоположением злоумышленников и различными типами уязвимостей. Для оценки разработанных компонентов верификации политики безопасности проведена серия экспериментов по проверке политики фильтрации межсетевого экрана. Для оценки эффективности реализации метода верификации были проведены тесты на различных наборах правил фильтрации с вычислением различных метрик, таких как время вычисления, полнота функциональности и потребление ресурсов. По результатам проведенных экспериментов было показано, что предлагаемый подход позволяет выявлять все аномалии в правилах фильтрации политики безопасности, однако имеет экспоненциальную вычислительную сложность в зависимости от количества верифицируемых правил. Таким образом, можно заключить, что предложенная методика может быть применима для малых и средних компьютерных сетей.Оценка разработанных компонентов проектирования безопасных встроенных систем показала, что осуществление автоматизированного процесса конфигурирования с использованием разработанного инструмента конфигурирования позволяет находить оптимальные конфигурации за приемлемое время. В частности, эксперименты показали, что процесс конфигурирования на множестве более чем 100 вариантов блоков на персональном компьютере выполняется менее чем за 1 секунду. Более того, при возрастании количества блоков до 1000 и более, временные затраты окажутся вполне приемлемыми.

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, распределенного искусственного интеллекта, моделирования и др.

3.8. Сопоставление полученных результатов с мировым уровнем

Все результаты, полученные в процессе выполнения проекта, соответствуют мировому уровню. Это подтверждается, в том числе, тем, что авторы проекта опубликовали полученные результаты в множестве российских и международных журналах, сборниках и трудах конференций, в том числе в международных (в издательствах Springer, IEEE и др.), а также апробировали на множестве различных российских и международных конференций.

Руководитель проекта выступал с приглашенными ключевыми докладами на нескольких российских и международных конференциях, в частности, на следующих конференциях: Международной конференции по киберконфликтам (Таллинн, Эстония. 15-18 июня 2010 г.), Международном семинаре "Научный анализ и поддержка политик безопасности в киберпространстве" (SA&PS4CS 2010, Санкт-Петербург, 11 сентября 2010 г.), Международной школе "Программные агенты, агентские системы и их приложения" (Танжер, Марокко, 15-23 сентября), Международном семинаре "Взаимодействие науки, технологии и безопасности: современные и будущие области приложения" (APCSS'2010, США, Гонолулу, 4-8 октября 2010 г.), Международном семинаре "Безопасные и надежные вычисления в мобильных и облачных средах" (Дели, Неемрана, Индия, 16-17 декабря 2010 г.), Международном семинаре EffectsPlus по координации проектов Европейского Сообщества (г. Амстердам, Голландия. 4-5 июля 2011 г.), VII Санкт-Петербургской межрегиональной конференции "Информационная безопасность регионов России (ИБРР-2011, Санкт-Петербург, 26-28 октября 2011 г.), Международном форуме по практической безопасности Positive Hack Days (PHD 2012, Москва, 30-31 мая 2012 г), Санкт-Петербургском научном форуме "Наука и общество" и VII Петербургской встрече лауреатов Нобелевской премии. (Санкт-Петербург, 8-12 октября 2012 г.), Международном семинаре "Научный анализ и поддержка политик безопасности в киберпространстве" (SA&PS4CS 2012, Санкт-Петербург, 20 октября 2012 г.).

Апробация результатов была также проведена нана 18-й, 19-й и 20 Европейской (Euromicro) международной конференции по параллельной, распределенной и сетевой обработке информации (PDP 2010, Пиза, Италия. 17-19 февраля 2010 г.; PDP 2011, Айа-Напа, Кипр, 9-11 февраля 2011 г.; PDP 2012, Мюнхен, 15-17 февраля 2012 г.), Международной конференции "Математические модели, методы и архитектуры для защиты компьютерных сетей" (MMM-ACNS-2010, Санкт-Петербург, 8-10 сентября 2010 г.; MMM-ACNS-2012, Санкт-Петербург, 17-19 октября 2012 г.), Международной конференции "Интеллектуальные распределенные вычисления" (IDC'2010, Танжер, Марокко, 15-23 сентября), Двенадцатой национальной конференции по искусственному интеллекту с международным участием (КИИ-2010, 20-24 сентября 2010 г., г. Тверь, Россия), Конференции по криптологии, стеганографии, цифровой подписи и системам защиты информации ("РусКрипто'2010, 2011, 2012), Общероссийской научно-технической конференции "Методы и технические средства обеспечения безопасности информации (МТСОБИ 2010, 2011, 2012, Санкт-Петербург), XII и XIII Санкт-Петербургской Международной Конференции "Региональная информатика-2010 (РИ-2010)" и «Региональная информатика-2012 (Санкт-Петербург, 2010, 2012 гг.), Шестой международной научной конференции по проблемам безопасности и противодействия терроризму и Девятой общероссийской научной конференции "Математика и безопасность информационных технологий МаБИТ-2010" (Москва, 11-13 ноября 2010 г.), Международном семинаре "Интеграция информации и ГИС: к цифровому океану" (IF&GIS-2011, Брест, Франция, 10-11 мая 2011 г.), Шестой IEEE международной конференции "Интеллектуальное приобретение данных и передовые

компьютерные системы: технологии и приложения" (IDAACS 2011, Прага, Чехия. 16-18 сентября 2011 г.), 16-й Международной конференции по безопасным информационным системам (NordSec 2011, Таллинн, Эстония. 26-28 октября 2011 г.), Пятой всероссийской научно-практической конференции по имитационному моделированию и его применению в науке и промышленности "Имитационное моделирование. Теория и практика" (ИММОД-2011, Санкт-Петербург, 19-21 октября 2011 г.), VII Санкт-Петербургской межрегиональной конференции "Информационная безопасность регионов России" (ИБРР-2011, 26-28 октября 2011 г.), Конференции "Информационная безопасность: Невский диалог – 2011" (Санкт-Петербург, 16 ноября 2011 г.), Международной конференции по безопасности и криптографии (SECRYPT 2012, Италия, Рим, 24-27 июля 2012 г.), Международной конференции по методологиям, технологиям и приложениям моделирования (SIMULTECH 2012, Италия, Рим, 28-31 июля 2012 г.), Международном конгрессе по интеллектуальным системам и информационным технологиям "IS&IT'12" (Дивноморское, 2-8 сентября, 2012 г.), 2-ом Международном семинаре по безопасности и надежности систем (3SL-2012, Безансьон, Франция, 20 ноября, 2012 г.); Международной конференциии по Интернету вещей (iThings 2012, Безансьон, Франция, 21-23 ноября, 2012 г.); 5-й Российской мультиконференции по проблемам управления (МКПУ-2012) - конференции "Информационные технологии в управлении" (ИТУ-2012, Санкт-Петербург, 9-11 октября, 2012 г.) и др.

3.9. *Методы и подходы, использованные в ходе выполнения проекта*

В качестве базиса для исследований использовались работы в следующих областях:
(1) механизмы обеспечения информационной безопасности в компьютерных сетях (в том числе новые технологии обнаружения вторжений и использования ложных информационных систем);
(2) методы агентно-ориентированного моделирования, генерации трафика на основе моделей, эмуляции и виртуализации сетевых процессов, имитационного моделирования на уровне сетевых пакетов;
(3) объединение (слияние) данных и информации;
(4) интеллектуальные агенты, включая модели командной работы агентов;
(5) онтологическое представление знаний;
(6) системы вывода, основанные на знаниях о выполняемых действиях и предсказании намерений и планов оппонента;
(7) рефлексивные процессы, модели антагонистических процессов;
(8) основанное на агентских технологиях моделирование;
(9) анализ рисков;
(10) элементы теории игр;
(11) методы верификации сложных систем;
(12) методы интеллектуального анализа данных, в том числе на базе статической и динамической информации, комбинирования классификаторов, обучения и классификации на зашумленных наборах данных и др.;
(13) методы адаптации и самообучения;
(14) методы теории исследования операций и оптимального управления;
(15) методы проектирования встроенных устройств и др.

3.10.1.1. *Количество научных работ, опубликованных в ходе выполнения проекта* 199

3.10.1.2. *Из них включенных в перечень ВАК* 38

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)* 28

3.10.2. *Количество научных работ, подготовленных в ходе выполнения проекта и принятых к печати в 2012 г.* 8

3.11. *Участие в научных мероприятиях по тематике проекта, которые проводились при финансовой поддержке Фонда* 12

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

3.13. *Финансовые средства, полученные от РФФИ*

3.15. Адреса (полностью) ресурсов в Internet, подготовленных авторами по данному проекту
http://comsec.spb.ru/ru/staff/kotenko
http://comsec.spb.ru/en/staff/kotenko
http://comsec.spb.ru/ru/projects/
http://comsec.spb.ru/en/projects

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

Публикации за 1-й год:

1. Десницкий В.А., Котенко И.В. Комбинированная защита программ от несанкционированных модификаций // Изв. вузов. Приборостроение, Т.53, № 11, 2010, С.36-41. ISSN 0021-3454.
2. Котенко И.В., Коновалов А.М., Шоров А.В. Исследование бот-сетей и механизмов защиты от них на основе методов имитационного моделирования // Изв. вузов. Приборостроение, Т.53, № 11, 2010, С.42-45. ISSN 0021-3454.
3. Чечулин А.А., Котенко И.В. Комбинирование механизмов защиты от сканирования в компьютерных сетях // Информационно-управляющие системы, 2010, № 12, С.21-27. ISSN 1684-8853.

4. Десницкий В.А., Котенко И.В. Защищенность и масштабируемость механизма защиты программного обеспечения на основе принципа удаленного доверия // Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). М., 2010.
5. Kotenko I. Agent-Based Modelling and Simulation of Network Cyber-Attacks and Cooperative Defence Mechanisms // Discrete Event Simulations. Rijeka: InTech. 2010. P.223-246. ISBN 978-307-115-2.
6. Komashinskiy D., Kotenko I. Malware Detection by Data Mining Techniques Based on Positionally Dependent Features // Proceedings of the 18th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2010). Pisa, Italy, 17-19 February, 2010. Los Alamitos, California. IEEE Computer Society. 2010. P.617-623. ISSN 1066-6192. ISBN 978-0-7695-3939-3.
7. Kotenko I., Konovalov A., Shorov A. Agent-based Modeling and Simulation of Botnets and Botnet Defense // Conference on Cyber Conflict. Proceedings 2010. CCD COE Publications. Tallinn, Estonia, June 15-18, 2010. P.21-44. ISBN 978-9949-9040-1-3.
8. Kotenko I., Scormin V. (Eds.) Computer Network Security. Lecture Notes in Computer Science, Springer-Verlag, Vol. 6258. The Fifth International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-2010). September 8-10, 2010, St. Petersburg, Russia. 346 p. ISSN 0302-974.
9. Saenko I., Kotenko I. Genetic Optimization of Access Control Schemes in Virtual Local Area Networks // Computer Network Security. Lecture Notes in Computer Science, Springer-Verlag, Vol. 6258. The Fifth International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-2010). September 8-10, 2010, St. Petersburg, Russia. P.209-216. ISSN 0302-9743
10. Desnitsky V., Kotenko I. Security and Scalability of Remote Entrusting Protection // Lecture Notes in Computer Science, Springer-Verlag, Vol. 6258. The Fifth International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-2010). September 8-10, 2010, St. Petersburg, Russia. P.298-306. ISSN 0302-9743
11. Kotenko I., Konovalov A., Shorov A. Simulation of Botnets: Agent-based approach // Intelligent Distributed Computing IV. Studies in Computational Intelligence. Springer-Verlag, Vol.315. Proceedings of 4th International Symposium on Intelligent Distributed Computing – IDC 2010. September 16-18, 2010. Tangier, Morocco. Springer. P. 247–252.
12. Комашинский Д.В., Котенко И.В. Концептуальные основы использования методов Data Mining для обнаружения вредоносного программного обеспечения // Защита информации. Инсайд, 2010. № 2, С.74-82.
13. Котенко И.В., Коновалов А.М., Шоров А.В. Агентно-ориентированное моделирование функционирования бот-сетей и механизмов защиты от них // Защита информации. Инсайд, 2010. № 4, С.36-45. № 5, С.56-61.
14. Котенко И.В., Саенко И.Б., Юсупов Р.М. Международная конференция «Математические модели, методы и архитектуры для защиты компьютерных сетей» // Защита информации. Инсайд, 2010. № 6, С.16-18.
15. Комашинский Д.В., Котенко И.В., Шоров А.В. Подход к обнаружению вредоносного программного обеспечения на основе позиционно-зависимой информации // Труды СПИИРАН, Выпуск 10. СПб.: Наука, 2010. С.144-159. ISBN 978-5-02-025507-4.
16. Котенко И.В., Коновалов А.М., Шоров А.В. Моделирование функционирования команд интеллектуальных агентов бот-сетей и систем защиты // Двенадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2010 (20-24 сентября 2010 г., г. Тверь, Россия): Труды конференции. Т. 3. – М.: Физматлит, 2010. С. 44-51. ISBN 978-5-7995-0543-1.
17. Десницкий В.А., Котенко И.В. Разработка и анализ протокола удаленного доверия // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Труды конференции. СПб., 2010. С.121-129. ISBN 978-5-904031-95-4.
18. Десницкий В.А., Котенко И.В. Защита программного обеспечения на основе принципа удаленного доверия // Пятая международная научная конференция по проблемам безопасности и противодействия терроризму. МГУ. 29-30 октября 2009 г. Том 2. Материалы Восьмой общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2009). Москва, Издательство МЦНМО, 2010. С.159-163. ISBN 978-5-94057-693-8.
19. Комашинский Д.В., Котенко И.В. Обнаружение malware на основе обработки статической позиционной информации методами Data Mining // Пятая международная научная конференция по проблемам безопасности и противодействия терроризму. МГУ. 29-30 октября 2009 г. Том 2. Материалы Восьмой общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2009). Москва, Издательство МЦНМО, 2010. С.136-140. ISBN 978-5-94057-693-8.
20. Комашинский Д.В., Котенко И.В. Комбинирование методов Data Mining для статического детектирования Malware // Двенадцатая Международная конференция "РусКрипто'2010". Московская область, г.Звенигород, 1-4 апреля 2010 г. http://www.ruscrypto.ru/
21. Чечулин А.А. Защита от сетевых атак на основе комбинированных механизмов анализа трафика // Двенадцатая Международная конференция "РусКрипто'2010". Московская область, г.Звенигород, 1-4 апреля 2010 г. http://www.ruscrypto.ru/
22. Зозуля Ю.В., Котенко И.В. Блокирование Web-сайтов с неприемлемым содержанием на основании выявления их категорий // Двенадцатая Международная конференция "РусКрипто'2010". Московская область, г.Звенигород, 1-4 апреля 2010 г. http://www.ruscrypto.ru/
23. Коновалов А.М., Шоров А.В., Котенко И.В. Агентно-ориентированное моделирование бот-сетей // Двенадцатая Международная конференция "РусКрипто'2010". Московская область, г.Звенигород, 1-4 апреля 2010 г. http://www.ruscrypto.ru/
24. Котенко И.В. Исследование бот-сетей и механизмов защиты от них на основе агентно-ориентированного

моделирования // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.40-41.
25. Десницкий В.А., Котенко И.В. Комбинированные механизмы защиты программ от несанкционированных модификаций // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.100-101.
26. Коновалов А.М., Котенко И.В., Шоров А.В. Среда моделирования для имитации сетевых атак и механизмов защиты // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.38-39.
27. Степашкин М.В., Котенко И.В., Чечулин А.А., Тулупьев А.Л., Тулупьева Т.В., Пащенко А.Е. Подход к анализу защищенности автоматизированных систем с учетом социо-инженерных атак // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.128-129.
28. Котенко И.В., Степашкин М.В., Чечулин А.А., Дойникова Е.В., Котенко Д.И. Инструментальные средства анализа защищенности автоматизированных систем // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.115-116.
29. Чечулин А.А. Интеграция механизмов защиты от сканирования и выбор их оптимальных параметров // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.25-26.
30. Десницкий В.А. Методика поиска оптимальной комбинации методов защиты для защиты программ от вмешательств // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.9-10.
31. Комашинский Д.В. Комбинирование методов интеллектуального анализа данных для детектирования вредоносных программ // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.112-113.
32. Шоров А.В. Моделировании стадии формирования и сдерживания распространения бот-сети // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С.50-51.
33. Десницкий В.А., Чечулин А.А., Котенко И.В. Конфигурационная модель встроенных систем // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.41-42. ISBN 978-5-904031-99-2.
34. Коновалов А.М., Котенко И.В. Библиотека модулей для моделирования бот-сетей // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.110-111. ISBN 978-5-904031-99-2.
35. Десницкий В.А., Чечулин А.А. Абстрактная модель встроенных систем // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.40-41. ISBN 978-5-904031-99-2.
36. Дойникова Е.В. Подходы к оценке рисков на основе графов атак // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.99-100. ISBN 978-5-904031-99-2.
37. Дойникова Е.В. Использование нечетких множеств для оценки рисков на основе графов атак // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.100. ISBN 978-5-904031-99-2.
38. Комашинский Д.В. Вредоносные программы: анализ метаданных средствами Data Mining // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.109-110. ISBN 978-5-904031-99-2.
39. Котенко Д.И. Анализ существующих подходов к построению графов атак и обеспечения их масштабируемости для корпоративных сетей // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.113-114. ISBN 978-5-904031-99-2.
40. Чечулин А.А. Интеграция механизмов обнаружения вредоносного трафика // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.149. ISBN 978-5-904031-99-2.
41. Чечулин А.А., Десницкий В.А., Степашкин М.В. Модель нарушителя в задаче обеспечения безопасности встроенных систем // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.150. ISBN 978-5-904031-99-2.
42. Шоров А.В. Анализ DDOS-Атак и механизмов защиты от них и требования к их моделированию // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010").

Материалы конференции. СПб., 2010. С.152. ISBN 978-5-904031-99-2.
43. Шоров А.В. Анализ биоинспирированных подходов в области защиты компьютерных систем // XII Санкт-Петербургская Международная Конференция "Региональная информатика-2010" ("РИ-2010"). Материалы конференции. СПб., 2010. С.151. ISBN 978-5-904031-99-2.
48. Котенко И.В., Саенко И.Б., Юсупов Р.М. Аналитический обзор докладов Международной конференции "Математические модели, методы и архитектуры для защиты компьютерных сетей" (MMM-ACNS-2010) // Труды СПИИРАН, Выпуск 12. СПб.: Наука, 2010. С.199–225.
49. Котенко И.В., Саенко И.Б., Юсупов Р.М. Аналитический обзор докладов Международного семинара "Научный анализ и поддержка политик безопасности в киберпространстве" (SA&PS4CS 2010) // Труды СПИИРАН, Выпуск 10. СПб.: Наука, 2012. С.226–248.

Публикации за 2-й год:
1. Котенко И.В., Саенко И.Б., Юсупов Р.М. Защита информационных ресурсов в компьютерных сетях // Вестник РАН, Москва: Издательство Наука. том 81, № 8, Август 2011. С.746-747. ISSN 0869-5873.
2. Котенко И.В., Саенко И.Б., Юсупов Р.М. Научный анализ и поддержка политик безопасности в киберпространстве // Вестник РАН, Москва: Издательство Наука. том 81, № 9, сентябрь 2011. С.844-845. ISSN 0869-5873.
3. Котенко И.В., Нестерук Ф.Г., Чечулин А.А. Комбинирование механизмов обнаружения сканирования в компьютерных сетях // Вопросы защиты информации, Москва: Издательство "Федеральное государственное унитарное предприятие Всероссийский научно-исследовательский институт межотраслевой информации - федеральный информационно-аналитический центр оборонной промышленности". № 3, 2011. С.30-34. ISSN 2073-2600.
4. Котенко И.В., Коновалов А.М., Шоров А.В. Агентно-ориентированное моделирование бот-сетей и механизмов защиты от них // Вопросы защиты информации, Москва: "Федеральное государственное унитарное предприятие Всероссийский научно-исследовательский институт межотраслевой информации - федеральный информационно-аналитический центр оборонной промышленности". № 3, 2011. С.24-29. ISSN 2073-2600.
5. Десницкий В.А., Чечулин А.А. Модели процесса построения безопасных встроенных систем // Системы высокой доступности, Москва: Закрытое акционерное общество "Издательство Радиотехника". № 2, 2011. С.97-101. ISSN 2072-9472.
6. Комашинский Д.В., Котенко И.В., Чечулин А.А. Категорирование веб-сайтов для блокирования веб страниц с неприемлемым содержимым // Системы высокой доступности, Москва: Закрытое акционерное общество "Издательство Радиотехника". № 2, 2011. С.102-106. ISSN 2072-9472.
7. Котенко И.В., Коновалов А.М., Шоров А.В. Моделирование бот-сетей и механизмов защиты от них // Системы высокой доступности, Москва: Закрытое акционерное общество "Издательство Радиотехника".№ 2, 2011. С.107-111. ISSN 2072-9472.
8. Саенко И.Б., Котенко И.В. Генетическая оптимизация схем ролевого доступа // Системы высокой доступности, Москва: Закрытое акционерное общество "Издательство Радиотехника". № 2, 2011. С.112-116. ISSN 2072-9472.
9. Котенко И.В, Степашкин М.В., Дойникова Е.В. Анализ защищенности автоматизированных систем с учетом социо-инженерных атак // Проблемы информационной безопасности. Компьютерные системы. СПб.: Издательство Государственного образовательного учреждения высшего профессионального образования Санкт-Петербургский государственный политехнический университет. 2011, № 3. С.40-57. ISSN 2071-8217.
10. Котенко И.В, Степашкин М.В., Котенко Д.И., Дойникова Е.В. Оценка защищенности информационных систем на основе построения деревьев социо-инженерных атак // Изв. вузов. Приборостроение, СПб.: Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. Т.54, № 12, 2011. С.5-9. ISSN 0021-3454.
11. Котенко И.В., Шоров А.В. Использование биологической метафоры для защиты компьютерных систем и сетей: предварительный анализ базовых подходов // Защита информации. Инсайд. СПб.: Издательский дом Афина, 2011. № 1, С.52-57. № 2, С.66-75.
12. Котенко И.В., Десницкий В.А., Чечулин А.А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд. СПб.: Издательский дом Афина, 2011, № 3, С.68-75.
13. Котенко И.В., Дойникова Е.В. Методы оценивания уязвимостей: использование для анализа защищенности компьютерных систем // Защита информации. Инсайд. СПб.: Издательский дом Афина, 2011, № 4, С.74-81.
14. Котенко И.В., Дойникова Е.В. Система оценки уязвимостей CVSS и ее использование для анализа защищенности компьютерных систем // Защита информации. Инсайд. СПб.: Издательский дом Афина, 2011, № 5, С.54-60.
15. Котенко И.В., Дойникова Е.В. Анализ систем оценки злоупотреблений и конфигураций (CMSS и CCSS) для унифицированного анализа защищенности компьютерных систем // Защита информации. Инсайд. СПб.: Издательский дом Афина, 2011, № 6. С.52-60.
16. Котенко И.В., Шоров А.В., Нестерук Ф.Г. Анализ биоинспирированных подходов для защиты компьютерных систем и сетей // Труды СПИИРАН. Вып.3 (18). СПб.: Наука, 2011. С.19–73. ISSN 2078-9181.
17. Котенко И.В., Коновалов А.М., Шоров А.В. Имитационное моделирование бот-сетей и механизмов защиты от них: среда моделирования и эксперименты // Труды СПИИРАН. Вып.4 (19). СПб.: Наука, 2011.

С.7–33. ISSN 2078-9181.
18. Десницкий В.А. Конфигурирование встроенных и мобильных устройств на основе решения оптимизационной задачи // Труды СПИИРАН. Вып.4 (19). СПб.: Наука, 2011. С.221-242. ISSN 2078-9181.
19. Kotenko I., Stepashkin M., Doynikova E. Security Analysis of Computer-aided Systems taking into account Social Engineering Attacks // Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2011). Ayia Napa, Cyprus, 9-11 February, 2011. Los Alamitos, California. IEEE Computer Society. 2011. P.611-618. ISSN 1066-6192.
20. Saenko I., Kotenko I. Genetic Algorithms for Role Mining Problem // Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2011). Ayia Napa, Cyprus, 9-11 February, 2011. Los Alamitos, California. IEEE Computer Society. 2011. P.646-650. ISSN 1066-6192.
21. Desnitsky V., Kotenko I., Chechulin A. An abstract model for embedded systems and intruders // Proceedings of the Work in Progress Session held in connection with the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2011). Ayia Napa, Cyprus, February 2011. SEA-Publications. SEA-SR-29. 2011. P.25-26. ISBN 978-3-902457-29-5.
22. Kotenko I.V. Cyber Security: Current State and Future Landscape. View from Russia // The Interface of Science, Technology & Security: Areas of most Concern, Now and Ahead. APCSS SEMINAR Proceedings, Honolulu, Hawaii, 4-8 October 2010. Asia-Pacific Center for Security Studies. USA. 2011.
23. Kotenko I., Polubelova O. Verification of Security Policy Filtering Rules by Model Checking // Proceedings of IEEE Fourth International Workshop on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS 2011). Prague, Czech Republic, 15-17 September 2011. P. 706-710. ISBN 978-1-4244-4882-1.
24. Kotenko I., Konovalov A., Shorov A. Simulation of botnets and protection mechanisms against them: software environment and experiments // 16th Nordic Conference on Secure IT-Systems. October 26th-28th, 2011. Tallinn, Estonia, Preproceedings, Cybernetica, 2011. P.119-126.
25. Kotenko I., Chechulin A., Doynikova E. Combining of Scanning Protection Mechanisms in GIS and Corporate Information Systems // Information Fusion and Geographic Information Systems. Proceedings of the 5th International Workshop on Information Fusion and Geographical Information Systems: Towards the Digital Ocean (IF&GIS 2011). Brest, France, May 10-11, 2011. Brest, France, 2011. Lecture Notes in Geoinformation and Cartography. Springer. 2011. P.45-58. ISSN 1863-2246.
26. Десницкий В.А., Котенко И.В., Чечулин А.А. Построение и тестирование безопасных встроенных систем // XII Санкт-Петербургская международная конференция "Региональная информатика" ("РИ-2010"). Труды конференции. Санкт-Петербург: СПОИСУ. 2011. С. 115-121.
27. Котенко И.В., Коновалов А.М., Шоров А.В. Моделирование защиты от бот-сетей в сети Интернет // XII Санкт-Петербургская международная конференция "Региональная информатика" ("РИ-2010"). Труды конференции. Санкт-Петербург: СПОИСУ. 2011. С.121-132.
28. Чечулин А.А., Котенко И.В. Комбинирование механизмов обнаружения сканирования // Девятая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2010). Москва, МГУ, 2011.
29. Десницкий В.А., Котенко И.В., Чечулин А.А. Абстрактная модель встроенных безопасных систем // Девятая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2010). Москва, МГУ, 2011.
30. Коновалов А.М., Котенко И.В., Шоров А.В. Эксперименты по исследованию бот-сетей // Девятая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2010). Москва, МГУ, 2011.
31. Чечулин А.А., Десницкий В.А. Модель нарушителя в задаче обеспечения безопасности встроенных систем // Девятая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2010). Москва, МГУ, 2011.
32. Котенко И.В. Моделирование и анализ механизмов кибербезопасности // Тринадцатая Международная конференция "РусКрипто 2011". Московская область, г.Солнечногорск, 30 марта-2 апреля 2011 г. http://www.ruscrypto.ru/
33. 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. http://www.ruscrypto.ru/
34. Комашинский Д.В., Чечулин А.А., Котенко И.В. Категорирование веб-страниц с неприемлемым содержимым // Тринадцатая Международная конференция "РусКрипто 2011". Московская область, г.Солнечногорск, 30 марта-2 апреля 2011 г. http://www.ruscrypto.ru/
35. Коновалов А.М., Шоров А.В. Моделирование противодействия бот-сетей и механизмов защиты от них // Тринадцатая Международная конференция "РусКрипто 2011". Московская область, г.Солнечногорск, 30 марта-2 апреля 2011 г. http://www.ruscrypto.ru/
36. Десницкий В.А., Чечулин А.А. Унификация процесса построения безопасных встроенных систем // Тринадцатая Международная конференция "РусКрипто 2011". Московская область, г.Солнечногорск, 30 марта-2 апреля 2011 г. http://www.ruscrypto.ru/
37. Дойникова Е.В., Котенко И.В. Расширение методики оценки информационных рисков за счет использования графов зависимостей сервисов // Методы и технические средства обеспечения безопасности информации. Материалы XX Общероссийской научно-технической конференции. 27 июня - 1 июля 2011 года. СПб.: Издательство Политехнического университета. 2011. С.131-132.

38. Дойникова Е.В., Котенко Д.И. Использование систем оценки уязвимостей для анализа защищенности компьютерных систем // Методы и технические средства обеспечения безопасности информации. Материалы XX Общероссийской научно-технической конференции. 27 июня - 1 июля 2011 года. СПб.: Издательство Политехнического университета. 2011. С.130-131.
39. Котенко И.В., Нестерук Ф.Г. Принципы создания адаптивных систем защиты информации // Методы и технические средства обеспечения безопасности информации. Материалы XX Общероссийской научно-технической конференции. 27 июня - 1 июля 2011 года. СПб.: Издательство Политехнического университета. 2011. С.32-33.
40. Саенко И. Б., Полубелова О.В., Котенко И.В. Разработка информационного хранилища системы управления информацией и событиями безопасности для гетерогенной инфраструктуры // Методы и технические средства обеспечения безопасности информации. Материалы XX Общероссийской научно-технической конференции. 27 июня - 1 июля 2011 года. СПб.: Издательство Политехнического университета. 2011. С.41-42.
41. Чечулин А.А. Применение методик комбинирования в задаче защиты от сетевого сканирования // Методы и технические средства обеспечения безопасности информации. Материалы XX Общероссийской научно-технической конференции. 27 июня - 1 июля 2011 года. СПб.: Издательство Политехнического университета. 2011. С.63-64.
42. 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. СПб.: Издательство Политехнического университета. 2011. С.34-36.
43. Десницкий В.А. Модель унифицированного процесса построения безопасных встроенных систем // Методы и технические средства обеспечения безопасности информации. Материалы XX Общероссийской научно-технической конференции. 27 июня - 1 июля 2011 года. СПб.: Издательство Политехнического университета. 2011. С.15-16.
44. Комашинский Д.В. Комбинирование методов классификации и кластеризации для детектирования и идентификации malware // Методы и технические средства обеспечения безопасности информации. Материалы XX Общероссийской научно-технической конференции. 27 июня - 1 июля 2011 года. СПб.: Издательство Политехнического университета. 2011. С.136-137.
45. Коновалов А.М. Исследование бот-сетей и распределенных механизмов защиты от них на основе имитационного моделирования // Методы и технические средства обеспечения безопасности информации. Материалы XX Общероссийской научно-технической конференции. 27 июня - 1 июля 2011 года. СПб.: Издательство Политехнического университета. 2011. С.52-53.
46. Полубелова О.В. Верификация правил фильтрации политики безопасности методом «проверки на модели» // Методы и технические средства обеспечения безопасности информации. Материалы XX Общероссийской научно-технической конференции. 27 июня - 1 июля 2011 года. СПб.: Издательство Политехнического университета. 2011. С.87-88.
47. Шоров А.В. Теоретико-множественные модели для имитационного моделирования инфраструктурных атак на компьютерные сети и механизмов защиты от них // Методы и технические средства обеспечения безопасности информации. Материалы XX Общероссийской научно-технической конференции. 27 июня - 1 июля 2011 года. Санкт-Петербург. Издательство Политехнического университета. 2011. С.64-66.
48. Шоров А.В., Котенко И.В. Теоретико-множественное представление имитационных моделей инфраструктурных атак и механизмов защиты от них // Пятая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности "Имитационное моделирование. Теория и практика (ИММОД-2011)". Санкт-Петербург, 19-21 октября 2011 г. Сборник докладов. СПб.: ОАО "Центр технологии судостроения и судоремонта". 2011. С.306-310.
49. Чечулин А.А., Котенко И.В. Анализ происходящих в реальной сети событий на основе использования системы моделирования сетевых атак // VII Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России (ИБРР-2011)". 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.97-98.
50. Десницкий В.А., Котенко И.В., Чечулин А.А. Конфигурационная модель комбинированной защиты информационных систем со встроенными устройствами // VII Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России (ИБРР-2011)". 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.69-70.
51. Дойникова Е.В., Чечулин А.А., Котенко И.В., Котенко Д.И. Расширение методики оценки информационных рисков для учета атак нулевого дня // VII Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России (ИБРР-2011)". 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.71-72.
52. 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 // VII Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России (ИБРР-2011)". 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.79-80.
53. Комашинский Д.В., Котенко И.В. Методы машинного обучения в системах противодействия киберугрозам // VII Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России (ИБРР-2011)". 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.76-77.

54. Нестерук Ф.Г., Котенко И.В. Компоненты разработки адаптивной системы защиты информации компьютерной сети // VII Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России (ИБРР-2011)". 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.84-85.
55. Саенко И. Б., Котенко И.В. Усовершенствованный генетический алгоритм для решения задачи "извлечения ролей" в RBAC-системах // VII Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России (ИБРР-2011)". 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.92-93.
56. Чечулин А.А. Кооперация механизмов обнаружения сетевого сканирования // VII Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России (ИБРР-2011)". 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.96-97.
57. Десницкий В.А. Оценка эффективности конфигурирования комбинированных механизмов защиты на основе решения оптимизационной задачи // VII Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России (ИБРР-2011)". 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.69.
58. Дойникова Е.В., Котенко Д.И. Расширение методики оценки информационных рисков за счет использования графов зависимостей сервисов // VII Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России (ИБРР-2011)". 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.70-71.
59. Комашинский Д.В. Методы машинного обучения и динамическое детектирование malware // VII Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России (ИБРР-2011)". 26-28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.75-76.
60. 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.
61. 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.
62. 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.

Публикации за 3-й год:
1. Котенко И.В., Нестерук Ф.Г., Шоров А.В. Методы защиты компьютерных сетей на основе биоинспирированных подходов // Вопросы защиты информации, Москва: Издательство "Федеральное государственное унитарное предприятие Всероссийский научно-исследовательский институт межотраслевой информации - федеральный информационно-аналитический центр оборонной промышленности". № 2, 2012. С.35-46. ISSN 2073-2600.
2. Десницкий В.А., Котенко И.В., Чечулин А.А. Конфигурирование защищенных систем со встроенными и мобильными устройствами // Вопросы защиты информации, Москва: Издательство "Федеральное государственное унитарное предприятие Всероссийский научно-исследовательский институт межотраслевой информации - федеральный информационно-аналитический центр оборонной промышленности". № 2, 2012. С.20-28. ISSN 2073-2600.
3. Комашинский Д.В., Котенко И.В. Исследование структурных особенностей вредоносных документов методами Data Mining // Информационные технологии и вычислительные системы, Москва: Издательство Института системного анализа РАН. № 2, 2012, С.76-92.
4. Комашинский Д.В., Котенко И.В. Обнаружение вредоносных документов формата PDF на основе интеллектуального анализа данных // Проблемы информационной безопасности. Компьютерные системы. СПб.: Издательство Государственного образовательного учреждения высшего профессионального образования Санкт-Петербургский государственный политехнический университет. № 1, 2012, С.19-35. ISSN 2071-8217.
5. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. СПб.: Издательство Государственного образовательного учреждения высшего профессионального образования Санкт-Петербургский государственный политехнический университет. № 2, 2012. С.57-68. ISSN 2071-8217.
6. Десницкий В.А., Котенко И.В., Чечулин А.А. Конфигурирование компонентов комбинированной защиты встроенных устройств на основе решения оптимизационной задачи // Системы высокой доступности, Москва: Закрытое акционерное общество "Издательство Радиотехника". № 2, 2012. С.50-56. ISSN 2072-9472.
7. Чечулин А.А., Котенко И.В., Десницкий В.А. Методики анализа информационных потоков для построения защищенных систем со встроенными устройствами // Системы высокой доступности, Москва: Закрытое акционерное общество "Издательство Радиотехника". № 2, 2012. С.116-122. ISSN 2072-9472.
8. Котенко И. В., Полубелова О.В., Саенко И.Б., Чечулин А.А. Применение онтологий и логического вывода

для управления информацией и событиями безопасности // Системы высокой доступности, Москва: Закрытое акционерное общество "Издательство Радиотехника". № 2, 2012. С.100-108. ISSN 2072-9472.
9. Новикова Е.С., Котенко И.В. Механизмы визуализации в SIEM-системах // Системы высокой доступности, Москва: Закрытое акционерное общество "Издательство Радиотехника". № 2, 2012. С.91-99. ISSN 2072-9472.
10. Комашинский Д.В., Котенко И.В. Метод извлечения структурных признаков для задачи обнаружения вредоносного программного обеспечения // Изв. вузов. Приборостроение, СПб.: Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. Т.55, № 11, 2012, С.58-62. ISSN 0021-3454.
11. Десницкий В.А., Котенко И.В. Модель конфигурирования защищенных и энергоэффективных встроенных устройств // Изв. вузов. Приборостроение, СПб.: Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. Т.55, № 11, 2012, С.52-57. ISSN 0021-3454.
12. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. Вып.1 (20). СПб.: Наука, 2012. С.27-56. ISSN 2078-9181.
13. Котенко Д.И., Котенко И.В., Саенко И.Б. Методы и средства моделирования распределенных атак в больших компьютерных сетях: состояние проблемы // Труды СПИИРАН. Вып.3 (22). СПб.: Наука, 2012. С.5-30. ISSN 2078-9181.
14. Котенко И.В., Шоров А.В. Имитационное моделирование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода "нервная система сети" // Труды СПИИРАН. Вып.3 (22). СПб.: Наука, 2012. С.45-70. ISSN 2078-9181.
15. Полубелова О.В., Котенко И.В. Верификация правил фильтрации с временными характеристиками методом "проверки на модели" // Труды СПИИРАН. Вып.3 (22). СПб.: Наука, 2012. С.113-138. ISSN 2078-9181.
16. Котенко И.В., Саенко И.Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. Вып.3 (22). СПб.: Наука, 2012. С.84-100. ISSN 2078-9181.
17. Новикова Е.С., Котенко И.В. Технологии визуализации для управления информацией и событиями безопасности // Труды СПИИРАН. Вып.4 (23). СПб.: Наука, 2012. С.7-29. ISSN 2078-9181.
18. Котенко Д.И., Котенко И.В., Саенко И.Б. Методика итерационного моделирования атак в больших компьютерных сетях // Труды СПИИРАН. Вып.4 (23). СПб.: Наука, 2012. С.50-79. ISSN 2078-9181.
19. Котенко И.В., Нестерук Ф.Г., Шоров А.В. Концепция адаптивной защиты информационно-телекоммуникационных систем на основе парадигм нервных и нейронных сетей // Труды СПИИРАН. Вып.4 (23). СПб.: Наука, 2012. С.100-115. ISSN 2078-9181.
20. Новикова Е.С. Проектирование новой дисциплины «Компьютерная вирусология и методы нарушения безопасности» как обновление раздела базового курса» // Известия СПбГЭТУ «ЛЭТИ». СПб.: Издательство СПбГЭТУ «ЛЭТИ»2012. № 4. С.44-48. ISSN 2071-8985.
21. Коновалов А.М., Котенко И.В., Шоров А.В. Исследование бот-сетей и механизмов защиты от них на основе имитационного моделирования // Известия РАН. Теория и системы управления, М.: МАИК "Наука/Интерпериодика". № 1, 2013, С.45-68. ISSN 0002-3388. (принято к печати).
22. Konovalov A.M., Kotenko I.V., Shorov A.V. Simulation-Based Study of Botnets and Defense Mechanisms against Them // Journal of Computer and Systems Sciences International, Vol.52, Issue 1, 2013. P.43-65. Pleiades Publishing, Ltd., ISSN 1064-2307. DOI: 10.1134/S1064230712060044. (принято к печати).
23. Полубелова О.В., Котенко И. В. Построение онтологий уязвимостей и применение логического вывода для управления информацией и событиями безопасности // Безопасность информационных технологий, М.: ВНИИПВТИ. № 1, 2013 (принято к печати).
24. Igor Kotenko and Andrey Chechulin. Attack Modeling and Security Evaluation in SIEM Systems // International Transactions on Systems Science and Applications, SIWN Press. 2013. ISSN 1751-1461. (принято к печати).
25. Igor Kotenko, Andrey Shorov, Evgenia Novikova. Simulation of Protection Mechanisms Based on "Network Nervous System" against Infrastructure Attacks // Proceedings of the 21th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013). Belfast, Northern Ireland, UK. 27th February – 1st March 2013. Los Alamitos, California. IEEE Computer Society. 2013. (принято к печати).
26. Evgenia Novikova, Igor Kotenko. Analytical Visualization Techniques for Security Information and Event Management // Proceedings of the 21th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013). Belfast, Northern Ireland, UK. 27th February - 1st March 2013. Los Alamitos, California. IEEE Computer Society. 2013. (принято к печати).
27. Igor Kotenko, Andrey Shorov, Andrey Chechulin, Evgenia Novikova. Dynamical Attack Simulation for Security Information and Event Management // Proceedings of the 6th International Workshop on Information Fusion and Geographical Information Systems: Environmental and Urban Challenges (IF&GIS' 2013). St.Petersburg, Russia, May 12-15, 2013. Lecture Notes in Geoinformation and Cartography. Berlin: Springer-Verlag. 2013. (принято к печати).
28. Igor Kotenko, Olga Polubelova, Igor Saenko. Logical Inference Framework for Security Management in Geographical Information Systems // Proceedings of the 6th International Workshop on Information Fusion and Geographical Information Systems: Environmental and Urban Challenges (IF&GIS' 2013). St.Petersburg, Russia, May 12-15, 2013. Lecture Notes in Geoinformation and Cartography. Berlin: Springer-Verlag. 2013. (принято к печати).

29. Котенко И.В., Коновалов А.М., Шоров А.В. Исследовательское моделирование бот-сетей и механизмов защиты от них // Приложение к журналу "Информационные технологии", М.: Издательство "Новые технологии", № 1, 2012, 32 с. ISSN 1684-6400.
30. Kotenko I., Konovalov A., Shorov A. Agent-based simulation of cooperative defence against botnets // Concurrency and Computation: Practice and Experience, USA: John Wiley & Sons, Ltd., Vol. 24, Issue 6, 25 April 2012. P.573-588.
31. Kotenko I., Konovalov A., Shorov A. Discrete-Event Simulation of Botnet Protection Mechanisms // Discrete Event Simulations Development and Applications. Edited by Eldin Wee Chuan Lim. Rijeka, Croatia: InTech. 2012 P.143-168. ISBN 978-953-51-0741-5.
32. Kotenko I., Leszczyna R. Software agents for network security // NATO Science for Peace and Security Series, Software Agents, Agent Systems and Their Applications, Volume 32, 2012. Edited by M.Essaaidi, M.Ganzha, and M.Paprzycki. Amsterdam, Netherlands: IOS Press. 2012. P. 260-285. ISSN: 1874-6268. ISBN-10: 1607508176. ISBN-13: 978-1607508175.
33. Leszczyna R., Kotenko I. Security and anonymity of agent systems // NATO Science for Peace and Security Series, Software Agents, Agent Systems and Their Applications, Volume 32, 2012. Edited by M.Essaaidi, M.Ganzha, and M.Paprzycki. Amsterdam, Netherlands: IOS Press. 2012. P. 157-177. ISSN: 1874-6268. ISBN-10: 1607508176. ISBN-13: 978-1607508175.
34. Saenko I., Kotenko I. Design and Performance Evaluation of Improved Genetic Algorithm for Role Mining Problem // Proceedings of the 20th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2012). Garching near Munich, Germany. February 15-17, 2012. Los Alamitos, California. IEEE Computer Society. 2012. P.269-274. ISSN 1066-6192.
35. Jose Fran. Ruiz, Rajesh Harjani, Antonio Maña, Vasily Desnitsky, Igor Kotenko, Andrey Chechulin. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components // Proceedings of the 20th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2012). Garching near Munich, Germany. February 15-17, 2012. Los Alamitos, California. IEEE Computer Society. 2012. P.261-268. ISSN 1066-6192.
36. Igor Kotenko, Andrey Chechulin and Elena Doynikova. Analytical Attack Modeling in Security Information and Event Management Systems // Proceedings of the Work in Progress Session held in connection with the 20th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2012). Garching/Munich, Germany. February 2012. SEA-Publications. SEA-SR-31. Institute for Systems Engineering and Automation, Johannes Kepler University Linz, Austria. 2012. P.27-28. ISBN 978-3-902457-31-8.
37. Igor Kotenko, Olga Polubelova and Igor Saenko. Hybrid Data Repository Development and Implementation for Security Information and Event Management // Proceedings of the Work in Progress Session held in connection with the 20th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2012). Garching near Munich, Germany. February 15-17, 2012. SEA-Publications. SEA-SR-29. 2012. P.29-30. ISBN 978-3-902457-29-5.
38. Igor Kotenko, Andrey Chechulin and Evgenia Novikova. Attack Modelling and Security Evaluation for Security Information and Event Management // SECRYPT 2012. International Conference on Security and Cryptography. Proceedings. Rome, Italy. 24-27 July 2012. Portugal: SciTePress. P.391-394. ISBN 978-989-8565-24-2.
39. Igor Kotenko, Olga Polubelova and Igor Saenko. Data Repository for Security Information and Event Management in Service Infrastructures // SECRYPT 2012. International Conference on Security and Cryptography. Proceedings. Rome, Italy. 24-27 July 2012. Portugal: SciTePress. P.308-313. ISBN 978-989-8565-24-2.
40. Igor Kotenko and Andrey Shorov. Simulation of Protection Mechanisms against Botnets on the basis of "Nervous Network" Framework // The 2nd International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH 2012). Proceedings. Rome, Italy. 28-31 July 2012. Portugal: SciTePress. P.164-169. ISBN 978-989-8565-20-4.
41. Andrey Chechulin, Igor Kotenko, and Vasily Desnitsky. A Combined Approach for Network Information Flow Analysis for Systems of Embedded Components // Lecture Notes in Computer Science, Springer-Verlag, Vol. 7531. The Sixth International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-2012). October 17-19, 2012, St. Petersburg, Russia. P.146-155.
42. Dmitry Komashinskiy and Igor Kotenko. Using Low-Level Dynamic Attributes for Malware Detection based on Data Mining Methods // Lecture Notes in Computer Science, Springer-Verlag, Vol. 7531. The Sixth International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-2012). October 17-19, 2012, St. Petersburg, Russia. P.254-269.
43. Vasily Desnitsky, Igor Kotenko, and Andrey Chechulin. Configuration-based approach to embedded device security // Lecture Notes in Computer Science, Springer-Verlag, Vol. 7531. The Sixth International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-2012). October 17-19, 2012, St. Petersburg, Russia. P.270-285.
44. Igor Kotenko and Andrey Chechulin. Common Framework for Attack Modeling and Security Evaluation in SIEM Systems // 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing. Besançon, France, November 20-23, 2012. Los Alamitos, California. IEEE Computer Society. 2012. P. 94-101. ISBN: 978-0-7695-4865-4/12. DOI 10.1109/GreenCom. 2-12.24
45. Igor Kotenko, Olga Polubelova and Igor Saenko. The Ontological Approach for SIEM Data Repository Implementation // 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing. Besançon, France, November 20-23,

2012. Los Alamitos, California. IEEE Computer Society. 2012. P. 761-766. ISBN: 978-0-7695-4865-4/12. DOI 10.1109/GreenCom. 2-12.24
46. Kotenko I.V. Cyber Wars of Intelligent Agents in the Internet // The Second International Workshop "Scientific Analysis and Policy Support for Cyber Security" (SA&PS4CS 2012). St.Petersburg, Russia, October 20, 2012. P.10.
47. Котенко И.В., Дойникова Е.В. Анализ протокола автоматизации управления данными безопасности SCAP // Защита информации. Инсайд, СПб.: Издательский дом Афина, 2012, № 2, С.56-63.
48. Котенко И.В., Дойникова Е.В., Чечулин А.А. Общее перечисление и классификация шаблонов атак (CAPEC): описание и применение // Защита информации. Инсайд, СПб.: Издательский дом Афина, 2012, № 4, С.54-66.
49. Котенко И.В., Саенко И.Б. SIEM-системы для управления информацией и событиями безопасности // Защита информации. Инсайд, СПб.: Издательский дом Афина, 2012, № 5, С.54-65.
50. Чечулин А.А., Котенко И.В. Анализ происходящих в реальной сети событий на основе использования системы моделирования сетевых атак // VII Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2011"). Труды конференции. СПб.: СПОИСУ, 2012. С. 93-98.
51. Котенко И.В., Саенко И.Б., Юсупов Р.М. Интеллектуальные сервисы защиты как инструмент кибернетического противоборства // Научно-технический сборник по проблемам информационного противоборства, Совет Безопасности Российской Федерации. Москва, 2012.
52. Котенко И.В., Шоров А.В., Нестерук Ф.Г. Анализ биоинспирированных подходов для защиты компьютерных систем и сетей // XIV Всероссийская научно-техническая конференция "Нейроинформатика-2012": Сборник научных трудов. Том 2. М.: НИЯУ МИФИ, 2012. С.61-71.
53. Котенко И.В., Чечулин А.А. Аналитическое моделирование атак для управления информацией и событиями безопасности // Труды конгресса по интеллектуальным системам и информационным технологиям "IS&IT". Россия, Краснодарский край, пос. Дивноморское. 2-9 сентября 2012. М.: Физматлит, 2012. С.385-391. ISBN 978-5-9221-1339-8.
54. Саенко И.Б., Котенко И.В. Применение генетических алгоритмов в оптимизационных задачах разграничения доступа к информации // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'12». Научное издание в 4-х томах. М.: Физматлит, 2012. Т. 1. С.40-45. ISBN 978-5-9221-1339-8.
55. Полубелова О.В., Котенко И.В., СаенкоИ.Б. Онтологический подход к построению интеллектуальных сервисов хранения и обработки событий безопасности // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'12». Научное издание в 4-х томах. М.: Физматлит, 2012. Т. 2. С.394-399. ISBN 978-5-9221-1329-8.
56. Десницкий В.А. Конфигурирование компонентов комбинированной защиты встроенных систем на основе решения оптимизационной задачи // Труды конгресса по интеллектуальным системам и информационным технологиям "IS&IT". Россия, Краснодарский край, пос. Дивноморское. 2-9 сентября 2012. М.: Физматлит, 2012. С.383-384. ISBN 978-5-9221-1339-8.
57. Котенко И.В. Кибервойны программных агентов: применение теории командной работы интеллектуальных агентов для построения киберармий // Международный форум по практической безопасности Positive Hack Days. Москва. 30-31 мая 2012 г. http://www.phdays.ru
58. Котенко И.В., Юсупов Р.М. Кибербезопасность: текущее состояние и тенденции развития // Санкт-Петербургский научный форум "Наука и общество". "Наука и прогресс человечества". VII Петербургская встреча лауреатов Нобелевской премии. Тезисы пленарных докладов. Санкт-Петербург. Издательство Политехнического университета. 2012. С.55-56.
59. Шоров А.В., Котенко И.В. Использование биоинспирированных подходов для защиты компьютерных сетей от инфраструктурных атак // Санкт-Петербургский научный форум "Наука и общество". "Наука и прогресс человечества". VII Петербургская встреча лауреатов Нобелевской премии. Тезисы секционных докладов. Санкт-Петербург. Издательство Политехнического университета. 2012. С.149-150.
60. Новикова Е.С., Чечулин А.А., Котенко И.В. Технологии визуализации для противодействия компьютерным атакам в системах управления информационной безопасностью // Санкт-Петербургский научный форум "Наука и общество". "Наука и прогресс человечества". VII Петербургская встреча лауреатов Нобелевской премии. Тезисы секционных докладов. Санкт-Петербург. Издательство Политехнического университета. 2012. С.151-152.
61. Котенко И.В. Юсупов Р.М. Текущее состояние и тенденции развития в области построения безопасных компьютерных систем // Часть 5-й Российской мультиконференции по проблемам управления (МКПУ-2012) - конференция "Информационные технологии в управлении" (ИТУ-2012). 09–11 октября 2012 г. Материалы конференции. СПб, 2012. С.671-675.
62. Десницкий В.А., Котенко И.В., Чечулин А.А. Проектирование безопасных встроенных систем в проекте европейского сообщества SecFutur // Часть 5-й Российской мультиконференции по проблемам управления (МКПУ-2012) - конференция "Информационные технологии в управлении" (ИТУ-2012). 09–11 октября 2012 г. Материалы конференции. СПб, 2012. С.699-708.
63. Чечулин А.А., Котенко И.В., Новикова Е.С., Дойникова Е.В. Моделирование атак и механизмов защиты в системах управления информацией и событиями безопасности // Часть 5-й Российской мультиконференции по проблемам управления (МКПУ-2012) - конференция "Информационные технологии в управлении" (ИТУ-2012). 09–11 октября 2012 г. Материалы конференции. СПб, 2012. С.735-739.
64. Полубелова О.В., Саенко И.Б., Котенко И.В. Методы представления данных и логического вывода для управления информацией и событиями безопасности // Часть 5-й Российской мультиконференции по

проблемам управления (МКПУ-2012) - конференция "Информационные технологии в управлении" (ИТУ-2012). 09–11 октября 2012 г. Материалы конференции. СПб, 2012. С.723-728.
65. Котенко И.В. Аналитическое моделирование и анализ событий в системах управления информацией и событиями безопасности // Четырнадцатая Международная конференция "РусКрипто'2012". Московская область, г.Солнечногорск, 28-30 марта 2012 г. http://www.ruscrypto.ru/
66. Родригез Х.Ф.Р., Десницкий В.А. Проектирование защищенных информационно-телекоммуникационных систем со встроенными устройствами // Четырнадцатая Международная конференция "РусКрипто'2012". Московская область, г.Солнечногорск, 28-30 марта 2012 г. http://www.ruscrypto.ru/
67. Фидж К., Чечулин А.А. Анализ информационных потоков для построения защищенных систем со встроенными устройствами // Четырнадцатая Международная конференция "РусКрипто'2012". Московская область, г.Солнечногорск, 28-30 марта 2012 г. http://www.ruscrypto.ru/
68. Полубелова О.В. Применение онтологического подхода и логического вывода для управления информацией и событиями безопасности // Четырнадцатая Международная конференция "РусКрипто'2012". Московская область, г.Солнечногорск, 28-30 марта 2012 г. http://www.ruscrypto.ru/
69. Новикова Е.С. Механизмы визуализации в SIEM-системах // Четырнадцатая Международная конференция "РусКрипто'2012". Московская область, г.Солнечногорск, 28-30 марта 2012 г. http://www.ruscrypto.ru/
70. Десницкий В.А., Котенко И.В. Конфигурирование информационно-телекоммуникационных систем со встроенными устройствами // Методы и технические средства обеспечения безопасности информации. Материалы XXI Общероссийской научно-технической конференции. 24 - 29 июня 2012 года. Санкт-Петербург. Издательство Политехнического университета. 2012. С.14-17.
71. Дойникова Е.В., Котенко Д.И., Котенко И.В. Реагирование на компьютерные вторжения с использованием графов атак и графов зависимостей сервисов // Методы и технические средства обеспечения безопасности информации. Материалы XXI Общероссийской научно-технической конференции. 24 - 29 июня 2012 года. Санкт-Петербург. Издательство Политехнического университета. 2012. С.45-47.
72. Котенко И.В., Чечулин А.А. Аналитическое моделирование атак в системах управления информацией и событиями безопасности // Методы и технические средства обеспечения безопасности информации. Материалы XXI Общероссийской научно-технической конференции. 24 - 29 июня 2012 года. Санкт-Петербург. Издательство Политехнического университета. 2012. С.57-58.
73. Нестерук Ф.Г., Котенко И.В. Формирование нечеткой базы знаний для адаптивных систем защиты информации // Методы и технические средства обеспечения безопасности информации. Материалы XXI Общероссийской научно-технической конференции. 24 - 29 июня 2012 года. Санкт-Петербург. Издательство Политехнического университета. 2012. С.64-65.
74. Саенко И.Б., Котенко И.В., Полубелова О.В. Применение онтологического подхода для построения модели уязвимостей на основе стандарта SCAP // Методы и технические средства обеспечения безопасности информации. Материалы XXI Общероссийской научно-технической конференции. 24 - 29 июня 2012 года. Санкт-Петербург. Издательство Политехнического университета. 2012. С.74-76.
75. Чечулин А.А. Десницкий В.А., Котенко И.В. Анализ информационных потоков для построения защищенных систем со встроенными устройствами // Методы и технические средства обеспечения безопасности информации. Материалы XXI Общероссийской научно-технической конференции. 24 - 29 июня 2012 года. Санкт-Петербург. Издательство Политехнического университета. 2012. С.35-37.
76. Десницкий В.А., Чечулин А.А. Анализ несовместимостей компонентов защиты в процессе проектирования безопасных встроенных устройств // Методы и технические средства обеспечения безопасности информации. Материалы XXI Общероссийской научно-технической конференции. 24 - 29 июня 2012 года. Санкт-Петербург. Издательство Политехнического университета. 2012. С.17-19.
77. Десницкий В.А. Моделирование нефункциональных свойств защиты в процессе конфигурирования безопасных встроенных устройств // Методы и технические средства обеспечения безопасности информации. Материалы XXI Общероссийской научно-технической конференции. 24 - 29 июня 2012 года. Санкт-Петербург. Издательство Политехнического университета. 2012. С.12-14.
78. Комашинский Д.В. Системы детектирования malware на основе Data Mining и методы повышения их точности // Методы и технические средства обеспечения безопасности информации. Материалы XXI Общероссийской научно-технической конференции. 24 - 29 июня 2012 года. Санкт-Петербург. Издательство Политехнического университета. 2012. С.159-160.
79. Новикова Е.С. Механизмы визуализации графов атак // Методы и технические средства обеспечения безопасности информации. Материалы XXI Общероссийской научно-технической конференции. 24 - 29 июня 2012 года. Санкт-Петербург. Издательство Политехнического университета. 2012. С.69-70.
80. Чечулин А.А. Методика оценки эффективности применения комбинированной защиты от сетевого сканирования // Методы и технические средства обеспечения безопасности информации. Материалы XXI Общероссийской научно-технической конференции. 24 - 29 июня 2012 года. Санкт-Петербург. Издательство Политехнического университета. 2012. С.79-81.
81. Шоров А.В. Защита от атак на инфраструктуру компьютерных сетей на основе подхода "нервная система сети" // Методы и технические средства обеспечения безопасности информации. Материалы XXI Общероссийской научно-технической конференции. 24 - 29 июня 2012 года. Санкт-Петербург. Издательство Политехнического университета. 2012. С.81-82.
82. Десницкий В.А. Анализ подходов к построению anytime-алгоритмов для решения вычислительно сложных задач // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-

2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С.90.
83. Десницкий В.А. Конфигурирование безопасных встроенных устройств на основе нефункциональных свойств защиты // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С.91.
84. Десницкий В.А., Чечулин А.А. Анализ несовместимости компонентов защиты встроенных устройств // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С.93.
85. Десницкий В.А., Чечулин А.А., Котенко И.В. Использование anytime-алгоритмов для моделирования атак и оценки защищенности в siem-системах // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С.92.
86. Дойникова Е.В., Котенко И.В. Комплексный подход к формированию системы показателей защищенности для оценки рисков и реагирования на компьютерные вторжения // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С.94.
87. Котенко И.В., Нестерук Ф.Г. О разработке адаптивной системы защиты информации компьютерных сетей // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С.102.
88. Нестерук Ф.Г. Методика разработки адаптивной системы защиты информации // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С.113.
89. Нестерук Ф.Г. О важных задачах обеспечения адаптивной безопасности систем ИТ // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С. 112.
90. Новикова Е.С. Техники визуального анализа защищенности компьютерных сетей // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С.114.
91. Новикова Е.С. Проектирование подсистемы визуализации для системы управления событиями безопасности и информации // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С.115.
92. Полубелова О.В. Применение линейной темпоральной логики для верификации правил фильтрации политики безопасности методом «проверки на модели» // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С.121.
93. Чечулин А.А., Котенко И.В. Построение графов атак на основе моделей нарушителей и данных об уязвимостях и шаблонах атак // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С. 129.
94. Чечулин А.А. Распознавание цели нарушителя на основе анализа событий безопасности и графов атак // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С.130.
95. Чечулин А.А., Десницкий В.А. Анализ сетевых информационных потоков в задаче анализа встроенных систем // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С. 129.
96. Шоров А.В. Использование биоинспирированного подхода «нервная система сети» для защиты компьютерных сетей от инфраструктурных атак // XIII Санкт-Петербургская Международная Конференция "Региональная информатика-2012" ("РИ-2012"). Материалы конференции. СПб.: СПОИСУ, 2012. С.132.

3.17. *Приоритетное направление развития науки, технологий и техники РФ, которому, по мнению исполнителей, соответствуют результаты данного проекта*информационно-телекоммуникационные системы

3.18. *Критическая технология РФ, в которой, по мнению исполнителей, соответствуют результаты данного проекта*Технологии и программное обеспечение распределенных и высокопроизводительных вычислительных систем

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

Подпись руководителя проекта