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 **01-201 01-202 01-217**
ВИД КОНКУРСА **а - Инициативные проекты**		
ФАМИЛИЯ, ИМЯ, ОТЧЕСТВО РУКОВОДИТЕЛЯ ПРОЕКТА **Котенко Игорь Витальевич**		ТЕЛЕФОН РУКОВОДИТЕЛЯ ПРОЕКТА **(812)3282642**
ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ, ГДЕ ВЫПОЛНЯЕТСЯ ПРОЕКТ **Учреждение Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН**		
ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ, ЧЕРЕЗ КОТОРУЮ ОСУЩЕСТВЛЯЕТСЯ ФИНАНСИРОВАНИЕ **Учреждение Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН**		
ЧИСЛО УЧАСТНИКОВ ПРОЕКТА (включая руководителя) **10**	ЧИСЛО УЧАСТНИКОВ, ИМЕЮЩИХ УЧЕНУЮ СТЕПЕНЬ **2**	ЧИСЛО МОЛОДЫХ (до 35 лет включительно) УЧАСТНИКОВ **9**
Десницкий Василий Алексеевич		
Дойникова Елена Владимировна		
Комашинский Дмитрий Владимирович		
Коновалов Алексей Михайлович		
Котенко Дмитрий Игоревич		
Полубелова Ольга Витальевна		
Степашкин Михаил Викторович		
Шоров Андрей Владимирович		
Чечулин Андрей Алексеевич		

ОТЧЕТ ЗА 2011 ГОД ПО ПРОЕКТУ РФФИ 10-01-00826-а

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
2012

1.6. Вид отчета
этап 2011 года

1.7. Аннотация
Разработаны 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). Предложены формальные модели и программные прототипы компонентов автоматического обнаружения и реагирования против сетевых атак на основе комбинированного анализа сетевого трафика. Предложены формальные модели и программные прототипы компонентов детектирования вредоносного программного обеспечения на основе методов интеллектуального анализа данных. Разработаны формальные модели и программные прототипы компонентов анализа защищенности и оценки рисков безопасности ресурсов компьютерных сетей и систем. Разработаны формальные модели безопасности встроенных систем. Проведена теоретическая и экспериментальная оценка предложенных моделей и методов комплексной защиты.

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

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

Подпись руководителя проекта

Форма 502. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ НА АНГЛИЙСКОМ ЯЗЫКЕ

2.1. Номер проекта 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
2012

2.5. Вид отчета
этап 2011 года

2.6. Аннотация

The 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) were developed. We proposed the formal models and software prototypes of components to automatically detect and respond against network attacks based on combined analysis of network traffic. The formal models and software prototypes of components for detection of malicious software on the basis of data mining methods were suggested. We developed the formal models and software prototypes of components for security analysis and security risk assessment of computer network and system resources. The formal models of security of embedded systems were also proposed. We carried out the theoretical and experimental evaluation of the proposed models and methods of integrated protection.

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

Подпись руководителя проекта

Форма 503. РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1. Номер проекта
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
01-201 01-202 01-217

3.4. Объявленные ранее цели проекта на 2011 год

Основными целями проекта на 2011 год являлись:

(1) разработка 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) разработка формальных моделей и программных прототипов компонентов автоматического обнаружения и реагирования против сетевых атак на основе комбинированного анализа сетевого трафика;

(3) разработка формальных моделей и программных прототипов компонентов детектирования вредоносного программного обеспечения на основе методов интеллектуального анализа данных;

(4) разработка формальных моделей и программных прототипов компонентов анализа защищенности и оценки рисков безопасности ресурсов компьютерных сетей и систем;

(5) разработка формальных моделей безопасности встроенных систем;

(6) теоретическая и экспериментальная оценка предложенных моделей и методов комплексной защиты.

3.5. Степень выполнения поставленных в проекте задач
Все задачи, запланированные в проекте на второй год, выполнены полностью.

3.6. Полученные за отчетный период важнейшие результаты

Важнейшие результаты, полученные за отчетный период, таковы:

1. Разработаны 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). В результате работы на втором этапе 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.

2. Разработаны 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.

3. Разработаны 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.

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.

4. Разработаны 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. Модель анализируемой КС расширена за счет добавления таких атакуемых нарушителем объектам как автоматизированное рабочее место (хост КС), коммутаторы второго и третьего уровней и т.п., объектов типа «санкционированный пользователь» и «информационный блок». Санкционированные пользователи имеют физический доступ в контролируемую зону, обладают заданными правами на доступ к техническим средствам и к блокам информации, обрабатываемым в ней.

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. Для описания атак используются предусловия и постусловия. Предусловия атак определяются с использованием основных положений теорий человеческих потребностей (А. Маслоу, К. Альдерфер и др.). В качестве постусловий определены:

а) получение нарушителем сведений, доступных санкционированному пользователю (сведений о структуре система, данные аутентификации и т.п.);

б) получение нарушителем возможности выполнения атак, требующих физического доступа в контролируемую зону;

в) возможность выполнения атак, требующих взаимодействия с пользователем и др.

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.

5. Разработаны формальные модели безопасности 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 широкому кругу 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.

6. Проведена теоретическая и экспериментальная оценка предложенных

моделей и методов комплексной защиты.

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. 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.

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 второго года проекта, соответствуют мировому уровню. Авторы проекта опубликовали полученные результаты в нескольких рецензируемых журналах, сборниках и трудах конференций, а также апробировали результаты на множестве различных российских и международных конференций, в частности, на 19-я Европейской (Euromicro) международной конференции по параллельной, распределенной и сетевой обработке информации (PDP 2011, Айа-Напа, Кипр, 9-11 февраля 2011 г.), Тринадцатой конференции «РусКрипто 2011» по криптологии, стеганографии, цифровой подписи и системам защиты информации (Московская область, г.Солнечногорск, 30 марта – 2 апреля 2011 г.), Международном семинаре «Интеграция информации и ГИС: к цифровому океану» (IF&GIS-2011, Брест, Франция, 10-11 мая 2011 г.), Международном семинаре EffectsPlus по координации проектов Европейского Сообщества (г. Амстердам, Голландия. 4-5 июля 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.), XX Общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (МТСОБИ 2011, 27 июня - 1 июля 2011 года, Санкт-Петербург), 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.) 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 и др.

3.10.1.1. Количество научных работ, опубликованных в ходе выполнения проекта
115

3.10.1.2. Из них включенных в перечень ВАК
20

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)
49

3.10.2. Количество научных работ, подготовленных в ходе выполнения проекта и принятых к печати в 2011 г.
9

3.11. Участие в научных мероприятиях по тематике проекта, которые проводились при финансовой поддержке Фонда
4

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

3.13. Финансовые средства, полученные от РФФИ

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

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

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. Sciyo, In-teh. 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. Моделирование 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.
44. 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.
45. 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, том 81, № 8, Август 2011. С.746-747.

Москва: Издательство Наука. ISSN 0869-5873.

2. Котенко И.В., Саенко И.Б., Юсупов Р.М. Научный анализ и поддержка политик безопасности в киберпространстве // Вестник РАН, том 81, № 9, сентябрь 2011. С.844-845. Москва: Издательство Наука. ISSN 0869-5873.

3. Котенко И.В., Нестерук Ф.Г., Чечулин А.А. Комбинирование механизмов обнаружения сканирования в компьютерных сетях // Вопросы защиты информации, № 3 (94), 2011. С.30-34. Москва: Издательство "Федеральное государственное унитарное предприятие Всероссийский научно-исследовательский институт межотраслевой информации - федеральный информационно-аналитический центр оборонной промышленности". 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, № 3 (94), 2011. С.24-29. Москва: "Федеральное государственное унитарное предприятие Всероссийский научно-исследовательский институт межотраслевой информации - федеральный информационно-аналитический центр оборонной промышленности". ISSN 2073-2600.

5. Десницкий В.А., Чечулин А.А. Модели процесса построения безопасных встроенных систем // Системы высокой доступности, № 2, 2011. С.97-101. Москва: Закрытое акционерное общество "Издательство Радиотехника". 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, № 2, 2011. С.102-106. Москва: Закрытое акционерное общество "Издательство Радиотехника". ISSN 2072-9472.

7. Котенко И.В., Коновалов А.М., Шоров А.В. Моделирование бот-сетей и механизмов защиты от них // Системы высокой доступности, № 2, 2011. С.107-111. Москва: Закрытое акционерное общество "Издательство Радиотехника". ISSN 2072-9472.

8. Саенко И.Б., Котенко И.В. Генетическая оптимизация схем ролевого доступа // Системы высокой доступности, № 2, 2011. С.112-116. Москва: Закрытое акционерное общество "Издательство Радиотехника". 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. 2011, № 3. С.40-57. СПб.: Издательство Государственного образовательного учреждения высшего профессионального образования Санкт-Петербургский государственный политехнический университет. 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, Т.54, № 12, 2011. С.5-9. СПб.: Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. 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. ISSN 2078-9181. (принято к печати).

18. Десницкий В.А. Конфигурирование встроенных и мобильных устройств на основе решения оптимизационной задачи // Труды СПИИРАН. Вып.4 (19). СПб.: Наука, 2011. ISSN 2078-9181. (принято к печати).

19. Котенко И.В., Коновалов А.М., Шоров А.В. Исследовательское моделирование бот-сетей и механизмов защиты от них // Приложение к журналу "Информационные технологии", Москва: Издательство "Новые технологии". № 1, 2012 . ISSN 1684-6400. (принято к печати).

20. Kotenko I., Konovalov A., Shorov A. Agent-based simulation of cooperative defence against botnets // Concurrency and Computation: Practice Experience. John Wiley Sons, 2011. Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/cpe.1858. ISSN 1532-0634.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. Kotenko I., Leszczyna R. Software agents for network security // NATO Science for Peace and Security Series. Software Agents, Agent Systems and Their Applications, 2011. Edited by M.Essaaidi, M.Ganzha, and M.Paprzycki. IOS Press. 2012. P.260-284. ISSN 1874-6268. (принято к печати).

29. Leszczyna R., Kotenko I. Security and anonymity of agent systems // NATO Science for Peace and Security Series, Software Agents, Agent Systems and Their

Applications, 2011. Edited by M.Essaaidi, M.Ganzha, and M.Paprzycki. IOS Press. 2012. P.157-177. ISSN 1874-6268. (принято к печати).

30. 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. ISSN 1066-6192. (принято к печати).

31. Jose Fran. Ruiz, Rajesh Harjani, Antonio Mana, 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. ISSN 1066-6192. (принято к печати).

32. 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 near Munich, Germany. February 15-17, 2012. SEA-Publications. 2012. ISBN 978-3-902457-29-5. (принято к печати).

33. 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. 2012. ISBN 978-3-902457-29-5. (принято к печати).

34. 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.

35. 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.

36. Чечулин А.А., Котенко И.В. Комбинирование механизмов обнаружения сканирования // Девятая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2010). Москва, МГУ, 2011.

37. 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.

38. 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.

39. 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.

40. 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/

41. 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/

42. 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/

43. 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/

44. 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/

45. 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. Санкт-Петербург. Издательство Политехнического университета. 2011. С.131-132.

46. 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. Санкт-Петербург. Издательство Политехнического университета. 2011. С.130-131.

47. 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. Санкт-Петербург. Издательство Политехнического университета. 2011. С.32-33.

48. 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. Санкт-Петербург. Издательство Политехнического университета. 2011. С.41-42.

49. 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. Санкт-Петербург. Издательство Политехнического университета. 2011. С.63-64.

50. Морозов И.В., Чечулин А.А. Разграничение доступа к информации в геоинформационных системах // Методы и технические средства обеспечения безопасности информации. Материалы Юбилейной 20-й научно-технической конференции. 27 июня - 01 июля 2011 года. Санкт-Петербург. Издательство Политехнического университета. 2011. С.34-36.

51. 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. Санкт-Петербург. Издательство Политехнического университета. 2011. С.15-16.

52. 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. Санкт-Петербург. Издательство Политехнического университета. 2011. С.136-137.

53. 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. Санкт-Петербург. Издательство Политехнического университета. 2011. С.52-53.

54. 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. Санкт-Петербург. Издательство Политехнического университета. 2011. С.87-88.

55. 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.

56. 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.

57. 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.

58. 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.

59. 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.

60. 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.

61. 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.

62. 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.

63. 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.

64. 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.

65. 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.

66. 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.

67. 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.

68. 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.

69. 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.

70. 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.

3.17. Приоритетное направление развития науки, технологий и техники РФ, в котором, по мнению исполнителей, могут быть использованы результаты данного проекта

информационно-телекоммуникационные системы

3.18. Критическая технология РФ, в которой, по мнению исполнителей, могут быть использованы результаты данного проекта

Технологии и программное обеспечение распределенных и высокопроизводительных вычислительных систем

3.19. Основное направление технологической модернизации экономики России, в котором, по мнению исполнителей, могут быть использованы результаты завершенного проекта

Стратегические информационные технологии, включая вопросы создания суперкомпьютеров и разработки программного обеспечения

Подпись руководителя проекта

Форма 510. ЗАЯВКА НА 2012 г.

10.1. Номер проекта 10-01-00826

10.2.1. Основной код классификатора 01-217

10.2.2. Дополнительные коды классификатора 01-201 01-202

10.3. Ключевые слова защита информации, компьютерные сети, моделирование процессов защиты информации, распределенные скоординированные атаки на компьютерные сети, обнаружение вредоносного программного обеспечения, интеллектуальный анализ данных, распределенный искусственный интеллект, адаптивное поведение, анализ защищенности, мониторинг политик безопасности

10.4. Цели очередного годичного этапа, связь с основной задачей проекта

Основными целями очередного годичного этапа является 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.

10.5. Ожидаемые в конце 2012 г. научные результаты

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.

10.6. Общий объем финансирования на 2012 год 700000

10.7.1. Сроки проведения в 2012 г. экспедиции по тематике проекта

10.7.2. Ориентировочная стоимость экспедиции (в руб.)

10.7.3. Регион проведения экспедиции

10.7.4. Название района проведения экспедиции

10.8. Планируемая численность участников проекта в 2012 году

Десницкий Василий Алексеевич, Дойникова Елена Владимировна, Комашинский Дмитрий Владимирович, Коновалов Алексей Михайлович, Котенко Дмитрий Игоревич, Степашкин Михаил Викторович, Полубелова Ольга Витальевна, Чечулин Андрей Алексеевич, Шоров Андрей Владимирович

Подпись руководителя проекта