<table>
<tr><td colspan="2">НОМЕР ПРОЕКТА
07-01-00547</td><td>Учетная карточка проекта (заполняется в РФФИ)</td></tr>
<tr><td colspan="2">НАЗВАНИЕ ПРОЕКТА
Модели и методы построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации, основывающиеся на моделировании поведения систем защиты, реализации верифицированных политик безопасности, оценке защищенности и проактивном мониторинге</td><td></td></tr>
<tr><td>ОБЛАСТЬ ЗНАНИЯ
(цифровой код)
01</td><td rowspan="2">КОД(Ы) КЛАССИФИКАТОРА
(должны соответствовать п. 3.3 формы 503).
01-201, 01-202, 01-217</td><td></td></tr>
<tr><td>ВИД КОНКУРСА (а, б, в, г, д ...) а</td><td></td></tr>
<tr><td colspan="2">ФАМИЛИЯ, ИМЯ, ОТЧЕСТВО РУКОВОДИТЕЛЯ ПРОЕКТА (полностью)
Котенко Игорь Витальевич</td><td>ТЕЛЕФОН РУКОВОДИТЕЛЯ ПРОЕКТА (код города – в скобках)
(812) 3282642</td></tr>
<tr><td colspan="3">ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ, ГДЕ ВЫПОЛНЯЕТСЯ ПРОЕКТ
Санкт-Петербургский институт информатики и автоматизации РАН</td></tr>
</table>

ОТЧЕТ ЗА 2007 ГОД ПО ПРОЕКТУ РФФИ 07-01-00547-а

Статус отчета: подписан

Дата подписания: 10.01.2008

Подписал: Котенко Игорь Витальевич

Отчет распечатан: 10.01.2008

Форма 501. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ

1.1. Номер проекта
07-01-00547

1.2. Руководитель проекта
Котенко Игорь Витальевич

1.3. Название проекта
Модели и методы построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации, основывающиеся на моделировании поведения систем защиты, реализации верифицированных политик безопасности, оценке защищенности и проактивном мониторинге

1.4. Вид конкурса
а - Инициативные проекты

1.5. Год представления отчета
2008

1.6. Вид отчета
этап 2007 года

1.7. Аннотация
Проведен анализ состояния исследований в указанной предметной области. Разработаны формальная постановка задачи исследования и основные требования к компонентам, реализующим интеллектуальные механизмы защиты и поддержку жизненного цикла распределенных защищенных компьютерных систем. Разработаны принципы построения, структура и фрагмент основанной на онтологии, распределенной базы знаний для интеллектуальных механизмов защиты, а также среды поддержки жизненного цикла распределенных защищенных компьютерных систем. Разработаны формальные модели отдельных компонентов интеллектуальных механизмов защиты и среды поддержки жизненного цикла распределенных защищенных компьютерных систем, в частности спецификации политик безопасности и конфигурации защищаемой системы (сети), верификации политик безопасности, определения уровня безопасности и мониторинга выполнения политики безопасности. Выполнена первоначальная экспериментальная оценка полученных результатов с помощью создания исследовательских прототипов и компьютерного моделирования. Решен также ряд дополнительных задач: разработка общего подхода к верификации политики безопасности; совершенствование моделей компьютерных атак и нарушителя; разработка автоматизированной методики детального анализа защищенности компьютерных сетей; разработка моделей и программного прототипа системы проактивного мониторинга выполнения политики безопасности в компьютерных сетях и др.

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

"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
07-01-00547

2.2. Руководитель проекта
Kotenko Igor Vitalevich

2.3. Название проекта
Models and methods of construction and functioning support of intelligent adaptive security systems based on modeling and simulation of security systems behavior, realization of verified security policies, security evaluation and proactive monitoring

2.4. Год представления отчета
2008

2.5. Вид отчета
этап 2007 года

2.6. Аннотация
The state of the art in the specified subject domain was analyzed. The formal statement of the research problem and the basic requirements to the components realizing the intelligent security mechanisms and the life cycle support of distributed protected computer systems were offered. The principles of construction, structure and a fragment of the distributed knowledge base for intelligent security mechanisms based on subject domain ontology, and the life cycle support environment of distributed protected computer systems are developed. The formal models of particular components of intelligent security mechanisms and the life cycle support environment of distributed protected computer systems are developed. In particular, the components for the specification of security policies and protected system (network) configuration, security policy verification, determination of security level and monitoring of security policy performance are suggested. The initial experimental evaluation of the developed results was executed by creating the research prototypes and computer simulation. A number of additional tasks were solved: the development of the general approach to verification of security policy of computer networks; the perfection of the models of computer attacks and malefactor; the development of automated technique of detailed analysis of computer network security; the development of the models and software prototype of proactive monitoring of security policy performance in computer networks, etc.

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
07-01-00547

3.2. Название проекта
Модели и методы построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации, основывающиеся на моделировании поведения систем защиты, реализации верифицированных политик безопасности, оценке защищенности и проактивном мониторинге

3.3. Коды классификатора, соответствующие содержанию фактически проделанной работы
01-201 01-202 01-217

3.4. Объявленные ранее (в исходной заявке) цели проекта на 2007 год
Цели проекта формулируются как разработка и исследование моделей и методов проектирования, разработки и поддержания функционирования основывающихся на политиках безопасности, интеллектуальных адаптивных систем защиты информации (СЗИ) компьютерных систем функционирующих в открытых информационно-телекоммуникационных сетях.
Основными подзадачами проекта являются: (1) разработка и исследование моделей и методов защиты информации, реализующих интеллектуальную надстройку над традиционными механизмами защиты, а также (2) разработка и исследование моделей и методов построения единой унифицированной среды для создания и поддержки функционирования систем защиты информации на всем их жизненном цикле, включая адаптивное управление политиками безопасности.
Основными целями проекта на 2007 год являлись: (1) анализ состояния исследований в указанной предметной области; (2) разработка формальной постановки задачи исследования и основных требований к компонентам, реализующим интеллектуальные механизмы защиты, и поддержку жизненного цикла распределенных защищенных компьютерных систем; (3) разработка принципов построения, структуры и фрагмента основанной на онтологии, распределенной базы знаний для интеллектуальных механизмов защиты, и среды поддержки жизненного цикла распределенных защищенных компьютерных систем; (4) разработка формальных моделей отдельных компонентов интеллектуальных механизмов защиты, а также среды поддержки жизненного цикла распределенных защищенных компьютерных систем, в частности спецификации политик безопасности и конфигурации защищаемой системы (сети), верификации политик безопасности, определения уровня безопасности и мониторинга выполнения политики безопасности; (5) первоначальная экспериментальная оценка полученных результатов с помощью создания исследовательских прототипов и компьютерного моделирования.

3.5. Степень выполнения поставленных в проекте задач
Все задачи, запланированные в проекте на первый год, выполнены полностью. Решены также следующие дополнительные задачи: разработка общего подхода к верификации политики безопасности корпоративных компьютерных сетей; совершенствование моделей компьютерных атак и нарушителя, формирования дерева атак и оценки уровня защищенности компьютерных сетей; разработка автоматизированной методики детального анализа защищенности компьютерных сетей и программного прототипа анализа защищенности компьютерных сетей; разработка моделей и программного прототипа системы проактивного мониторинга выполнения политики безопасности в компьютерных сетях; совершенствование моделей команд агентов, реализующих атаки "распределенный отказ в обслуживании", и механизмы защиты от них, а также моделей их взаимодействия; разработка методики проведения многоагентного моделирования механизмов защиты от атак "распределенный отказ в обслуживании" в сети Интернет.

3.6. Полученные за отчетный год важнейшие результаты
Важнейшие результаты, полученные за отчетный период, таковы:

1. Предложена формальная постановка задачи исследования и основные требования к компонентам, реализующим интеллектуальные механизмы защиты и поддержку жизненного цикла распределенных защищенных компьютерных систем. Разработаны принципы построения, структура и фрагмент распределенной базы знаний для интеллектуальных механизмов защиты, основанной на онтологии предметной области, и среды поддержки жизненного цикла распределенных защищенных компьютерных систем. Разработаны формальные модели отдельных компонентов интеллектуальных механизмов защиты и среды поддержки жизненного цикла распределенных защищенных компьютерных систем, в частности спецификации политик безопасности и конфигураций защищаемой системы (сети), верификации политик безопасности, определения уровня безопасности и мониторинга выполнения политики безопасности.
2. Разработаны общий подход к верификации политики безопасности корпоративных компьютерных сетей, основанный на использовании гибридной многомодульной архитектуры системы верификации, модели отдельных компонентов верификации и программный комплекс верификации. Используя преимущества многомодульной архитектуры, подход позволяет комбинировать модули общего назначения со специализированными методами. Модули общего назначения построены на основе методов доказательства теорем с использованием исчисления событий и методов проверки на модели. Они позволяют обрабатывать противоречия различных типов, в том числе и динамические. Специализированные методы направлены на более эффективную обработку противоречий конкретных типов.
3. Выполнено совершенствование моделей компьютерных атак и нарушителя, формирования дерева атак и оценки уровня защищенности компьютерных сетей. В отличие от существующих моделей, модель компьютерных атак позволяет использовать для наполнения множества атакующих действий как экспертные знания, так и открытые базы данных уязвимостей. Модель нарушителя позволяет учитывать не только права нарушителя на компьютерах сети и хост, с которого им реализуются атакующие действия, но и уровень знаний и умений нарушителя, а также его первичные знания об атакуемой сети. Важной особенностью данных моделей является также учет характеристик нарушителя при формировании сценариев атак. Модель формирования дерева атак использует анализ зависимостей предусловий и постусловий атакующих действий нарушителя. Данная модель обладает следующими особенностями: вершины дерева атак представляются в виде тройки <состояние сети, атакующее действие, атакуемый объект>, что обеспечивает возможность определения понятий “трасса атаки” и “угроза”; при построении дерева атак явно учитываются правила фильтрации сетевого трафика, заданные на межсетевых экранах. Модель оценки уровня защищенности компьютерных сетей использует подход Common Vulnerability Scoring System (CVSS) для определения первичных показателей защищенности, что значительно упрощает их расчет, а для определения качественного интегрального показателя защищенности компьютерной сети используется объединение подхода CVSS и методики анализа рисков Facilitated Risk Analysis and Assessment Process (FRAAP).
4. Разработана автоматизированная методика детального анализа защищенности компьютерных сетей, которая обладает следующими особенностями: использует единый подход (построение и анализ дерева атак) как для этапа проектирования сети, так и для этапа ее эксплуатации; основные этапы методики автоматизированы; не задействуются программные средства активного анализа защищенности, способные нарушить функционирование отдельных сервисов или сети в целом. Разработанная методика позволяет: учитывать разнообразие первоначального местоположения нарушителя, его знания об атакуемой сети; использовать не только конфигурацию компьютерной сети, но и правила реализуемой в ней политики безопасности; учитывать различные типы атакующих действий; использовать актуализированные открытые базы данных об уязвимостях; рассчитывать множество показателей, характеризующих защищенность компьютерной сети в целом и отдельных ее

компонентов; определять "узкие места" в безопасности компьютерных сетей (хостов, ответственных за большее количество трасс атак и уязвимостей); рассчитывать интегральный показатель защищенности сети.
5. Разработан программный прототип системы анализа защищенности компьютерных сетей, который базируется на предложенных моделях и методике анализа защищенности. Проведение экспериментов с использованием тестовых компьютерных сетей показало его работоспособность и более высокую эффективность по сравнению с существующими аналогичными системами.
6. Разработаны модели и программный прототип системы проактивного мониторинга выполнения политики безопасности в компьютерных сетях. Предлагаемые модели мониторинга политики безопасности базируются на активной имитации действий пользователей (как разрешенных, так и запрещенных политикой безопасности) и определении расхождений реакций системы от предписанных. В отличие от релевантных исследований данный подход применим к различным категориям политики безопасности (аутентификации, разграничения доступа и авторизации, фильтрации, защиты каналов связи и др.). Модели мониторинга основываются на оптимизации последовательности применения тестовых воздействий, которая затрагивает следующие аспекты: удаление избыточных тестовых воздействий; нахождение оптимальной последовательности тестовых воздействий; нахождение последовательностей тестовых воздействий, которые можно выполнять параллельно. Подход основан на планировании и формировании комплекса сценариев для проведения мониторинга политик, использовании распределенной системы сканеров, сбора и корреляции полученной от них информации. Разработанные модели и программные компоненты позволяют осуществить проверку соответствия политики безопасности, сформулированной на этапе проектирования, ее реализации в реальной системе, а также анализ адекватности этой политики целям обеспечения защиты информационных ресурсов компьютерной системы от текущих угроз безопасности.
7. Осуществлено совершенствование моделей команд агентов, реализующих атаки "распределенный отказ в обслуживании" и механизмы защиты от них, а также модели их взаимодействия. Модели команд агентов отличаются использованием в качестве базиса методов командной работы агентов. Особенностью этих моделей является применение процедур обеспечения согласованности действий, мониторинга и восстановления функциональности агентов, а также обеспечения селективности коммуникаций. Отличительные черты моделей взаимодействия команд агентов: выделение различных видов взаимодействий команд, которые основываются на антагонистическом противоборстве, кооперации и адаптации; использование различных схем кооперации команд агентов защиты, позволяющих вести обмен данными о трафике между агентами защиты и задействовать разные классы агентов защиты; возможность адаптации команд агентов посредством генерации новых экземпляров атак и механизмов защиты и сценариев их реализации.
8. Разработана методика проведения многоагентного моделирования механизмов защиты от атак "распределенный отказ в обслуживании" в сети Интернет, базирующаяся на моделях команд агентов и их взаимодействия. Особенности методики: учитываются ключевые параметры исследуемых процессов (параметры сети и ее узлов, параметры команды атаки и реализации атаки, параметры команды защиты и механизмов защиты, параметры взаимодействия команд и др.); основные этапы методики автоматизированы; на основе выходных параметров производится оценка и сравнение различных механизмов защиты. Разработанные модели и методика могут быть обобщены для целей решения достаточно большого класса задач, в частности, задачи информационной борьбы в Интернет, конкуренции в сфере электронного бизнеса и др. Предложенную методику можно использовать для исследования эффективности разнообразных механизмов защиты, оценки защищенности существующих сетей и выработки рекомендаций для построения перспективных систем защиты.

3.7. Степень новизны полученных результатов

Основные научные результаты являются новыми. Предлагаемый подход к построению информационно-безопасных распределенных систем, основанных на политиках безопасности, является новаторским и перспективным подходом к построению систем защиты информации в компьютерных сетях. Отличительной особенностью результатов является то, что они направлены на формализацию комплексного антагонистического характера обеспечения информационной безопасности как сложного организационно-технического процесса. Система обеспечения информационной безопасности представляется в работе как единая холическая система, состояние которой определяется множеством взаимодействий между отдельными процессами кибер-противоборства и развивающегося динамического характера этих процессов, используя достижения в теории и практике построения многоагентных систем, современные тенденции в противоборстве методов нападения и защиты и перспективные подходы к обеспечению информационной безопасности.

3.8. Сопоставление полученных результатов с мировым уровнем

Все результаты, полученные в процессе выполнения первого года проекта, соответствуют мировому уровню. Авторы проекта апробировали и опубликовали полученные результаты на нескольких российских и международных конференциях, семинарах, а также в журналах, в частности, на 21-й Европейской конференции по моделированию ECMS 2007 (Прага, Чехия, 4-6 июня 2007 г.), Международной конференции по защите информации и криптографии SECRYPT 2007 (Барселона, Испания, 28-31 июля 2007 г.), Международном семинаре "Политики для распределенных систем и сетей (Policy 2007)" (Болонья, Италия, 13-15 июня 2007 г.), Международной конференции "Математические методы, модели и архитектуры безопасности компьютерных сетей (MMM-ACNS-2007)" (Санкт-Петербург, Россия. 13-15 сентября 2007 г.), Международном семинаре "Интеграция информации и геоинформационные системы (IF&GIS-2007)" (Санкт-Петербург, Россия. 27-29 мая 2007 г.), Международном семинаре "Интеграция информации и геоинформационные системы (IF&GIS-2007)" (Санкт-Петербург, Россия, 27-29 мая 2007 г.), Четвертом IEEE международном семинаре "Интеллектуальное приобретение данных и передовые компьютерные системы: технологии и приложения (IDAACS 2007)" (Дортмунд, Германия, 6-8 сентября 2007 г.), Международной конференции "Интеллектуальные системы (AIS 2007)" (Дивноморское, Россия, 3-10 сентября 2007 г.), Общероссийской научно-технической конференции "Методы и технические средства обеспечения безопасности информации (МТСОБИ 2007)" (Санкт-Петербург, Россия, 27-29 июня 2007 г.), 13-й Всероссийской конференции "Математические методы распознавания образов (ММРО-13)" (г. Зеленогорск, 30 сентября - 6 октября 2007 г.), Третьей всероссийской научно-практической конференции по имитационному моделированию и его применению в науке и промышленности "Имитационное моделирование. Теория и практика (ИММОД-2007)" (Санкт-Петербург, Россия. 17-19 октября 2007 г.), Шестой общероссийской научной конференции "Математика и безопасность информационных технологий (МаБИТ-2007)" (Москва, Россия. 25-27 октября 2007 г.) и др.

3.9. Методы и подходы, использованные в ходе выполнения проекта

В качестве базиса для исследований использовались работы в следующих областях: агентно-ориентированное моделирование; командная работа агентов; системы вывода, основанные на предсказании намерений и планов оппонента; рефлексивные процессы; теоретико-игровое моделирование; моделирование атак на компьютерные сети; моделирование процессов защиты информации; системы защиты, основанные на политиках безопасности; теория адаптивного управления и др. При разработке предложенных формальных постановок, моделей, архитектур и прототипов были применены методы системного анализа и теории больших систем, методы распределенного искусственного интеллекта, теории защиты информации, теории имитационного моделирования, теории слияния информации, обнаружения знаний и данных, методы объектно-ориентированного проектирования, теории протоколов и

языков взаимодействия агентов, формальной логики и проверки на модели (model checking).

3.10. Количество научных работ, опубликованных в ходе выполнения проекта

1. 55

3.10. Количество научных работ, подготовленных в ходе выполнения проекта и принятых к

2. печати в 2007 г.

6

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

6

3.12. Использовалось ли оборудование центров коллективного пользования

нет

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

3.14. Финансовые средства, полученные от РФФИ

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

3.16. Адреса (полностью) ресурсов в Internet, подготовленных авторами по данному проекту

http://comsec.spb.ru/index.cgi?l=ru&m=Staff&p=Kotenko
http://comsec.spb.ru/index.cgi?l=en&m=Staff&p=Kotenko
http://comsec.spb.ru/index.cgi?l=ru&m=Projects&p=
http://comsec.spb.ru/index.cgi?l=en&m=Projects&p=

3.17. Библиографический список всех публикаций по проекту

1. Котенко И.В., Уланов А.В. Агентно-ориентированная среда для моделирования и оценки механизмов защиты от распределенных атак "Отказ в обслуживании" // Изв. вузов. Приборостроение, Т.50, № 1, 2007, С.18-21.
2. Котенко И.В., Юсупов Р.М. Технологии компьютерной безопасности // Вестник РАН, Т.77, № 4, 2007. С.323-333.
3. Котенко И.В., Уланов А.В. Многоагентное моделирование защиты информационных ресурсов компьютерных сетей в сети Интернет // Известия РАН. Теория и системы управления, № 5, 2007, С.74-88.
4. Котенко И.В., Тишков А.В., Черватюк О.В., Резник С.А., Сидельникова Е.В. Система верификации политики безопасности компьютерной сети // Вестник компьютерных и информационных технологий, № 11, 2007. С.48-56.
5. Котенко И.В., Уланов А.В. Моделирование адаптивной кооперативной защиты от компьютерных атак в сети Интернет // Проблемы управления рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Москва, URSS, 2007. (Принята к печати)
6. Котенко И.В., Степашкин М.В. Оценка защищенности компьютерных сетей на основе анализа графов атак // Проблемы управления рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Москва, URSS, 2007. (Принята к печати)
7. Уланов А.В., Котенко И.В. Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия // Защита информации. Инсайд, № 1, 2007. С.60-67; № 2, 2007. С.70-77; № 3, 2007. С.62-69.
8. Богданов В.С., Котенко И.В. Проактивный мониторинг выполнения политики безопасности в компьютерных сетях // Защита информации. Инсайд, № 3, 2007. С.42-47; № 4, 2007. С.66-72.
9. Котенко И.В., Уланов А.В. Компьютерные войны в Интернете: моделирование

противоборства программных агентов // Защита информации. Инсайд, № 4, 2007. С.38-45.
10. Котенко И.В. Автоматическое обнаружение и сдерживание распространения Интернет-червей: краткий анализ современных исследований // Защита информации. Инсайд, № 4, 2007. С.46-56.
11. Котенко И.В. Международная конференция "Математические модели, методы и архитектуры для защиты компьютерных сетей" (MMM-ACNS-2007) // Защита информации. Инсайд, № 3, 2007, С.12; № 4, 2007, С.56.
12. Котенко И.В., Тишков А.В., Сидельникова Е.В., Черватюк О.В. Проверка правил политики безопасности для корпоративных компьютерных сетей // Защита информации. Инсайд, № 5, 2007. С.46-49; № 6, 2007. С.52-59.
13. Котенко И. В., Воронцов В. В. Аналитические модели распространения сетевых червей // Труды СПИИРАН. Вып.4, т.1. СПб.: Наука, 2007. С.208-224.
14. Котенко И. В., Воронцов В. В., Уланов А. В. Модели и системы имитационного моделирования распространения сетевых червей // Труды СПИИРАН. Вып.4, т.1. СПб.: Наука, 2007. С.225-238.
15. Котенко И.В. Актуальные проблемы моделирования процессов защиты информации на основе технологии интеллектуальных агентов // Известия СПбГЭТУ "ЛЭТИ". Специальный выпуск. Проблемы информатики: философия, науковедение, образование. СПб.: СПбГЭТУ "ЛЭТИ", 2007. С.93-109.
16. Котенко И.В., Уланов А.В. Противостояние в Интернет: моделирование противодействия распределенным кибератакам // Проблемы безопасности и противодействия терроризму. Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. М.: МЦНМО, 2007. С.485-494.
17. Богданов В.С., Котенко И.В. Проактивный подход к мониторингу выполнения политики безопасности компьютерных сетей // Проблемы безопасности и противодействия терроризму. Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. М.: МЦНМО, 2007. С.373-382.
18. Тишков А.В., Котенко И.В., Сидельникова Е.В., Черватюк О.В. Обнаружение и разрешение противоречий в политиках безопасности // Проблемы безопасности и противодействия терроризму. Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. М.: МЦНМО, 2007. С.172-185.
19. Котенко И.В., Степашкин М.В. Оценка защищенности компьютерных сетей на основе анализа графов атак // Проблемы безопасности и противодействия терроризму. Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. М.: МЦНМО, 2007. С.466-481.
20. Bogdanov V.S., Kotenko I.V., Stepashkin M.V. Proactive Approach to Network Security Policy Monitoring // Proceedings of the International Security and Counteracting Terrorism Conference. Moscow. Lomonosov Moscow State University Intellectual Center. 2007. 4 p.
21. Stepashkin M.V., Kotenko I.V., Bogdanov V.S. Network Security Evaluation based on Analysis of Attack Graphs // Proceedings of the International Security and Counteracting Terrorism Conference. Moscow. Lomonosov Moscow State University Intellectual Center. 2007. 5 p.
22. Tishkov A.V., Kotenko I.V., Sidelnikova E.V., Chervatuk O.V. Detection and Resolution of Inconsistencies in Security Policy // Proceedings of the International Security and Counteracting Terrorism Conference. Moscow. Lomonosov Moscow State University Intellectual Center. 2007. 5 p.
23. Kotenko I.V., Ulanov A.V. Confrontation in the Internet: Simulation of Counteraction to Distributed Cyber-Attacks // Proceedings of the International Security and Counteracting Terrorism Conference. Moscow. Lomonosov Moscow State University Intellectual Center. 2007. 4 p.

24. Kotenko I., Tishkov A., Chervatuk O., Sidelnikova E. Security Policy Verification Tool for Geographical Information Systems // Information Fusion and Geographical Information Systems. Lecture Notes in Geoinformation and Cartography. Springer. Popovich, Vasily V.; Schrenk, Manfred; Korolenko, Kyrill V. (Eds.). 2007. P.128-146.
25. Bourgeois J., Ganame A.K., Kotenko I., Ulanov A. Software Environment for Simulation and Evaluation of a Security Operation Center // Information Fusion and Geographical Information Systems. Lecture Notes in Geoinformation and Cartography. Springer. Popovich, Vasily V.; Schrenk, Manfred; Korolenko, Kyrill V. (Eds.). 2007. P.111-127.
26. Kotenko I.V., Ulanov A.V. Multi-agent Framework for Simulation of Adaptive Cooperative Defense against Internet Attacks // Proceedings of International Workshop on Autonomous Intelligent Systems: Agents and Data Mining (AIS-ADM-07). St. Petersburg, Russia. June 3-5, 2007. Lecture Notes in Artificial Intelligence, Vol.4476, 2007. P.212-228.
27. Kotenko I., Ulanov A. Agent-based Simulation Environment and Experiments for Investigation of Internet Attacks and Defense Mechanisms // Proceedings of 21th European Conference on Modelling and Simulation (ECMS 2007). Prague, Czech Republic. 4-6 June 2007. P.146-155.
28. Kotenko I., Chervatuk O., Sidelnikova E., Tishkov A. Hybrid Multi-module Security Policy Verification // 2007 IEEE Workshop on Policies for Distributed Systems and Networks (Policy 2007). 13-15 June 2007. Bologna, Italy. 2007. P.277.
29. Богданов В.С., Котенко И.В. Проактивный мониторинг выполнения политики безопасности компьютерной сети // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.32.
30. Котенко И.В., Воронцов В.В., Уланов А.В. Проактивное обнаружение и сдерживание распространения сетевых червей // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.91.
31. Котенко И.В., Уланов А.В. Моделирование адаптивного противостояния систем защиты распределенным атакам // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.92.
32. Kotenko I., Ulanov A. Investigation of Cooperative Defense against DDoS // SECRYPT 2007. International Conference on Security and Cryptography. Proceedings. Barcelona, Spain. 28-31 July 2007. P.180-183.
33. Котенко И.В., Воронцов В.В. Проактивный подход к обнаружению и сдерживанию сетевых червей // Труды Международных научно-технических конференций "Интеллектуальные системы (AIS 07)" и "Интеллектуальные САПР (CAD-2007)". Том.2. М.: Физматлит, 2007. С.61-68.
34. Десницкий В.А., Котенко И.В. Модели удаленной аутентификации для защиты программ // Труды Международных научно-технических конференций "Интеллектуальные системы (AIS 07)" и "Интеллектуальные САПР (CAD-2007)". Том.3. М.: Физматлит, 2007. С.43-50.
35. Kotenko I. Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security // Proceedings of IEEE Fourth International Workshop on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS 2007). Dortmund, Germany, 6-8 September, 2007. P.614-619.
36. Mathematical Methods, Models and Architectures for Computer Networks Security. The Forth International Conference, MMM-ACNS 2007. St. Petersburg, Russia, September 13–15, 2007. Communications in Computer and Information Science (CCIS). Springer. Vladimir Gorodetsky, Igor Kotenko, Victor Skormin (Eds.). Vol.1, 2007. 416 p.
37. Bogdanov V., Kotenko I. Policy-based Proactive Monitoring of Security Policy

Performance // Mathematical Methods, Models and Architectures for Computer Networks Security. The Forth International Conference, MMM-ACNS 2007. St. Petersburg, Russia, September 13–15, 2007. Proceedings. Communications in Computer and Information Science (CCIS). Springer. Vladimir Gorodetsky, Igor Kotenko, Victor Skormin (Eds.). Vol.1, 2007. P.197-212.
38. Tishkov A., Sidelnikova E., Kotenko I. Event Calculus based Checking of Filtering Policies // Mathematical Methods, Models and Architectures for Computer Networks Security. The Forth International Conference, MMM-ACNS 2007. St. Petersburg, Russia, September 13–15, 2007. Proceedings. Communications in Computer and Information Science (CCIS). Springer. Vladimir Gorodetsky, Igor Kotenko, Victor Skormin (Eds.). Vol.1, 2007. P.248-253.
39. Котенко И.В. Модели и методы построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации // Математические методы распознавания образов: 13-я Всероссийская конференция (ММРО-13). Ленинградская обл., г. Зеленогорск, 30 сентября - 6 октября 2007 г.: Сборник докладов. М.: МАКС Пресс, 2007. С.599-602.
40. Уланов А.В., Котенко И.В. Многоагентная среда для проведения экспериментов по защите компьютерных сетей // Математические методы распознавания образов: 13-я Всероссийская конференция (ММРО-13). Ленинградская обл., г. Зеленогорск, 30 сентября - 6 октября 2007 г.: Сборник докладов. М.: МАКС Пресс, 2007. С.631-634.
41. Котенко И.В., Воронцов В.В. Использование проактивного подхода для защиты от сетевых червей // Научно-практический симпозиум "Национальные информационные системы и безопасность государства". Тезисы. Москва, ОИТВС РАН, 2007. С.41-44.
42. Десницкий В.А., Котенко И.В. Удаленная аутентификация для защиты программ от несанкционированного изменения // Научно-практический симпозиум "Национальные информационные системы и безопасность государства". Тезисы. Москва, ОИТВС РАН, 2007. С.32-34.
43. Уланов А.В., Котенко И.В. Моделирование адаптивных кооперативных стратегий защиты от компьютерных атак в сети Интернет // Третья всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2007). Санкт-Петербург, 17-19 октября 2007 г. Сборник докладов. СПб.: ФГУП ЦНИИ технологии судостроения. 2007. Том II. С.211-215.
44. Котенко И.В., Уланов А.В., Тишков А.В., Богданов В.С., Воронцов В.В., Чечулин А.А. Имитационное моделирование механизмов обнаружения и сдерживания сетевых червей в компьютерных сетях // Третья всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2007). Санкт-Петербург, 17-19 октября 2007 г. Сборник докладов. СПб.: ФГУП ЦНИИ технологии судостроения. 2007. Том II. С.106-109.
45. Котенко И.В., Юсупов Р.М. Актуальные проблемы и решения в области защиты компьютерных сетей и систем // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.55-56.
46. Тишков А.В., Котенко И.В. Система защиты компьютерной сети, основанная на политике безопасности // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.122-123.
47. Десницкий В.А., Котенко И.В. Модель защиты программ от несанкционированных изменений на основе механизма удаленного доверия // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.81.
48. Воронцов В.В., Котенко И.В. Модели обнаружения и сдерживания сетевых червей на основе проактивного подхода // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25

октября 2007 г. Материалы конференции. СПб, 2007. С.47-48.
49. Чечулин А.А., Котенко И.В. Механизмы защиты от сетевых червей на основе метода порогового случайного прохождения // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.70.
50. Уланов А.В. Модели противоборства команд агентов, реализующих атаки «распределенный отказ в обслуживании» и механизмы защиты от них // Труды Международных научно-технических конференций "Интеллектуальные системы (AIS 07)" и "Интеллектуальные САПР (CAD-2007)". М.: Физматлит, 2007. С.120-127.
51. Резник С.А., Черватюк О.В. Обнаружение конфликтов фильтрации и защиты каналов в политике безопасности на основе методов верификации на модели // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.37.
52. Десницкий В.А. Удаленная аутентификация как механизм защиты программ на удаленных клиентах // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.5.
53. Уланов А.В. Архитектура и модель среды многоагентного моделирования атак DDoS и защиты от них // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.96.
54. Воронцов В.В. Моделирование распространения сетевых червей // Методы и технические средства обеспечения безопасности информации. Материалы XVI Общероссийской научно-технической конференции. 27-29 июня 2007 года. Санкт-Петербург. Издательство Политехнического университета. 2007. С.88.
55. Уланов А.В. Методика проведения имитационного моделирования противостояния систем защиты атакам DDOS в сети Интернет // Научно-практический симпозиум "Национальные информационные системы и безопасность государства". Тезисы. Москва, ОИТВС РАН, 2007. С.38-40.
56. Десницкий В.А. Аспектно-ориентированный подход к реализации механизма мобильного модуля в системе защиты программного обеспечения // Научно-практический симпозиум "Национальные информационные системы и безопасность государства". Тезисы. Москва, ОИТВС РАН, 2007. С.35-37.
57. Воронцов В.В. Механизм обнаружения и ограничения распространения сетевых червей на основе кредитов доверия // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.46-47.
58. Десницкий В.А. Реализация механизма замещения мобильного модуля на основе парадигмы аспектно-ориентированного программирования // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.49-50.
59. Сидельникова Е.В. Верификация правил фильтрации с помощью исчисления событий и абдуктивного вывода // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.95.
60. Черватюк О.В. Верификация правил фильтрации политики безопасности методом проверки на модели // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.69-70.
61. Чечулин А.А. Исследование механизмов обнаружения и сдерживания сетевых червей, базирующихся на методике "Virus Throttling" // V Санкт-Петербургская

межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007). 23-25 октября 2007 г. Материалы конференции. СПб, 2007. С.99-100.