НОМЕР ПРОЕКТА **07-01-00547**		
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**		
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**		

ОТЧЕТ ЗА 2008 ГОД ПО ПРОЕКТУ РФФИ 07-01-00547-а

Статус отчета: не подписан

Дата последнего изменения: 12.01.2009

Изменения внес: Котенко Игорь Витальевич

Отчет распечатан: 12.01.2009

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
2009

1.6. Вид отчета
этап 2008 года

1.7. Аннотация
Уточнена формальная постановки задачи исследования и основные требования к компонентам, реализующим интеллектуальные механизмы защиты и поддержку жизненного цикла распределенных защищенных компьютерных систем. Осуществлена доработка принципов построения, структуры и фрагмента основанной на онтологии, распределенной базы знаний для интеллектуальных механизмов защиты, и среды поддержки жизненного цикла распределенных защищенных компьютерных систем. Разработаны формальные модели отдельных компонентов интеллектуальных механизмов защиты. Предложен проактивный подход к защите от сетевых червей, основанный на комбинировании различных механизмов обнаружения и сдерживания сетевых червей и автоматической настройке основных параметров механизмов защиты. Выполнено совершенствование программной реализации исследовательской среды для изучения компьютерных атак и механизмов защиты от них. Исследованы модели защиты программного обеспечения на основе механизма удаленного доверия. Проведена теоретическая и экспериментальная оценка предложенных моделей и методов построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации и разработанной системы моделирования, а также разработаны рекомендации по их использованию для защиты информации в компьютерных сетях.

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
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*2009

*2.5. Вид отчета*этап 2008 года

2.6. Аннотация

The formal statement of the research problem and the main requirements to the components realizing the intelligent security mechanisms and the life cycle support of distributed protected computer systems were defined more exactly. The principles of construction, the 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 elaborated. The formal models of particular components of intelligent security mechanisms were developed. The proactive approach to protection against network worms, which is based on a combination of various mechanisms of network worm detection and containment and automatic adjustment of key parameters of protection mechanisms, was offered. The software realization of the research environment for studying the computer attacks and protection mechanisms against them was improved. The models of software protection based on remote entrusting mechanism were investigated. The theoretical and experimental evaluation of suggested models and methods for construction and support of intellectual adaptive information protection systems as well as the developed simulation system was carried out. The recommendations on their use for protection of the information in computer networks were also developed.

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 2008 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 2008 год являлись: (1) уточнение формальной постановки задачи исследования и основных требований к компонентам защиты и поддержки жизненного цикла распределенных защищенных компьютерных систем; (2) разработка формальных моделей отдельных компонентов интеллектуальных механизмов защиты; (3) разработка проактивного подхода к защите от сетевых червей; (4) совершенствование программной реализации исследовательской среды для изучения компьютерных атак и механизмов защиты от них; (5) исследование моделей защиты программного обеспечения на основе механизма удаленного доверия; (6) теоретическая и экспериментальная оценка предложенных моделей и методов построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации и разработанной системы моделирования, а также разработка рекомендаций по их использованию для защиты информации в компьютерных сетях.

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. Уточнена формальная постановка задачи исследования и основные требования к компонентам, реализующим интеллектуальные механизмы защиты, и поддержку жизненного цикла распределенных защищенных компьютерных систем. Осуществлена доработка принципов построения, структуры и фрагмента основанной на онтологии, распределенной базы знаний для интеллектуальных механизмов защиты, и среды поддержки жизненного цикла распределенных защищенных компьютерных систем. 2. Разработаны формальные модели отдельных компонентов интеллектуальных механизмов защиты, в частности модели сбора информации о состоянии информационной системы и ее анализа за счет механизмов обработки и слияния информации из различных источников, модели обнаружения аномальной активности и явных атак, а также нелегитимных действий и отклонений работы пользователей от политики безопасности, и модели мониторинга функционирования и контроля корректности текущей политики безопасности и конфигурации сети. 3. Разработан проактивный подход к защите от сетевых червей, основанный на комбинировании различных механизмов обнаружения и сдерживания сетевых червей и автоматической настройке основных параметров механизмов защиты в соответствии

с текущей сетевой конфигурацией и сетевым трафиком. Для разработки проактивного подхода предложено использовать комбинацию следующих особенностей: "многорезолюционный" подход, сочетающий использование нескольких интервалов времени ("окон") наблюдения сетевого трафика и применение различных порогов для отслеживаемых параметров; гибридный подход, заключающийся в использовании различных алгоритмов и математических методов; многоуровневое комбинирование алгоритмов в виде системы базовых классификаторов, обрабатывающих данные о трафике, и мета-классификатора, осуществляющего выбор решения; адаптивные механизмы обнаружения и сдерживания сетевых червей, способные изменять критерии обнаружения на основе параметров сетевого трафика. Разработан программный комплекс моделирования и оценки механизмов обнаружения и сдерживания сетевых червей, который включает следующие компоненты: источники трафика или генератор трафика (формирующий нормальный трафик и трафик сетевого червя); анализатор трафика; библиотеки механизмов защиты от сетевых червей; сценарии тестирования и базовый тестовый комплекс или компонент оценки. Проведена серия экспериментов по исследованию данного подхода для выбора оптимальных параметров функционирования механизмов защиты.4. Выполнено совершенствование программной реализации исследовательской среды для изучения компьютерных атак и механизмов защиты от них, основанной на агентно-ориентированном и имитационном моделировании на уровне сетевых пакетов. Для реализации исследовательской среды использована архитектура системы моделирования, включающая базовую систему имитационного моделирования, модуль (пакет) моделирования сети Интернет, подсистему агентно-ориентированного моделирования и модуль (библиотеку) атак "распределенный отказ в обслуживании" и механизмов защиты от них. Созданная среда моделирования позволяет проводить различные эксперименты с целью исследования стратегий реализации атак "распределенный отказ в обслуживании" и перспективных методов защиты от них. Проведены эксперименты по исследованию кооперативных механизмов защиты, включающих моделирование таких распределенных механизмов защиты, как DefCOM, COSSACK, "без кооперации", " кооперация на уровне фильтров", "кооперация на уровне сэмплеров", "полная кооперация". Исследовались также различные адаптивные схемы взаимодействия команд агентов. 5. Исследованы модели защиты программного обеспечения на основе механизма удаленного доверия, предназначенного для обнаружения несанкционированных изменений клиентской программы, функционирующей в потенциально враждебном окружении, а также возможные классы атак на указанные механизмы защиты. Предложен механизм замещения мобильного модуля в клиентской программе на основе использования концепции аспектно-ориентированного программирования, в соответствии с которой различные функциональности клиентской программы программируются отдельно, а затем встраиваются в целевой код. 6. Проведена теоретическая и экспериментальная оценка предложенных моделей и методов построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации и разработанной системы моделирования, а также разработка рекомендаций по их использованию для защиты информации в компьютерных сетях.

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 опубликовали полученные результаты в нескольких журналах, сборниках и трудах конференций, а также апробировали на множестве различных российских и международных конференций, в частности, на 16-й Европейской (Euromicro) международной конференции по параллельной, распределенной и сетевой обработке информации PDP 2008 (Тулуза, Франция. 13-15 февраля 2008 г.), Международной конференции по доверенным вычислениям TRUST2008 (Филах, Австрия. 11-12 марта 2008 г.), Десятой конференции "РусКрипто'2008" по криптологии, стеганографии, цифровой подписи и системам защиты информации (Звенигород, 3-5 апреля 2008 г.), XVII Общероссийской научно-технической конференции "Методы и технические средства обеспечения безопасности информации (МТСОБИ 2008)" (Санкт-Петербург, 27-29 июня 2008 г.), Международном семинаре по логике для агентов и мобильности LAM'08 и Европейской летней школе по логике, языку и информации ESSLLI 2008 (Гамбург, Германия, 4-15 августа 2008), Международной конференции "Интеллектуальные системы (AIS 2008)" (Дивноморское, 3-10 сентября 2008 г.), XI Национальной конференции по искусственному интеллекту с международным участием (КИИ-2008) (Дубна, 29 сентября - 3 октября 2008 г.), Международном семинаре и ярмарке идей по седьмой рамочной программе Европейского союза ERANIS 2008 (Варшава, Польша, 9-10 октября 2008 г.), Первом международном семинаре по удаленному доверию RE-TRUST 2008 (Тренто, Италия, 15-16 октября 2008 г.), XI Санкт-Петербургской Международной Конференции "Региональная информатика-2008 (РИ-2008)" (Санкт-Петербург, 21-23 октября 2008 г.), Четвертой международной научной конференции по проблемам безопасности и противодействия терроризму и Седьмой общероссийской научной конференции "Математика и безопасность информационных технологий МаБИТ-2008" (Москва, 30-31 октября 2008 г.), Международной конференции "Информационные и коммуникационные технологии в седьмой рамочной программе Европейского союза. Сотрудничество Россия-ЕС" (Москва, 21-23 октября 2008 г.) и др.

3.9. Методы и подходы, использованные в ходе выполнения проекта

В качестве базиса для исследований использовались методы и подходы, применяемые 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 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.

3.10.1. Количество научных работ, опубликованных в ходе выполнения проекта

34

3.10.2. Количество научных работ, подготовленных в ходе выполнения проекта и принятых к печати в 2008 г.

5

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

5

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

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/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=

3.16. Библиографический список всех публикаций по проекту

Публикации за 1-й год:

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.

Публикации за 2-й год:

1. Kotenko I. Multi-agent modeling and the simulation of computer network security processes: "a game of network cats and mice" // NATO Science for Peace and Security Series, D: Information and Communication Security. Volume 17, 2008.
2. Aspects of Network and Information Security. P.56-73. ISBN 978-1-58603-856-
4.Kotenko I., Ulanov A. Packet Level Simulation of Cooperative Distributed Defense against Internet Attacks // Proceedings of the 16th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2008). Toulouse, France. February 13-15 2008. IEEE Computer Society. 2008. P.565-572.
3. Kotenko I. Multi-agent Simulation of Attacks and Defense Mechanisms in Computer Networks // The Journal of Computing, Vol. 7, Issue 2, 2008. P.35-43.
4. Kotenko I., Ulanov A. Simulation of Adaptable Agent Teams in Internet // Proceedings of the 1st International Workshop on Logics for Agents and Mobility (LAM08). The European Summer School on Logic, Language and Information (ESSLLI 2008), Hamburg, Germany. 4 - 15 August, 2008. P.67-79.
5. Котенко И.В., Воронцов В.В., Тишков А.В., Чечулин А.А., Уланов А.В. Исследование проактивных механизмов защиты от сетевых червей // Проблемы безопасности и противодействия терроризму. Материалы третьей международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. М.: МЦНМО, 2008. С.278-283.
6. Уланов А.В., Котенко И.В. Моделирование кооперативных механизмов защиты

компьютерных сетей // Проблемы безопасности и противодействия терроризму. Материалы третьей международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им.М.В.Ломоносова. М.: МЦНМО, 2008. С.266-271.
7. Котенко И.В., Юсупов Р.М. Актуальные исследования в области защиты компьютерных сетей и систем // V Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2007"). Труды конференции. Санкт-Петербург. 2008. С. 21-31.
8. Котенко И.В., Воронцов В.В., Чечулин А.А. Анализ механизмов обнаружения и сдерживания сетевых червей // V Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2007"). Труды конференции. Санкт-Петербург. 2008. С.113-119.
9. Десницкий В.А., Котенко И.В. Модель защиты программ на основе механизма "удаленного доверия" // V Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2007"). Труды конференции. Санкт-Петербург. 2008. С.172-177.
10. Котенко И.В., Уланов А.В. Исследование механизмов защиты от атак DDOS: имитация противоборства интеллектуальных агентов в сети Интернет // Международная конференция "РусКрипто 2008". 2008. CD ROM. http://www.ruscrypto.ru/
11. Котенко И.В. Проактивные механизмы защиты от быстро распространяющихся сетевых червей // Международная конференция "РусКрипто 2008". 2008. CD ROM. http://www.ruscrypto.ru/
12. Котенко И.В., Десницкий В.А. Аспектно-ориентированный подход к реализации мобильного модуля в модели защиты, основанной на механизме "удаленного доверия" // Информационные технологии и вычислительные системы, № 2, 2008. (Принята к печати)
13. Десницкий В.А., Котенко И.В. Защита программного обеспечения на основе механизма "удаленного доверия" // Изв. вузов. Приборостроение, Т.51, № 11 , 2008, С.26-30. ISSN 0021-3454.
14. Воронцов В.В., Котенко И.В. Анализ механизма обнаружения и сдерживания эпидемий сетевых червей на основе «кредитов доверия» // Изв. вузов. Приборостроение, Т.51, № 11, 2008, С.21-26. ISSN 0021-3454.
15. Сидельникова Е.В., Тишков А.В., Котенко И.В. Верификация политик фильтрации с помощью исчисления событий и абдуктивного вывода // Изв. вузов. Приборостроение, Т.51, № 11, 2008, С.31-35. ISSN 0021-3454.
16. Полубелова О.В., Котенко И.В. Верификация правил фильтрации политики безопасности методом "проверки на модели" // Изв. вузов. Приборостроение, Т.51, № 12, 2008. С.44-49. ISSN 0021-3454.
17. Котенко И.В., Чечулин А.А. Исследование механизмов защиты от сетевых червей на основе методик Virus Throttling // Защита информации. Инсайд, № 3, 2008. С.68-73.
18. Десницкий В.А., Котенко И.В., Резник С.А. Разработка и верификация протокола обмена сообщениями для защиты программ на основе механизма "удаленного доверия" // Защита информации. Инсайд, № 4, 2008. С.59-63; № 5, 2008. С.68-74.
19. Десницкий В.А., Котенко И.В., Резник С.А. Разработка и анализ протокола обмена сообщениями для защиты программ посредством "удаленного доверия" // Методы и технические средства обеспечения безопасности информации. Материалы XVII Общероссийской научно-технической конференции. 7-11 июля 2008 года. Санкт-Петербург. Издательство Политехнического университета. 2008.
20. Котенко И.В., Воронцов В.В., Чечулин А.А. Обнаружение и сдерживание распространения злонамеренного программного обеспечения на основе комбинированных механизмов // Методы и технические средства обеспечения безопасности информации. Материалы XVII Общероссийской научно-технической конференции. 7-11 июля 2008 года. Санкт-Петербург. Издательство Политехнического университета. 2008.

21. Котенко И.В., Тишков А.В., Воронцов В.В. Комбинирование механизмов защиты от злонамеренного программного обеспечения // Труды Международных научно-технических конференций "Интеллектуальные системы (AIS 08")" и "Интеллектуальные САПР (CAD-2008)". М.: Физматлит, 2008.
22. Десницкий В.А., Котенко И.В., Резник С.А. Разработка и анализ протокола обмена сообщениями для механизма удаленного доверия // Труды Международных научно-технических конференций "Интеллектуальные системы (AIS 08)" и "Интеллектуальные САПР (CAD-2008)". М.: Физматлит, 2008.
23. Котенко И.В., Уланов А.В. Моделирование адаптации противоборствующих команд интеллектуальных агентов // КИИ-2008. XI Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. Том 1. М.: URSS, 2008. С.32-40.
24. Котенко И.В. Интеллектуальные механизмы управления кибербезопасностью // Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Москва, URSS, 2008. (Принята к печати)
25. Десницкий В.А., Котенко И.В. Проектирование и анализ протокола удаленного доверия // Седьмая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2008). Москва, МГУ, 2008. (Принята к печати)
26. Комашинский Д.В., Котенко И.В. Исследование проактивных механизмов обнаружения вредоносного программного обеспечения на базе методов DATA MINING // Седьмая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2008). Москва, МГУ, 2008. (Принята к печати)
27. Чечулин А.А., Котенко И.В. Защита от сетевых атак методами нормализации протоколов транспортного и сетевого уровня стека TCP/IP // Седьмая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2008). Москва, МГУ, 2008. (Принята к печати)
28. Котенко И.В., Юсупов Р.М. Информационные технологии для борьбы с терроризмом // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.39-40.
29. Шоров А.В., Котенко И.В. Защита компьютерной сети от инфраструктурных атак на основе реализации "нервной системы сети" // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.118-119.
30. Богданов В.С. Оптимизация тестирования политики безопасности компьютерных сетей // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.93.
31. Десницкий В.А. Разработка и анализ протокола для защиты программ от злонамеренных изменений // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.98-99.
32. Комашинский Д.В. Проактивная технология обнаружения вредоносного программного обеспечения на базе методов интеллектуального анализа данных (Data Mining) // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.101.
33. Коновалов А.М. Моделирование сетевого трафика в задачах защиты от инфраструктурных сетевых угроз // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.101-102.
34. Котенко Д.И. Построение графа атак для оценки защищенности компьютерной сети // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.102-103.
35. Полубелова О.В. Верификация правил фильтрации политики безопасности, содержащих временные параметры, методом проверки на модели // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.110-111.

36. Резник С.А. Комплексный подход к верификации протоколов безопасности на примере протокола RE-TRUST // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.111.
37. Сидельникова Е.В. Абдуктивный конфигуратор правил фильтрации межсетевого экрана // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.112.
38. Чечулин А.А. Защита от сетевых атак методами нормализации протоколов транспортного и сетевого уровня стека TCP/IP // XI Санкт-Петербургская Международная Конференция "Региональная информатика-2008" ("РИ-2008"). Материалы конференции. СПб., 2008. С.115-116.
39. Сидельникова Е.В. Верификация политик фильтрации с помощью исчисления событий и абдуктивного вывода // V Межрегиональная конференция "Информационная безопасность регионов России" ("ИБРР-2007"). Труды конференции. Санкт-Петербург. 2008. С.133-136.

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 обработки, хранения, передачи и защиты информации

Подпись руководителя проекта